MATHEMATICS 300 — FALL 2018

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Contents

Part I

1 Introduction

These notes are about ***mathematical proofs***. We are going to get started by presenting some examples of proofs. Later, after we have seen several proofs, we will discuss in general, in great detail,

- What proofs are.
- How to read proofs.
- How to write and how not to write proofs.
- What proofs are for.
- Why proofs they are important.

But first, in this section, I am going to show you several examples of ***proofs***.

In each of these examples, we are going to prove a ***theorem***. Theorems have ***statements***. Each statement expresses a ***proposition***, and the fact that the statement has been proved implies that the proposition is ***true***, in which case we say that the statement is true.

So maybe it is a good idea to start by clarifying the meanings of the words "theorem", "statement", "proof", and of other related words such as "proposition", "fact", and "conclusion".

1.1 Propositions, statements, theorems and proofs

Basically, a ***proposition*** is something that can be true or false and can be the objects of belief. For example, if I believe that snow is white, my Mexican friend Alicia believes that "la nieve es blanca", and my French friend Gaston believes that “la neige est blanche”, then all three of us believe the same thing. That thing that I, Alicia and Gsston believe, is a proposition.

A ***fact*** is a true proposition.

A ***statement*** is a linguistic object (a sequence of words or sysmbols) that expresses a proposition. The same proposition can be expressed by different statements in different languages. For example,

- “snow is white”, ”la nieve es blanca”, and “la neige est blanche”, are three different statements that express the same proposition in three different languages: English, Spanish and French.

- “two plus two equals four”, “dos más dos es igual a cuatro”, “deux plus deux égale quatre”, and ”$2 + 2 = 4$”, are four different statements that express the same proposition in four different languages: English, Spanish, French, and mathematical language.

A ***proof*** of s proposition P is a logical argument[1] that establishes the truth of P by moving step by step from proposition to proposition until P is reached. The proof ends with the proposition P, which is called the ***conclusion***. A proof can by written in a particular language by writing in that language the statements that express the propositions that are the steps of the proof. Most of our proofs will be written in a combination mathematical language and English, but later will also explain how to write proofs in purle mathematical language[2]

Why are proofs important? Again, this is an issue that will be taken up later, but let me sketch the answer right away: ***a methematical proof of a proposition P absolutely guarantees, with complete certainty, that P is true.*** This is so for a simple reason:

[1] If you are worried because it is not clear to you what a “logical argument” is, do not worry. We are going to spend the whole semester discussing logical arguments and explaining what they are and how to read them and write them, so by the end of the semester you *will* know.

[2] And we will discuss why having a purely mathematical language is important: one of the main reasons is that ***mathematical language is a universal language***, that is, a language understandable by all the mathematicall educated people in the world.

> ***The rules of logic are designed in such a way that one can only prove, using them, propositions that are true.***
>
> ***Therefore, if you write a correct proof of a proposition P, that is, a proof that obeys the rules of logic, then you can be sure that P is true.***
>
> ***On the other hand, if you produce a purported proof of a proposition P that is not true, then we can all be sure that your proof is incorrect, in the sense that in at least one step you violeted the rules of logic.***

And, in case you ask *what are those "rules of logic" that you are talking about?* The answer is: *I am about to tell you! But it is going to take me a few weeks to tell you. And, once I have told you, you will see that the rules are very simple. But you have to be patient and allow me to get you there step by step*[3].

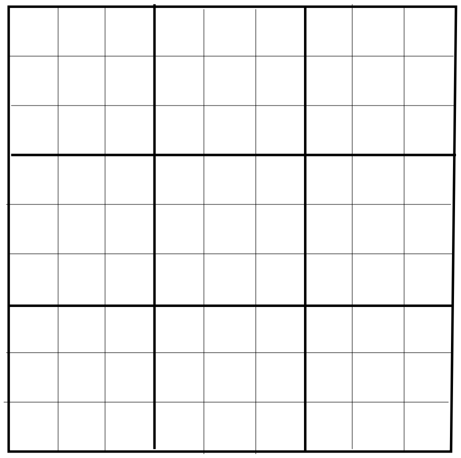
1.2 An example: a Sudoku puzzle

Our first proof will be about a Sudoku puzzle.

Remark 1.

- A 3×3 Sudoku grid consists of a square dovided into 81 square ***cells***, arranged as 9 ***rows*** and 9 ***columns***, and partitioned into nine 3×3 ***blocks***:

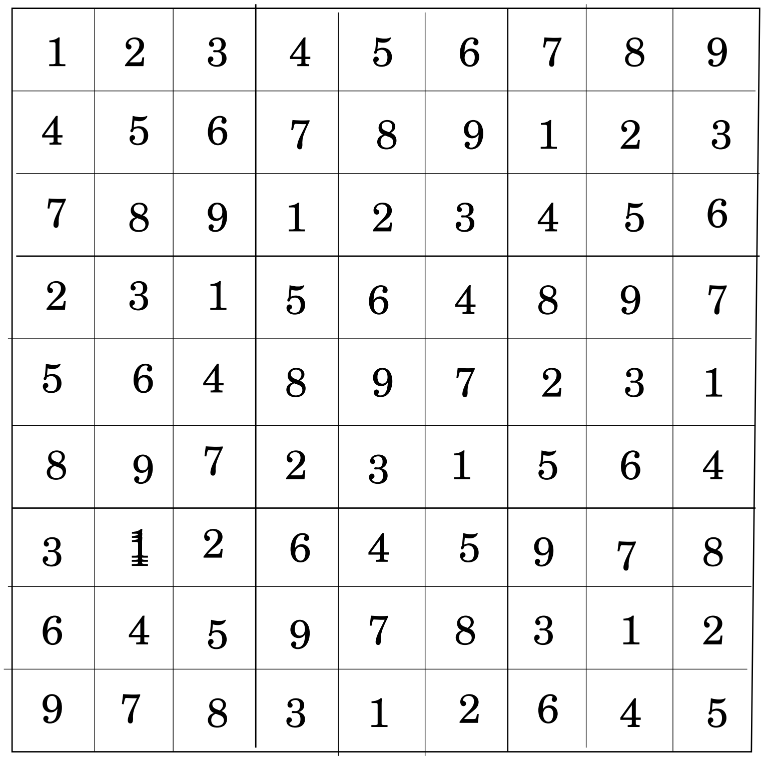
[3] It's like swimming. Once you have learned to swim, it seems simple to you. But most people need to learn to swim gradually, by first practicing floating, then exhaling under water, then kicking, then maybe doing a backstroke, treading water, and so on. And, once you have learned all that, it all looks very simple.



- A completed 3×3 Sudoku grid is a 3×3 Sudoku grid in which each cell is filled in with a nonzero digit[4] in such a way that
  - every row contains all nine nonzero digits,
  - every column contains all nine nonzero digits,
  - every block contains all nine nonzero digits.

  Here is an example of a completed 3×3 Sudoku grid:

[4] The digits are the numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. The nonzero digits are the numbers $1, 2, 3, 4, 5, 6, 7, 8, 9$. So there are 10 digits and 9 nonzero digits.



1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
2	3	1	5	6	4	8	9	7
5	6	4	8	9	7	2	3	1
8	9	7	2	3	1	5	6	4
3	1	2	6	4	5	9	7	8
6	4	5	9	7	8	3	1	2
9	7	8	3	1	2	6	4	5

- A 3×3 Sudoku puzzle is a 3×3 Sudoku grid in which some of the cells are filled in with nonzero digits.

- A solution of a 3×3 Sudoku puzzle P is a completed 3×3 Sudoku grid that can be obtained from P by filling in the cells of P that are not filled in in P.

- A Sudoku puzzle P is solvable if it has a solution.

- A Sudoku puzzle P is uniquely solvable if it has one and only one solution. □

Example 1.

Here is a 3×3 Sudoku puzzle

	2		4	5	6	7		9
4		6				1		
7		9	1		3		5	6
	3	1	5		4	8	9	7
	6			9	7		3	1
8			2	3	1			4
3	1	2		4	5	9		8
		5			8			
					2			5

and here is a solution:

1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
2	3	1	5	6	4	8	9	7
5	6	4	8	9	7	2	3	1
8	9	7	2	3	1	5	6	4
3	1	2	6	4	5	9	7	8
6	4	5	9	7	8	3	1	2
9	7	8	3	1	2	6	4	5

Theorem 1. *The following Sudoku puzzle*

			3				4	
	6							
			4			3		
						7	2	
		8		2				
3			9					
4				1				

has no solution.

Proof.
COMMENT: We are going to do a ***proof by contradiction***[5]*:*

I. We assume *(that is, imagine) that the puzzle has a solution,*

II. we explore an imaginary world in which the problem has a solution, until

III. we prove a contradiction

The logic here is as follows: we prove that a world in which the problem has a solution is impossible, because in that world a contradiction would have to be true, and a contradiction cannot possibly be true.

So a world in which our Sudoku puzzle has a solution is an impossible world. Hence in the real world that puzzle does not have a solution.

We now carry out this program:

1. Let us assume that our puzzle has a solution.

[5] Proofs by contradiction are explained in Subsection 1.4 below. You should read the explanation now.

COMMENT.This means that we have entered an imaginary world W in which the puzzle has a solution. To indicate that this world we are working in is different, we use an extra indentation. World W is different from the real world because in W our puzzle has a solution.

2. Since our puzzle has a solution, we pick one solution and give it a name: we call it S.

COMMENT. This is something that we are going to be doing a lot in the course: if we find out that an object of a certain kind exists, then we "pick" one and give it a name, so we can talk about it.

3. Also, let us give names to some other objects of interest: let us use B for the top left 3×3 block, R_1, R_2, R_3 for the top three rows of S (so each one has nine cells) and r_1, r_2, r_3 for the three rows of B (so each one has three cells).

4. In S, block B must contain all nine nonzero digits $1, 2, 3, 4, 5, 6, 7, 8, 9$. However, row r_1 cannot have a 3 or a 4, because R_1 already has a 3 and a 4 elsewhere. (To be precise: since a row of the big square has 9 cells, and all 9 nonzero digits must occcur in it, each of these nonzero digits must occur exactly one. So, since R_1 already has a 1, a 2, a 3 and a 4 elsewhere, these digits cannot occur in R_1.)

5. A similar argument shows that 3 and 4 cannot occur in r_3.

6. So 3, and 4 must occur in r_2.

7. But neither the 3 nor the 4 can occur in the leftmost cell of r_2, because the first column already has a 3 and a 4 elsewhere.

8. Also, neither the 3 nor the 4 can occur in the second cell of r_2, because thhere is a 6 there.

9. Hence $\boxed{\text{both the 3 and the 4 must occur in the third cell of } r_2}$.

10, But $\boxed{\text{both the 3 and the 4 cannot occur in the third cell of } r_2}$, because each cell is suppose to conatin only one digit.

11. So we have reached a contradiction.

COMMENT. The contradiction is the statement "A and no A", where A is the statement "3, and 4 occur in the third cell of r_2".

So we have proved that ***the puzzle of the previous figure has no solution***. **Q.E.D.**

And here is the same proof, without the comments:
Proof.

1. Let us assume that our puzzle has a solution.
2. Since our puzzle has a solution, we pick one solution and give it a name: we call it S.
3. Also, let us give names to some other objects of interest: let us use B for the top left 3×3 block, R_1, R_2, R_3 for the top three rows of S (so each one has nine cells) and r_1, r_2, r_3 for the three rows of B (so each one has three cells).
4. In S, block B must contain all nine nonzero digits $1, 2, 3, 4, 5, 6, 7, 8, 9$. However, row r_1 cannot have a 3 or a 4, because R_1 already has a 3 and a 4 elsewhere. (To be precise: since a row of the big square has 9 cells, and all 9 nonzero digits must occcur in it, each of these nonzero digits must occur exactly one. So, since R_1 already has a 1, a 2, a 3 and a 4 elsewhere, these digits cannot occur in R_1.)
5. A similar argument shows that 3 and 4 cannot occur in r_3.
6. So 3, and 4 must occur in r_2.
7. But neither the 3 nor the 4 can occur in the leftmost cell of r_2, because the first column already has a 3 and a 4 elsewhere.
8. Also, neither the 3 nor the 4 can occur in the second cell of r_2, because thhere is a 6 there.
9. Hence $\boxed{\text{both the 3 and the 4 must occur in the third cell of } r_2}$.

10, But $\boxed{\text{both the 3 and the 4 cannot occur in the third cell of } r_2}$, because each cell is suppose to conatin only one digit.

11. So we have reached a contradiction.

So we have proved that ***the puzzle of the previous figure has no solution***. **Q.E.D.**

1.2.1 What is “Q.E.D.”?

What does “Q.E.D.” mean?

“Q.E.D.” stands for the Latin phrase *quod erat demonstrandum*, meaning “which is what was to be proved”. It is used to indicate the end of a proof.

1.2.2 Two Sudoku problems

Problem 1. Prove that the following Sudoku puzzle

						8		7
2	3							
				7				
					8			
		8						
				8	7			
		7						

is not solvable.

Problem 2. Prove that the following Sudoku puzzle

1	2		4		6			9
	5			8	9	1	2	
	8	9	1	2		4	5	6
2		1	5	6	4	8	9	
5		4	8	9		2		1
	9		2		1	5	6	4
	1	2		4	5	9		8
6	4	5	9		8		1	2
		8		1	2	6	4	5

is not uniquely solvable.

1.2.3 Proof strategies we have used in the proof of Theorem 1

In our proof of Theorem 1 we have used two important proof strategies.

1. We used the ***proof by contradiction*** strategy, described in Section 1.4.
2. We used the ***rule for using existential statements***, described in Section 1.3.

1.3 The rule for using existential statements

An existential statement is a statement that says that an object of a certain kind exists. (That is, there is at least one object of

The rule for using existential statements says that, ***if you know that an existential statement, saying that an object of a certain kind exists, is true, then you can pick one and give it a name and start talking about it.***

For example:

i. If you know that Polonius has been killed, but you do not know who did it, then you can talk about the person who killed Polonius and give a name to that person, for example, call him (or her) "the killer".

ii. If you know that Sudoku puzzle P has a solution (that is, a solution exists), then you can pick one solution and call it S.

iii. if you know that an equation (say, the equation $3x^2 + 5x = 8$) has a solution (that is, you know that the existential statement "there exists a real number x such that $3x^2 + 5x = 8$" is true) then you are allowed to pick a solution and call it, for example[6], "a".

[6] Can you call this solution x? This is a complicated issue. Think of this as follows: the letter x is really a slot where you can put in a number. A number that can be put in the slot so as to make the formula true is called a "solution". The solution and the slot are two different things. So it is not a good idea to use the same name for both. If you do things *very* carefully, it turns out that it is O.K. to call both the slot and a solution with the same name, but I strongly recommend that you do not do it. For example the equation $3x^2 + 5x = 8$ has are two solutions, namely, 1 and $-\frac{8}{3}$. Which one is "x"? You cannot call both of them "x", because they are different. So I think it is better to call one of the solutions a (or A, or u, or U, or p, or P, or α, or $\heartsuit$) and then call the other one a different name (say b, or B, or v, or V, or q, or Q, or β, or $\clubsuit$).

1.4 Proofs by contradiction

Proof by contradiction is probably the most important and most widely used of all proof strategies. So you should not only learn what proofs by contradiction are, but ***acquire the habit of always***[a] ***seriously considering the possibility of using the proof by contradiction strategy when you are trying to figure out how to do a proof.***

[a] Sure, I am exaggerating a little bit. There are quite a few direct proofs (that is, proofs that are not by contradiction). But the number of proofs by contradiction is huge.

Let me first explain what proofs by contradiction are, and then I will tell you why they are so important.

And the first thing I need to explain is what a ***contradiction*** is.

1.4.1 What is a contradiction?

The precise definition of "contradiction" is complicated, and requires some knowledge of logic. So let me give you a simplified definition that is easy to understand and is good enough for our purposes.

Temporary definition of "contradiction". A <u>contradiction</u> is a statement of the form "A and no A", that is, "A is true and A is not true". □

Example 2.

- The sentence "$2+2=7$" is ***not*** a contradiction. It is a false statement, of course, but not every false statement is a contradiction.

- The sentence "$2+2=7$ and $2+2=4$" is ***not*** a contradiction either. It is a false statement (because it is the conjunction of two sentences one of which is false), but that does not make it a contradiction.

- The sentence "$2+2=7$ and $2+2\neq 7$" ***is*** a contradiction. because it is of the form "A and no A", with the sentence "$2+2=7$" in the role of A.

- The sentence “$n = 1$ and $n \neq 1$” is a contradiction.
- The sentence “John Adams was the first U.S. president” is false, but it ***not*** a contradiction.
- The sentence “John Adams was the first U.S. president and was the second U.S. president” is false, but it ***not*** a contradiction.
- The sentence “John Adams was the first U.S. president and was not the first U.S. president” ***is*** a contradiction. □

1.4.2 What is a proof by contradiction?

A ***proof by contradiction*** is a proof in which you start by assuming that the statement you want to prove is false, and you prove a contradiction.

To do a proof by contradiction, you would write something like this:

> We want to prove A.
>
> > Assume that A is false.
> >
> > ⋮
> >
> > $2 = 1$ and $2 \neq 1$.
>
> So assuming that A is false has led us to a contradiction.
>
> Hence A is true. **Q.E.D.**

> WHAT DOES “ASSUME” MEAN?
>
> ***“Assume” means “imagine”.*** In order to prove that some statement S is true, we imagine that it is not true, that is, we explore an imaginary world W in which S is not true, and we prove that in this imaginary world something impossible (such as a contradiction, ”A is true and A is not true”) would have to happen. And from this we draw the conclusion that a world in which S is not true is impossible, so un the real world S must be true.

WARNING

Having explained very precisely what a contradiction is, I have to warn you that mathematicians will often say things like "'$2+2=7$'" is a contradiction".

This is not quite true, but when a mathematician says that every mathematician will understand what is really intended.

What the person who said "'$2+2=7$' is a contradiction" really meant is something like this:

> Now that I have proved that $2+2=7$, I can easily get a contradiction from that, because we all know how to prove that $2+2\neq 7$, and then we can deduce from these two formulas the sentence "$2+2=7$ and $2+2\neq 7$", which is truly a contradiction.
>
> In other words, once I get to "$2+2=7$", it is clear to me, and to every mathematician, how to get to a contradiction from there, so there is no need to go ahead and do it, so I can stop here.

This is something mathematicians do very often[a]: ***once we get to a point where it is clear how to go on and finish the proof, we just stop there.***

For a beginning student I would recommend that you actually write your proof until you get a real contradiction, because this is the only way to make it clear to the person reading (and grading) your work that you do understand what a contradiction is.

[a] And not only mathematicians! In chess, once you get to a position from which it is clear that you can take your rival's King and win, you say "checkmate" and the game stops there.

1.5 More proofs: Pythagoras' Theorem

Pythagoras' Theorem is one of the oldest and most important theorems in Mathematics. It is named after the Greek mathematician and philosopher Pythagoras, who lived approximately from 570 to 495 BCE, although there is a lot of evidence that the theorem (but probably not the proof) was known before, by the ancient Babylonians.

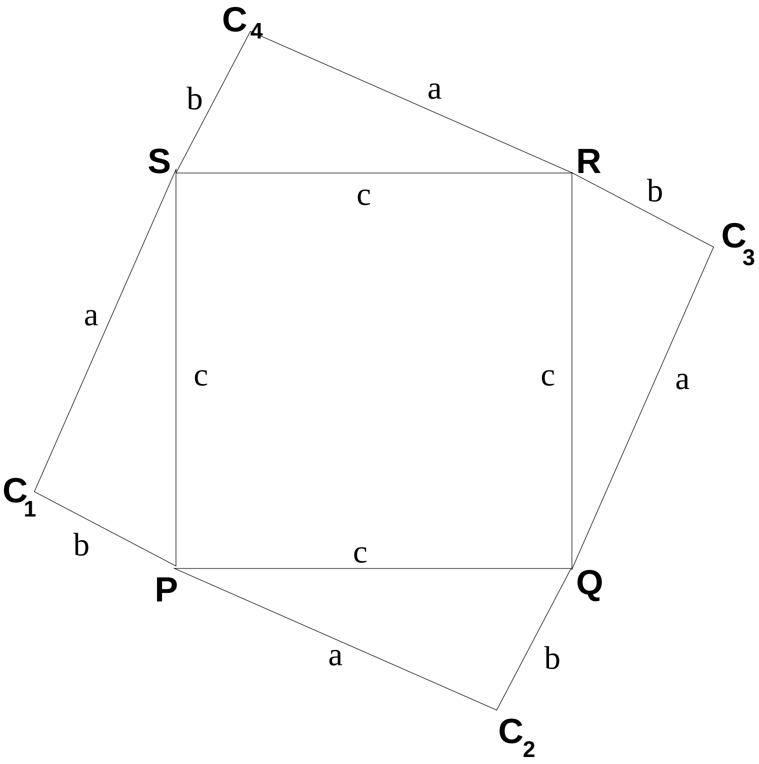
The statement of the theorem is as follows:

Theorem 2. (Pythagoras' Theorem) *If T is a right triangle*[7]*, c is the length of the hypothenuse*[8] *of T, and a, b are the lengths of the other two sides, then*

$$a^2 + b^2 = c^2 \,. \tag{1.1}$$

There are many different proofs of Pythagoras' Theorem. I am going to give you two proofs.

Pythagoras' proof. We draw a $c \times c$ square $PQRS$, and then attach at each side a copy[9] of T as shown in the picture.



[7] A right triangle is a triangle having one right angle

[8] The hypothenuse of a right triangle T is the side opposite to the right angle of T.

[9] For those who have studied Euclidean Geometry in high school: a copy of a figure F is a figure F' congruent to F. "Congruent to F" means: "obtainable from F by combining displacements and rotations. For example, the triangles QC_3R, RC_4S, and SC_1P are all congruent to PC_2Q.

The point P lies on the straight line segment from C_1 to C_2, because

1. If α_1 is the angle at S of the triangle SC_1P, and α_2 is the angle at P of the triangle PC_2Q, then $\alpha_1 = \alpha_2$, because the triangles SC_1P and PC_2Q re congruent.

2. Similarly, if β_1 is the angle at P of the triangle SC_1P, and β_2 is the angle at Q of the triangle PC_2Q, then $\beta_1 = \beta_2$, because the triangles SC_1P and PC_2Q are congruent.

3. Since SC_1P and PC_2Q are both right triangles, and the sum of the angles of every triangle is 180^o, we have

$$\alpha_1 + \beta_1 + 90^o = 180^o \text{ and } \alpha_2 + \beta_2 + 90^o = 180^o\,,$$

so

$$\alpha_1 + \beta_1 = 90^o \text{ and } \alpha_2 + \beta_2 = 90^o\,.$$

4. Since $\alpha_1 = \alpha_2$, it follows that $\alpha_2 + \beta_1 = 90^o$,

5. Hence the angle θ between the segments PC_1 and PC_2 is equal to $\alpha_2 + 90^o + \beta_1$, i.e., to 180^o. This proves that the segments PC_1 and PC_2 lie on the same straight line, so P lies on the segment C_1C_2.

A similar argument shows that Q lies on the segment C_2C_3, R lies on the segment C_3C_4, and S lies on the segment C_4C_1.

So the polygonal $C_1PC_2QC_3RC_4SC_1$ is a square.

Let $d = a + b$. Then the sides of the square $C_1C_2C_3C_4$ have length d.

Therefore the area of the square $C_1C_2C_3C_4$ is d^2.

On the other hand, the smaller square $PQRS$ has side of length c, so its area is c^2. Each of the four triangles has area $\frac{ab}{2}$. So the area of $C_1C_2C_3C_4$ is equal to $c^2 + 4 \times \frac{ab}{2}$, i.e., to $c^2 + 2ab$.

It follows that

$$\begin{aligned}(a+b)^2 &= d^2\\ &= c^2 + 4 \times \frac{ab}{2}\\ &= c^2 + 2ab\,.\end{aligned}$$

On the other hand, $(a + b)^2 = a^2 + b^2 + 2ab$. It follows that

$$a^2 + b^2 + 2ab = c^2 + 2ab\,.$$

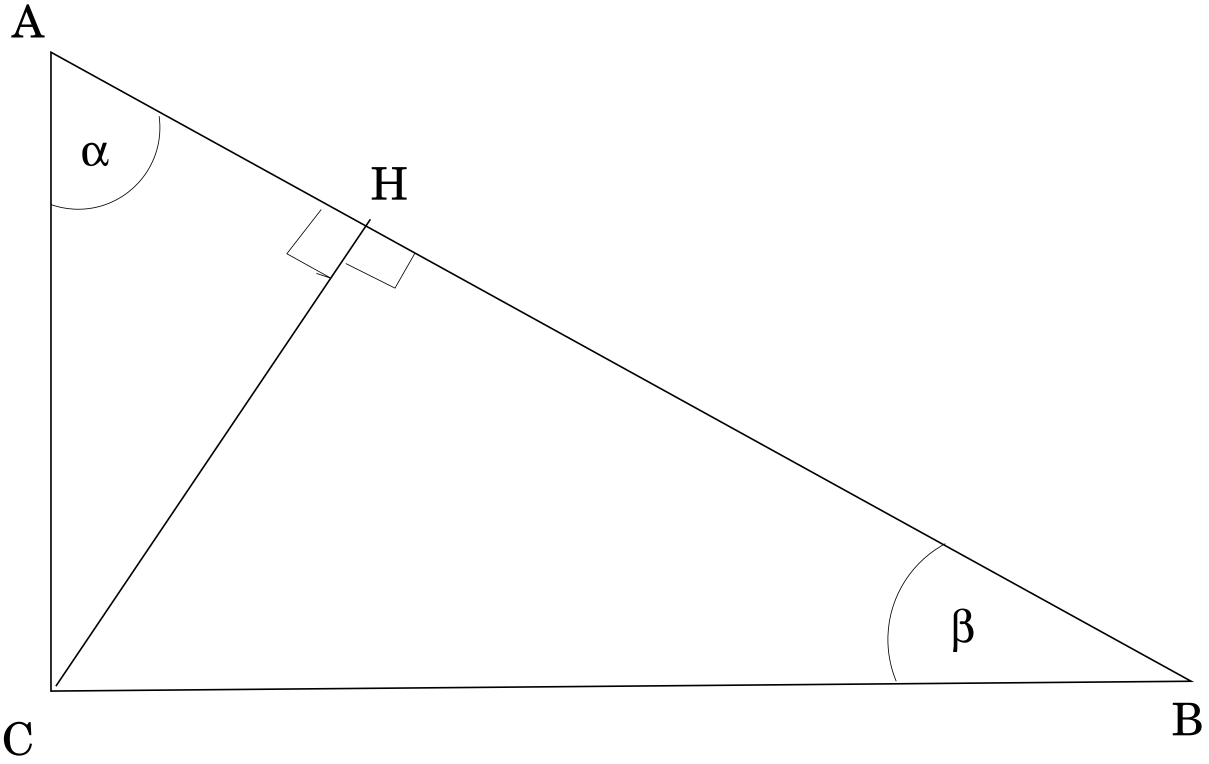
Subtracting $2ab$ from both sides, we get

$$a^2 + b^2 = c^2\,,$$

which is the desired result. **Q.E.D.**

Proof using similar triangles. Let C be the vertex of T where the right angle is located, and let A, B be the other two vertices.

Draw a line through C perpendicular to the line AB, and let H be the point where this line intersects the line AB.



Let α, β be the angles of T at A, B, so $\alpha + \beta = 90^o$. The angle of ACH at H is also 90^o, and the angle at A is α. Hence the angle of ACH at C is β. So the triangles ABC and ACH are similar. Hence the sides opposites to equal angles are proportional. That is:

$$\frac{|AC|}{|AH|} = \frac{|AB|}{|AC|}\,,$$

from which it follows that

$$|AC|^2 = |AH| \cdot |AB| .$$

A similar argument shows that

$$|BC|^2 = |BH| \cdot |AB| .$$

Adding both equalities we get

$$\begin{aligned} a^2 + b^2 &= |AH| \cdot |AB| + |HB| \cdot |AB| \\ &= \Big(|AH| + |HB|) \cdot |AB| \\ &= |AB| \cdot |AB| \\ &= |AB|^2 \\ &= c^2 . \end{aligned}$$

So $a^2 + b^2 = c^2$, as desired. **Q.E.D.**

1.6 Irrational numbers

In this section we will prove a very important fact, namely, that "the number $\sqrt{2}$ is irrational". This means, roughly, the same thing as "there does not exist a rational number r such that $r^2 = 2$." (The two statements do not say exactly the same thing. I will discuss how they differ later.)

But first I want to explain what this means and why this result is so important. And to do this we need a small philosophical digression into the question: ***what is a "number"?***. (If you are not interested in philosophical questions, you may skip this discussion and move on to subsection 1.7.3.)

1.7 What are "numbers"?

This is not an easy question to answer, and I will not even try. But there are some tings that can be said.

1. ***Numbers*** are, basically, tags (or labels) that we use to specify the amount or quantity of something, i.e., to answer the questions "how much ...?" or "how many ...?"

2. Since ancient times, it was understood that there are at least two kinds of “numbers”:

   (a) The ***counting numbers***, that we use to specify amounts of discrete quantities, such as coins, people, animals, stones, books, etc.

   - counting numbers are used to ***count***: 1, 2, 3, 4, 5, and so on,
   - they are the ones that ***answer questions of the form “how many ... are there?”***;
   - they ***vary in discrete steps***: they start with the number 1, then they “jump” from 1 to 2, and there is no other counting number between 1 and 2, then they “jump” from 2 to 3, and there is no other counting number between 2 and 3, and so on.

   (b) The ***measuring numbers***, that we use to specify amounts that can vary continuously, such as lengths, areas, volumes, weights.

   - measuring numbers are used to ***measure*** continuously varying quantities;
   - they are the ones that ***answer questions of the form “how much ... is there?”***;
   - they ***vary continuously***, so that, for example, when you pour water into a cup, if at some time point there are 10 ounces in the cup, and later there are 12 ounces, it does not occur to us that the amount of water in the cup may have jumped directly from 10 to 12 ounces: we understand that at some intermediate time there must have been 11 ounces, and at some time before that there must have been 10.5 ounces, and at some time before that there must have been 10.25 ounces, and at some time before the amount of water in the cup was 10.15309834183218950482 ounces; and so on[10]. At no time did the amount of water “jump”[11] from some value u to some larger value v.

[10] WARNING: The words “and so on” here are very imprecixse. It’s not at all what they mean. When I talk about the counting numbers and I write “1, 2, 4, 5, and so on”, you know exacrtly what comes next: it’s 6. But when I write “11, 10.5, 10.25, 10.15309834183218950482, and so on”, I haven’t the faintest idea what comes next! So the “and so on” for counting numbers is acceptable, but the “and so on” for measuring numbers is not, and when we do things rigorusly and precisely we must get rid of it.

[11] To make this precise, one needs to use tha language of Calculus: if $w(t)$ is the amount

- they ***can be subdivided indefinitely***: for example
    - You can take a segment of length 1 (assuming we have fixed a unit of length), and divide it into seven equal segments, each one of which has length $\frac{1}{7}$. And then you can draw segments whose lengths are $\frac{3}{7}$, or $\frac{4}{7}$, or $\frac{9}{7}$, or $\frac{23}{7}$, thus getting fractional lengths.
    - And, instead of 7, you can use any denominator you want, and get lengths such as $\frac{5}{2}$, $\frac{12}{5}$, $\frac{29}{17}$, $\frac{236{,}907}{189{,}276}$, and so on.
    - Hence, if n and m are any natural numbers, then we can (at least in principle) construct segments of length $\frac{m}{n}$. That is, we can construct segments of length f, for any fraction f.

The measuring numbers such as $\frac{5}{2}$, $\frac{12}{5}$, $\frac{29}{17}$, or $\frac{236{,}907}{189{,}276}$, that can obtained by dividing a counting number m into n equal parts, where n is another counting number, are called ***fractions***.

And this suggests an idea:

Idea 1: *Perhaps the measuring numbers are exactly the same as the fractions.*

In other words: suppose we use the length u of some straight-line segment U as the unit for measuring length. (That is, we call the lenght of this segment "meter", or "yard", or "foot", or "mile", and then we try to express every length in meters, or yards, or feet, or miles.) When we do that, we will of course need fractions to expres some lenghts because, for example, if we measure distances in miles, not every distance will be 1 mile, or 2 miles, or n miles for some counting number n. Some distances will be, say, half a mile, or three quarters of a mile, on thirteen hundredths of a mile, or forty-seven thousandths of a mile[12].

of water at time t, then w is a ***continuous function*** of t. The trouble with this is: at this point you only have a nonrigorous, not very precise idea of what a "continuous function" is. You will learn to define the notion of "continuous function", and work with it, and prove things about it, in your next "Advanced Calculus" or "Real Analysis" course.

[12] Here is another important difference between counting and measuring numbers: to count things using counting numbers you do not need units, but to measure amounts using measuring numbers you do. If you are asked how many pills there are in a bottle, then you answer "six", or "twenty-five', or whatever, and nobody is going to ask "six what?". But if you are asked how much water there are in the bottle, and you answer "six", then

Then Idea 1 suggests that the length of every segment V should be equal to a fraction $\frac{m}{n}$ times u (wnere m, n are natural numbers, i.e., counting numbers). That means that if we divide the segment U into n equal segments of length $w = \frac{u}{n}$, then the length of U is n times w, and the length of V is m times w. So U and V are commensurable. Since we can take U and V to be any two segments we want, we find that ***If Idea 1 i true, then any two segments are commensurable.***

COMMENSURABLE LENGTHS

“Commensurable” means “measurable together”. Precisely:

Definition 1.

- Two segments U, V, are commensurable if you can use a ruler of the same length w to “measure u and v together”, that is, to express both lengths u and v as integer multiples mw, nw of the unit of length w.
- Two segments U, V, are incommensurable if they are not commensurable.

But then a momentous discovery of far-reaching consequences was made:

$$\boxed{\textbf{\textit{There are incommensurable lenghts.}}}$$

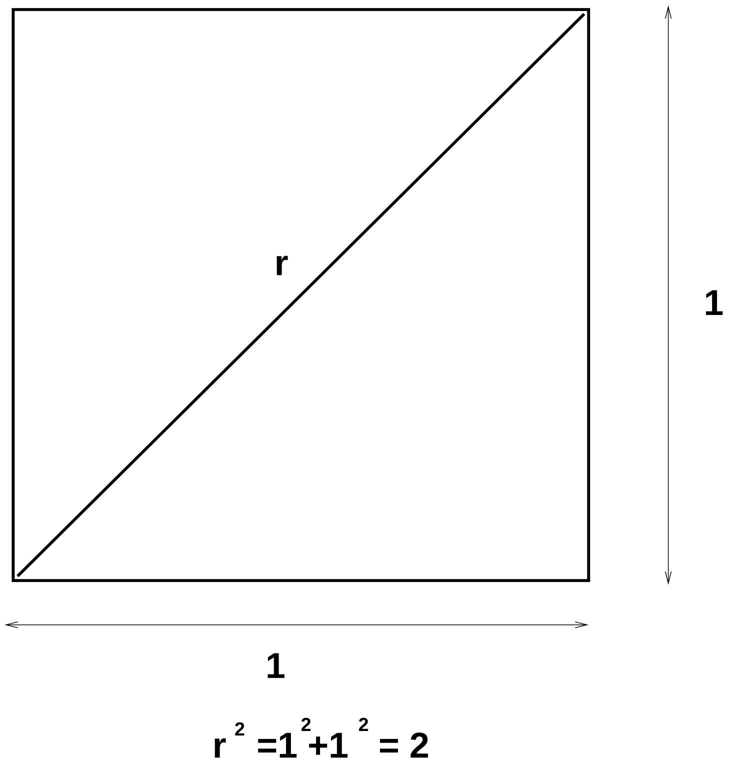
That is, ***it is not true that any two lengths are commensurable***.

Precisely: it is possible to construct geometricallly[13] a segment whose length r satisfies $r^2 = 2$. For example, if we draw a square whose sides have

somebody is going to ask “six what?”, expecting that you will say something like “six ounces”, or “six liters”, because if you do not specify the units of your measurement the number you gave is meaningless.

[13] What does “constructing geometrically” mean? This is tricky. For Euclid (who lived about 23 centuries ago), “constructing geometrically” meant “constructing with a ruler and compass”. (See the Wikipedia article ”Compass and straightedge consrtuctions”.) Using ruler and compass, one can construct lines and circles, but there are lots of other curves—for example, ellipses—that cannot be constructed that way. On the other hand, there are other equally “geometric” methods that can be used to construct some of those curves. For example, ellipses can be constructed using pins and strings. (See the Wikipedia article “Ellipses”.)

length 1, then the length r of the diagonal of the square will satisfy $r^2 = 2$, by Pythagoras' theorem.



And it was discovered that ***there is no fraction*** r ***such that*** $r^2 = 2$. This means that

I. If you believe that "number" means "fraction", then there is no number that measures the length of the diagonal of a square whose sides have lengt 1.

II. If you are willing to accept that there could be "numbers" that are not fractions, then maybe there is a number r that measures the length of the diagonal of a square whose sides have lengt 1, but that number r, that we could call "$\sqrt{2}$", is not a fraction.

Today we would say that

- Those numbers that are not fractions, such as $\sqrt{2}$, do indeed exist, and we call them "real numbers".
- The fractions, called "rational[14] numbers", are real numbers, but many real numbers are "irrational" numbers, that is, numbers that are not rational.
- Actually, most[15] real numbers are not rational.
- It took mathematicians more than 2,000 years after the discovery of the irrationaly of $\sqrt{2}$ to come up with a truly rigorous definition of the concept of "real number". (The name "real number" was introduced by Descartes in the 17th century. The first rigorous definition was given by George Cantor in 1871, and the most widely used definitions were proposed by Karl Weierstrass and Richard Dedekind.

1.7.1 Why was the irrationality of $\sqrt{2}$ so important?

The discovery of the inconmensurability of $\sqrt{2}$ was made, according to legend, by ***Hippasus of Metapontum***, who lived in the 5th century B.C.E and was a member of the religious sect of the Pythagoreans, i.e., the followers of the philosopher and mathematician Pythagoras[16]. And the legend also says that the discovery was so shocking to the Pythagoreans that Hippasus was drowned at sea, as punishment for having divulged the secret. (But this is a legend, and there is no evidence that it is true.)

[14] The word "rational" here has nothing to do with "rationality" in the sense of "in accordance withb reason or logic". It comes from the word "ratio", which means "quotient". An "irrational number" is a number that is not the quotient ("'ratio") of two integers. If you hear somebody say something like "scientists have shown that nature is irrational: mathematicians have shown that irrrationality is everywhere present, because most numbers are irrational", then you shoud realize that thit is an ignorant statement by somebody who does not understand what "irratioanl numbers" are. The "irrationality" of irrational numbers has nothing to do with their being unreasonable, absurd, or illogical; it just means that they are not quotients of two integers.

[15] If this statement does not strike you as incomprehensible because you don't know what it means, you should think again, and ask yourself "what could it possibly mean to say that most real numbers are irrational"? It turns out that this can be made precise, but making it precise is hard.

[16] Yes, that's the same Pythagoras of Pythagoras's theorem.

Why was the existence of inconmensurable magnitudes so upsetting to the Pythagoreans? The reason is this: the Pythagoreans were a mystical-religious cult.

> The Pythagoreans honored the effort put into mathematics, and coordinated it with the observation of the cosmos in various ways, for example: by including number in their reasoning from the revolutions and their difference between them, by theorizing what is possible and impossible in the organization of the cosmos from what is mathematically possible and impossible, by conceiving the heavenly cycles according to commensurate numbers with a cause, and by determining measures of the heaven according to certain mathematical ratios, as well as putting together the natural science which is predictive on the basis of mathematics, and putting the mathematical objects before the other observable objects in the cosmos, as their principles.
>
> From the *Wikipedia* article on *Pythagoreanism*, which quotes the *Protrepticus*, by D. S. Hutchinson and M. R. Johnson, a 2015 reconstruction of a lost dialogue of Aristotle.

In other words, for the Pythagoreans everything in the world was determined by ratios (i.e. quotients) of "numbers", and for them "number" meant "natural number" (i.e., counting number). The discovery that some lengths were not ratios of "numbers" undermined the Pythagorean system to such an extent that the members of the sect felt it necessary to conceal this fact from the general public.

But it is important to put all this in proper perspective: there is no real proof that Hippasus truly was the discoverer of the irrationality of $\sqrt{2}$, or that he was drowned at sea for that discovery.

1.7.2 What is a "real number", really?

The discovery that there are lengths that are inconmensurable with one another naturally forced mathematicians to ask a fundamental question: ***what is a "number", really?***

And, as we have explained, it took more than 2,000 years until mathematicians found a satisfactory answer.

1.7.3 The most important number systems: real numbers vs. integers and natural numbers

Now let us look at the main number systems[17] that mathematicians use today.

1. The measuring numbers, together with their negatives, and zero, are called ***real numbers***.
2. The set of all real numbers is called $\mathbb{R}$. (It is also called "the set of all real numbers", or "the real line".)
3. The counting numbers are called ***natural numbers***. (They are also called "positive integers".)
4. The set of all natural numbers is called $\mathbb{N}$.
5. The natural numbers, together with their negatives and zero, are called ***integers***.
6. The set of all integers called $\mathbb{Z}$.
7. The real numbers that are quotients of two integers are called ***rational numbers***. That is, we have

   Definition 2. A <u>rational number</u> is a real number r such that there exist integers m, n for which:

   (a) $n \neq 0$

   (b) $r = \frac{m}{n}$. □

8. The set of all rational numbers is called $\mathbb{Q}$.

[17] There are many number systems. What we will do here is barely scratch the surfaceof a very rich theory.

1.7.4 A remark about sets

We will spend a lot of time in this course studying ***sets***. At this point, all you need to know is that

- ***sets have members***.
- If S is a set and x is an object (for example, a number or a person or a giraffe or a set) then "$x \in S$" is a way of saying that x is a member of S.
- "$x \in S$" is read as "x belongs to S", or "x is in S", or "x is a member of S".
- We write "$x \notin S$" to indicate that x is not a member of S.
- So, for example,
  - If C is the set of all cows, then to say that Suzy is a cow we can equally well say "Suzy$\in C$".
  - You can read "Suzy$\in C$ in any of the following ways:
    1. Suzy belongs to C,
    2. Suzy is in C,
    3. Suzy belongs to the set of all cows,
    4. Suzy is a cow.

    But the third reading, although correct, is very stupid, because there is no reason to say "Suzy is a member of the set of all cows" when you can say the same thing in a much shorter and simpler way by saying "Suzy is a cow".
  - Similarly, you can read "Suzy$\notin C$ in any of the following ways:
    1. Suzy does not belong to C,
    2. Suzy is not in C,
    3. Suzy does not belong to the set of all cows,
    4. Suzy is not a cow.

    And the third reading, though correct, sounds silly, so you would never say it that way.
- Here is another example.

- "$\mathbb{N}$", as we know, is the set of all natural numbers. So, to say that 3 is a natural number we can equally well say "$3 \in \mathbb{N}$".
- You can read "$3 \in \mathbb{N}$ in any of the following ways:
  1. 3 belongs to $\mathbb{N}$,
  2. 3 is in $\mathbb{N}$,
  3. 3 belongs to the set of all natural numbers,
  4. 3 is a natural number.

  But the third reading, althogh correct, is very stupid, because there is no reason to say "3 is a member of the set of all natural number" when you can say the same thing in a much shorter and simpler way by saying "3 is a natural number".

Problem 3. For each of the following formulas,

(a) indicate how to read it in English,

(b) indicate whether it is true or false.

1. $-3 \in \mathbb{N}$,
2. $0 \in \mathbb{N}$,
3. $0 \notin \mathbb{Z}$,
4. $0 \in \mathbb{Z}$,
5. $-3 \in \mathbb{R}$,
6. $0 \in \mathbb{R}$,
7. $0 \notin \mathbb{R}$,
8. $0 \in \mathbb{R}$,
9. $0 \in \mathbb{Q}$,
10. $3 \in \mathbb{Q}$,
11. $-3 \in \mathbb{Q}$,
12. $\frac{237}{42} \in \mathbb{Q}$,

13. $\sqrt{2} \in \mathbb{Q}$,
14. $\sqrt{2} \notin \mathbb{Q}$,
15. $\pi \in \mathbb{Q}$.

1.7.5 Proof of the irrationality of $\sqrt{2}$

As explained before, we could state the theorem on the irrationality of $\sqrt{2}$ by saying that "$\sqrt{2}$ is irrational". This, however, would mean that there is a "number $\sqrt{2}$", i.e., a number whose square is 2. But the issue whether such a number exists is different from the one that concerns us here, namely, whether there exists a rational number r such that $r^2 = 2$. So I prefer to state the theorem in a way that does not imply any *a priori* commitment to the existence of a "number" r such that $r^2 = 2$.

And, before we give the proof, we introduce a few concepts and state some facts that will be used in the proof, (These facts will be proved later in the course.)

THE DEFINITION OF "DIVISIBILITY" AND "FACTORS"

Definition 3. Let a, b be integers. We say that a is divisible by b (or that b is a factor of a) if there exists an integer k such that $a = bk$.

THE DEFINITION OF "EVEN" AND "ODD" INTEGERS

Definition 4. Let a be an integer. We say that a is even if it is divisible by 2. And we say that a is odd if it is not even.

The integers 1 are -1 are factors of every integer, because if $n \in \mathbb{Z}$ then $n = n \times 1$ and $n = (-n) \times (-1)$, so n is divisible by 1 and by -1. So 1 and -1 are not very interesting factors, because they are always there. So we refer to 1 and -1 as the ***trivial factors*** of an integer.

THE DEFINITION OF "COPRIME" INTEGERS

Definition 5. Let a, b be integers. We say that a and b are coprime if they do no have any nontrivial common factors.

Example 3. The integers 12 and 35 are coprime. Indeed:

- The factors of 12 are 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12 and -12.
- The factors of 35 are 1, -1, 5, -5, 7, -7, 35 and -35.

So the only common factors are 1 and -1, i.e., the trivial factors. Hence 12 and 35 are coprime. □

Fact 1. *Every rational number is equal to a quotient* $\frac{m}{n}$ *of two coprime integers.*

Fact 2. *The product of two odd integers is odd.*

And now, finally, we are ready to prove our third theorem

Theorem 3. *There does not exist a rational number* r *such that* $r^2 = 2$.

Proof. We give a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 2$.
Pick one such number and call it r.
Using Fact 1, we may pick integers m, n such that

(1) $n \neq 0$,
(2) $r = \frac{m}{n}$,
(3) m and n have no nontrivial common factors.

Since $r^2 = 2$, we have $\frac{m^2}{n^2} = 2$.
Therefore $m^2 = 2n^2$.
So m^2 is even.
But then m is even. (Reason: Assume[18] that m is not even. Then m is odd. So by Fact 2, m^2 is odd. But we have proved that m^2 is even. So m^2 is not odd. Therefore m^2 is odd and m^2 is not odd, which is a contradiction.)

[18] Notice that we have a proof by contradiction within our main proof by contradiction.

Since m is even, m is divisible by 2.

So we may pick an integer k such that $m = 2k$.

Then $m^2 = 4k^2$.

But $m^2 = 2n^2$.

Hence $2n^2 = m^2 = (2k)^2 = 4k^2$.

Therefore $n^2 = 2k^2$.

So n^2 is even.

But then n is even. (Reason: Assume[19] that n is not even. Then n is odd. So n^2 is odd by Fact 2. But we have proved that n^2 is even. So n^2 is not odd. Therefore n^2 is odd and n^2 is not odd, which is a contradiction.)

So m is even and n is even.

Therefore m and n are divisible by 2.

So m and n have a nontrivial common factor.

But m and n do not have a nontrivial common factor.

So m and n have a nontrivial common factor and m and n do not have a nontrivial common factor.

So we have proved a contradiction.

So the assumption that there exists a rational number r such that $r^2 = 2$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 2}$.**Q.E.D.**

1.8 More irrationality proofs

We now use the same tecbnique to prove that $\sqrt{3}$ is irrational. The key point here is to realize that "even vs. odd" now has to be replaced by "divisible by 3 vs. not divisible by 3". And, in order to do the crucial step (the analogue of "if m^2 is divisible by 2 then m is divisible by 2") we need a generalization of Fact 2:

Fact 3. *If p is a prime number, then the product of two integers that are not divisible by p is not divisible by p either.*

(We will prove Fact 3 later.)

[19] Another proof by contradiction !

Theorem 4. *There does not exist a rational number r such that $r^2 = 3$.*

Proof. We will do a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 3$.

Pick one such number and call it r.

Using Fact 1, we may pick integers m, n such that

(1) $n \neq 0$,

(2) $r = \frac{m}{n}$,

(3) m and n have no nontrivial common factors.

Since $r^2 = 3$, we have $\frac{m^2}{n^2} = 3$.

Therefore $m^2 = 3n^2$.

So m^2 is divisible by 3.

But then m is divisible by 3. (Reason: By Fact 3, if m was not divisible by 3, it would follow that m^2 is not divisible by 3 either. But m^2 is divisible by 3, and we got a contradicition.)

Since m is divisible by 3, we may pick an integer k such that $m = 3k$.

Then $m^2 = 9k^2$.

But $m^2 = 3n^2$.

Hence $3n^2 = 9k^2$, so

$$n^2 = 3k^2 \,. \tag{1.2}$$

So n^2 is divisible by 3.

But then n is divisible by 3. (Reason: By Fact 3, if n was not divisible by 3, it would follow that n^2 is not divisible by 3 either. But n^2 is divisible by 3, and we got a contradicition.)

So 3 is a factor of m and 3 is a factor of n.

Hence m and n have a nontrivial common factor.

But m and n do not have a nontrivial common factor.

Therefore

$\boxed{\text{$m$ and n have a nontrivial common factor, and m and n do not have a nontrivial common factor,}}$

which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 3$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number r such that $r^2 = 3$}}$.**Q**.**E**.**D**.

1.8.1 What happens when you make a mistake in a proof

Can we do the same that we did before to prove that

THEOREM: There does not exist a rational number r such that $r^2 = 4$.
Proof. We will do a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 4$.

Pick one such number and call it r.

Using Fact 1, we may pick integers m, n such that

(1) $n \neq 0$,
(2) $r = \frac{m}{n}$,
(3) m and n have no nontrivial common factors.

Since $r^2 = 4$, we have $\frac{m^2}{n^2} = 4$.

Therefore $m^2 = 4n^2$.

So m^2 is divisible by 4.

But then m is divisible by 4. (Reason: By Fact 3, if m was not divisible by 4, it would follow that m^2 is not divisible by 4 either. But m^2 is divisible by 4, and we got a contradicition.)

Since m is divisible by 4, we may pick an integer k such that $m = 4k$.

Then $m^2 = 16k^2$.

But $m^2 = 4n^2$.

Hence $n^2 = 4k^2$, so

$$n^2 = 3k^2\,. \tag{1.3}$$

So n^2 is divisible by 4.

But then n is divisible by 4. (Reason: By Fact 3, if n was not divisible by 4, it would follow that n^2 is not divisible by 3 either. But n^2 is divisible by 4, and we got a contradicition.)

So 3 is a factor of m and 4 is a factor of n.

Hence m and n have a nontrivial common factor.

But m and n do not have a nontrivial common factor.

Therefore

$\boxed{\text{$m$ and n have a nontrivial common factor, and m and n do not have a nontrivial common factor,}}$

which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 4$ has led us to a contradiction,

Therefore $\boxed{\text{there does not exist a rational number r such that $r^2 = 4$}}$.**Q.E.D.**

Same proof, right?

WRONG!!!!!

What is wrong here?

1. The result is ***false***. It is not true that there does not exist a rational number r such that $r^2 = 4$. Indeed, if we take $r = 2$ then r is ratinal and $r^2 = 4$.

2. Since the conclusion of the proof is false, the proof itself must be wrong. That is, whoever wrote this proof must have cheated[20] in some step.

   In our case, Fact 3 explicitly says that "if p is prime then if a is not divisible by p it follows that a^2 is not divisible by p". So we are allowed to apply Fact 3 if p is prime, but we are not allowed to apply it if p isnot prime.

   So the two steps where we applied Fact 3 are wrong. In those steps, we cheated, by violating the rules.

The general principle is this: ***If a proof is correct then you can be sure that the conclusion is true.***

And another way to say that is this: ***if the conclusion of a proof is false, then the proof must be wrong. There has to be a mistake in the proof itself.***

So, if I give you a proof of a conclusion that is false, you have to be able to find where in the proof the author cheated. I will not be satisfied with a statement such as "the proof is wrong because the conclusion is false." I will want to know where in the proof a mistake was made.

Consider the following analogy: If I am trying to drive to Boston and end up in New York, then of course I can conclude thta I did something worng. But I will want to know what I did wrong, where I made a wrong turn. The same happens with proofs.

1.8.2 More complicated irrationality proofs

I hope it is clear to you that the same method, exactly, will apply to prove that $\sqrt{5}$, $\sqrt{7}$, $\sqrt{11}$, and, more generally, $\sqrt{p}$ for any prime number, is irrational.

Now let us try a more complicated case. Let us prove that

Theorem 5. *There does not exist a rational number r such that $r^2 = 12$.*

Remark 2. The number 12 is not prime. (Actually, $12 = 4 \times 3$.) So we cannot apply Fact 3 with 12 in the role of p.

[20] Nothing personal here. "Cheat" means "violate the rules." Of course, I haven't told you yet what the rules are, but let me anticipate one of them. ***You are allowed to use a result that has been proved, but you are now allowed to make up a statement that has not been proved and use it as if it was true.***

Proof. We will do a proof by contradiction .

Assume that there exists a rational number r such that $r^2 = 12$.

Pick one such number and call it r, so $r^2 = 12$..

Using Fact 1, we may pick integers m, n such that

(1) $n \neq 0$,
(2) $r = \frac{m}{n}$,
(3) m and n have no nontrivial common factors.

Since $r^2 = 12$, we have $\frac{m^2}{n^2} = 12$.

Therefore $m^2 = 12n^2$.

Hence $m^2 = 3 \times 4n^2$.

So m^2 is divisible by 3.

But then m is divisible by 3. (Reason: By Fact 3, if m was not divisible by 3, it would follow that m^2 is not divisible by 3 either. But m^2 is divisible by 3, and we got a contradicition.)

Since m is divisible by 3, we may pick an integer k such that $m = 3k$.

Then $m^2 = 9k^2$.

But $m^2 = 12n^2$.

Hence $12n^2 = 9k^2$, so

$$4n^2 = 3k^2 \,. \tag{1.4}$$

So $4n^2$ is divisible by 3.

But then n is divisible by 3. (Reason: By Fact 3, assume n is not divisible by 3; then by Fact 3 n^2 is not divisible by 3; since 4 is not divisible by 3, another application of Fact 3 tells us that $4n^2$ is not divisible by 3. But $4n^2$ is divisible by 3, so we got a contradiction.)

So 3 is a factor of m and 3 is a factor of n.

Hence m and n have a nontrivial common factor.

But m and n do not have a nontrivial common factor.

Therefore

m and n have a nontrivial common factor, and m and n do not have a nontrivial common factor,

which is a contradiction,

So the assumption that there exists a rational number r such that $r^2 = 12$ has led us to a contradiction,

Therefore there does not exist a rational number r such that $r^2 = 12$.**Q.E.D.**

Problem 4. ***Prove*** that each of the following numbers is irrational:

1. $\sqrt[3]{5}$,
2. $\sqrt{28}$,
3. $\sqrt{2+\sqrt{2}}$.
4. $\sqrt[3]{9}$. □

Problem 5. ***Prove or disprove***[21] each of the following statements:

1. The sum of two rational numbers is a rational number.
2. The product of two rational numbers is a rational number.
3. The sum of two irrational numbers is a rational number.
4. The product of two irrational numbers is a rational number.
5. The sum of two irrational numbers is an irrational number.
6. The product of two irrational numbers is an irrational number.
7. The sum of a rational number and an irrational number is an irrational number.

[21] To ***disprove*** a stetement means “to prove that the statement is false”. For example, when we proved that 1 is not even we disproved the statement ‘1 is even”.

8. The product of a rational number and an irrational number is an irrational number. □

Problem 6.

1. ***Explain*** why the following "proof" that $\sqrt{2}+\sqrt{3}$ is irrational is wrong:

   We know that $\sqrt{2}$ is irrational.

   We know that $\sqrt{3}$ is irrational.

   Hence the sum $\sqrt{2}+\sqrt{3}$ is irrational. **Q.E.D.**

2. ***Explain*** why the following "proof" that $\sqrt{6}$ is irrational is wrong:

   We know that $\sqrt{2}$ is irrational.

   We know that $\sqrt{3}$ is irrational.

   Hence the product $\sqrt{2}.\sqrt{3}$ is irrational.

   So $\sqrt{6}$ is irrational. **Q.E.D.**

3. ***Give a correct proof*** that $\sqrt{2}+\sqrt{3}$ is irrational. □

Problem 7. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational. (NOTE: This requires some hard thinking on your part.) □

Problem 8. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is irrational. (NOTE: This requires ***quite a lot*** of thinking on your part.) □

Problem 9. ***Prove*** that, if $n \in \mathbb{N}$, and $p_1, p_2, \ldots, p_n$ are n distinct primes, then $\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_n}$ is irrational. (NOTE: This is very difficult.) □

Part II

2 The languages of mathematics: formal, natural, and semiformal

In these notes, we will be talking mostly about ***mathematical objects***, that is, numbers of various kinds (natural numbers, integers, rational numbers, real numbers, complex numbers, integers modulo n, etc.), sets, functions, relations, graphs, geometric objects (such as points, lines, segments, angles, circles, planes, curves and surfaces of various kinds, etc.), and many other kinds of objects (such as groups, rings, fields, algebras, modules, vector spaces, manifolds, bundles, Lie groups, etc.) that mathematicians have invented and you will learn about in more advanced courses.

And we will talk about these mathematical objects using ***mathematical language***. But mathematical language is a special kind of language, in many ways similar to other languages such as English, and in many ways different. So, in order to talk about mathematical language we will want to say a few words about language in general, so that we can explain what makes mathematical language special.

Mathematical language, as commonly used, is ***semiformal language***, that is, a mixture of ***formal language*** and the ***natural language*** (English, Chinese, French, whatever) that one uses in a particular country. (Formal lamguage is a language consisting entirely of formulas. For example, the statement "$A = \pi R^2$" is an expression in formal language.)

For example, when we say

$$\text{from the facts that } 2+2=4 \text{ and } 4+2=6 \text{ we deduce that } (2+2)+2=6 \tag{2.5}$$

this is a mixture of formal mathematical language and English. (The formal language part consists of the formulas "$2+2=4$", "$4+2=6$", and "$4+2=6$". The English part is the rest.)

If we wanted to say the same thing in French, we would say

$$\text{des faits que } 2+2=4 \text{ et } 4+2=6 \text{ on deduit que } (2+2)+2=6\,. \tag{2.6}$$

Notice that ***the formal language part does not change***. That's because ***formal language is universal***. The formula "$2+2=4$" is exactly the same in English, French, Chinese, or any other language.

As we will see in the course, ***it is possible to formalize mathematics fully***, that is, to develop a formal language into which we can translate every mathematical statement.

For example, statement (2.5) would become, in purely formal language:

$$(2+2=4 \wedge 4+2=6) \Longrightarrow (2+2)+2=6\,. \tag{2.7}$$

And, once you get to this level, the texts you get are no longer in English or Franch or Chinese, because ***formal language is the same everywhere***, exactly as the formula "$1+1=2$' is the same everywhere and can be understood by all people, no matter what language they speak.

This means that if we could write all of mathematics in formal language, we would have a language that permits people of all nationalities, speaking all kinds of lamguages, to communicate easily: if a mathematician who speaks Chinese says something, and a mathematician who speaks English does not understand, then all these two mathematicians have to do is switch to formal language, and then they would have no problem communicating.

Formal language has other advantages that we will talk about soon. So you would think that mathematicians must use formal language all the time. But in fact we do not. We use a semiformal language which is a mixture of formal language and our own natural languages, because formal language is too dry and to hard to read. But formal language remains the means of communication of last resort: if I don't understand something you wrote, then I would ask you to say it in formal language. I you cannot say it in formal language, then what you wrote is meaningless. If you can say it in formal language, then I will understand what you said, and I will be able to decide if it is right or wrong.

Example 4. Suppose you are trying to define "prime number", and write "a prime number is a number that is only divisible by 1 and itself". Then I do not understand what you are saying, so I cannot tell if it is right or wrong.

Why do I not understand?

- Fisrt of all, I do not understand what “number” means. There are lots of different kinds of numbers: natural numbers, integers, rational numbers, real numbers, complex numbers, integers modulo n, etc. When you say “number”, which one do you mean?
- Also: what does “only divisible” mean? You may say that when yoy write “p is only divisible by 1 and itself”, what you mean is that “the only factors of p are 1 and p”. But then I would reply: “so 3 is not prime, because the factors of 3 are 3, 1, -1 and -3, so it’s not true that the only factors are 1 and 3; so 3 is not prime.” Then you would probably reply: “I did not mean to count negative factors as factors”, And I would aswer: “why didn’t you say that?”

If I ask you to write your statement in formal language, then that will force you to make your meanings precise. For example, you will write something like[22]

$$\text{if } p \in \mathbb{N}\,, \text{then } p \text{ is } \underline{\text{prime}} \text{ if } (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\,. \tag{2.8}$$

This is now completely clear, so at this point I will finally have understood what you are saying. And then I will be able to tell if this is right or wrong.

The answer is: as a definition of “prime number”, this is wrong, because 1 is not prime, but according to (2.8) 1 is prime.

But we can make it right by writing:

$$\text{if } p \in \mathbb{N}\,, \text{then } p \text{ is } \underline{\text{prime}} \text{ if } p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\,. \tag{2.9}$$

2.1 Things and their names

In any language, whether it is English, French, Russian, Spanish, Chinese, or formal or semiformal mathematical language, we talk about ***things*** (objects, entities), and in order to do that we give them ***names***.

[22] This is not yet a fully formal definition. To make it fully formal we need to introduce a symbolic way to say “p is prime”. We can do this by using “$P(x)$” for “x is prime”, and then your statement would become: $(\forall p \in \mathbb{N})\Bigg(P(p) \Longleftrightarrow (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\Bigg)$. This is not yet a correct definition of “prime number” but at least it is pefectly clear.

THINGS

In these notes, the word ***thing*** refers to an object of any kind: a concrete inanimate material object such as a table or a molecule or a planet, a "living thing" such as a plant, an animal, a person, or an amoeba, or an abstract thing such as a mathematical object.

So, in these notes, Mount Everest is a thing, and the chair on which you are sitting is a thing, and a book is a thing, but so are a giraffe, a spider, and you, and I, and my uncle Jim, and the number four, and the set $\mathbb{N}$ of all natural numbers.

Some students don't like using the word "thing" to refer to people, perhaps because they are thinking that "people are not things". My answers to that are:

1. We can use words in any way we like, as long as we do it consistently. So in this course we can decide how to use the word "thing", and there should be no problem as long as what we mean is clear to everybody.
2. We often do talk about "living things", and that includes people.
3. If you don't like using the word "thing" in this way, there is a word that's perfect for you: you can talk about "entities" instead. An entity is anything that exists. It can be a table, a river, a planet, an atom, a cell, a plant, a giraffe, a person, a number, a triangle, a matrix, a set, or a function. So just substitute the word "entity" for "thing" throughout these notes, and you will be fine.

2.1.1 Giving things individual names

The simplest way to give names to things is to give each thing an individual name, as when you call people with names such as "Mary", "John", or "George Washington", you give cities names such as "New York City", "Paris", or "London", or you give mountains names such as "Mount Everest" or "Mount Aconcagua".

But this way of naming things is not very convenient, because in our daily life we have to talk about an enormous number of things of many different kinds, and it would be truly impossible to give an individual name to each one.

Just imagine if every fork, every knife, every spoon, every plate, every glass, every cup, every napkin, every table, every pencil, every pen, every cell phone, every toothbrush, every animal, every plant, every cell in every person's or animal's or plant's body, every molecule and every atom in the Universe, every electron and every proton and every neutron and every particle of every kind, had to have its own individual name, and you had to know the name of each of those things before you can talk about it! Imagine how difficult life would be if every time you want to ask a waiter for a spoon you had to find out first the name of that particular spoon!

2.1.2 Variable noun phrases

So languages have developed a special device for naming things without having to give each individual thing its own name. We do this by using ***variables***, that is, noun phrases that can be temporarily designated to stand for a particular thing but can then be ***re-used***, as needed, to stand for a different thing.

NOUN PHRASES

A ***noun phrase*** is a word or phrase that stands for or is the name of something or somebody. For example: "he", "she", "the giraffe", "my uncle Jimmy', "Mount Everest", "the pencil", "the Math 300 final exam", "the table that I bought yesterday", "the President of the United States", "Mary", "New York City", "the most expensive restaurant in New York City", "the owner of the most expensive restaurant in New York City", are all noun phrases.

Example 5. When I say "I am going to open the door and let you in", the noun phrases "I", "the door", and "you" stand, respectively, for the speaker, a door, and the person that the speaker is talking to. But later, if somebody else says the same thing to somebody else, the words "I", "the door", and "you" will stand for two different people and a different door.

These noun phrases are ***variables***: at each particular time they are used they stand for some definite thing or person, called the ***referent***, or the

value of the variable. In each particular instance, it must be clear what the value is. (For example, if you and I are on a beach, and there is no door in sight, then when I say "I am going to open the door and let you in" you will not understand what I am talking about[23].). □

Variable noun phrases are re-usable: after I have used "the door" to refer to one particular door, I may use "the door" again later to refer to a different door.

Example 6. In a court of law, the noun phrase "the defendant" is used as a variable. When a trial begins, someone announces in some way that, for the duration of this trial, the words "the defendant" will refer to a certain specific person. Then, during the trial, everybody refers to that person as "the defendant". When the trial is over, the variable "the defendant" becomes ***free***, that is, not attached to any particular person, and is free to be used to refer to a new defendant when a new trial begins. □

Example 7. When you buy a house, the contract will probably contain a clause at the beginning declaring the words "the buyer" to stand for you for that particular contract. This means that the phrase "the buyer" is a variable, whose value is you for this contract. Later, for a new house sale, where the buyer is a different person, a new contract will be signed, in which the phrase "the buyer" has a totally different value. So the value of the phrase "the buyer" is fixed only within a specific contract, and changes when you go to another contract. □

2.1.3 Declaring the value of a variable

When we communicate our thoughts by speaking or writing, we use variable noun phrases all the time. But in order to be understood we also have to communicate to the reader or listener what each variable stands for each time we use it. That is, we have to ***declare*** the values of the variables we use. How is that done?

In English, values of variables are declared in dozens of different ways. For example,

[23] Unless my statement is part of some larger context that makes the value of the noun phrase "the door" clear. For example, I could be telling you that later, when we get home, I will open the door and let you in. In that context, the value of "the door" is clear.

- Often, we first mention a person by his or her name, and then when we use the pronouns “he”, “him”, “his”, “she”, “her”, it is understood that the pronoun stands for that person. For example, suppose I write

  > George Washington was the first president of the United States, and ***he*** served as president for two terms. ***He*** was succeeded by John Adams, who served only one term. When Adams ran for reelection to a second term, ***he*** was the object of malicious attacks by his opponents, and eventually lost the election to Thomas Jefferson.

  In this text, the pronoun “he” appears three times. The first two times, it clearly refers to George Washington, but the third time it refers to John Adams. The mention of John Adams undoes the declaration that “he” stands for George Washington, and assigns the new value “John Adams” to the pronoun.

- The pronoun “I” is understood to stand for whoever is speaking or writing.

- The pronoun “you” is understood to stand for whoever the speakers or writers are addressing themselves to.

- Values of variables are often declared by pointing. For example, if I say “please give me that book”, and I point to a book, then that book is the value of the variable “the book”.

- Sometimes, the value of a variable is clearly determined by the fact that there is only one thing within sight that the variable can stand for. For example, if I say “please give me the book”, and there is only one book within sight, then that book is the value.

- Often, the value of a variable is announced explicitly, as in the examples we gave above of the variable “the defendant” in a trial, and “the buyer” in a contract.

2.1.4 Using variables to name things in mathematical language

In mathematical language, it is customary to use ***letters*** as variables. The most commonly used letters are

- lower case letters such as x, y, r, p, q, a, b, atc.,
- capital letters such as X, Y, P, Q, A, B, etc.,
- lower case Greek letters (α, β, φ, ψ, σ, etc.),
- capital Greek letters[24] (Φ, Ψ, Σ, etc.).

But it is perfectly possible to use as variables other symbols such as

- longer strings such as "*abb*" or "the number I have been talking about",
- other symbols, such as $\diamond$, or $\clubsuit$.

Actually, ***you can use as a variable any symbol or string of symbols you want*** (except only for symbols such as $=$, $<$, $\leq$, $>$, $\geq$, $+$, $\times$, $\rightarrow$, $\Rightarrow$, $\wedge$, $\vee$, $\Leftrightarrow$, etc., that already stand for something else), ***provided that you declare its value*** (i.e. tell the reader clearly what the symbol or string of symbols stands for).

Remark 3. The symbols π and e stand for the well known real numbers $3.141592653589793238\ldots$ and $2.718281828459045235\ldots$, respectively. But even those symbols can be (and sometimes are) used as variables with other values, provided that the reader is told clearly what these symbols stand for[25]. □

2.1.5 Free (i.e. open) vs. bound (i.e. closed) variables

A free variable (or "open variable") in a text is a letter (or string of symbols) that is "unattached", in the sense that it has not been assigned a value, and is therefore free to be assigned any value we want.

A bound variable (or "closed variable") is a variable that has been assigned a value.

For instance, suppose a student starts a proof by writing:

[24] Some capital Greek letters are not used, because they are identical to their Latin counterparts. For example, A (capital alpha) and B (capital beta) are identical to the Latin A and B.

[25] For example: the symbol π is sometimes used to stand for a permutation; the expression $\pi_k(S)$ stands for the k-th homotopy group of a space S; the letter e is sometimes used for the charge of an electron.

(*)

$$\boxed{x^2 = 1 + x\,.}$$

or

(**) I am going to prove that $x^2 = 1 + x$.

In these texts, the letter x is a free variable. The formula says that "x-squared is equal to $x+1$", but it does not tell us who x is. So we have no way to know whether the formula is true or false. Therefore ***texts such as (*) or (**) are unacceptable, because they are meaningless.***

On the other hand, suppose a student writes

(***) Let $x = \frac{1+\sqrt{5}}{2}$.
Then

$$x^2 = 1 + x\,.$$

In this text, ***the phrase "let $x = \frac{1+\sqrt{5}}{2}$" effectively declares the variable x to have the value $\frac{1+\sqrt{5}}{2}$.***

So, after this value declaration, "x" stands for the number $\frac{1+\sqrt{5}}{2}$.

Then the meaning of (***) is perfectly clear, so ***(***) is acceptable, because in it the variable x is used correctly: before it is used, a value for it is declared.***

And then the meaning of (***) is perfectly clear: (***) is just a roundabout way to say that

$$\Big(\frac{1+\sqrt{5}}{2}\Big)^2 = 1 + \frac{1+\sqrt{5}}{2}\,.$$

Once this particular use of the variable x is over, you could, if you want to, use the same letter to represent some other number or object of any kind. But in that case it would have to be very clear that the old declaration that $x = \frac{1+\sqrt{5}}{2}$ no longer applies.

You could do this, for example, by saying something like

(****) Let $x = \frac{1+\sqrt{5}}{2}$. Then $x^2 = 1 + x$.
Now suppose, instead, that $x = \frac{1-\sqrt{5}}{2}$. Then it is also true that $x^2 = 1 + x$.

In (****), the word "now" serves the purpose of telling the reader that "we are starting all over again, and the old declared value of x no longer applies." (And the word "instead", which is unnecessary, strictly speaking, reinforces that.)

2.1.6 Arbitrary things

There is another way to assign a value to a variable: we can declare the value to be an ***arbitrary*** object of a certain kind.

ARBITRARY THINGS

An ***arbitrary thing*** of a certain kind is a fixed thing about which we know nothing, except that it is of that kind. For example, an "arbitrary integer" is an integer about which you know nothing other than that it is an integer.
The way you should think about "arbitrary things " is as follows.

- Imagine that you are playing a game against somebody (a friend, or a computer, or an alien from another planet) that we will call the **CAT** ("creator of arbitrary things").
- The CAT's job is as follows: every time you say or write "let a be an arbitrary thing of such and such kind," the CAT picks one such thing, writes down what that thing is on a piece of paper, puts the paper in an envelope, and seals the envelope.

  So, for example, if you say "let a be an arbitrary natural number" then the CAT will pick a natural number and write down what it is on a piece of paper that will go inside the envelope.
- Later. after you have finished talking or writing, you or the CAT will open the envelope, and you will know who a really was.
- At that point,
  - if what you said about a turns out to be true, then you win, and the CAT loses.
  - if what you said about a is not true, then the CAT wins, and you lose.

The key fact is this: ***In order to win, you have to be sure that everything you say about*** a ***is true of all the things of the given kind,*** because if there is just one thing for which what you said is not true, then a could turn out to be that thing, and then you will have been proved wrong, and will lose.

Example 8. Suppose you say:

Let n be an arbitrary integer.

What can you say after that, being sure that it is true?

Certainly, you cannot say that $n = 2$, because n could be 1, or -7, or 25.

And you cannot say that n is even, because n could be odd.

But here are a few things you *can* say:

- $n = n$.
- $|n| \geq 0$.
- n is either a natural number, or the negative of a natural number, or zero.
- $n + n^2$ is even. (Reason: n is either even or odd. If n is even, then n^2 is also even, so the sum $n + n^2$ is even. If n is odd, then n^2 is also odd, and the sum of two odd integers is even, so $n + n^2$ is even. So, no matter who n is, whether it is even, or odd, positive or negative, yuuo can be sure that $n + n^2$ is even.)
- $n^2 \geq 0$. (Reason: the square of every real number, and in particular of every integer, is ≥ 0.)
- If n is even then n^2 is divisible by 4. (This sentence is true for ***every*** natural number n. Indeed, the sentence is an implication: n is even$\Longrightarrow$ n^2 is divisible by 4. The integer n could be even or odd, and you have no control over that, because the CAT chooses n, and the CAT can choose n any way he or she wamts to. But: if n is odd, then the implication "n is even$\Longrightarrow$ n^2 is divisible by 4" is true, because the premise "n is even" is false; and if n even then we may pick an integer k such that $n = 2k$, and then $n^2 = 4k^2$, so n^2 is divisible; by 4, so the conclusion "'n^2 is divisible by 4" is true. So the sentence is true for every n.)
- $n(n + 1)(n + 2)$ is divisible by 6.
- If $n > 4$ then $n^2 > n+11$. (Reason: as we will see later, an implication "If A then B" is true if A is false or if B is true. Using this: if $n \leq 4$ then the implication "if $n > 4$ then $n^2 > n + 11$" is true because "'$n > 4$" is false. And if $n > 4$ then the implication "if $n > 4$ then $n^2 > n + 11$" is true because $n^2 > n + 11$' is true.)

On the other hand, you cannot say "$n^2 > 0$", because if you say that then the CAT will pick n to be 0, and you lose. □

Example 9. Suppose you say:

Let m, n be arbitrary natural numbers.

What can you say after that, being sure that it is true?

Certainly, you cannot say that $m = n$, because m and n could be different.

And you cannot say that $m \neq n$, because m and n could be equal.

And you cannot say that $m > n$, because m could be smaller than n.

But here are a few things you *can* say:

- $m + n \geq 2$. (Reason: $m \geq 1$ and $n \geq 1$, so $m + n \geq 2$.)
- $m.n$ is a natural number.
- $(m + n)^2 = m^2 + 2m + n^2$.
- $(m + n)^3 = m^3 + 3m^2n + 3mn^2 + n^3$.
- $m^2 - n^2 = (m - n)(m + n)$.
- $n + n^2$ and $m + m^2$ are even.
- Either $m > n$ or $m = n$ or $m < n$. □

2.1.7 Universal quantifiers and arbitrary things

Suppose you want to make sure (that is, prove) that something is true for ***all*** the members of some set S. For example, you may want to make sure that every student in a class knows that there is an exam next Tuesday.

You could do this in two ways:

1. You can use the ***exhaustive search method***: chack, one by one, all the memers of S, and verify that they all know about the exam.
2. You can use ***general reasoning***: you try to come up with an ***argument*** that shows that every student knows about the exam. (For example: maybe you have sent an e-mail to a mailing list of all the students, telling them about the exam. And yyou are sure that all the students get the messages to this mailing list, and that they all read them. Then you can be sure that they all know about the exam.)

If the set S is very large then it may be very difficult to use the exhaustive search method. And if the set is infinite then using exhaustive search is impossible. And this is the situation we encounter most of the time in Mathematics: the sets S about we want to make sure that statements of the form "$P(x)$ is true for every member x of S" are usually infinite, or finite but very large. So the only way to prove that something is true for all members of some set S is to use ***reasoning***:

This is why, in order to prove universal sentences $(\forall x \in S)P(x)$, we use the following method:

- we imagine that we have an arbitrary member x of S,
- we reason about x, prove facts about x,
- and, maybe, eventually, we prove that $P(x)$, the fact about x that we wanted to make sure is true, is indeed true.

If we can do that for an ***arbitrary*** member of S, then we have established that $P(x)$ is true for every $x \in S$, that is, that $(\forall x \in S)P(x)$. ("$(\forall x \in S)P(x)$" is a "universally quantified sentence". We will study such sentences in great detail in Section 4, on page 58.)

The method for proving universally quantified sentences $(\forall x \in S)P(x)$ by proving that $P(x)$ is true for an arbitrary member x of S is the ***Rule for proving universal sentences***, that we will call $\boxed{\text{Rule } \forall_{prove}}$, This rule will be discussed in section 4.5, on page 71 below.

Problem 10. Indicate whether each of the following statements about n is true for an arbitrary integer n. If the answer is "yes", prove it. If the answer is "no", prove it by giving a counterxample, that is, a particular value of n for which the statement is false.

1. n is even.
2. n is even or n is odd.
3. n is even and n is odd.
4. n is even or $n + 1$ is even.
5. $n(n + 1)$ is even.

6. $n(n+1)(n+2)$ is divisible by 3.
7. $n(n+1)(n+2)$ is divisible by 6.
8. $n^2 > 0$.
9. $n^2 \geq 0$.
10. $n(n+1) \geq 0$.
11. $(\forall m \in \mathbb{Z})(n < m \Longrightarrow n^2 < m^2)$.
12. $(\forall m \in \mathbb{Z})(n > m \Longrightarrow n^2 > m^2)$.
13. $(\forall m \in \mathbb{Z})(n = m \Longrightarrow n^2 = m^2)$.
14. $(\forall m \in \mathbb{Z})(n^2 = m^2 \Longrightarrow n = m)$.

3 Dealing with equality

Throughout these notes, the symbols "$=$" and "$\neq$" will be used.

- The symbol "$=$" is read as "is equal to".
- The symbol "$\neq$" is read as "is not equal to".

The meaning of "$=$" in mathematics is quite simple: if a and b are any two things, then "$a = b$" (read as "a is equal to b", or "a equals b") means that a and b are the same thing.

Example 10.

- The sentence "$3 = 2 + 1$" is read as "three is equal to two plus one".
- The sentence "$3 = 2 + 2$" is read as "three is equal to two plus two".
- The sentence "$3 \neq 2 + 1$" is read as "three is not equal to two plus one".
- The sentence "$3 \neq 2 + 2$" is read as "three is not equal to two plus two".
- The sentences "$3 = 2 + 1$" and "$3 \neq 2 + 2$" are true.
- The sentences "$3 = 2 + 2$" and "$3 \neq 2 + 1$" are false. □

3.1 The substitution rule (Rule SEE, a.k.a. Rule $=_{use}$) and the axiom $(\forall x)x = x$

There are two basic facts you need to know about equality.

THE TWO BASIC FACTS ABOUT EQUALITY

First, there is the ***substitution rule***, which tells you that in a proof you can always "substitute equals for equals":

RULE SEE (substitution of equals for equals): If in a step of a proof you have an equality $s = t$ or $t = s$, and in another step you have a sentence P, then you can write as a step any statement obtained by substituting t for s in one or several of the occurrences of s in P.

The second thing you need to know is the following axiom:

EQUALITY AXIOM (*The "everything is equal to itself" axiom*):

$$x = x \text{ for every } x\,.$$

Example 11. In the sentence "$2 + 2 = 4$", the symbol "2" occurs twice. Suppose you have "$2 + 2 = 4$" as one of the steps in a proof. And suppose that in another step you have "$1 + 1 = 2$". Then you can substitute "$1 + 1$" for "2" in the first occurrence of "2" in the sentence "$2+2 = 4$", thus getting "$(1 + 1) + 2 = 4$". Or you can substitute "$1 + 1$" for "2" in the second occurrence of "2" in "$2 + 2 = 4$", thus getting "$2 + (1 + 1) = 4$". Or you can substitute "$1 + 1$" for "2" in both occurrences of "2" in "$2 + 2 = 4$", thus getting "$(1+1)+(1+1) = 4$". Or you can substitute "$1+1$" for "2" in none of occurrences, in which case you get back "$2 + 2 = 4$". □

Example 12. The following are true thanks to the equality axiom:

1. $3 = 3$,

2. $(345 + 1,031) \times 27 = (345 + 1,031) \times 27$,

3. Jupiter=Jupiter[26]

4. $\pi = \pi$.

5. My uncle Billy=My uncle Billy. □

[26] But you have to be ***very*** careful here! There are at least three different things named "Jupiter": a planet, a Roman god, and a Mozart symphony. When you write "Jupiter=Jupiter", you have to make sure that the two "Jupiter" in the equation have the same meaning. It would be false if you said that the planet Jupiter is the same as the Roman god Jupiter!

3.2 Equality is reflexive, symmetric, and transitive

Most textbooks will tell you that equality has the following three properties:

I. Equality is a ***reflexive*** relation. That is:

$$\text{for every } x\,,\ \ x = x\,. \tag{3.10}$$

II. Equality is a ***symmetric*** relation. That is:

$$\text{for every } x\,, y\,,\ \text{ if } x = y \text{ then } y = x\,. \tag{3.11}$$

III. Equality is a ***transitive*** relation. That is:

$$\text{for every } x\,, y\,, z\,,\ \text{ if } x = y \text{ and } y = z \text{ then } x = z \tag{3.12}$$

And, in addition, they will also tell you that the following important property holds:

IV. ***If two things are equal to a third thing then they are equal to each other.*** That is,

$$\text{for every } x\,, y\,, z\,,\ \text{ if } x = z \text{ and } y = z \text{ then } x = y\,. \tag{3.13}$$

We could have put these properties as axioms, but we are not doing that because all these facts can easily be proved from our two basic facts about equality.

Theorem 6. *Facts I, II, III, and IV above follow from the two basic facts about equality described in the box on page 55 above.*

Proof. Fact I is exactly our Equality Axiom, so you don't need to prove it.

And now I am doing to do the proof of Fact II for you. So ***what you have to do is prove III and IV***.

Proof of Fact II.

Let x, y be arbitrary.

Assume $x = y$.

We want to prove that $y = x$.

> By the Equality Axiom, $x = x$.
>
> Since we have "$x = y$", Rule SEE tells us that, in the sentence "$x = x$", we can substitute "y" for any of the two occurrences of x in "$x = x$". So we choose to substitute "y" for the first of the two xs that occur in "$x = x$".
>
> This yields $\boxed{y = x}$.

Since we have proved that $y = x$ assuming that $x = y$, we have shown that

$$\text{if } x = y \text{ then } y = x\,. \tag{3.14}$$

(This is because of Rule $\Longrightarrow_{prove}$, discussed later in these notes in section 6.7.3 on page 138.)

Since we have proved (3.14) for arbitrary x, y, it follows that

$$\text{For all } x, y, \text{ if } x = y \text{ then } y = x\,. \tag{3.15}$$

(This is because of Rule $\forall_{prove}$, discussed later in these notes in section 4.5 on page 71.) This completes our proof. **Q.E.D.**

Proof of Facts III and IV. **YOU DO THEM.**

Problem 11. Write proofs of Fact III and Fact IV, following the model of the proof given here for Fact II. □

4 Universal sentences and how to prove and use them

A ***universal sentence*** is a sentence that says that something is true for every object x of a certain kind.

For example, the sentence

$$\text{every natural number is either even or odd} \tag{4.16}$$

says that every natural number has the property of being even or odd.

So this is a universal sentence.

Other examples of universal sentences are:

- Every natural number is an integer.
- Every real number has a square root[27].
- Every real number has a cube root[28].
- If n is any natural number then n is even or odd. □
- Every cow has four legs.
- Every cow has nine legs[29].
- All humans are thinking beings.
- All giraffes have a long neck.
- Every giraffe has a long neck.
- Every real number is positive[30].
- Every natural number can be written as the sum of three squares of integers[31].

[27] False!

[28] True!

[29] Sure, this one is false. But ***it is*** a universal sentence.

[30] This one is false.

[31] False again!

- Every natural number can be written as the sum of four squares of integers[32].
- Every integer is even[33].
- If a, b, c are integers, then if a divides b and c it follows that a divides $b + c$.

Universal sentences can always be rephrased is terms of "arbitrary things". For example, sentence (4.16) says

$$\text{If } n \text{ is an arbitrary natural number then } n \text{ is either even or odd}\,. \tag{4.17}$$

We can say this in a more formal (and shorter) way by using the ***universal quantifier symbol***:

$$\forall$$

(This symbol is an inverted "A". The symbol is chosen to remind us that "$\forall$" stand for "for all".)

Precisely, the symbol is used as follows:

- Using the universal quantifier symbol, we form ***restricted universal quantifiers***, that is, expressions of the form

  $$\Big(\forall x \in S\Big)\,,$$

  where

  - x is a variable,
  - S is the name of a set.

- It is also possible to form ***unrestricted universal quantifiers***, that is, expressions of the form

  $$\Big(\forall x\Big)\,,$$

[32] This one, believe it or not, is true. But it is very hard to prove, and precisely for that reason, if you are interested in mathematics, I recommend that you read the proof. It is truly beautiful. The result is called "Lagrange's four squares theorem".

[33] Also false.

where x is a variable,

- A restricted or unrestricted universal quantifier can be attached to a sentence by writing it before the sentence. This operation is called ***universal quantification***, and the result is a **universally quantified sentence**.
- So,

If S is a set, and $P(x)$ is a statement involving the variable x, then

$$(\forall x \in S)P(x)$$

is a universally quantified sentence, obtained by universally quantifying the sentence $P(x)$.

If $P(x)$ is a statement involving the variable x, then

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

is a universally quantified sentence, obtained by universally quantifying the sentence $P(x)$.

4.1 How to read universal sentences

4.1.1 Sentences with restricted universal quantifiers

The universal sentence

$$(\forall x \in S)P(x)$$

can be read as follows:

- for every member x of S, $P(x)$ is true[34],

or as

- for every member x of S, $P(x)$,

[34] See Remark 4 below.

or as

- for all members x of S, $P(x)$ is true,

or as

- for all members x of S, $P(x)$,

or as

- if x is an arbitrary member of S then $P(x)$ is true,

or as

- if x is an arbitrary member of S then $P(x)$.

4.1.2 Sentences with restricted universal quantifiers

The universal sentence

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

can be read as follows:

- for every x, $P(x)$ is true[35],

or as

- for every x, $P(x)$,

or as

- for all x, $P(x)$ is true,

or as

- for all x, $P(x)$,

or as

- if x is arbitrary then $P(x)$ is true,

or as

- if x is arbitrary then $P(x)$.

[35] See Remark 4 below.

4.1.3 A recommendation

Of all these ways of reading "$(\forall x \in S)P(x)$" and "$(\forall x)P(x)$", ***I strongly recommend the ones involving "arbitrary"*** x, because once you get used to reading universal statements that way it becomes very clear how to go about proving them.

Remark 4. If A is any sentence, then saying "A is true" is just another way of asserting A. For example, saying that

$$\text{“all animals are made of cells}'' \text{ is true} \tag{4.18}$$

is just another way of saying

$$\text{all animals are made of cells}\,. \tag{4.19}$$

Similarly, saying

$$P(n) \text{ is true} \tag{4.20}$$

is just another way of saying

$$P(n)\,. \tag{4.21}$$

This is why the sentence "$(\forall n \in \mathbb{Z})P(n)$" can be read either as "if n is an arbitrary integer then $P(n)$ is true", or as "if n is an arbitrary integer then $P(n)$". □

4.2 Using the universal quantifier symbol to write universal statements

4.2.1 What is formal language?

As we explained before, ***formal language*** is a language in which you use only formulas, and no words.

For example, you know from your early childhood how to take the English sentence "two plus two equals four" and say the same thing in formal language. i.e., with a formula. You just write

$$2 + 2 = 4\,. \tag{4.22}$$

We can say more complicated things in formal language by introducing more symbols. For example, here is the definition if "divisible" that we saw earlier:

DEFINITION Let a, b be integers. We say that a is divisible by b (or that b is a factor of a) if there exists an integer k such that $a = bk$. □

Then, we can agree to introduce the new symbol "|" to stand for "is a factor of", and write

$$b|a \tag{4.23}$$

instead of "b is a factor or a", or "a is divisible by b".

In particular, we can now say "x is even" in formal language, as follows: "$2|x$". So, for example the assertion that "the sum of two even integers is even" becomes, in formal language:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big((2|a \wedge 2|b) \Longrightarrow 2|a+b\Big)\,. \tag{4.24}$$

Can you say more complicated things in formal language? For example, can you rewrite the English sentence

(#) If we take any two real numbers and compute the square of their sum, then you get the same result as when you add the squares of the two numbers plus twice their product.

in formal language?

You know since high school that you can take a big part of (#) and rewrite it in formal language. The trick is to ***give names*** to the two integers that you want to talk about. Then you can write

(#1) If we take any two real numbers and call them a and b, then

$$(a+b)^2 = a^2 + b^2 + 2ab\,,$$

or

(#2) If a, b are arbitrary real numbers, then

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

Naturally, you could use any names you want, For example, you could equally well have written

(#3) If x, y are arbitrary real numbers, then

$$(x+y)^2 = x^2 + y^2 + 2xy\,.$$

or

(#4) If we take any two real numbers and call them x and y, then

$$(x+y)^2 = x^2 + y^2 + 2xy\,.$$

Sentences (#1), (#2), (#3), (#4) are statements in ***semiformal language***: they are a mixture of formal language and ordinary English.

These statements are universal sentences. And now you have learned how to ***formalize***[36] universal statements. So you can write

(#5) $(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(a+b)^2 = a^2 + b^2 + 2ab\,.$

or

(#6) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x+y)^2 = x^2 + y^2 + 2xy\,.$

Statements (#5) and (#6) are ***formal sentences***, that is, formulas with no words.

4.2.2 The road to full formalization.

What we have done is get started moving towards full formalization.

You started doing this in your childhood, when you learned how to formalize "two plus two equals four" by writing "$2 + 2 = 4$".

And now you have learned how to formalize more complicated sentences, Using the universal quantifier symbol, you are now able to say many more things in formal language.

[36] that is, how to say in formal language

Example 13. Suppose you wanted to say “every natural number is positive”. You can write

$$(\forall n \in \mathbb{N}) n > 0 \,. \tag{4.25}$$

This is a formula, that is, a sentence in formal language. □

Example 14. Although we do not know yet how to write something like

(#7) If we have any two integers, when say that the first one is divisible by the second one what we mean is that there exists an integer that multiplied by the second one results in the first one.

in full formal language, we are able, using what we know so far, to go a long way, and rewrite (#7) in semiformal language, with very few words, i.e., getting very close to a fully formal sentence. We can write

(#8) $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})$(“$a|b$” means “there exists k such that $k \in \mathbb{Z}$ and $b = ak$.”) □

Example 15. Let us say “If a, b, c are integers, then if a divides b and c it follows that a divides $b + c$” in semiformal language.

We can say:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big(\text{if } a|b \text{ and } a|c \text{ then } a|b + c\Big)\,, \tag{4.26}$$

which is, again, a sentence in semiformal language. □

Later, when we learn how to say “means”, “there exists”, “if … then” and “and”, we will be able to say (#8) and (4.26) in fully formal language, as follows:

- We can translate (#8) into fully formal language as

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(a|b \Longleftrightarrow (\exists k \in \mathbb{Z})b = ak)\,. \tag{4.27}$$

- We can translate (4.26) into fully formal language as

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big((a|b \wedge a|c) \Longrightarrow a|b + c\Big)\,, \tag{4.28}$$

4.3 Open and closed variables and quantified sentences

Let us recall that

A free variable is a letter (or string of symbols) that is "unattached", in the sense that it has no particular value, and is free to be assigned any value we want.
A bound variable is a variable that has been assigned a specific value, by means of a ***value declaration***.
We can turn a free variable into a temporary constant by ***declaring its value.***

Let me add a couple of points to that:

- Free variables are also called open variables.
- Bound variables are also called closed variables.

  (They are called "bound" variables because they are "bound", attached to a value, by contrast with free variables, that are free to be assigned any value because they do not have a value already assigned to them. And they are called "closed" because they are not open to be assigned a value, since they already have one.)
- ***A value declaration is valid until it expires***. When the value declaration expires, the variable becomes free again, and you can assign a new value to it.

Example 16. Here is an example of declaring a value for a variable, and of making that declaration expire. You could write:

1. Let $x = \frac{1+\sqrt{5}}{2}$.
2. Then $x^2 = 1 + x$.
3. Now suppose, instead, that $x = \frac{1-\sqrt{5}}{2}$.
4. Then it is also true that $x^2 = 1 + x$.

Here, step 1 assigns the value $\frac{1+\sqrt{5}}{2}$ to the variable, so this variable, which until then was open, is now attached to the value $\frac{1+\sqrt{5}}{2}$, so x is bound, no longer free.

But then, in step 3, we are ssigning a new value to x, which means that the previous value declaration has expired. The fact that the previous value declaration has expired is signaled by the word “now”’, and reinforced by the word “instead”.

Notice that if you had written

1. Let $x = \frac{1+\sqrt{5}}{2}$.
2. Then $x^2 = 1 + x$.
3. Let $x = \frac{1-\sqrt{5}}{2}$.
4. Then it is also true that $x^2 = 1 + x$.

this would have been confusing for many readers, because they would have wondered: “wasn’t x equal to $\frac{1+\sqrt{5}}{2}$? How come suddenly it seems to have a different value?”

The words “now” and “instead” make it crystal clear to the reader that the first value declaration has just expired and we are free to assign to x a new value if we so desire. □

4.4 A general principle: two rules for each symbol

Every time we introduce a new symbol, we need two rules telling us how to work with it:

- We need a rule that tells us how to ***use*** statements involving that symbol.

and

- We need a rule that tells us how to ***prove*** statements involving that symbol.

Example 17. Let us look at the new symbol “|” (“divides”) that we introduced in Part I of these notes. What is the “use” rule’? What is the “prove” rule?

The “use” rule is:

If you get to a point in a proof where you have a statement

$$a|b\,,$$

then you can go from this to

We may pick an integer k such that $b = ak$.

And the "prove" rule is:

If you get to a point in a proof where you have integers a, b, c and you know that

$$b = ak\,,$$

then you can go from this to

$$a|b\,.$$

These rules are just another way of stating the definition of "divides". □

4.4.1 Naming sentences

Sentences are also things that we can talk about, so we can give them names.

One common way mathematicians use to name sentences is to give a sentence a capital letter name, such as A, or B, or P, or Q, or S.

So we could talk about the sentence "x eats grass" by giving it a name, that is, by picking a capital letter and declaring its value to be this sentence.

We could do this by writing

Let P be the sentence "x eats grass".

However, there is a much more convenient way to do this: ***If a sentence has an open variable, we include this open variable in the name of the sentence, thus signaling to the reader that the sentence contains that open variable.***

So, for example, a good name for the sentence "x eats grass" could be $P(x)$ (or $A(x)$, or $S(x)$, etc.). We could declare the value of the variable $P(x)$ by saying

(*) Let $P(x)$ be the sentence "x eats grass".

An important convention about names of sentences is this: suppose we want to talk about the sentence obtained from $P(x)$ by substituting (i.e., "plugging in") the name of a particular thing for the open variable x. If we already have a name for that thing, say "a", then the name of the sentence arising from the substitution is $P(a)$.

So, for example, after we make the value declaration (*), then "$P(\text{Suzy})$" is the name of the sentence "Suzy eats grass".

What if you have a sentence with, say, two or more open variables? You do the same thing: if, for example, you want to give a name to the sentence "x told y that z does not like w", you can call that sentence $P(x, y, z, w)$. You could make the value declaration

> Let $P(x, y, z, w)$ be the sentence "x told y that z does not like w"."

And then,

- If you want want to talk about the sentence "Alice told Jim that Bill does not like Mary", then that sentence would have the name $P(\text{Alice}, \text{Jim}, \text{Bill}, \text{Mary})$.

- If you want want to talk about the sentence "Alice told Jim that Bill does not like her" (that is, does not like Alice), that sentence would be called $P(\text{Alice}, \text{Jim}, \text{Bill}, \text{Alice})$.

- If you want want to talk about the sentence "Alice told Jim that Bill does not like him" (that is, does not like Jim), that sentence would be called $P(\text{Alice}, \text{Jim}, \text{Bill}, \text{Jim})$.

- And, if, for some reason, you want to talk about the sentence with two open variables "x told y that Bill does not like Mary", that sentence would be $P(x, y, \text{Jim}, \text{Mary})$.

4.4.2 Universal sentences bound variables but at the end let them free

If $P(x)$ is a sentence with the open variable x, and C is a set, then the sentence

$$(\forall x \in C)P(x)$$

should be read as

> Let x be an arbitrary member of C; then $P(x)$ is true; and now the value declaration of "x" expires, and x is a free variable again.

Why do we want to do this?

The reason is that the value declaration ("Let x be an arbitrary member of C") was made for the sole purpose of explaining which condition this arbitrary member of C is supposed to satisfy. Once this has been explained, there is no need to keep the variable x bound forever. It is better to let it be free again, so that the next time we need a variable for something, we can use x.

So, for example, when I explain to you that

(F) If x is an arbitrary integer then $(x+1)^2 = x^2 + 2x + 1\,,$

the important thing that I want you to remember is that "if you take an integer, add one to it, and square the result, then what you get is the sum of the square of your integer, plus two times it, plus one". There is no need for you to remember, in addition, the name that I used for that integer for the purpose of explaining Fact (F) to you. You should not have to waste any time or effort trying to remember "was that fact that was explained to me about x? Or was it about y? Or was it about n?" There is not need for you to remember that, because ***it does not matter which variable was used***. And, more importantly: ***Fact (F) is not really about a specific integer called*** x***. It is a fact about an arbitrary integer, and it does not matter whether you call it*** x***, or*** y***, or*** z***, or*** n***, or*** α***, or*** β***, or*** $\diamond$***, or even "Suzy" or "my uncle Jimmy". The letter*** x ***is used as a device within the conversation in which you explain Fact (F) to me, and once this conversation is over we can forget about*** x***.***

Example 18. Suppose you have written, in a proof:

$$(\forall n \in \mathbb{Z})n(n+1) \text{ is even}\,. \tag{4.29}$$

Can you write, in the next step of your proof:

Since $n(n+1) = n + n^2$, it follows that $n + n^2$ is even. ?

The answer is ***no***. Why? Because after the end of the sentence (4.29), n is a free variable again, so it does not have a value, so when you use "n" in the next step, nobody knows what you are talking about, so what you wrote is meaningless, so it's not acceptable.

Suppose you want to go from (4.29) to

$$(\forall n \in \mathbb{Z}) n + n^2 \text{ is even} . \tag{4.30}$$

How can you do that? The answer is: you use the rules for using and proving universal sentences. But ***you do it correctly***. And for that you need to read the next section. □

4.5 Proving and using universal sentences (Rules $\forall_{prove}$ and $\forall_{use}$)

Now that we know that for every new symbol we introduce we need a "use" rule and a "prove" rule, it is natural to ask: *What are the "use" rule and the "prove" rule for the universal quantifier symbol ∀ ?"*

Both are very simple, very natural rules.

Here is the "use" rule:

The rule for using universal sentences (Rule $\forall_{use}$, also known as the "universal specialization rule")

- If you have proved
$$(\forall x)P(x)\,,$$
and you have an object called a, then you can go to $P(a)$.
- If you have proved
$$(\forall x \in S)P(x)\,,$$
and you have an object called a for which you know that $a \in S$, then you can go to $P(a)$.

The reason Rule $\forall_{use}$ is called called the ***universal specialization rule***, is that the rule says that if a statement is true in general (that is, for all things that belong to some set S), then it is true in each special case (that is, for a particular thing that belongs to S).

Example 19. If you know that $(\forall x)x = x$, then you can conclude from that, using Rule $\forall_{use}$, that
$$3 = 3\,,$$
and that
$$5 + 3 = 5 + 3\,.$$

Example 20. Suppose you know that

(&) All cows eat grass.

and that

(&&) Suzy is a cow.

Then, from (&) amd (&&) you can conclude, thanks to the specialization rule, that

(&&) Suzy eats grass.

In formal language. you would say this as follows: Let $P(x)$ be the sentence "x eats grass", and let C be the set of all cows. Then $P(\text{Suzy})$ is the sentence "Suzy eats grass". And (&) says

(&') $(\forall x \in C)P(x)\,,$

whereas (&&) says

(&&') $\text{Suzy} \in C.$

So we are precisely in the situation where we can apply the rule for using universal sentences, and conclude that $P(\text{Suzy})$, that is that Suzy eats grass. $\Box$.

And here is the "prove" rule:

The rule for proving universal sentences

- To prove $(\forall x)P(x)$, you start by writing

  Let x be arbitrary,

  and then prove $P(x)$

  If you manage to do that, then you are allowed to write
  $$(\forall x)P(x)$$
  in the next step of your proof.

- To prove $(\forall x \in S)P(x)$, you start by writing

  Let x be an arbitrary member of S,

  and then prove $P(x)$

  If you manage to do that, then you are allowed to write
  $$(\forall x \in S)P(x)$$
  in the next step of your proof.

This rule is also called the ***generalization rule***, because it says that if you can prove a statement for an arbitrary object that belongs to a set S then you can "generalize", i.e., conclude that the statement is true in general, for all members of S.

4.6 An example: Proof of the inequality $x + \frac{1}{x} \geq 2$

Let us illustrate the use of the proof rules for universal quantifiers with an example. We will first present a version of the proof with lots of comments. The comments are explanations to help the reader follow what is going on, but are not really necessary for the proof. We will then present another, much shorter version, in which the comments are omitted.

Theorem 7. *If x is a positive*[37] *real number, then $x + \frac{1}{x} \geq 2$. (In formal language: $(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)$.)*

PROOF, WITH LOTS OF COMMENTS. (The comments are in Italics.)

The assertion we want to prove is a universal sentence, so we are going to use Rule $\forall_{prove}$. For that purpose, we imagine we have in our hands an arbitrary real number called x, and we work with that number.

Let x be an arbitrary real number.

Now we want to prove that $x > 0 \Longrightarrow x+\frac{1}{x} \geq 2$. This is an implication. So we are going to apply Rule $\Longrightarrow_{prove}$. For that purpose, we assume that the premise of our implication is true, i.e., that $x > 0$. The reason for this is as follows: x is an arbitrary real number, so x could be any ral number, and in particular x could be positive, negative, or zero. If x is not positive, then the implication is true, because an implication whose premise is false is true. So all we need is to look at the cases when $x > 0$, and prove in that case that $x + \frac{1}{x} \geq 2$.

Assume that $x > 0$.

We want to prove that

$$x + \frac{1}{x} \geq 2\,. \tag{4.31}$$

We will prove this by contradiction.

Assume that (4.31) is not true.

Then

$$x + \frac{1}{x} < 2\,. \tag{4.32}$$

We now use a fact from real number arithmetic, namely, that if we multiply both sides of a true inequality by a positive real number then the result is a true inequality, that is:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})\Big((a < b \wedge c > 0) \Longrightarrow ac < bc\Big)\,. \tag{4.33}$$

[37] The meaning of the word "positive" was discussed in Lecture 1, in a subsection called "positive, negative, nonnegative, and nonpositive numbers". As explained there, "positive" means "> 0".

In our case. we can use Rule $\forall_{use}$ *to plug in* $x + \frac{1}{x}$ *for* a*,* 2 *for* b*, and* x *for* c *in (4.33), and get*

$$\Big(x + \frac{1}{x} < 2 \wedge x > 0\Big) \Longrightarrow \Big(x + \frac{1}{x}\Big)x < 2x\,. \tag{4.34}$$

Since $x + \frac{1}{x} < 2 \wedge x > 0$ *is true (because we are assuming that* $x + \frac{1}{x} < 2$ *and that* $x > 0$*), we can apply Rule* $\Longrightarrow_{use}$ *to conclude that* $\Big(x + \frac{1}{x}\Big)x < 2x$*. But* $\Big(x + \frac{1}{x}\Big)x = x^2 + 1$*, so we have shown that* $x^2 + 1 < 2x$*. Summarizing:*

Since $x > 0$, we can multiply both sides of (4.32) by x, getting

$$x^2 + 1 < 2x\,. \tag{4.35}$$

Now we use another fact from real number arithmetic, namely, that if we add a real number to both sides of a true inequality, then the result is a true inequality, that is:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})(a < b \Longrightarrow a + c < b + c)\,. \tag{4.36}$$

In our case. we can use Rule $\forall_{use}$ *to plug in* $x^2 + 1$ *for* a*,* $2x$ *for* b*, and* $-2x$ *for* c *in (4.36), and get*

$$x^2 + 1 - 2x < 2x - 2x,\,. \tag{4.37}$$

Since $2x - 2x = 0$*, we can conclude that* $x^2 + 1 - 2x < 0$*. Summarizing:*

We add $-2x$ to both sides, and get

$$x^2 + 1 - 2x < 0\,. \tag{4.38}$$

But $x^2 + 1 - 2x = (x - 1)^2$.

(This is easy to prove it. Try to do it.)

So

$$(x - 1)^2 < 0\,. \tag{4.39}$$

Now we use a third fact from real number arithmetic, namely, that the square of every real number is nonnegative, that is:

$$(\forall u \in \mathbb{R})u^2 \geq 0\,. \tag{4.40}$$

We use Rule $\forall_{use}$ to plug in $x-1$ for u, and get

$$(x-1)^2 \geq 0\,. \tag{4.41}$$

Next, we use a fourth fact from real number arithmetic, namely, that if a real number is nonnegative then it it is not negative[38], that is:

$$(\forall u \in \mathbb{R})(u \geq 0 \Longrightarrow \sim u < 0)\,. \tag{4.42}$$

It then follows from (4.41) that

$$\sim (x-1)^2 < 0\,. \tag{4.43}$$

From (4.39) and (4.43), we get

$$(x-1)^2 < 0 \wedge \Big(\sim (x-1)^2 < 0\Big)\,. \tag{4.44}$$

So we have proved a contradiction.

We have proved that a world in which the inequality $x+\frac{1}{x} > 2$ is not true is an impossible world. Hence

$x+\frac{1}{x} > 2$.

We have proved that $x+\frac{1}{x} > 2$ assuming that $x > 0$. Hence Rule $\Longrightarrow_{prove}$ allows us to conclude that

$$x > 0 \Longrightarrow x + \frac{1}{x} \geq 2\,. \tag{4.45}$$

Finally, we have proved (4.45) for an arbitrary real number x. Hence

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \tag{4.46}$$

Q.E.D.

[38] Remember that: "positive" means ">0", "negative" means "<0", "nonnegative" means "≥ 0", and "nonpositive" means "≤ 0".

THE SAME PROOF, WITHOUT THE COMMENTS.

Let x be an arbitrary real number.

Assume that $x > 0$.

We want to prove that

$$x + \frac{1}{x} \geq 2\,. \tag{4.47}$$

Assume that (4.47) is not true.
Then

$$x + \frac{1}{x} < 2\,. \tag{4.48}$$

Since $x > 0$, we can multiply both sides of (4.48) by x, getting

$$x^2 + 1 < 2x\,. \tag{4.49}$$

We add $-2x$ to both sides, and get

$$x^2 + 1 - 2x < 0\,. \tag{4.50}$$

But $x^2 + 1 - 2x = (x-1)^2$. So

$$(x-1)^2 < 0\,. \tag{4.51}$$

Now we use the fact that the square of every real number is nonnegative, that is:

$$(\forall u \in \mathbb{R})u^2 \geq 0\,. \tag{4.52}$$

We use Rule $\forall_{use}$ to plug in $x - 1$ for u, and get

$$(x-1)^2 \geq 0\,. \tag{4.53}$$

Then

$$\sim (x-1)^2 < 0\,. \tag{4.54}$$

From (4.51) and (4.54), we get

$$(x-1)^2 < 0 \wedge \Big(\sim (x-1)^2 < 0 \Big)\,. \tag{4.55}$$

So we have proved a contradiction.

Hence

$x + \frac{1}{x} > 2$.

We have proved that $x + \frac{1}{x} > 2$ assuming that $x > 0$. Hence Rule $\Longrightarrow_{prove}$ allows us to conclude that

$$x > 0 \Longrightarrow x + \frac{1}{x} \geq 2\,. \tag{4.56}$$

Finally, we have proved (4.54) for an arbitrary real number x. Hence

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \tag{4.57}$$

Q.E.D.

THE SAME PROOF, IN A MUCH SHORTER VERSION.

Let x be an arbitrary real number.

Assume that $x > 0$. We want to prove that

$$x + \frac{1}{x} \geq 2\,. \tag{4.58}$$

Assume that (4.58) is not true. Then

$$x + \frac{1}{x} < 2\,. \tag{4.59}$$

Since $x > 0$, (4.59) impliues

$$x^2 + 1 < 2x\,. \tag{4.60}$$

Therefore

$$x^2 + 1 - 2x < 0\,. \tag{4.61}$$

But $x^2 + 1 - 2x = (x-1)^2$. So

$$(x-1)^2 < 0\,. \tag{4.62}$$

On the other hand.

$$(x-1)^2 \geq 0\,. \tag{4.63}$$

Clearly, 4.62 and 4.63 lead to a contradiction.

Hence
$x + \frac{1}{x} > 2$.

Therefore

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \tag{4.64}$$

Q.E.D.

4.6.1 A few more examples of proofs involving universal sentences

Theorem 8. *If a, b are real numbers, then*

$$ab \le \frac{a^2+b^2}{2}\,.$$

(In formal language: $(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})ab \le \frac{a^2+b^2}{2}$.)

PROOF. YOU DO IT

Problem 12. Prove Theorem 8.

Problem 13. Explain what is wrong with the following proof of Theorem 8.

Take the inequality $ab \le \frac{a^2+b^2}{2}$.
Multiplying both sides by 2, we get $2ab \le a^2 + b^2$.
Subtracting $2ab$ from both sides, we get

$$0 \le a^2 + b^2 - 2ab\,.$$

But $a^2 + b^2 - 2ab = (a-b)^2$. So we have $0 \le (a-b)^2$, which is true.

So the inequality checks out. **Q.E.D.**

Theorem 9. *If x, α, β are positive real numbers then*

$$\alpha x + \frac{\beta}{x} \ge 2\sqrt{\alpha\beta}\,.$$

(In formal language: $(\forall \alpha \in \mathbb{R})(\forall \beta \in \mathbb{R})(\forall x \in \mathbb{R})\Big((\alpha > 0 \land \beta > 0 \land x > 0) \Longrightarrow \alpha x + \frac{\beta}{x} \ge 2\sqrt{\alpha\beta}\Big)$.)

I am going to give you two proofs. The first one follows the same pattern as the proof of Theorem 7. The second one, much shorter, uses Theorem 7.

FIRST PROOF.

Let α, β, x be arbitrary positive real numbers[39].

[39] In this one step I am conflating six real steps: let α be an arbitrary real number, let β be an arbitrary real number, let x be an arbitrary real number, assume $\alpha > 0$, assume $\beta > 0$, assume $x > 0$.

Let $q = 2\sqrt{\alpha\beta}$, so $\frac{q^2}{4\alpha} = \beta$..

Assume $\sim \alpha x + \frac{\beta}{x} \geq q$.

Then $\alpha x + \frac{\beta}{x} < q$.

Therefore $\alpha x^2 + \beta < qx$.

Hence $\alpha x^2 - qx + \beta < 0$.

But

$$\begin{aligned} \alpha x^2 - qx + \beta &= \alpha x^2 - 2\sqrt{\alpha}x\frac{q}{2\sqrt{\alpha}} + \beta \\ &= \alpha x^2 - 2\sqrt{\alpha}x\frac{q}{2\sqrt{\alpha}} + \frac{q^2}{4\alpha} - \frac{q^2}{4\alpha} + \beta \\ &= \Big(\sqrt{\alpha}x - \frac{q}{2\sqrt{\alpha}}\Big)^2 \\ &\geq 0\,. \end{aligned}$$

So we obtain a contradiction, and then we can conclude that $\alpha x + \frac{\beta}{x} \geq q$, i.e. that

$$\alpha x + \frac{\beta}{x} \geq 2\sqrt{\alpha\beta}\,.$$

Q.E.D.

SECOND PROOF. Let us try to write $\alpha x + \frac{\beta}{x}$ as $p\Big(u + \frac{1}{u}\Big)$ for some positive u, and use the fact that $u + \frac{1}{u} \geq 2$. Let $x = hu$, where h and u are to be determined later.

Then $\alpha x + \frac{\beta}{x} = \alpha hu + \frac{\beta}{hu}$. If we could make $\alpha h = \frac{\beta}{h}$, we would get

$$\begin{aligned} \alpha x + \frac{\beta}{x} &= \alpha hu + \frac{\beta}{hu} \\ &= \alpha hu + \alpha h\frac{1}{u} \\ &= \alpha h\Big(u + \frac{1}{u}\Big)\,, \end{aligned}$$

as desired.

So we need to chose h such that $\alpha h = \frac{\beta}{h}$, that is, such that $h = \sqrt{\frac{\beta}{\alpha}}$.

With this choice of h, we get

$$\begin{array}{rcl} \alpha x + \dfrac{\beta}{x} & = & \alpha h\Big(u + \dfrac{1}{u}\Big) \\ & \geq & 2\alpha h \\ & = & 2\alpha\sqrt{\dfrac{\beta}{\alpha}} \\ & = & 2\sqrt{\alpha\beta}\,. \end{array}$$

Q.E.D.

4.6.2 * The inequality $\frac{x^n}{n} - ax \geq -\frac{n-1}{n}a^{\frac{n}{n-1}}$: a proof using Calculus

Theorem 10. *Let a and b be positive real numbers, and let n be a positive integer. Then*

$$ab \leq \frac{1}{n}\Big(a^n + (n-1)b^{\frac{n}{n-1}}\Big)\,. \tag{4.65}$$

Remark 5. For $n = 2$, inequality (4.65) says that

$$ab \leq \frac{a^2 + b^2}{2}\,,$$

which is Theorem 8.

So (4.65) is a generalization of Theorem 8. □

Proof of Theorem 10. We will use Calculus.

Let a, b be arbitrary positive real numbers.

Define a function f by letting

$$f(x) = \frac{x^n}{n} - bx \;\text{ for }\; x \in \mathbb{R}\,,\; x \geq 0\,.$$

We would like to find the value of x where f has its minimum value of f for all positive x. That is, we would like to find a positive real number c such that $f(c) \leq f(x)$ for all positive x.

For this purpose, we compute the derivative f' of f.

We have

$$f'(x) = x^{n-1} - b \text{ for every } x \in \mathbb{R}\,.$$

Let $c = b^{\frac{1}{n-1}}$. Then $c^{n-1} = b$, so $f'(c) = c^{n-1} - b = 0$.

This means that c is a candidate for our minimum. That is, it is possible that c is where f has its minimum value, in which case it would follow that

$$f(x) \geq f(c) \text{ for all } x \in \mathbb{R} \text{ such that } x > 0\,. \tag{4.66}$$

We now prove (4.66) rigorously

If $0 < x < c$, then $x^{n-1} < c^{n-1} = b$, so $x^{n-1} - b < 0$, so $f'(x) < 0$.

This means that the function f is decreasing for $0 < x < c$. So $f(x) \geq f(c)$ for $0 < x < c$.

If $x > c$, then $x^{n-1} > c^{n-1} = b$, so $x^{n-1} - b > 0$, so $f'(x) > 0$.

This means that the function f is increasing for $x > c$. So $f(x) \geq f(c)$ for $x > c$.

We have shown that $f(x) \geq f(c)$ when $0 < x < c$ and when $x > c$. And clearly $f(x) = f(c)$ when $x = c$. Hence (4.66) is true.

It follows from (4.66) that for every positive $x \in \mathbb{R}$ we have $f(x) \geq f(c)$, that is,

$$\frac{x^n}{n} - bx \geq \frac{c^n}{n} - bc\,. \tag{4.67}$$

Since (4.67) holds for every positive x, we can use it for $x = a$, thereby obtaining

$$\frac{a^n}{n} - ab \geq \frac{c^n}{n} - bc\,. \tag{4.68}$$

Since $c = b^{\frac{1}{n-1}}$ and $c^{n-1} = b$, we have

$$\begin{aligned}
\frac{c^n}{n} - bc &= \frac{b^{\frac{n}{n-1}}}{n} - b \times b^{\frac{1}{n-1}} \\
&= \frac{b^{\frac{n}{n-1}}}{n} - b^{1+\frac{1}{n-1}} \\
&= \frac{b^{\frac{n}{n-1}}}{n} - b^{\frac{n}{n-1}} \\
&= \Big(\frac{1}{n} - 1\Big) b^{\frac{n}{n-1}} \\
&= -\frac{n-1}{n} b^{\frac{n}{n-1}} \,.
\end{aligned}$$

In view of (4.68), we get

$$\frac{a^n}{n} - ab \geq -\frac{n-1}{n} b^{\frac{n}{n-1}} \,, \tag{4.69}$$

that is,

$$\frac{a^n}{n} - ab + \frac{n-1}{n} b^{\frac{n}{n-1}} \geq 0 \,, \tag{4.70}$$

from which it follows that

$$ab \leq \frac{a^n}{n} + \frac{n-1}{n} b^{\frac{n}{n-1}} \,, \tag{4.71}$$

that is,

$$ab \leq \frac{1}{n}\Big(a^n + (n-1) b^{\frac{n}{n-1}}\Big) \,, \tag{4.72}$$

which is exactly what we were trying to prove. **Q.E.D.**

5 Existential sentences

5.1 Existential quantifiers

- The symbol

$$\exists$$

  is the ***existential quantifier symbol***.

- An ***existential quantifier*** is an expression "$(\exists x)$" or "$(\exists x \in S)$" (if S is a set). More precisely,

  "$(\exists x)$" is an ***unrestricted existential quantifier***,

  and

  "$(\exists x \in S)$" is a ***restricted existential quantifier***.

- Existential quantifiers are read as follows:

  1. "$(\exists x)$" is read as

     ∗ "there exists x such that"

     or

     ∗ "for some x"

     or

     ∗ "it is possible to pick x such that".

  2. "$(\exists x \in S)$" is read as

     ∗ "there exists x belonging to S such that"

     or

     ∗ "there exists a member x of S such that"

     or

     ∗ "for some x in S"

     or

     ∗ "it is possible to pick x in S such that" or

- ∗ "it is possible to pick a member x of S such that"

Example 21. The sentence

$$(\exists x \in \mathbb{R})x^2 = 2 \tag{5.73}$$

could be read as

> There exists an x belonging to the set of real numbers such that $x^2 = 2$.

But this is horrible! A much better way to read it is:

> There exists a real number x such that $x^2 = 2$.

An even better way is

> There exists a real number whose square is 2.

And the nicest way of all is

> 2 has a square root.

And you can also read (5.73) as:

$$\boxed{\text{It is possible to pick a real number } x \text{ such that } x^2 = 2}.$$

I strongly recommend this reading, because when you read an existential sentence this way it becomes clear that the next thing to do is to actually pick an x, that is, to apply the rule for using an existential sentence, i.e. Rule $\exists_{use}$ □

5.1.1 How not to read existential quantifiers

Students sometimes read an existential sentence such as

$$(\exists x \in \mathbb{R})x^2 = 2) \tag{5.74}$$

as follows: *there exists a real number x and $x^2 = 2$.*

This is completely wrong, and should be avoided at all costs, because if you read an existential sentence that way you are going to be led to making lots of other mistakes.

Why is this wrong?

- If you read (5.74) as "there exists a real number x and $x^2 = 2$", then you give the impression that (5.74) makes two assertions:
    1. that there exists a real number,
    2. that $x^2 = 2$.
- But (5.74) does not say that at all! What it does is make ***one*** assertion, namely, that there exists a real number x such that $x^2 = 2$. ("Such that" means "for which it is true that".)

If you are asked to prove (5.74) and you read is as "there exists a real number x and $x^2 = 2$", then you will think that you have to prove two things, namely, (1) that there exists a real number, and (2) that $x^2 = 2$. But what you have to prove is one thing: that it is possible to pick a real number whose square is 2.

The word "and" in this bad reading is particularly pernicious, because it makes you see two sentences where there is only one sentence. ***The quantifier*** $(\exists x \in \mathbb{R})$ ***is not a sentence.***

You can see this even more clearly if you read (5.74) as "for some real numbers x, $x^2 = 2$". It is clear that "for some real numbers x" is not a sentence. And it's nonsense to say "for some real numbers x and $x^2 = 2$".

Since "for some real numbers x" is another way to read the quantifier $(\exists x \in \mathbb{R})$, it should be clear that there is no "and" in such a quantifier,

5.1.2 Witnesses

A witness for an existential sentence $(\exists x)P(x)$ is an object a such that $P(a)$ is true.

A witness for an existential sentence $(\exists x \in S)P(x)$, is an object a such that $a \in S$ and $P(a)$ is true.

5.2 How do we work with existential sentences in proofs?

As you may have guessed, I am going to give you two rules, one for *proving* existential sentences, and one for *using* them. And the names of these rules are going to be—yes, you guessed it!—Rule $\exists_{prove}$ and Rule $\exists_{use}$.

5.2.1 The rule for using existential sentences (Rule $\exists_{use}$)

Rule $\exists_{use}$ says something very simple and natural: ***if you know that an object of a certain kind exists, then you can pick one and give it a name***.

In other words, ***if you know that*** $(\exists x)P(x)$ ***or that*** $(\exists x \in S)P(x)$***, then you are allowed to pick a witness and give it a name***.

Example 22. Suppose "$P(x)$" stands for "x eats grass", and C is the set of all cows. Suppose you know that

$$(\exists x \in C)P(x)\,, \tag{5.75}$$

that is, you know that there are grass-eating cows.

Then the thing you can do, according to Rule $\exists_{use}$, is pick a cow and give her a name.

So, for example, you could write

Pick a cow that eats grass and call her Suzy.

Or you could write

Let Suzy be a witness for the sentence (5.75,
so Suzy is a grass-eating cow.

or

Let Suzy be a grass-eating cow.

Example 23. Suppose you have a real number x and you know that

$$(\exists y \in \mathbb{R})y^5 - y^3 = x\,. \tag{5.76}$$

Then you can say, in the next step of your proof: :

Pick a witness for (5.76) and call it r, so $r \in \mathbb{R}$ and $r^5 - r^3 = 5$.

or you could write

Let r be a real number such that $r^5 - r^3 = 5$.

And you could even say

Let y be a real number such that $y^5 - y^3 = 5$.

□

Remark 6. When you pick a witness, as in the previous example, you can give it any name you want: you can call it r, k, m, u, $\hat{r}$, a, α, $\diamond$, $\clubsuit$, Alice, Donald Duck, whatever.

You can even call it y, if you wish.

The key point is: ***the name you use cannot be already in use as the name of something else***.

So "y" qualifies as an acceptable name because, within the sentence "$(\exists y \in \mathbb{R})y^5 - y^3 = x$", y is a bound variable, but as soon as the sentence ends, "y" becomes a free variable, with no declared value, so you are allowed to use it.

However, I recommend that you do not use the same letter that appeared in the existential quantifier. □

There is, however, one thing that is absolutely forbidden:

You cannot give the new object that you are picking a name that is already in use as the name of another object.

The reason for this prohibition is very simple: if you could use the name r to name this new object that you are introducing, while r is already the name of some other object that was introduced before, then you would be forcing these two objects to be the same. But there is no reason for them to be the same, so you cannot give them the same name.

Example 24. Suppose you know that Mr. Winthrop has been murdered. That means, if we use "$P(x)$" for the predicate "x murdered Mr. Winthrop". that you know that $(\exists x)P(x)$ (that is, somebody murdered Mr. Winthrop). Then you can introduce a new character into your discourse, and call this person "the murderer", or "the killer". (This is useful, because you want to be able to talk about that person, and say things such as "the murderer must have had a key so as to be able to get into Mr. Winthrop's apartment".) But you cannot call the murderer "Mrs. Winthrop", because if you do so you would be stipulating that it was Mrs. Winthrop that killed Mr. Winthrop, which could be true but you do not know that it is. □

And here is a precise statement[40] of Rule $\exists_{use}$:

Rule $\exists_{use}$

(I) If

1. $P(x)$ is a sentence,
2. the letter a is not in use as the name of anything,
3. you have proved $(\exists x)P(x)$,

then

* you can introduce a witness and call it a, so that this new object will satisfy $P(a)$

(II) In addition, if S is a set, and you have proved that $(\exists x \in S)P(x)$, then you can stipulate that $a \in S$ as well.

5.2.2 The rule for proving existential sentences (Rule $\exists_{prove}$)

This rule is very simple, and very easy to remember:

- ***to prove that there is money here, show me the money***;
- ***to prove that cows exist, show me a cow***;
- ***to prove that good students exist, show me a good student***,
- ***to prove that incorruptible politicians exist, show me an incorruptible politician***,
- ***to prove that prime numbers exist, show me a prime number,***

and so on.

Example 25. Suppose you want to prove that $(\exists x \in \mathbb{Z})x^2 + 3x = 10$.

You can say "Take $x = 2$. Then $x^2 + 3x = 10$, because $x^2 = 4$ and $3x = 6$, so $x^2 + 3x = 4 + 6 = 10$". So 2 is a witness for the sentence $(\exists x \in \mathbb{Z})x^2+3x = 10$. Then Rule $\exists_{prove}$ allows us to go to $(\exists x)x^2+3\cdot x = 10$. □

[40] In this statement, we use the same convention explained earlier: $P(a)$ is the sentence obtained from $P(x)$ by substituting a for x. For example, if $P(x)$ is the sentence "x eats grass", then $P(\text{Suzy})$ is the sentence "Suzy eats grass". If $P(x)$ is the sentence "$x + 3y = x^2$", then $P(a)$ is the sentence "$a + 3y = a^2$".

And here is a precise statement of the witness rule:

Rule $\exists_{prove}$

If:

1. $P(x)$ is a sentence,

2. a is a witness for $(\exists x)P(x)$ (that is, you have proved that $P(a)$),

then

* you can go to $(\exists x)P(x)$.

In addition, if S is a set, and you have proved that $a \in S$, then you can go to $(\exists x \in S)P(x)$.

In other words, ***Rule*** $\exists_{prove}$ ***says that you can prove the sentences*** $(\exists x)P(x)$ ***or*** $(\exists x \in S)P(x)$ ***by producing a witness.***

5.3 Examples of proofs involving existential sentences

5.3.1 Some simple examples

Problem 14. Consider the sentence

$$(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x^2 - y^2 = 17\,. \tag{5.77}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (5.77) is true. Here is a proof:

Take $x = 9$, $y = 8$. Then $x^2 = 81$ and $y^2 = 64$. So $x^2 - y^2 = 81 - 64 = 17$. Therefore the pair $(9, 8)$ is a witness for (5.77). By Rule $\exists_{prove}$, this proves (5.77). **Q.E.D.**

Problem 15. Consider the sentence

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})n < m\,. \tag{5.78}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (5.78) is true. Here is a proof.

> Let m be an arbitrary integer.
>
> We want to prove that $(\exists n \in \mathbb{Z})n < m$.
>
> For this purpose, we produce a witness. First we say who the witness is, and then we prove it works, that is, that it really is a witness.
>
> Let $\hat{n} = m - 1$.
>
> Then $\hat{n} \in \mathbb{Z}$ and $\hat{n} < m$. So the integer $\hat{n}$ is a witness for the sentence $(\exists n \in \mathbb{Z})n < m$
>
> Therefore $(\exists n \in \mathbb{Z})n < m$. [Rule $\exists_{prove}$]

Since we have proved that $(\exists n \in \mathbb{Z})n < m$ for an arbitrary integer m, we can conclude that $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})n < m$. [Rule $\forall_{prove}$] **Q.E.D.**

Problem 16. Consider the sentence

$$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})n < m\,. \tag{5.79}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (5.79) is false. Here is a proof.

> Asssume (5.79) is true.
>
> Them by Rule $\forall_{use}$ we can plug in a value for m, and the result wil be a true sentence. So we plug in $m = 1$.
>
> Them by Rule $\forall_{use}$ iimplies that $(\exists n \in \mathbb{N})n < 1$.
>
> But there is no natural number that is less than 1, so so $\sim (\exists n \in \mathbb{N})n < 1$.
>
> So we have attained a contradcition.

Therefore (5.79) is false.

Problem 17. Consider the sentence

$$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{5.80}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (5.80) is false. Here is a proof of its negation, that is, of

$$\sim (\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{5.81}$$

We are going to prove (5.81) by contradiction .

> Assume that
>
> $$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{5.82}$$
>
> Pick a witness for Statement (5.82), that is, an integer n for which the statement "$(\forall m \in \mathbb{Z})n < m$" holds, and call it n_0. [Rule $\exists_{use}$]
>
> Then $n_0 \in \mathbb{Z}$ and $(\forall m \in \mathbb{Z})n_0 < m$.
>
> Since $n_0 \in \mathbb{Z}$, we can conclude that $n_0 < n_0$. [Rule $\forall_{use}$, from $(\forall m \in \mathbb{Z})n_0 < m$]
>
> Then $\sim n_0 = n_0$. [Trichotomy law]
>
> But $n_0 = n_0$. [Equality Axiom $(\forall x)x = x$.]

So we have proved a contradiction assuming (5.82). Hence, by the proof-by-contradiction rule, (5.82) is false, that is, (5.81) is true. **Q.E.D.**

Problem 18. For each of the following sentences,

1. Indicate whether the sentence is true or false.
2. If it is true, prove it.
3. If it is false, prove that it is false (that is, prove its negation).

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{N})n > m\,, \tag{5.83}$$
$$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})n < m\,, \tag{5.84}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{Z})n < m\,, \tag{5.85}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})n < m\,, \tag{5.86}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})n \le m\,, \tag{5.87}$$
$$(\exists x \in \mathbb{R})(\forall m \in \mathbb{N})x < m\,. \tag{5.88}$$

5.3.2 A detailed proof of an inequality with lots of comments

Problem 19. Let C be a circle with center $(5,1)$. Let L be the line with equation $y = x + 4$. Prove that if the radius of the circle is less than 5 then C and L do not intersect.

Solution.
Let R be the radius of C.
*COMMENT: This is very important. Every time you will have to deal repeatedly with some object—a number, a set, an equation, a statement—**give it a name**.*

Assume that $R < 5$.

We want to prove that

$$\sim (\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2 + (y-1)^2 = R^2 \wedge y = x + 4\Big) . \quad (5.89)$$

Assume (5.89) isn't true.

Then

$$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2 + (y-1)^2 = R^2 \wedge y = x + 4\Big) . \quad (5.90)$$

Pick witnesses for (5.90) and call them x, y.

COMMENT: Remember that after a quantified sentence ends the quantified variables become free again, so they can be re-used. That's why it is perfectly legitimate to name the witnesses x and y.

Then

$$(x-5)^2 + (y-1)^2 = R^2 \wedge y = x + 4 . \quad (5.91)$$

In particular,

$$(x-5)^2 + (y-1)^2 = R^2 . \quad (5.92)$$

And also

$$y = x + 4 . \quad (5.93)$$

*COMMENT: How did we go from (5.91) to (5.92) and (5.93)? It's clear, isn't it? But in a proof **every step must be justfied (or justifiable) by the rules**. So which is the rule used here?*

The answer is: it's the logical rule for using conjunctions, that is, Rule $\wedge_{use}$: if you have a conjunction $A \wedge B$, then you can go to A, and you can go to B. You may think this is a very stupid rule, but it is certainly a reasonable rule. When we went from (5.91) to (5.92) and (5.93), it seemed obvious to you, didn't it? That's because Rule $\wedge_{use}$ is an obvious rule, so obvious that you use it all the time without even noticing it. But that doesn't mean that the rule isn't there. ***It is there.*** *If you wanted to write a computer program that checks proofs and tells you whether a proof is valid, how would the program know that going from (5.91) to (5.92) and (5.93) are valid steps? You have to put that in the program. That is, you have to put Rule $\wedge_{use}$ in your program.*

Since $y = x + 4$, we can substitute $x + 4$ for y in (5.92), and get

$$(x-5)^2 + (x+4-1)^2 = R^2\,, \tag{5.94}$$

that is

$$(x-5)^2 + (x+3)^2 = R^2\,. \tag{5.95}$$

But

$$\begin{aligned}
(x-5)^2 + (x+3)^2 &= x^2 - 10x + 25 + x^2 + 6x + 9\\
&= 2x^2 - 4x + 34\\
&= 2(x^2 - 2x + 17)\\
&= 2(x^2 - 2x + 1 - 1 + 17)\\
&= 2(x^2 - 2x + 1 + 16)\\
&= 2\Big((x-1)^2 + 16\Big)\\
&\geq 2 \times 16\\
&= 32
\end{aligned}$$

so

$$(x-5)^2 + (x+3)^2 \geq 32\,. \tag{5.96}$$

But

$$(x-5)^2 + (x+3)^2 = R^2\,. \tag{5.97}$$

So

$$R^2 \geq 32\,. \tag{5.98}$$

COMMENT: How did we go from (5.96) and (5.97) to (5.98)? It's clear, isn't it? But in a proof ***every step must be justfied (or justifiable) by the rules****. So which is the rule used here? The answer is: it's the logical rule for using equality, that is, Rule* $=_{use}$ *(also called Rule SEE, "susbtitution of equals for equals"): if you know that an equality* $s = t$*—or* $t = s$*—holds, and you also know that some statement* P *involving* s *holds, then you can go to* $P(s \to t)$*, where* $P(s \to t)$ *is the statemenet pbtained from* P *by substituting* t *for* s *in* P*. You may think this is a very stupid rule, but it is certainly a reasonable rule. When we went from (5.96) and (5.97) to (5.98), it seemed obvious to you, didn't it? That's because Rule SEE is an obvious rule, so obvious that you use it all the time without even noticing it. But that doesn't mean that the rule isn't there.* ***It is there.*** *If you wanted to write a computer program that checks proofs and tells you whether a proof is valid, how would the program know that going from (5.96) and (5.97) to (5.98) is a valid step? You have to put that in the program. That is, you have to put Rule SEE in your program.*

But we are assuming that $R < 5$, and then $R^2 < 25$.

COMMENT: That's because R *is positive. If all you know about was that* R *is a real number and* $R < 5$*, then* R *could be* -10*, in which case it would not follow that* $R^2 > 25$*. But in our case* R *is the radius of a circle, so* $R > 0$*, and the conclusion that* $R < 25$ *follows.*

So $\sim R^2 \geq 32$. But $R^2 \geq 32$. So we have proved a contradiction.

COMMENT: The contradiction is the statement "$R^2 \geq 32 \wedge \sim R^2 \geq 32$*". This is a contradiction because it is fo the form* $Q \wedge \sim Q$*, where* Q *is the statement "*$R^2 \geq 32$*".*

So (5.89) is proved. **Q.E.D.**

5.3.3 The same proof without the comments

Proof. Let R be the radius of C.

Assume that $R < 5$.

We want to prove that

$$\sim (\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big(\,(x-5)^2+(y-1)^2 = R^2 \wedge y = x+4\Big)\,. \quad (5.99)$$

Assume (5.99) isn't true. Then

$$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big(\,(x-5)^2+(y-1)^2 = R^2 \wedge y = x+4\Big)\,. \quad (5.100)$$

Pick witnesses for (5.100) and call them x, y.

Then $(x-5)^2+(y-1)^2 = R^2 \wedge y = x+4$, so in particular,

$$(x-5)^2+(y-1)^2 = R^2\,. \quad (5.101)$$

Since $y = x+4$, we can substitute $x+4$ for y in (5.101), and get $(x-5)^2+(x+4-1)^2 = R^2$, that is

$$(x-5)^2+(x+3)^2 = R^2\,. \quad (5.102)$$

But

$$\begin{array}{rcl} (x-5)^2+(x+3)^2 & = & x^2-10x+25+x^2+6x+9 \\ & = & 2x^2-4x+34 \\ & = & 2(x^2-2x+17) \\ & = & 2(x^2-2x+1-1+17) \\ & = & 2(x^2-2x+1+16) \\ & = & 2\Big((x-1)^2+16\Big) \\ & \geq & 2\times 16 \\ & = & 32 \end{array}$$

so

$$(x-5)^2+(x+3)^2 \geq 32\,. \quad (5.103)$$

But $(x-5)^2+(x+3)^2 = R^2$, so $R^2 \geq 32$.

But we are assuming that $R < 5$, and then $R^2 < 25$.

So $\sim R^2 \geq 32$. But $R^2 \geq 32$. So we have proved a contradiction.

So (5.99) is proved. **Q.E.D.**

5.4 Existence and uniqueness

Suppose $P(x)$ is a one-variable predicate. We write

$$(\exists! x)P(x)$$

for "there exists a unique x such that $P(x)$."

This means "there is one and only one x such that $P(x)$".

The precise meaning of this is that

1. there exists an x such that $P(x)$,

and

2. if x_1, x_2 are such that $P(x_1) \wedge P(x_2)$, then $x_1 = x_2$.

In formal language:

$$(\exists! x)P(x) \iff \Big((\exists x)P(x) \wedge (\forall x_1)(\forall x_2)(P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2\Big)\,.$$

It follows that, in order to prove that there exists a unique x such that $P(x)$, you must prove two things:

Existence: There exists x such that $P(x)$,

Uniqueness: Any two x's that satisfy $P(x)$ must be equal.

That is:

To prove

$$(\exists! x)P(x)$$

it suffices to prove

$$(\exists x)P(x) \tag{5.104}$$

and

$$(\forall x_1)(\forall x_2)\Big((P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2\Big)\,. \tag{5.105}$$

(Formula (5.104) is the existence assertion, and Formula (5.105) is the uniqueness assertion.)

Example 26. “I have one and only one mother” means:

- I have a mother,

and

- Any two people who are my mother must be the same person. (That is: if u is my mother and v is my mother than $u = v$.) □

5.4.1 Examples of proofs of existence and uniqueness

Problem 20. Prove that there exists a unique natural number n such that $n^3 = 2n - 1$.

Solution. We want to prove that

$$(\exists! n \in \mathbb{N}) n^3 = 2n - 1\,.$$

First let us prove existence. We have to prove that $(\exists n \in \mathbb{N}) n^3 = 2n - 1$. To prove this, we exhibit a witness: we take $n = 1$. Then n is a natural number, and $n^3 = 2n - 1$. So $(\exists n \in \mathbb{N}) n^3 = 2n - 1$.

Next we prove uniqueness. We have to prove that if u, v are natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$, then it follows that $u = v$.

So let u, v be natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$. We want to prove that $u = v$.

Since $u^3 = 2u - 1$ and $v^3 = 2v - 1$, we have

$$\begin{aligned} u^3 - v^3 &= 2u - 1 - (2v - 1) \\ &= 2u - 2v \\ &= 2(u - v)\,, \end{aligned}$$

so

$$u^3 - v^3 - 2(u - v) = 0\,.$$

But it is easy to verify that

$$u^3 - v^3 = (u - v)(u^2 + uv + v^2)\,.$$

(If you do not believe this, just multiply out the right-hand side and you will find that the result equals $u^3 = v^3$.) Hence

$$\begin{aligned} 0 &= u^3 - v^3 - 2(u - v) \\ &= (u - v)(u^2 + uv + v^2) - 2(u - v) \\ &= (u - v)(u^2 + uv + v^2 - 2)\,. \end{aligned}$$

We know that if a product of two real numbers is zero then one of the numbers must be zero. Hence

$$u - v = 0 \quad \text{or} \quad u^2 + uv + v^2 - 2\,.$$

But $u^2 + uv + v^2 - 2$ cannot be equal to zero, because u^2, uv and v^2 are natural numbers, so each of them is gretar than or equal to 1, and then $u^2 + uv + v^2 \geq 3$, so $u^2 + uv + v^2 - 2 \geq 1$, and then $u^2 + uv + v^2 - 2 \neq 0$. Therefore $u - v = 0$, so $u = v$, and our proof of uniqueness is complete.

Problem 21. Prove that there exists a unique real number x such that

$$x^7 + 3x^5 + 23x = 6\,.$$

You are allowed to use everything you know from Calculus. □

6 An introduction to logic

6.1 First-order predicate calculus

The language most mathematicians use to talk about mathematical objects (numbers of various kinds, sets, functions, lists, points, lines, planes, curves of various kinds, spaces where we can do geometry, graphs, and millions of other things) is a ***first-order predicate calculus***.

So let us explain what this means.

- The language is a "predicate calculus" because we can use it to express predicates.

So let us review what "predicates" are.

6.1.1 Predicates

Remember that

A ***predicate*** is a sentence[a] involving one or more (or zero) variables, in such a way that the sentence has a definite truth value[b] for each choice of values of the variables.

[a] "Sentence" means the same as "statement", or "assertion".

[b] The ***truth value*** of a sentence is "true" if the sentence is true and "false" if the sentence is false.

For example:

- "Alice likes Mark" is a zero-variables predicate. It is either true or false.
- "x likes Mark" is a one-variable predicate. It is true or false depending on who x is. For example, suppose that Alice likes Mark but Andrew does not like Mark. Then "x likes Mark" is true when $x =$Alice but "x likes Mark" is false when $x =$Andrew.

  If we call this predicate $P(x)$, then $P(Alice)$ is true and $P(Andrew)$ is false.
- "x likes y" is a two-variables predicate. It is true or false depending on who x and y are. For example, suppose that Alice likes Mark, Andrew does not like Mark, Andrew likes Alice, and Mark does not like Andrew. Then "x likes y" is true when $x =$Alice and $y =$Mark, and when $x =$Andrew and $y =$Alice, but "x likes y" is false when $x =$Andrew and $y =$Mark.

  If we call this predicate $P(x, y)$, then $P(Alice, Mark)$ is true but on the other hand $P(Mark, Andrew)$ is false.
- If S is the set of all people, then "$(\forall x \in S) x \,\text{likes}\, y$" says "everybody likes y". This is a one-variable predicate. We could call this predicate $Q(y)$, and then we could define $Q(y)$ as follows:

  $$\text{if } y \in S \text{ then } Q(y) \text{ means } (\forall x \in S) P(x, y)\,, \tag{6.106}$$

  or, in purely formal language:

  $$(\forall y \in S)\Big(Q(y) \Longleftrightarrow (\forall x \in S) P(x, y)\Big) \tag{6.107}$$
- "x likes y more than x likes z" is a three-variables predicate.
- "$2 + 2 = 4$" and "$2 + 2 = 5$" are zero-variables predicates. They are either true or false. (And, of course, "$2+2 = 4$" is true and "$2+2 = 5$" is false.)
- "$x > 0$" and "$2|n$" are one-variable predicates. They are true or false depending on who x (or n) is. For example, "$x > 0$" is true $x = 3$ but is false for $x = -5$. And "$2|n$" is true for $n = 4$ but is false for $n = 5$.

- "$x > y$" and "$m|n$" are two-variables (i.e., binary) predicates. They are true or false depending on who x and y (or m and n) are. For example, "the sentence $x > y$" is true for $x = 5$ and $y = 4$, but is false for $x = 5$ and $y = 6$. And "$m|n$" is true for $m = 3$ and $y = 6$, but is not true for $m = 3$ and $y = 7$.

- "$x+y = z$", "$x+y > z$", and "$n|m+q^2$" are three-variables predicates. The predicate "$x + y = z$" is,true for $x = 2$, $y = 3$ and $z = 5$, but is false for $x = 2$, $y = 3$ and $z = 4$. The predicate "$x + y > z$" is true for $x = 2$, $y = 3$ and $z = 4$. but is false for $x = 2$, $y = 3$ and $z = 5$. The predicate "$n|m + q^2$" is true for $n = 5$, $m = 9$, and $q = 6$, but is false $n = 5$, $m = 7$, and $q = 6$.

- "$x + 2y^2 - z > u$" and "$a = bq + r$ and $0 \leq r < |b|$" are four-variables predicates. The predicate "$x + 2y^2 - z > u$" is true for $x = 2$, $y = 4$. $z = 3$, $u = 4$, but is false for $x = 2$, $y = 1$. $z = 3$, $u = 3$, The predicate "$a = bq+r$ and $0 \leq r < |b|$" is true for $a = 23$, $b = 5$, $q = 4$ and $r = 3$, but is false for $a = 23$, $b = 5$, $q = 4$ and $r = 2$.

6.2 Free and bound variables, quantifiers, and the number of variables of a predicate

As was explained in the previous section, in a predicate such as "$x > y$", the variables x, y are ***free variables***, that is, variables that are free to be given any value we want. We can plug in values for x and y, and for each choice of values the resulting sentence has a definite truth value, that is, is true or false.

You should think of a predicate as a ***processing device***, with several "input channels". The input channels are the ***open variables***. Each input channel is ***open***, in the sense that the entrance to the channel is open so you can can put things in, or ***free***, in the sense that we are free to put things in there. Once you have put in a value for, say, the variable x, then x is no longer open: it becomes ***closed***, or ***bound***.
Once you have put in values in all the input channels, the device processes these inputs, and produces a answer: true, or false.

If, on the other hand, the predicate "$x > y$" appears in a text after a statement such as

$$\text{Let } x = 5,\ y = 3.$$

then the variables x and y are no longer free: they are ***bound variables***[41], because they are "attached" to particular values.

We now look at another, very important way to turn free variables into bound variables.

Let us consider, for example, the predicates

$$(\forall y \in \mathbb{R})x + 2y^2 - z > u \tag{6.108}$$

and

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r\,,\ \text{and}\ \ 0 \leq r < |b|)\,. \tag{6.109}$$

You may think that these are four-variables predicates, because each one of them contains four variables. (Predicate (6.108) contains the variables x, y, z and u. Predicate (6.109) contains the variables a, b, a and r.)

But this is not right:

(6.108) is a three-variables predicate, and ***(6.109) is two-variables predicate.***.

Let me explain.

[41] Bound variables are also called ***closed variables***, because they are not open: the "input channel" through which we can input values for the variables is closed.

6.2.1 An example: a predicate with three free variables and one bound variable

We first look at the predicate

$$(\forall y \in \mathbb{R})x + 2y^2 - z > u\,. \tag{6.110}$$

- The predicate (6.110) is built from the predicate "$x + 2y^2 - z > u$" by ***quantifying*** it, i.e., putting a universal quantifier $(\forall y \in \mathbb{R})$ in front.
- The unquantified predicate "$x + 2y^2 - z > u$" contains the variables x, y, z, u. These are four open variables.
- So, if you are asked the "truth question"

  Is "$x + 2y^2 - z > u$" true or false?

  then you have to reply with a question of your own:

  Who are x, y, z and u?

- But in the quantified predicate (6.110) ***the variable*** y ***is quantified***.
- So, if you are asked the "truth question"

  Is "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" true or false?

  then you have to reply with the question:

  Who are x, z and u?

- In the predicate "$x + 2y^2 - z > u$", the four variables x, y, z and u are open variables, that is, "slots", or "input channels", where you can put in (or "plug in") values for each of the variables.
- When you fill in the four slots by plugging in values for the variables, you get a ***proposition***, i.e., a sentence that has a definite truth value.

A ***proposition*** is a sentence with no open variables

So a proposition is just true or false, whereas a predicate with open variables is true or false depending on the values of the variables.

Example:

1. The sentence "$m \geq n$" has two open variables. It is true if, for example, $m = 3$ and $n = 1$, and it is false if, for example, $m = 3$ and $n = 4$.
2. The sentence "$(\forall m \in \mathbb{N}) m \geq n$" is true if, for example, $n = 1$, and it is false if, for example, $n = 2$. So this sentence has one open variable, namely, n.
3. The sentences

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N}) m \geq n$$

and

$$(\forall n \in \mathbb{N})(\forall m \in \mathbb{N}) m \geq n$$

do not have any open variables. So they are propositions. The first one is true. (Reason: Take $n = 1$. Then for arbitrary $m \in \mathbb{N}$ $m \geq 1$.) The second one is false. (Reason: Take $m = 1$, $n = 2$. Then it is not true that $m \geq n$.)

- So, for example, if you plug in the values $x = 2$, $y = 4$, $z = 3$, $u = 4$, into the sentence

$$x + 2y^2 - z > u$$

you get the proposition

$$19 > 4,,$$

which is true.

- But in the quantified predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$", there is no y-slot. The three variables x, z and u are open variables, that is, slots or input channels where you can put in values. But y is not an open variable.
- When you fill in the slots by plugging in values for the three open variables, you get a proposition.
- So, for example, if you plug in the values $x = 2$, $z = -3$, $u = 4$, into the sentence

  $$(\forall y \in \mathbb{R})x + 2y^2 - z > u$$

  then you get the sentence

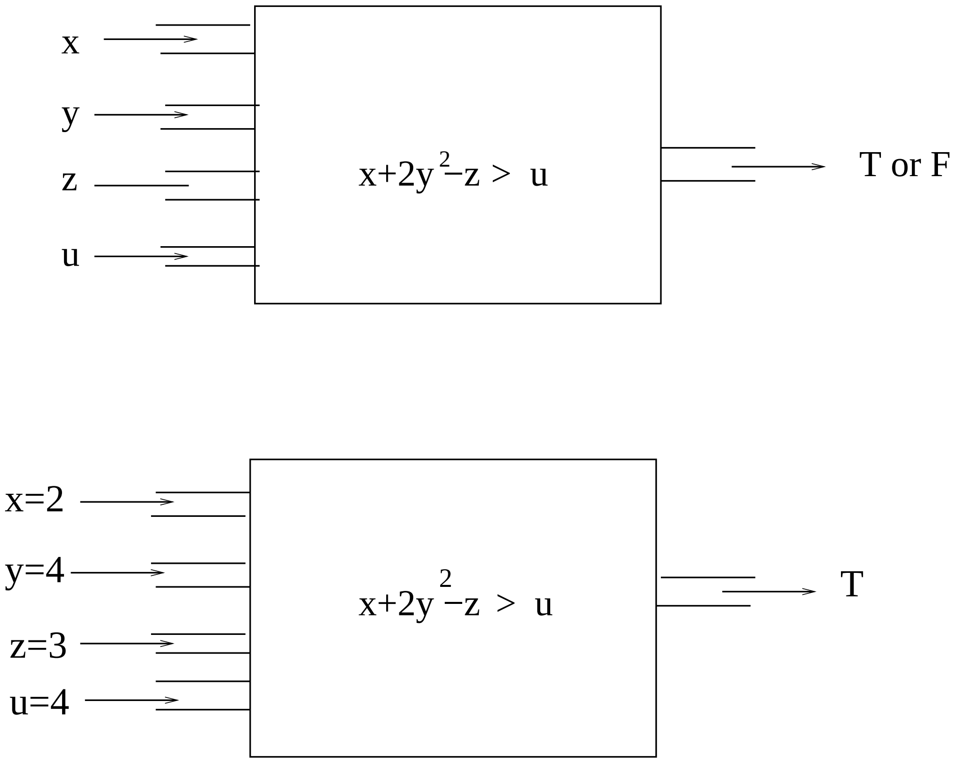
  $$(\forall y \in \mathbb{R})2 + 2y^2 + 3 > 4$$

  which is equivalent to the sentence

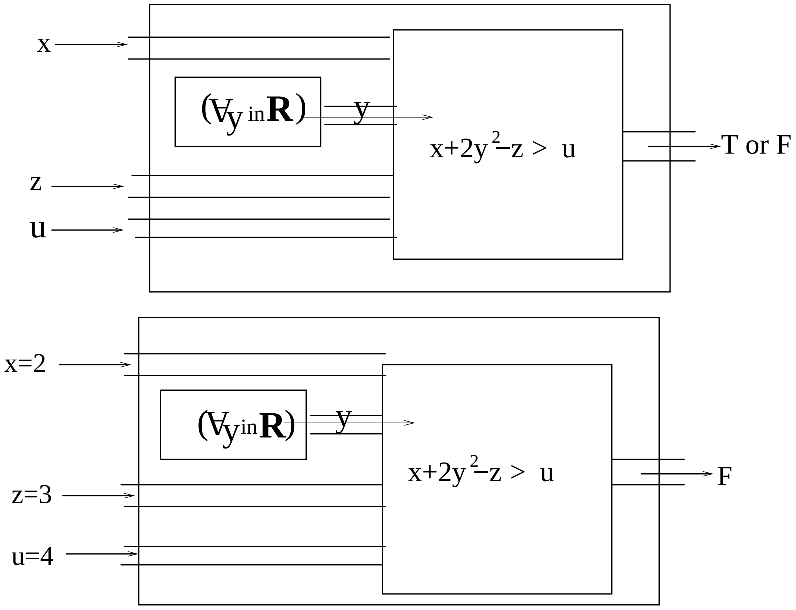
  $$(\forall y \in \mathbb{R})2y^2 + 5 > 4\,.$$

  And this sentence is true. (Proof: Let $y \in \mathbb{R}$ be arbitrary. Then $2y^2 \geq 0$. But $5 > 4$. So $2y^2 + 5 > 4$. Hence "$2y^2 + 5 > 0$" is true for arbitrary $y \in \mathbb{R}$. Therefore "$(\forall y \in \mathbb{R})2y^2 + 5 > 4$" is true.)
- The key point here is that ***the sentence "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" does not have a y-slot where you can plug in a value of y.*** That's because ***the sentence itself decides which value or values of y to plug in.*** The quantifier $(\forall y \in \mathbb{R})$ says: "let y be an arbitrary real number". And then, with the values of x, z and u supplied by you, the truth value of the resulting sentence is determined. ***There is no need to ask "who is y?"***

Another way to see this is as follows: when you universally quantify a sentence by putting in front of it the universal quantifier "$(\forall y \in \mathbb{R})$", this adds to the sentence a "generator of y-values", that is, a new component that tells the sentence what value of y to use. More precisely, the universal quantifier "$(\forall y \in \mathbb{R})$" says "Let y be an arbitrary real number". And this ***closes*** the y-input channel, so that it is no longer possible to plug a y-value into the sentence from outside.



The sentence $\boxed{x+2y^2-z>u}$ is a processing device that has four input channels: the x-channel, the y-channel, the z-channel, and the u-channel. When values for the four variables are inputted into the sentence, the sentence produces a truth value. The four variables x, y, z, u are ***open***, or ***free***. They are open, because the input channels are open so that values of the variables can be put into them. They are free, because the variables are not tied to any particular value.



The quantified sentence $\boxed{(\forall y \in \mathbb{R})x + 2y^2 - z > u}$ is a combination of two interconnected processing units: the original unquantified sentence "$x + 2y^2 - z > u$", and the quantifier "$(\forall y \in \mathbb{R})$". The quantifier generates a value for the quantified variable y (by saying "let y be an arbitrary real number") and, by doing so, it ***closes*** the y input channel, so that y is no longer free; we cannot choose a value for y and plug it in. The other three channels remain open. So in this sentence x, z and u are open variables. but y is ***closed***, or ***bound.***

The other three letter variables (x, z and u) remain open. So we can plug in values for them in order to obtain propositions that have a definite truth value.

Summarizing:

- Even though the predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" appears to contain four letter variables, only three of these variables (x, z and u) are open. The other variable, y, is ***bound***, or ***closed.***

- This means that the predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is a ***three variables***, or ***three arguments***, predicate. Therefore:
  - For each choice of values for x, z and u, the predicate becomes a proposition, i.e. a sentence with a definite truth value.

  - If we want to give a name to this predicate, then we can of course call it P, but if we want to indicate the names of the free variables, we should call it $P(x, z, u)$.
  - But ***we must not call it*** $P(x, y, z, u)$, because if we give it such a name we would erroneously be suggesting that this predicate has a "y-channel" where we can input values for the variable y.

- For example, "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is true for $x = 4$, $z = 2$, $u = 1$. (Proof: We want to prove that $(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$, that is, that $(\forall y \in \mathbb{R})2 + 2y^2 > 1$. Let $y \in \mathbb{R}$ be arbitrary. Then $y^2 \geq 0$, so $2y^2 \geq 0$, so $2 + 2y^2 \geq 2$, and $2 > 1$, so $2 + 2y^2 > 1$. Since "$2 + 2y^2 > 1$" has been proved to be true for arbitrary real y, it follows that $(\forall y \in \mathbb{R})2 + 2y^2 > 1$. Q.E.D.)

- The predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is false for $x = 4$, $z = 2$, $u = 8$. (Proof: We want to prove that "$(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$" is not true, i.e., that "$(\forall y \in \mathbb{R})2 + 2y^2 > 8$" is not true. Take $y = 0$. Then "$2 + 2y^2 > 8$" is not true, because "$2 + 0 > 8$" is not true. So "$(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$" is not true.Q.E.D.)

- The "truth question", i.e., the extra question we need to ask is order to be able to tell if "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is true or false, is the question: ***"who are*** x***,*** z ***and*** u***?"***

- ***in order to have enough information to determine if the sentence "***$(\forall y \in \mathbb{R})x + 2y^2 - z > u$***" is true or false, we do not have to ask "who is*** y***?", because once you are given the values of*** x***,*** z ***and*** u***, the quantified sentence itself determines if it is true or false, because it is up to the sentence to decide if it's true for all*** y ***or not, and it's not up to you to choose a value for*** y***.***

6.2.2 A second example: a predicate with two free variables and two bound variables

We now look at the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,. \qquad (6.111)$$

As I said before, on page 104, ***(6.109) is a two-variables predicate.***.

- Predicate (6.111) contains the variables a, b, q and r. But q ***and*** r ***are quantified***. So, if you are asked the "truth question"

  $$\text{Is} \qquad \text{“}(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\text{” true or false?}$$

  then you have to reply with a question of your own:

  Who are a and b?

  The variables a and b in (6.111) are "slots", or "input channels", where you can put in (or "plug in") a value for each of the variables, and then you get a proposition.

- So, for example, if you plug in the values $a = 23$, $b = 11$, into the sentence

  $$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

  then you get the sentence

  $$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)\,.$$

  And this sentence is true. (Proof: To prove an existential statement we use rule $\exists_{use}$: we exhibit values of q and r for which the proposition "$23 = 11q + r \wedge 0 \leq r < 11$" is true. Take $q = 2$, $r = 1$. Then $23 = 11q + r$ and $0 \leq r < 11$. Hence "$23 = 11q + r \wedge 0 \leq r < 11$" is true for some $q, r \in \mathbb{Z}$. Therefore "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11$" is true.)

- The key point here is that ***the sentence***

  $$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)$$

  does not have a q-slot or an r-slot where you can plug in values for q and r. That's because ***the sentence itself decides***

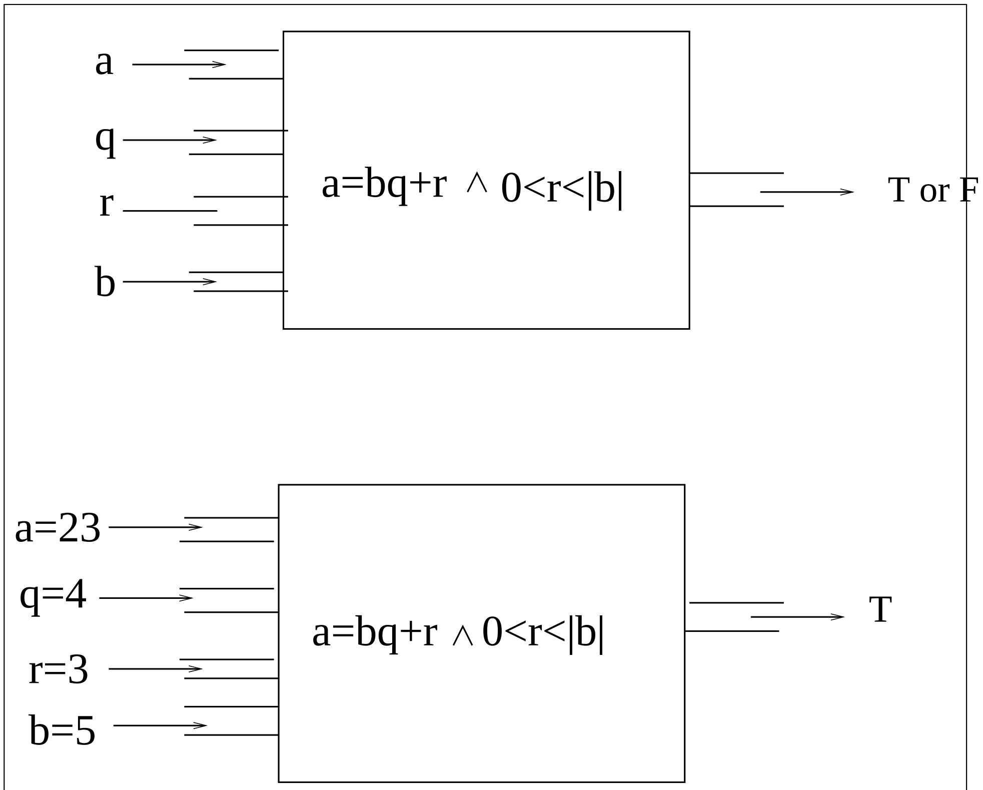
which value or values of q ***and*** r ***to plug in***. The sentence itself[42] decides which values of q and r it has to look at, and then, with the values of a and b supplied by you, the truth value of the resulting sentence is determined.

- Another way to see this is as follows: the sentence "$a = bq + r \wedge 0 \leq r < |b|$" has four input channels that are open, or free, so you can put into each channel a value of the corresponding variable.

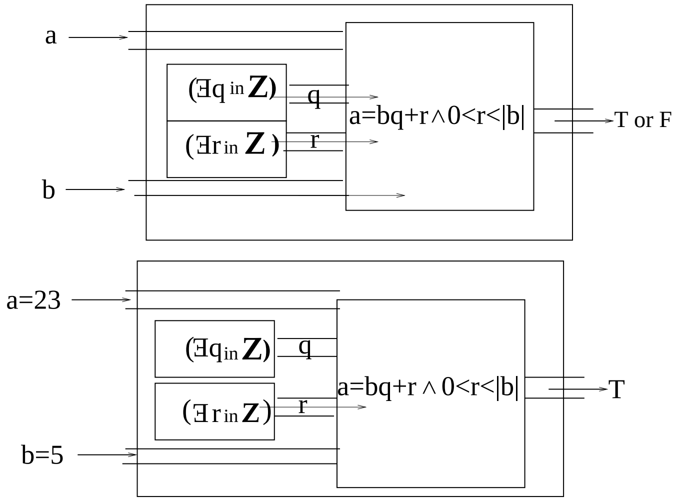
  But when you existentially quantify the sentence twice by putting in front of it the two existential quantifiera "$(\exists q \in \mathbb{Z})$" and "$(\exists r \in \mathbb{Z})$", this adds to the sentence a "generator of q-values" and a "generator of r-values", that is, two new components that tell the sentence what values of q and r to look at. More precisely, the existential quantifiers "$(\exists q \in \mathbb{R})$" and "$(\exists r \in \mathbb{R})$" do the following:

  - They look for a q-value and an r-value that make the sentence "$a = bq + r \wedge 0 \leq r < |b|$" true.
  - If they find such values, then they send to the sentence the message "yes, we have found values that make you true", and then the sentence produces the final verdict "yes, true".
  - If they do not find such values, then they send to the sentence the message "no, we have not found values that make you true", and then the sentence produces the final verdict "no, not true".

[42] Remember: you must think of a sentence as a processing device. The unquantified sentence "$a = bq + r \wedge 0 \leq r < |b|$" does the following: once it has been fed values for a, b, q and r, it finds out if "$a = bq + r \wedge 0 \leq r < |b|$" is true or not; if it is true is says "yes"; if it is false it says "no". The quantified sentence "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)$" does a much more complicated job: once it has been fed values for a and b, the sentence looks at all possible values of q and r, and sees whether it can find one choice of values of q and r for which "$23 = 11q + r \wedge 0 \leq r < 11$" is true; and then, if it find such values, it says "yes"; and if it cannot find any values of q and r for which "$23 = 11q + r \wedge 0 \leq r < 11$" is true, it says "no".



The sentence $\boxed{a = bq + r \wedge 0 \leq r < |b|}$ is a processing device that has four input channels:the a-channel, the q-channel, the r-channel, and the b-channel. When values for the four variables are inputted into the sentence, the sentence produces a truth value. The four variables a, q, r, b are ***open***, or ***free***. They are open, because the input channels are open so that values of the variables can be put into them. They are free, because the variables are not tied to any particular value.



The quantified sentence $\boxed{(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)}$ is a combination of three interconnected processing units: the original unquantified sentence "$a = bq + r \wedge 0 \leq r < |b|)$", and the two quantifiers "$(\exists q \in \mathbb{Z}$", "$(\exists r \in \mathbb{Z}$". The quantifiers generate values for the quantified variablea q, r. (They look for values of q, r that will make "$a = bq + r \wedge 0 \leq r < |b|)$" true. If they find them, then they send one pair of such values to the main processing unit "$a = bq + r \wedge 0 \leq r < |b|)$", which then says "yes, true". If they do not find them, then they send some values to the main processing unit, but these values will not work, so the main processing unit wil say "no, not true".) By doing so, the quantifiers ***close*** the q and r input channels, so that q and f are no longer free; we cannot choose values for q and r and plug them in. The other two channels remain open. So in this sentence a and b are open variables. but q and r are ***closed***, or ***bound***.

The other two letter variables (a and b) remain open. So we can plug in values for them in order to obtain propositions that have a definite truth value.

Summarizing:

- Even though the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

appears to contain four letter variables, only two of these variables (a and b) are open. The other variables, q and r, are ***bound***, or ***closed.***

- This means that the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

is a ***two variables***, or ***two arguments***, predicate. Therefore:

  - For each choice of values for a and b, the predicate becomes a proposition, i.e. a sentence with a definite truth value. (And the Division Theorem tells us that the truth value is "true" for all choices of integers a and b such that $b \neq 0$, that is, that the proposition[43]

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(b \neq 0 \Longrightarrow (\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\Big) \tag{6.112}$$

  is true.

  - Suppose we want to give a name to the two-variables predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,.$$

  We can, of course, call it P. But if we want to indicate the names of the free variables, we should call it $P(a, b)$.

  - But ***we must not call it*** $P(a, b, q, r)$, because if we give it such a name we would erroneously be suggesting that this predicate has a "q-channel" and an "r-channel", where we can input values for the variables q, r.

- The "truth question", i.e., the extra question we need to ask is order to be able to tell if "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$" is true or false, is the question: ***"who are a and b?"***

[43] Notice that (6.112) is a proposition, i.e., a predicate with no open variables at all (or, if you prefer, with zero open variables), because in (6.112) all four variables that occur are quantified, so a, b, q and r are closed variables. For the sentence (6.112), if you are asked "is this true", you do not need to ask any "truth question", because you do not need values of any variables to determine if the sentence is true.

- ***in order to have enough information to determine if the sentence "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$" is true or false, we do not have to ask "who are q and r?", because once you are given the values of a and b, the quantified sentence itself determines if it is true or false, because it is up to the sentence to decide if the required values of q and r exists or not, and it's not up to you to choose valuea for q and r.***

6.2.3 Another example, illustrating the fact that only open variables really matter

Some natural numbers are products of two prime numbers; for example, $4 = 2 \times 2$, $6 = 2 \times 3$, $35 = 5 \times 7$, and so on, Other natural numbers are not products of two prime numbers; for example, $18 = 2 \times 3 \times 3$, and the Fundamental Theorem of Arithmetic tells us that that there is no other way to write 18 as a product of primes, so in particular 18 is not the product of two primes.

So we can consider the predicate "n is a product of two prime numbers". And we can call this predicate $A(n)$. (We could just have called is "A", but we choose the name "$A(n)$" to emphasize the fact that this predicate has the open variable n.) Then, according to the conventions we made before about naming predicates, $A(6)$ is the proposition "6 is the product of two primes", and $A(7)$ is the proposition "7 is the product of two primes", so $A(6)$ is true, and $A(7)$ is false.

You can think of the predicate $A(n)$ as a "black box": you input a value of n, the predicate does some work, and produces an answer: "true" or "false". (For example, for $n = 6$ $A(n)$ is true, and for $n = 7$ $A(n)$ is false.)

But we can also look inside the box, and analyze in more detail how this predicate works. That is, we can observe that $A(n)$ says that

$$\text{There exist prime numbers } p, q \text{ such that } n = pq.$$

So now our predicate has three variables, p, q, and n!

How come? Has the number of variables of $A(n)$ suddenly changed? Has $A(n)$ become a three-variables predicate? You may think so, because now $A(n)$ seems to have three variables: p, q and n.

But the answer is: ***No! $A(n)$ is still a one-variable predicate!*** The variables p and q are ***bound***, because they are quantified.

Precisely, $A(n)$ says, in semiformal (almost formal) language:

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p \text{ is prime} \wedge q \text{ is prime} \wedge n = pq)\,. \tag{6.113}$$

So, even though $A(n)$ appears to have three variables, namely, p, q and n, two of them are ***internal variables***[44], within the sentence (6.113). The sentence itself generates the values of p and q that it needs in order to answer its true-false question, and when the sentence ends p and q are free variables again. And, in particular, ***outside the sentence***

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p \text{ is prime} \wedge q \text{ is prime} \wedge n = pq)$$

the variables p ***and*** q ***have no value.***

Another way to see that p and q have no value, is to observe that $A(n)$ can equally well be written as

$$(\exists x \in \mathbb{N})(\exists y \in \mathbb{N})(x \text{ is prime} \wedge y \text{ is prime} \wedge n = xy)\,, \tag{6.114}$$

or as

$$(\exists u \in \mathbb{N})(\exists v \in \mathbb{N})(u \text{ is prime} \wedge v \text{ is prime} \wedge n = uv)\,. \tag{6.115}$$

Sentences (6.113), (6.114), and (6.115) say exactly the same thing. The only difference is in the names of the variables that, inside the box, the sentence uses to process the inputs and produce an output.

From outside the box, we do not see these variables. ***That's why the letters*** p, q ***in (6.113), as well as the letters*** x, y ***in (6.114), and the letters*** u, v ***in (6.115), are internal variables, that have no value outside the sentence.***

And this is not the end of the story. "p is prime" is itself a complex predicate. In fact, "p is prine" stands for

$$p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\,. \tag{6.116}$$

[44] If you think of the sentence "$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p$ is prime)" as a processing unit, you will see that it has two existential quantifiers that generate values of p and q. But outside the processing unit all one sees is that certain values of n are fed in and certain 'true"s and "false"s come out. The variables p and q are part of the internal operation of the device.

This means that $A(n)$ can also be written as

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})\Bigg(\bigg(p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\bigg)$$
$$\wedge\bigg(q > 1 \wedge (\forall k \in \mathbb{N})\Big(k|q \Longrightarrow (k = 1 \vee k = q)\Big)\bigg) \wedge n = pq\Bigg) \tag{6.117}$$

Now one may think that $A(n)$ is a four-variables predicate, because it involves the variables n, p, q and k. But by now you know better: the new variable k is also bound, so the only open variable in (6.117)) is still n. That means that ***even if you write it in the form (6.117),*** $A(n)$ ***is still a one-variable predicate.***

Actually, the story doesn't end here either. "$k|p$" is also a complex preddcate with an internal structure of its own: is stands for "$(\exists j \in \mathbb{Z})p = kj$". So, if we substitute this for "$k|p$" in (6.117), we get an even more detalied version of $A(n)$, namely,

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})$$
$$\Bigg(\bigg(p > 1 \wedge (\forall k \in \mathbb{N})\Big((\exists j \in \mathbb{Z})p = kj \Longrightarrow (k = 1 \vee k = p)\Big)\bigg)$$
$$\wedge\bigg(q > 1 \wedge (\forall k \in \mathbb{N})\Big((\exists j \in \mathbb{Z})q = kj \Longrightarrow (k = 1 \vee k = q)\Big)\bigg)$$
$$\wedge n = pq\Bigg). \tag{6.118}$$

Now $A(n)$ apears to involve five variables: n, p, q, k and j. But this time you will have no problem figuring out that $A(n)$ ***is still a one-variable predicate, because the only open variable in (6.118) is still*** n***, and all the other variables are bound***.

Problem 22. Draw a diagram of the sentence (6.118) as a processing unit, similar to the diagrams that appear on pages 109 and 114.

Make sure that your diagram shows that there is only only one input channel. □

6.2.4 Dummy variables

So far, we have seen that variables that appear in a sentence but are quantified are “internal variables”, or “closed variables”, or “bound variables”. If you think of a sentence as a “processing unit”, or “processing device”, that takes in certain inputs and produces “true-false” outputs, then the closed (or bound, or internal) variables are variables that the sentence itself generates and uses to do its processing work. So the sentence does not need to be fed the values of these variables, and does not produce values of those variables that an outside obsevrer can see.

There is another way in which a variable appearing in a sentence can be a closed (or bound, or internal) variable. The sentence may contain a part that generates values of some variable in order to do a computation.

Consider. for example, the sentence

$$\sum_{k=1}^{n}(a+r^k)=b\,, \tag{6.119}$$

This sentence contains five letter variables, namely, a, r, b, k, and n.

Which ones of these five variables are open?

The best way to answer this question is by thinking of (6.119) as a processing device, opening it up to look into its internal structure, and figuring out what the device does.

Suppose you ask the device the truth question:

Is it true that $\sum_{k=1}^{n}(a+r^k)=b$?

Then the device will not know what to do, because in order to get started the device needs to be given the values of a, b, r, and n. (Maybe we should think of (6.119) as an inteligent device, that can ask questions. Then if you ask the truth question, the device will answer with a question: ***who are*** a***,*** b***,*** r ***and*** n***?***)

Suppose you do feed the device by inputting values for a, b,r and n. Then the device will do the following:

1. First, the CPU (central procssing unit) will report to the summation component Σ—that is, the component that computes the summation $\sum_{k=1}^{n}(a+r^k)$—the values of a, b, r and n that it has received from you.
2. Then Σ will perform the following calculation:

(a) First, it will write the list of all values of k, from 1 to n. (This is something it can do, because it knows who n is, since it has received this information from the CPU.)

(b) Then it will compute $a + r^k$ for each of the values of k in the list. (Again, Σ knows how to do this, because it knows who a and r are.)

(c) Then it will take all those values of $a + r^k$ that it has computed, and add them.

(d) Finally, it will report the result to the CPU. (Maybe, in order to facilitate communication between Σ and the CPU, they will introduce letter variables. For example, they may decide to call the result of the summation s, and then Σ will report the value of s to the CPU. But we need not concern ourselves with the variable s, because that's an internal variable used within the device for the various parts to communicate with each other.)

3. The CPU will then compare the result reported by the summation unit with b, and determine if they are equal.

4. If they are equal, the CPU will report to you the answer "true".

5. If they are not equal, the CPU will report to you the answer "false".

The main point of this is that k ***is an internal variable used by the sentence to perform its calculation. The values of*** k ***are generated by the sentence itself. So the sentence need not be given the value of*** k. And that's why

1. If asked the truth question, the sentence will ask "who are a, b, r and n""."

2. The sentence will not ask "who is k?", because ***the sentence itself generates the values of*** k ***it needs***.

3. k ***is not an open variable in (6.119)***

4. The open variables of (6.119) are a, b, r and n.

Let's just look at one more example. Let us analyze the following four sentences

$$(\forall n \in \mathbb{N})\Big((\exists m \in \mathbb{N})\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N})n = p^2\Big)\,, \tag{6.120}$$

$$(\forall n \in \mathbb{N})\Big((\exists m \in \mathbb{N})\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N})n = p^3\Big)\,, \tag{6.121}$$

$$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})\Big(\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N})n = p^2\Big) \tag{6.122}$$

and

$$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})\Big(\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N})n = p^3\Big) \tag{6.123}$$

Each of these sentences contains four variables, namely, n, m, k, and p.

And I am sure that this time you can see right away what is going on: ***all four variables are closed***. Three of them (n, m, and p) are quantified. and the variable k is also closed because the sentence itself generates the values of k that it needs to perfom its calculations.

So ***the sentences (6.120), (6.121), (6.122), and (6.123), are propositions***.

And then of course each of the sentences is true or false. Which leads me to a natural question, that I will ask you to answer.

Problem 23. Which of the propositions (6.120), (6.121), (6.122), (6.123), are true, and which ones are false?

NOTE: All these propositions are of the form $(\forall n \in \mathbb{N})P(n)$, where $P(n)$ is a one-variable predicate having n as the open variable.

If you want to prove that a sentence of this form is true, then you need a reasoned argument, starting with "Let n be an arbitrary natural number." (You may also try a proof by induction, but in this case I would not recommend that.) If you want to prove that it is false, then you need a counterexample, i.e., an example of an n for which the one-variable sentence $P(n)$ is false.

HINT: The answer to this problem is actually very easy. All you have to do is use the result of one of your earlier homework problems. (I can narrow this down a bit further: *it's one of the problems in the third set of lecture notes*.) Using this, plus a little bit of logic (for example, truth values of implications), each of the four propositions should just require a couple of lines on your part.) □

A variable such as the k in $\sum_{k=1}^{n} t(k)$ (where $t(k)$ is some expression containing k, such as k, or k^2, or r^k, or $a+r^k$), is called a "dummy variable".

Let us define this term precisely. (The definition I am about to give is taken from Wolfram MathWorld.)

Definition 6. A dummy variable is ***a variable that appears in a calculation only as a placeholder and which disappears completely in the final result.*** □

And ***every dummy variable is bounded***.

Example 27. Naturally, summations are not the only type of expressions where some of the variables are bound variables

Examples of dummy variables are:

1. the k in a summation such as $\sum_{k=1}^{n} t(k)$,
2. the k in a product such as $\prod_{k=1}^{n} t(k)$,
3. the k in the name of a list, such as $(p_k)_{k=1}^{n}$,
4. the x in the name $\{x : P(x)\}$ of a set,
5. the x in an integral such as $\int_a^b f(x)dx$.
6. the x in a limit such as $\lim_{x\to a} f(x)$. □

Example 28. Let us look at the sentence

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{u \in \mathbb{R} : a \le u \le b\} \neq \emptyset \wedge \int_a^b x^2 dx = c\Big)\,. \qquad (6.124)$$

This sentence contains the letter variables a, b, u, x, and c.

Of these five letters, four are bound variables:

1. the variables a and b are bound because they are quantified;
2. the variable u is bound because it is a dummy variable, used as part of the name $\{u \in \mathbb{R} : a \le u \le b\}$ of a set;
3. the variable x is bound because it is a dummy variable, used as a variable of integration.

It follows from this analysis that

1. ***Sentence (6.124) defines a one-variable predicate.***
2. ***The open variable in sentence (6.124) is*** c.
3. If you think of sentence (6.124) as a processing device, then this device will take values of c as inputs, and produce a true-false answer as output.
4. If you ask the "truth question" ***is (6.124) true?***, then the device (6.124) cannot answer because it does not know who c is. So the device will answer your question with another question: ***who is*** c***?***
5. But, in order to be able to answer the truth question, the device does not need to ask "who is a?", or "who is b?" or "who is u?", or "who is x?". The device itself will generate the values of a, b, u and x it needs, and these values will be part of the calculations that (6.124) performs, and will not be seen by the outside world.

6.2.5 How to tell if a variable is dummy

Here are two ways to see that a variable is dummy.

1. The variable is dummy if "it isn't really there", in the sense that we can eliminate it completely. For example,

   (a) The set $\{u \in \mathbb{R} : a \le u \le\!< b\}$ is an object very well known to all of us: it is none other than the closed interval $[a, b]$. So we can say the same thing as (6.124) by writing "$[a, b]$" instead of "$\{u \in \mathbb{R} : a \le u \le\!< b\}$". And we get

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a,b] \neq \emptyset \wedge \int_a^b x^2 dx = c\Big)\,, \tag{6.125}$$

which says exactly the same thing as (6.124). but now there is no "u" anymore.

(b) The definite integral $\int_a^b x^2dx$ is a number that is completely determined by a and b. We do not need to ask "who is x?" in order to determine this number. Actually, the integral can be computed, and the result is $\frac{1}{3}(b^3 - a^3)$. So we can say the same thing as (6.125) by writing "$\frac{1}{3}(b^3 - a^3)$" instead of "$\int_a^b x^2dx$", and we get

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a,b] \neq \emptyset \wedge \frac{1}{3}(b^3 - a^3) = c\Big)\,, \tag{6.126}$$

or, more nicely,

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a,b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big)\,, \tag{6.127}$$

which say exactly the same thing as (6.125). but now there is no "x" anymore.

2. A variable is dummy if it can be replaced by any other variable (except with variables that are already being used for something else) without changing the meaning of the sentence. For example,

(a) If instead of the expression "$\{u \in \mathbb{R} : a \leq u \leq b\}$" we use a different letter and write something like "$\{v \in \mathbb{R} : a \leq v \leq b\}$", or "$\{z \in \mathbb{R} : a \leq z \leq b\}$", or maybe "$\{\alpha \in \mathbb{R} : a \leq \alpha \leq b\}$", or "$\{\diamond \in \mathbb{R} : a \leq \diamond \leq b\}$", nothing changes. So, for example, we can rewrite (6.124) as

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{q \in \mathbb{R} : a \leq q \leq b\} \neq \emptyset \wedge \int_a^b x^2dx = c\Big)\,, \tag{6.128}$$

which says exactly the same thing as (6.124). but now there is no u anymore.

(b) If we replace the definite integral $\int_a^b x^2dx$ by the expression $\int_a^b h^2dh$, or $\int_a^b \sigma^2d\sigma$, or $\int_a^b m^2dm$, nothing changes. So, for example, we can rewrite (6.128) as

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{q \in \mathbb{R} : a \leq q \leq b\} \neq \emptyset \wedge \int_a^b k^2dk = c\Big)\,, \tag{6.129}$$

which says exactly the same thing as (6.124). but now there is no u and no x anymore.

Summarizing: Sentence (6.124) defines a ***one-variable predicate, with the open variable*** c. So we can call this predicate $P(c)$.

And then we may ask: can we tell what this predicate $P(c)$ is? Can we find a simpler expression for $P(c)$?

It turns out that, in this case, the answer is "yes, we can":

$\boxed{P(c) \textbf{\textit{ just says "}} c \geq 0 \textbf{\textit{"}}}$.

Proof. We want to prove that $(\forall c \in \mathbb{R})(P(c) \iff c \geq 0)$.

Let $c \in \mathbb{R}$ be arbitrary.

We want to prove that $P(c) \iff c \geq 0$.

For that purpose, we will prove the implications $P(c) \Longrightarrow c \geq 0$ and $c \geq 0 \Longrightarrow P(c)$.

Proof that $P(c) \Longrightarrow c \geq 0$.

Assume $P(c)$.

This means that

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big)\,.$$

Pick real numbers a, b such that $a, b] \neq \emptyset$ and $b^3 - a^3 = 3c$.

Since $a, b] \neq \emptyset$, it follows that $a \leq b$. (Reason: if $a > b$ then the set $[a, b]$, i.e., the set $\{u \in \mathbb{R} : a \leq u \leq b\}$, would be empty.)

Since $a \leq b$, we have $a^3 \leq b^3$.

So $b^3 - a^3 \geq 9$.

So $3c \geq 0$.

Hence $\boxed{c \geq 0}$.

Proof that $c \geq 0 \Longrightarrow P(c)$.

Assume that $c \geq 0$.

Let $a = 0$, $b = \sqrt[3]{3c}$.

Then $b \geq 0$.

So the closed interval $[a, b]$ (i.e., the interval $[0, b]$) is nonemtpy.

And $b^3 - a^3 = 3c$.

Hence $[a, b] \neq \emptyset \wedge b^3 - a^3 = 3c$.

So

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big)\,.$$

That is, $\boxed{P(c) \text{ holds.}}$

Since we gave proved that $P(c) \Longrightarrow c \geq 0$ and that $c \geq 0 \Longrightarrow P(c)$, we can conclude that $P(c) \Longleftrightarrow c \geq 0$.

Since we have proved that $P(c) \Longleftrightarrow c \geq 0$ for arbitrary real c, we have proved that $(\forall c \in \mathbb{R})\Big(P(c) \Longleftrightarrow c \geq 0)$. **Q.E.D.**

6.3 First-order predicate calculus

The language we use in mathematics is a ***predicate calculus*** because it enables us to predicates. And it is ***first-order*** because we can quantify variables, and write things such as "$(\forall x \in P)x$ likes Mark" (meaning, if P is the set of all people, "everybody likes Mark"), but we cannot quantify over predicates. That is,

- We cannot say things such as "'for every predicate $P(x)$ and every predicate $Q(x)$ if $(\forall x)P(x)$ is true and $(\forall x)Q(x))$ is true, then if $(\forall x)(P(x) \wedge Q(x))$ is true."
- We can say this for a particular pair of predicates $P(x)$, $Q(x)$ (for example, we can say "if everybody likes coffee and everybody likes milk then everybdoy likes coffee and milk", or we can say "if everybody studies and everybody reads books then everybdoy studies and reads books"), but we cannot say the same thing for arbitrary predicates $P(x)$, $Q(x)$.

It turns out that there are "second order" languages, in which you can say things like "'for every predicate $P(x)$ and every predicate $Q(x)$ if $(\forall x)P(x)$ is true and $(\forall x)Q(x))$ is true, then if $(\forall x)(P(x) \wedge Q(x))$ is true." But the language we are using here is a ***first-order language***, in which those things cannot be said.

6.4 Logical connectives

In firts-order predicate calculus, one or more sentences can be combined to form other sentences. The symbols used to combine sentences are called the ***logical connectives.*** And there are exactly seven of them

6.4.1 The seven logical connectives

And here they are, in all their glory:

The seven logical connectives

1. The ***negation symbol*** $\sim$
(meaning “no”, “it’s not the case that”).

2. The ***conjunction symbol***, $\bigwedge$
(meaning “and”).

3. The ***disjunction symbol***, $\bigvee$
(meaning “or”).

4. The ***implication symbol***, $\Longrightarrow$
(meaning “implies”, or “if ... then”).

5. The ***biconditional symbol***, $\Longleftrightarrow$
(meaning “if and only if”).

6. The ***existential quantifier symbol***, $\exists$
(meaning “there exists ... such that”, or “it is possible to pick ... such that”).

7. The ***universal quantifier symbol***, $\forall$
(meaning “for all”,or “for avery”, or “for an arbitrary”).

6.4.2 How the seven logical connectives are used to form sentences

These seven symbols are used to form new sentences as follows:

1. The negation symbol $\sim$ is a ***one-argument connective***: it can be put in front of a sentence A to form the sentence $\sim A$ (meaning “no

A", or "it's not the case that A"). For example: "$\sim 3|5$" means "3 does not divide 5".

2. The conjunction symbol $\wedge$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sentence $A \wedge B$, (meaning "A and B"). For example: "$(\sim 3|5) \wedge 3|6$" means "3 does not divide 5 and 3 divides 6".

3. The disjunction symbol $\wedge$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sentence $A \vee B$, (meaning "A or B"). For example: "$x > 0 \vee x < 0$" means "$x > 0$ or $x < 0$".

4. The implication symbol $\Longrightarrow$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sentence $A \Longrightarrow B$, (meaning "A implies B", or "if A then B"). For example: "$x \neq 0 \Longrightarrow x^2 > 0$" means "if $x > 0$ then $x^2 > 0$".

5. The biconditional symbol $\Longleftrightarrow$ is a ***two-argument connective***, that is ***binary connective***: it can be put between two sentences A, B to form the sentence $A \Longleftrightarrow B$, (meaning "A if and only if B"). For example: "$(2|n \wedge 3|n) \Longleftrightarrow 6|n$" means "2 divides n and 3 divides n if and only if 6 divides n".

6. The existential quantifier symbol $\exists$ has a more complicated grammar:

   (a) Using $\exists$ we can form ***existential quantifiers***.

   (b) There are two kinds of existential quantifiers:

      i. ***Unrestricted existential quantifiers*** are expressions
      $$\Big(\exists x\Big),$$
      that is: left parenthesis, $\exists$, variable, right parenthesis.

      ii. ***Restricted existential quantifiers*** are expressions
      $$\Big(\exists x \in S\Big),$$
      that is: left parenthesis, $\exists$, variable, $\in$, name of a set, right parenthesis.

(c) Then we can take a sentence A (or $A(x)$) and put a restricted or unrestricted existential quantifier in front, forming the sentences $(\exists x)A$ ("there exists x such that A", or "it is possible to pick x such that A") and $(\exists x \in S)A$ ("there exists x belonging to S such that A", or "it is possible to pick x belonging to S such that A").

7. The universal quantifier symbol $\forall$ has a grammar similar to that of the existential quantifier symbol:

   (a) Using $\forall$ we can form ***universal quantifiers***.

   (b) There are two kinds of universal quantifiers:

      i. ***Unrestricted universal quantifiers*** are expressions
      $$\Big(\forall x\Big),$$
      that is: left parenthesis, $\forall$, variable, right parenthesis.

      ii. ***Restricted universal quantifiers*** are expressions
      $$\Big(\forall x \in S\Big),$$
      that is: left parenthesis, $\forall$, variable, $\in$, name of a set, right parenthesis.

   (c) Then we can take a sentence A (or $A(x)$) and put a restricted or unrestricted universal quantifier in front, forming the sentences $(\forall x)A$ ("for all x, A", or "A i strue for arbitrary x") and $(\forall x \in S)A$ ("for all x belonging to S, A", or "A is true for arbitrary x in S").

6.5 Conjunctions ("$\wedge$", i.e., "and")

The symbol

$$\bigwedge$$

is the ***conjunction symbol***, and means "and".

Hence,

- If P is the sentence

  Today is Friday

  and Q is the sentence

Tomorrow is Saturday

then “$P \wedge Q$” stands for the sentence

Today is Friday and tomorrow is Saturday.

- A sentence of the form $P \wedge Q$ is a ***conjunction***.
- In a conjunction $P \wedge Q$, the sentences P, Q are the ***conjuncts***.

6.5.1 Proving a conjunction: a stupid but important rule

The rule for proving a conjunction (Rule $\wedge_{prove}$)

If P, Q are sentences, and you have proved P and you have proved Q, then you are allowed to go to $P \wedge Q$.

IMPORTANT REMARK. You may wonder “what is the point of such a rule?” But you cannot dispute that it is a reasonable rule! Of course, if you know that “today is Friday” and you also know that “tomorrow is Saturday”, then you will have no doubt that “today is Friday and tomorrow is Saturday” is true. So you should have no problem accepting (and remembering) this rule. You may not understand why it is needed. So let me tell you why. Suppose it was a computer doing proofs, rather than a human being like you. Suppose the computer is told that today is Friday and then it is told that tomorrow is Saturday. How will the computer know that it can write “today is Friday and tomorrow is Saturday”. It won’t, unless you tell it. Computers do not ”know” anything on their own. If you want the computer to “know” that once it knows that “today is Friday” and also that “tomorrow is Saturday”, then it can write “today is Friday and tomorrow is Saturday”, then you have to **tell** the computer. In other words, you have to input Rule $\wedge_{prove}$ into the computer. Proofs are mechanical manipulations of strings of symbols, and should therefore be doable by a computer. So Rule $\wedge_{prove}$ is needed.

And now let’s go back to you, the human being. How do *you* know that, once you find out that “today is Friday” and also that “tomorrow is Saturday”, then you can say (or write) “today is Friday and tomorrow is Saturday”. **You know this because you know Rule $\wedge_{prove}$.** You know this rule so well, it is embedded so deeply in your mind, that you don't even realize that the rule is there. But **the rule is there!**

Here is another way to think about this. Suppose you didn't know any English at all. Then you would not know what the word "and" means, and you would not know that, if you have two sentences P and Q, then you can say or write "P and Q". As you learn English, at some point you would learn the meaning of the word "and" and then you would learn that when you have two sentences P and Q, then you can say or write "P and Q". (And I would even argue that this rule about that use of "and" is in fact what "and" means, but I will not pursue this now.) The point is: *there are* rules for using the word "and", and those rules have to be *learned*, and they only look obvious to you because you already learned them a long time ago and have grown accustomed to them.

What we are doing in Logic is **elucidating the laws of thought, making them explicit, bringing them to the surface, as it were**, so that we can, for example, pass them on from our minds to a computer: the computer does not "know" any of the things that you know, unless you tell the computer those things. And this applies even to the rules that you know so well that they are deeply embedded in your subconscious, so you take them for granted without even realizing that there is something to be known there.

Once you understand this, you will also see that **it is not an accident that modern Logic developed first, at the end of the 19th century and the beginning of the 20th century, and computers came into being soon afterwards.** □

6.5.2 Using a conjunction: another stupid but important rule

The rule for using a conjunction (Rule $\wedge_{use}$)

If P, Q are sentences, and you have proved $P \wedge Q$, then you are allowed to go to P, and you are also allowed to go to Q.

IMPORTANT REMARK. This looks like a very stupid rule. But you should reread the "Important Remark" on Page 130, where we talked about another "stupid rule", namely, Rule $\wedge_{prove}$. That remark also applies to Rule $\wedge_{use}$. □

6.6 Disjunctions ("$\vee$", i.e., "or")

The symbol

$$\bigvee$$

is the ***disjunction symbol***, and means "or".

So, for example,

- If P is the sentence

  today is Friday

  and Q is the sentence

  today is Saturday

  then "$P \vee Q$" stands for the sentence

  today is Friday or today is Saturday.

- A sentence of the form $P \vee Q$ is a ***disjunction***.
- In a disjunction $P \vee Q$, the sentences P, Q are the ***disjuncts***.

6.6.1 Using a disjunction: the "proof by cases" rule

The rule for using a disjunction, that we are going to call "Rule $\vee_{use}$", as you may have guessed, is extremely important. It is also called the "proof by cases rule", and is one of the most widely used rules in theorem proving.

Before I state the rule, let us look at an example.

Example 29. Suppose you want to prove that

$$(\forall x \in \mathbb{R})(x \neq 0 \Longrightarrow x^2 > 0\,. \tag{6.130}$$

Then you could reason as follows. Since $x \neq 0$, there are two possibilities: $0 < x$ or $x < 0$. We consider each of these two possibilities separately.

First we assume that $\boxed{0 < x.}$

Then we use the fact that we can multiply both sides of an inequality by a positive number[45]. Since $0 < x$ (because we are assuming that $0 < x$), we can multiply both sides of "$0 < x$" by x, and get $x.0 < x.x$.

But $x \cdot 0 = 0$ by a theorem[46]

And $x{\cdot}x = x^2$. (This is because the definition of x^2 says that $x^2 = x{\cdot}x$.)

So $\boxed{0 < x^2}$.

Next we assume that $\boxed{x < 0.}$

Then we usethat axiom that says that we can add a real number to both sides of an inequality and the result is an inequality going in the same direction[47]. So we add $-x$ to both sides of "$x < 0$" and get $0 < -x$.

Then we use the axiom about multiplication of both sides of an inequality by a positive number. Since $-x$ is positive, because we have proved that it is (under the assumption that $x < 0$), we can multiply both sides of "$0 < -x$" by $-x$, and get $(-x).0 < (-x).(-x)$.

But $x \cdot 0 = 0$ by a theorem proved before.

And $(-x) \cdot (-x) = x \cdot x$.

So $0 < x \cdot x$.

And $x \cdot x = x^2$, by the definition of "square".

So $\boxed{0 < x^2}$ in this case as well.

So we have analyzed each of the two possibilities $0 < x$ and $x < 0$, and in each case we arrived a the same conclusion, namely, that $0 < x^2$.

[45] This is one of the axioms of real number theory, that we will discuss later. Tha axiom says: $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})\Big((x < y \wedge 0 < z) \Longrightarrow xz < yz\Big)$.

[46] The theorem says that $(\forall x \in \mathbb{R})x.0 = 0$. This was proved earlier for integers, but the proof for real numbers is the same.

[47] Precisely, the axiom says: $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x < y \Longrightarrow x + z < y + z\Big)$.

Hence we have proved that $\boxed{\boxed{0 < x^2}}$.

What we have done in this example is this: we knew that a disjunction $A \vee B$ was true. (In our example, A was "$0 < x$" and B was "$x < 0$".) Then we proved that a ceartain conclusion C must hold if A is true, and also if B is true. (In our example, C was "$0 < x^2$".) Then we concluded that C must be true. And the reason is quite simple: one of A, B is true, and in either case C is true, so C is true.

This is exactly what the proof by cases rule says.

The rule for using a disjunction (Rule $\vee_{use}$, a.k.a. the proof by cases rule)

If P and Q are sentences, and you have proved $P \vee Q$ in a previous step, and then you prove another sentence R both assuming P and assuming Q, then you can go to R.

6.6.2 Proving a disjunction

The rule for proving a disjunction (Rule $\vee_{prove}$)

Suppose P and Q are sentences, and you want to prove $P \vee Q$. Here is what you can do. You look at the two possible cases, when P is true and when P is false. If P is true then of course $P \vee Q$ is true, so we are O.K. So all we have to do is look at the other case, when P is false, and prove that in that case Q is true.
So here is the rule:

I. If, assuming that P is false, you can prove Q, then you can go to $P \vee Q$.

II. If, assuming that Q is false, you can prove P, then you can go to $P \vee Q$.

6.7 Implications ("$\Longrightarrow$", i.e., "if ... then")

Implication: The symbol

$$\Longrightarrow$$

is the ***implication symbol***, and means "implies".

A sentence "$P \Longrightarrow Q$" is read as

$$P \text{ implies } Q$$

or as

$$\text{If } P \text{ then } Q\,.$$

Then

- If P is the sentence

  Today is Friday

  and Q is the sentence

  Tomorrow is Saturday

  then "$P \Longrightarrow Q$" stands for the sentence

  If today is Friday then tomorrow is Saturday.

- A sentence of the form $P \Longrightarrow Q$ is an ***implication***, or a ***conditional sentence***.

- In a conditional sentence $P \Longrightarrow Q$, P is the ***premiss*** (or ***antecedent***), and Q is the ***conclusion*** (or ***consequent***.

6.7.1 The rule for using an implication (Rule $\Longrightarrow_{use}$, a.k.a. "Modus Ponens")

We now come to one of the most important rules in Logic: the rule for using an implication. For us, this rule will be called— guess what!—"Rule $\Longrightarrow_{use}$", but it also has a couple of much more impressive names: **Modus Ponens**, and **implication elimination**[48]

[48] "Modus Ponens" is an abbreviation of "modus ponendo ponens", which is Latin for "the way that affirms by affirming".

The rule for using an implication (Rule $\Longrightarrow_{use}$, a.k.a. *Modus Ponens*)

Suppose P, Q are sentences. Suppose you have the sentences $P \Longrightarrow Q$" and "P" in previous steps of your proof. Then you can go to Q.

Example 30. Suppose you know that "If you are a student then you are entitled to a discount" and you also know that you are a student. Then you can conclude that you are entitled to a discount.

6.7.2 The "for all...implies" combination

One of the most important and widely used combinations of moves in proofs is what we may call ***the "for all...implies" combination***.

It works like this:

- First, you bring into your proof a statement S of the form "for every x of some kind, if something happens then something else happens". That is, $(\forall x)(A(x) \Longrightarrow B(x))$, or
$$(\forall x \in S)(A(x) \Longrightarrow B(x))\,. \tag{6.131}$$
- Then, you bring into your proof an object a for which you know that this object satisfies Property A, that is, you know that
$$A(a)\,. \tag{6.132}$$
- Then you derive the conclusion that $B(a)$ is true, in two steps:

  Step 1: Use the specialization rule to go from (6.131) to
$$A(a) \Longrightarrow B(a)\,. \tag{6.133}$$
  Step 2: Use Modus Ponens to go from (6.133) and (6.132) to
$$B(a)\,. \tag{6.134}$$

This combination is used all the time in proofs. The reason is that many theorems in Mathematics are of the form: "whenever something is true of an object, then something else is also true of that object", that is

$$(\forall x)(A(x) \Longrightarrow B(x))\,. \tag{6.135}$$

And what you often do in proofs is take one of those theorems and apply it to a particular situation. And this is exactly what the "for all...implies" combination does.

Here are some examples:

1. Take the statement that "Every positive real number has a real square root", which translates into

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

   This is exactly of the form (6.135), with "$x > 0$" in the role of $A(x)$, and "$(\exists y \in \mathbb{R})y^2 = x$" in the role of $B(x)$.

   Then you can prove that 2 has a square root, by applying the "for all ... implies" combination, with $a = 2$, and getting "$(\exists y \in \mathbb{R})y^2 = 2$".

2. Suppose you know that "If x is a positive real number then $x + \frac{1}{x} \geq 2$", that is, in formal language,

   $$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,.$$

   (We will prove this later.) Suppose you have a real number a, and have proved that a is positive (that is, $a > 0$). Then you can draw the conclusion that $a + \frac{1}{a} \geq 2$ by using the "for all...implies" combination, as follows:

   1. $(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)$ [Fact proven before]
   2. $a > 0\,.$[Known]
   3. $a > 0 \Longrightarrow a + \frac{1}{a} \geq 2\,.$[Rule $\forall_{use}$, from Step 1]
   4. $a + \frac{1}{a} \geq 2\,.$[Rule $\Longrightarrow_{use}$, from Steps 2,3]

6.7.3 Proving an implication (Rule $\Longrightarrow_{prove}$)

The rule for proving an implication (Rule $\Longrightarrow_{prove}$)

Suppose P, Q are sentences. Suppose you start a proof with "Assume P", and you prove Q. Then you can go to $P \Longrightarrow Q$.

Example 31. Say you are a Martian who just landed on Earth, you know nothing about the days of the week, and you want to prove that to your own satisfaction that "If today is Friday then tomorrow is Saturday". To apply Rule $\Longrightarrow_{prove}$, you would begin by "assuming that today is Friday." This means that you would imagine that today is Friday, and see what would happen in that case. For example, you could go to a public library and look at lots of newspapers published on a Friday, and you would see that every time such a paper talks about the following day it says something like "tomorrow is Saturday." Then you would be reasonably confident that the sentence "If today is Friday then tomorrow is Saturday" is true. And it would not matter whether today is Friday or not. □

6.7.4 The connectives "$\wedge$" and "$\Longrightarrow$" are very different

Students sometimes think that "If P then Q" is basically the same as "P and Q", or "P then Q". But this is very wrong and it important that you should understand the difference between "P and Q" and "If P then Q".

Take, for example, the sentences

Today is Friday and tomorrow is June 12.

and

If today is Friday then tomorrow is June 12.

Using "P" to represent the sentence "Today is Friday" and "Q" to represent the sentence "Tomorrow is June 2", the first sentence is $P \wedge Q$, and the second one is $P \Longrightarrow Q$.

What conditions have to be satisfied for $P \wedge Q$ to be true? What conditions have to be satisfied for $P \Longrightarrow Q$ to be true?

The sentence $P \wedge Q$ is true if both P and Q are true. In our example, the only way the sentence “Today is Friday and tomorrow is June 12” can be true is if today is Friday and tomorrow is June 12, So ***the sentence “Today is Friday and tomorrow is June 12” is true if today is Friday June 11, and in no other case***.

On the other hand, ***The sentence $P \Longrightarrow Q$ when Q is true, and also when P is false. And if neither one of these conditions hold (that is, if Q is false and P is true) then $P \Longrightarrow Q$ is false***. So, in our example, the only possible situation when “If today is Friday then tomorrow is June 12” would be false is if today is Friday but tomorrow is not June 12. So ***he sentence “If today is Friday then tomorrow is June 12” is true if today is not Friday, is also true if tomorrow is June 12, and is false if today is Friday but tomorrow is not June 12***.

We can summarize these observations by means of the following “truth tables” for the connectives “$\wedge$” and “$\Longrightarrow$”:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The first table gives you the truth value[49] of $P \wedge Q$ in terms of the truth values of P and Q, and the second table gives you the truth value of $P \Longrightarrow Q$ in terms of the truth values of P and Q.

Notice that ***what makes the truth tables for “wedge” and “$\Longrightarrow$” is the last two lines***. In particuler:

[49] Every sentence, when used correctly, has a ***truth value***: the truth value is T is the sentence is true, and F is the sentence is false. For example: the truth value of “$3 > 5$” is F, the truth value of “$3 < 5$” is T. How about the truth value of “$x < 5$”. If you tell me that $x < 5$ without having told me who x is, then I do not knwo the truth value of “$x < 5$”. But this would be an incorrect us of “$x < 5$”. If you were writing a proof, then you could never have “$x < 5$” as one of the steps, unless you have told the reader before, in some previous step, who x is, and once you have done that, the truth value of “$x < 5$” would be known. For example, if you said in a previous step “Let $x = \frac{1+\sqrt{5}}{2}$”, then I would know that “$x < 5$” is true. (Proof: $\sqrt{5} < 5$. So $1 + \sqrt{5} < 6$. So $\frac{1+\sqrt{5}}{2} < 3$. Hence $\frac{1+\sqrt{5}}{2} < 5$. So $x < 5$.)

$P \Longrightarrow Q$ is always true when Q is true, no matter whether P is true or false.

and

$P \Longrightarrow Q$ is always true when P is false, no matter whether Q is true or false.

So for example, the following sentences are true:

- If the Earth is a planet then 3 is a prime number.
- If the Earth is a comet then 3 is a prime number.
- If the Earth is a comet then 6 is a prime number.

The first one and the second one are true because the conclusion (that is, "3 is a prime number) is true. . (It does not matter, for the second sentence, that the premiss—"the Earth is a comet"— is false.)

And the second one and third one are true because the premiss ("the Earth in a comet" is false. (It does not matter whether for the second sentence, that the conclusion—"6 is a prime number"— is false.)

On the other hand, the sentence "If the Earth is a planet then 6 is a prime number" is false, because the premiss ("The Earth is a planet") is true, but the conclusion ("6 is a prime number") is false.

6.7.5 Isn't the truth table for $\Longrightarrow$ counterintuitive?

Students often ask questions about the implication connective $\Longrightarrow Q$ and in partuclar about the truth table for the implication.

One often raise question is "how can '$P \Longrightarrow Q$' be true if P and Q have nothing to do with each other?".

For example, we said that the sentence "If the Earth is a planet then 3 is a prime number" is true, but what does the fact that the Earth is a planet have to do with 3 being a prime number? That sounds like a good question, but let us think about it. I suggest that you do do this:

Think of "$P \Longrightarrow Q$" as saying "it does not happen that P is true without Q also being true".

In other words: what "$P \Longrightarrow Q$" does is exclude the possibility that you might ever run into a "bad situation", menaing, "a situation where P is true but Q is not". And this is the only possibilty excluded the implication. So, in particular,

- if P is false then you will not be in a bad situation, so "$P \Longrightarrow Q$" is true.
- if Q is true then you will not be in a bad situation, so "$P \Longrightarrow Q$" is true.

Once you understand this, you will see that it does not matter very much whether P and Q have something to do with each other. Maybe $P$and Q are totally unrelated, but if, for example, they both happen to be true then "$P \Longrightarrow Q$" is true. And also, "$P \Longrightarrow Q$" will be true if both P and Q are false, or if P is false and Q is true.

Example 32. Suppose a street sign says:

IF YOU ARE DRIVING AT MORE THAN 25MPH YOU WILL GET A FINE.

Supoose you want to prove to a friend of yours that the municipal government that put up the sign isn't really enforcing its own rule. What do you have to do to prove this?

Let "P" represent the premiss, i.e., "you are driving at more than 25mph", and let "Q" represent the conclusion, that is, "you will get a fine". Then the street sign asserts the implication "$P \Longrightarrow Q$".

Certainly,

- If you find someone driving at 20mph, that will do nothing to prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter whether that driver got a fine or not[50].

- If you find someone who got a fine, that will do nothing to prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter whether that driver was driving at more than 25mph or not.[51].

- The only way to prove that the injunction in the street sign is not being enforced is to find cases of drivers that were driving at more than 25mph but did not get a fine. ***That's because the onlt case when the implication "$P \Longrightarrow Q$" is false, according to the truth table for the implication, is when the premiss is true but the conclusion is false.***

Example 33. Alice is a cashier at a department store, and she has to follow the rule that

> ***IF A CUSTOMER PAYS CASH FOR A PURCHASE THEN ALICE HAS TO PUT THE MONEY SHE COLLECTED IN A DRAWER.***

Suppose you are a detective and you want to prove that Alice is not obeying the rule. What do you have to do?

- If you find a situation when there was not customer at all, or there was customer that did not pay cash, then that will do nothing prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter whether Alice put money is the drawer or not[52].

[50] The driver may have been given a fine for some other reason, e.g., using a cell phone while driving.

[51] The driver may have been driving at 20mph but may have been given a fine for some other reason, e.g., using a cell phone while driving.

[52] Why would Alice have put money in the drawer if she did not collect any cash from the customer? Who knows?

- If you find a situation where Alice put cash in the drawer even though she did not collect any money from a customer, then that will do nothing to prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter that there was no customer poaying cash[53].

- The only way you can prove that Alice is violating the rules is by showing that a customer paid cash but Alice did notput themoney in the drawer. ***That's because the only case when the implication "$P \Longrightarrow Q$" is false, according to the truth table for the implication, is when the premiss is true but the conclusion is false.***

Example 34. Suppose you have a natural number n, but you do not know which number it is. (For example, maybe someone gave you a sealed envelope containing a card where the number is written. So the number is there, it's a fixed number, but you just do not knwo which specific number it is.)

Suppose you are asked to prove that

(*) If n is even then n^2 is divisible by 4.

Then you could ask: could (*) possibly be false? Could there be a possible value of n for which (*) is false. (Remember that you do not know who n is. So if you want be able to assert for sure that (*) is true you have to consider all possible values of n. If you find one value of n for which (*) is not true, then you cannot be sure that n is true, because the number that you have in the envelope could be the one you have found, the one for which (*) is false. But if you can make sure that no such number exists, then you can be sure that (*) is true, even though you do not know who n is.)

What would have to happen for (*) to be false? Well, according to our truth table, the only case when the implication (*) is false is when the premiss is true but the conclusion is not. So to make sure that (*) is true, you have to consider numbers n that are even, because if n is not even then (*) is true. You indicate that you are going to do that by writing:

[53] Again, why would Alice put money in the drawer even if she did not collect the money from a customer? Who knows? And who cares? The point is: ***even if she put money in the drawer when there had been no customer that paid her the money, so P was false but Q was true, she did not violate the rules.***

Assume that n is even.

(In other words: ***you are allowed to assume that*** n ***is even because if*** n ***is not even then (*) is automatically true thanks to the truth table for the implication.***)

And then you move on to prove that n^2 is divisible by 4. (Since n is even, we can pick a natural number k such that $n = 2k$. Then $b^2 = 4k^2$, so n^2 is divisible by 4.)

And now you can be sure that (*) is true. The number n is even or odd, but in either case (*) is true, even though in each case it's true for a different reason: if n is not even, then (*) is true because of the truth table for the implication, and if n is even then (*) ia true because in that case we have proved that the conclusion (that is, "n^2 is divisble by 4") must be true.

Finally, we have prove that (*) must be true for any natural number, because we have proved for n, but n could be any number. So we can conclude that

$$(\forall n \in \mathbb{N})\Big(n \text{ is even} \Longrightarrow n^2 \text{ is divisible by } 4\Big)\,,$$

or, if you prefer,

$$(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big)\,.$$

So we can structure our proof as follows:

THEOREM. $(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big)$.

PROOF We want to prove that $(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big)$.

Let $n \in \mathbb{N}$ be arbitrary.

We want to prove that $2|n \Longrightarrow 4|n^2$.

Assume that $2|n$.

Then $(\exists k \in \mathbb{N})n = 2k$.

Pick one such k and call it k_*.

Then $k_* \in \mathbb{N}$ and $n = 2k_*$.

Then $n^2 = (2k_*) \cdot (2k_*) = 4k_*^2$.

Let $q = k_*^2$.

Then $n^2 = 4q$.

So $(\exists k)n^2 = 4k$.

Hence $4|n^2$.

We have proved that $4|n^2$ assuming that $2|n$. Hence

$$2|n \Longrightarrow 4|n^2\,.$$

We have proved that $2|n \Longrightarrow 4|n^2$ for an arbitrary n. Therefore

$$(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big)\,.$$

Q.E.D.

I hope that these remarks will suffice to clarify they way implication works. Implication will be discussed in great detail later.

6.8 Biconditionals ("$\Longleftrightarrow$", i.e., "if and only if")

The ***biconditional*** is the symbol

$$\boldsymbol{\Longleftrightarrow}.$$

It is a *binary connective*, like $\wedge$, $\vee$, and $\Longrightarrow$. That means that $\Longleftrightarrow$ ***can be used to connect two sentences***.

If P and Q are sentences, the sentence "$P \Longleftrightarrow Q$" is read as

$$\boxed{P \text{ if and only if } Q}$$

or

$$\boxed{P \text{ is equivalent to } Q}\,.$$

And mathematicians often use "iff" as shorthand for "if and only if", so they write "P iff Q."

$$\boxed{P \text{ iff } Q}\,.$$

The precise meaning of "equivalence" will be explained later. But, if you want to know right away what it means, it's very simple:

When you know that P is equivalent to Q then you can pass freely from P to Q. That is, if you know that P is true then you can write Q, and if you know that Q is true then you can write P.
So for all practical purposes if "$P \iff Q$" is true then P and Q are interchangeable.

6.8.1 The meaning of "if and only if"

You should think of "P iff Q" as meaning

$$(P \iff Q) \wedge (Q \iff P)\,.$$

That is, "$P \iff Q$" means[54]

If P then Q and if Q then P,

or

P implies Q and Q implies P.

In order to make this true, we will choose the rules for proving and using biconditional sentences as follows:

[54] *This note is only for philosophically minded nitpickers.* What does "means" mean? The point of view adopted here is that *the meaning of a word, phrase or symbol consists of the rules for the use of that word, phrase or symbol.* For example, the meaning of "and" is the specification that if P, Q are two sentences, then (i) if you have "P and Q" you can go to P and you can go to Q, and (ii) if you have P and you have Q then you can go to "P and Q." That is, *the meaning of "and" is captured by Rules $\wedge_{use}$ and $\wedge_{prove}$.* Naturally, this does not cover all the uses of "and" in our culture, such as, for example, to indicate a progression (as in "this is getting better and better"), or to indicate a causal relation, (as in "do that and I'll hit you"), or the literary use full of nuances (as 'in 'tomorrow and tomorrow and tomorrow"). And, most importantly for us, it does not cover the use of "and" to connect *nouns*, as in "slings and arrows". But it's what "and" means in logic and mathematics. If you want to program a computer so that it will know what "and" means, you have to tell the computer how to use "and". And this amounts to programming the computer to use rules $\wedge_{use}$ and $\wedge_{prove}$. And you don't need to tell the computer anything else. A similar situation arises with the biconditional. A computer that "knows" the rules $\iff_{use}$ and $\iff_{prove}$ "knows" all it needs to know to work with the biconditional, and for that reason I believe that knowing the meaning of "$\iff$" amounts to knowing the two rules for working with it.

- *To prove "$P \iff Q$" you do exactly the same thing that you would do to prove $(P \iff Q) \wedge (Q \iff P)$.*
- *To use "$P \iff Q$" you do exactly the same thing that you would do to use $(P \iff Q) \wedge (Q \iff P)$.*

So, for example, suppose you want to prove that

$$(\forall x \in \mathbb{R})\Big(x^2 = 4 \iff (x = 2 \vee x = -2)\Big)\,. \qquad (6.136)$$

Then you would start by introducing into your proof an arbitrary real number called x, and then you would prove that

$$(x^2 = 4 \iff (x = 2 \vee x = -2)\,. \qquad (6.137)$$

And to prove (6.137), which is an "iff" sentence, you would prove both implications $x^2 = 4 \Longrightarrow (x = 2 \vee x = -2)$ and $(x = 2 \vee x = -2) \Longrightarrow x^2 = 4$. (The proof of these two sentences is very simple: to prove that $x^2 = 4 \Longrightarrow (x = 2 \vee x = -2)$, you use the fact that a positive real number r cannot have more than two square roots[55]. Since 2 and -2 are two distinct square roots of 4, there cannot be a third square root. So, if $x^2 = 4$, so x is a square root of 4, it follows that x must be 2 or -2. So $x^2 = 4 \Longrightarrow (x = 2 \vee x = -2)$. To prove the other implication, i.e., that $(x = 2 \vee x = -2) \Longrightarrow x^2 = 4$, just observe that if $x = 2$ then $x^2 = 4$, and if $x = -2$ then $x^2 = 4$ as well,)

6.8.2 The rules for proving and using biconditionals

Now let us state explicitly the rules for proving and using biconditional sentences.

As I explained in the previous subsection, *these rules are designed so as to make "$P \iff Q$" mean precisely what we want it to mean, that is "$(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$".*

The rules are as follows.

[55] This was proved in the notes for Lectures 2,3,4 but, just in case, here is a quick proof: suppose r has three distinct square roots a, b, c. Then $a^2 = r$, $b^2 = r$ and $c^2 = r$. Hence $a^2 - b^2 = 0$. So $(a-b)(a+b) = 0$. Therefore $a - b = 0$ or $a + b = 0$. Since a and b are different, it cannot be the case that $a - b = 0$, so $a + b$ must be zero, and then $b = -a$. Now we can use exactly the same argument with c instead of b, and conclude that $c = -a$. But then $c = b$, contradicting the fact that $b \neq c$.

Rule $\Longleftrightarrow_{prove}$

If P, Q are sentences, and you have proved the sentences

$$P \Longrightarrow Q$$

and

$$Q \Longrightarrow P\,,$$

then you can go to

$$P \Longleftrightarrow Q\,.$$

Rule $\Longleftrightarrow_{use}$

If P, Q are sentences, and you have proved the sentence

$$P \Longleftrightarrow Q\,,$$

then you can go to

$$P \Longrightarrow Q$$

and you can also go to

$$Q \Longrightarrow P\,.$$

6.9 The other six rules

So far I have given you eight rules, two for each of the connectives $\wedge$, $\vee$, $\Longrightarrow$, and $\Longleftrightarrow$.

In addition, there are six more rules that we have already discussed:

1. Rule $\forall_{prove}$, the rule for proving a universal sentence. (This rule is sometimes called "universal generalization".)

2. Rule $\forall_{use}$, the rule for using a universal sentence. (This rule is sometimes called the "specialization rule".)

3. Rule $\exists_{prove}$, the rule for proving an existential sentence.. (This rule is sometimes called the "existential generalization rule".)

4. Rule $\exists_{use}$, the rule for using a universal sentence. (This rule is sometimes called the "existential specialization rule".)

5. The proof by contradiction rule.

6. Rule SEE, substitution of equals for equals (also called "Rule $=_{use}$").

So ***we now have all fourteen rules!***

6.10 Are the logical rules hard to understand and to learn and remember ?

Most of the logical rules are very simple and easy to remember. For example,

- The rules for using and proving $\wedge$ sentences are so stupid that you might object to having them because they are so obvious, but you certainly cannot find it hard to understand them.
- The rules for using and proving universal sentences are also natural:
  - if you know that all the items in this store cost 1 dollar, and you pick an item in this store, you can be sure that it costs 1 dollar. That's all that Rule $\forall_{use}$ says.
  - if you prove that a schmoo must be green, without using any information about that schmoo other than the fact that it is a schmoo, then you can conlude that all schmoos are green. And that's= all that Rule $\forall_{prove}$ says.
- And the rules for using and proving existential sentences are natural as well:
  - if you know that somewhere in this store there is a schmoo, then you can go and get a schmoo and call it any way you want, for example "my woderful schmoo". That's all that Rule $\exists_{use}$ says.
  - if you find a schmoo, then you can conclude that schmoos exist. And that's all that Rule $\exists_{prove}$ sats.

6.10.1 Proofwriting and rules for proofs

Writing proofs is like playing chess, checkers, or some other board game.

- There are rules that tell you which moves are allowed. (Notice that the rules for proofs never say "you ***have*** to do this". They say "you ***are allowed*** to do this". It's exactly like the moves you are allowed to make in a board game.)
- You have to obey the rules all the time.
- If you cheat, by violating the rules once, then you are out of the game.
- If you know how to play, you will never make a move that violates the rules.
- Once you know the moves, then the hard part begins: you have to figure out how to choose which moves to make in order to win. And that is where proofwriting becomes difficult and challenging: some people are better than others at figuring out how to win.
- From 1637 until 1995, many mathematicians tried very hard to prove Fermat's last theorem. Finally, Andrew Wiles suceeded in doing it in 1995.
- But the proofs we do in this course are not that hard.

7 What is a proof, really?

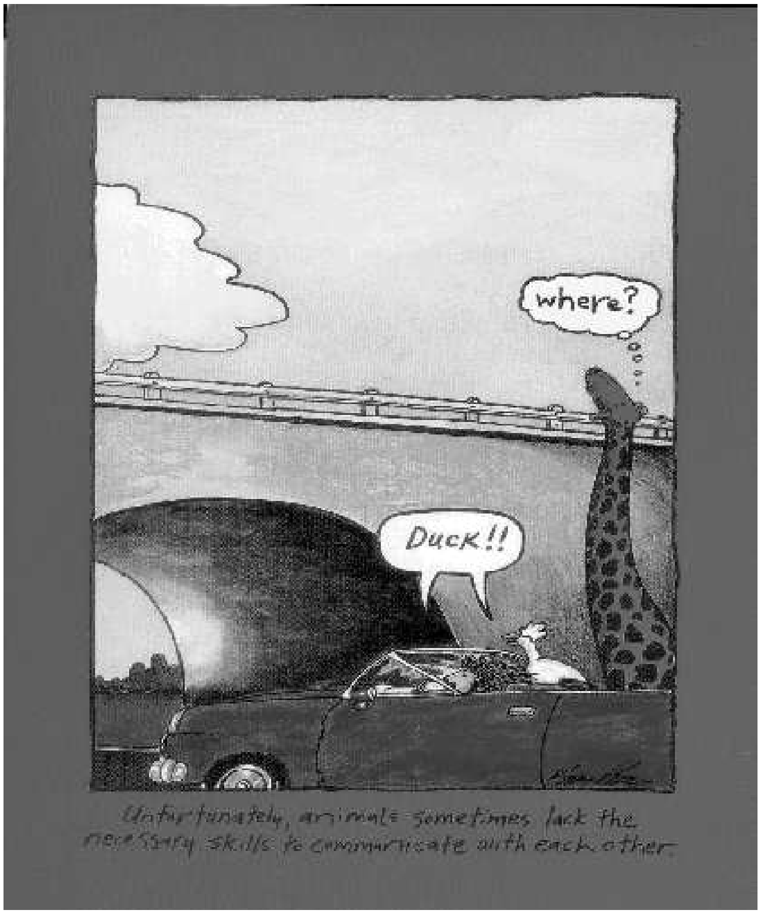
> Proofs employ logic but usually include some amount of natural language which usually admits some ambiguity. In fact, the vast majority of proofs in written mathematics can be considered as applications of rigorous informal logic. Purely formal proofs, written in symbolic language instead of natural language, are considered in proof theory. The distinction between formal and informal proofs has led to much examination of current and historical mathematical practice, quasi-empiricism in mathematics, and so-called folk mathematics (in both senses of that term). The philosophy of mathematics is concerned with the role of language and logic in proofs, and mathematics as a language.
>
> From the *Wikipedia* article on “Mathematical Proof”.

So far, we have been talking about “proofs” but I have not given you a completely precise definition of what a proof is. This is so for a reason: as the statement from *Wikipedia* quoted above says, the “proofs” we normally write “include some amount of natural language[56]”, and that means that they “admit some ambiguity”. (The precise meaning of “ambiguity” is “a situation where a statement occurs whose meaning has several different possible interpretations. Examples of ambiguous statements are “The university president promised to stop drinking on campus”, “I am having an old friend for dinner[57]”, “Duck!”, “A passerby helped a dog bite victim”, “One morning I shot an elephant in my pajamas[58].)”.

[56] That is, English, or French, or Chinese, or whatever language we are writing in.

[57] A line spoken by Hannibal Lecter in the 1991 film *The Silence of the Lambs*

[58] Line spoken by Groucho Marx in the 1930 film *Animal Crackers*. But Groucho then says “How he got in my pajamas, I don’t know”, and that removes the ambiguity.



Unfortunately, animals sometimes lack the necessary skills to communicate with each other

Since natural language always contains some ambiguity, mathematicians have given up on the idea of having a completely precise definition of "proof" that would apply to proofs that we write in semiformal language[59]

Wnat mathematicians have been able to do, instead, is this:

1. We have a completely precise definition of "proof" for proofs written in formal language.

2. For proofs written in natural language or semiformal language, we regard these proofs as narratives explaining to the reader how a true proof in formal language could be written.

[59] Semiformal language is a language that is a mixture of formal language and natural language. All the proofs we have written so far are in smeiformal language.

For example, in a proof in semiformal language we could write, after we have introduced an integer called a, and proved that $2|a$ (that is, that a is even):

(*) Since a is even, we pick an integer k such that $a = 2k$.

This tells the reader "I know how to go from '$2|a$' to '$k \in \mathbb{Z} \wedge a = 2k$' in a precise, rigorous way, in formal language, and I hope you accept this. If you don't know how to do it, or you don';t believe that I know how to do it, then I can show you".

The reader will probably understand how this could be done in formal language, following the rules for proofs, and will leave it there.

But, in case the reader does not know, or does not believe that the author knows, here is how the author could do it in formal language:

(i) $2|a$.

(ii) $(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})\Big(m|n \Longleftrightarrow (\exists k \in \mathbb{Z})n = mk\Big)$ [Definition of "|"]

(iii) $(\forall n \in \mathbb{Z})\Big(2|n \Longleftrightarrow (\exists k \in \mathbb{Z})n = 2k\Big)$ [Rule $\forall_{use}$ from (ii)]

(iv) $2|a \Longleftrightarrow (\exists k \in \mathbb{Z})a = 2k$ [Rule $\forall_{use}$ from (iii)]

(v) $2|a \Longrightarrow (\exists k \in \mathbb{Z})a = 2k$ [Rule $\Longleftrightarrow_{use}$ from (iv)]

(vi) $(\exists k \in \mathbb{Z})a = 2k$ [Rule $\Longrightarrow_{use}$ from (i),(vi)]

(vii) Pick a witness for (vi) and call it k, so $k \in \mathbb{Z} \wedge a = 2k$. [Rule ($\exists_{use}$, from (vi)]

3. Writing (*) is of course much shorter than writing the seven steps listed above. And the reader can figure out easily how those seven steps would go, so there is no need for the author to spell them out.

   But sometimes a reader may not agree that an author really has a proof in formal language. The author may say "I don't see how step (*) goes". In that case, the way to decide who is right is very simple: If the author can do it in formal language, then the author is right. If the author cannot do it in formal language, then the author does not have a proof.

4. A situation where an author writes a proof, some readers are not convinced and ask for a detailed proof in formal language, the author provides such a proof, and the readers do no agree that it is a proof, will almost never arise, because once you have written a text in formal language then it is either clear to everybody that it is corect, or clear clear to everybody that it is not corect[60]

5. For this reason, ***in mathematics it is very rare for a dispute as to whether a proof is right to remain unsettled for a long time***. A famous example of this is the 1995 proof by Andrew Wiles of Fermat's Last Theorem. Wiles announced his proof on June 23 1993. In September 1993 an arror in the proof was found. But there was no dispute. Wiles acknowledged immediately that the proof had an error. And then he went to work trying to fix it. It took him a year, until on September 19 1994 he figured out how to give a completely correct proof. The proof was published in 1996. Many mathematians have read it, and they all agree that the proof is right.

[60] A good analogy is the game of chess. If a player makes a move and the other player claims that this move is forbidden, the matter will be settled very quickly, because the rules for which moves are permitted in chess and which moves are not permitted are very clear and precise, so it will never happen that two players disagree about a move and go on disagreeing for ever. Compare this with, say, the rules set up by the U.S. Constituion. One clause in the Consitution says that to be eligible for holding the office of President or Vice President a person has to be a "natural-born citizen of the United Staes". But the Constitution does no say what "natural-born citizen" means. So disputes about the meaning of this rule continue and will continue forever. For example, Ted Cruz was born in Canada, his mother was a U.S. citizen, and his father was born in Cuba but became a naturalized U.S. Citizen. Did that make Ted Cruz eligible? Senator Cruz's supprters say "yes", his opponents say "no" and there is no way to settle this dispute.

7.1 The precise definition of "proof" in formal language

A ***proof in formal language***. or ***formal proof***, is a sequence of steps, such that

1. Each step consists of a closed sentence[a] in formal language, possibly preceded by the words "assume that" or by the word "Let" or by the words "Pick a witness for ... and call it ..., so"

2. In each step one of the following is true:

   (i) The step introduces an assumption A, by saying "Assume that A",

   (ii) The step declares a value for a variable ξ, by saying "Let $\xi = \cdots$" or "Let ξ be arbitrary", or "Let $\xi \in S$ be arbitrary", for some set S..

   (iii) The step declares a value for a variable ξ by saying "Pick a witness for $\cdots$ and call it ξ, so $\cdots$".

   (iv) The step follows from previous steps by one of the fourteen logical rules.

   (v) The step is a sentence known to be true for one of the following reasons:

      (a) the sentence appears as a previous step in the proof[b],

      (b) the sentence is a theorem that we are allowed to use,

      (c) the sentence is a definition,

      (d) the sentence is an axiom.

[a] A ***closed sentence*** is a sentence that has no open variables. This means that every variable that appears in the sentence either has a value declared in a previous step, or is under the scope of a quantifier.

[b] This just says that you are allowed to repeat a previous step

7.2 Some "pure logic" proofs

In this section we temporaraily forget about mathematics, and do some "pure logic".

As far back as in classical Greece, people realized that there are inferences[61] that are valid by virtue of the form of the sentences involved. For example, the inference

	All men are mmortal.
	Socrates is a man.
Therefore	Socrates is mortal.

is valid. (A ***valid inference*** is one in which the conclusion follows from the premises.)

But it is clear that it does not matter very much who Socrates is, what "man" means, or what "mortal" means. For example, the following inferences are equally valid:

Inference 2:

	All men are immortal.
	Socrates is a man.
Therefore	Socrates is immortal.

(In this case, one of the premises and the conclusion are false, but the inference is valid, in the sense that the conclusion is a consequence of the premises: if the premises were true, the conclusion would have to be true as well.)

Inference 3:

	All Klingons are mortal.
	Gnugnuux is a Klingon.
Therefore	Gnugnuuux is mortal.

Inference 4:

	All borogoves are mimsy.
	Gnugnuux is a borogove.
Therefore	Gnugnuuux is mimsy.

[61] An ***inference*** is a deduction, in which a ***conclusion*** is derived from some ***premises***, in the sense that we assert that the conclusion follows from the premises, meaning that the conclusion must betrue if the premises are true.

Let's just look at Inference No. 4. You probably have no idea what a "borogove" is[62], or what "mimsy" means, or who "Gnugnuuux" is, but I am sure it is clear to you that, if it is true that all borogoves are mimsy and that Gnugnuux is a borogove, then undoubtedly Gnugnuuux is mimsy.

What seems to be happening here is that there are certain inferences that are valid just because of the ***form*** of the sentences involved. For example, all the inferences in the above examples are of the form

(*)		All X are Y.
		A is an X.
	Therefore	A is a Y.

The general principle then seems to be: every inference of the form (*) is valid.

And this observation suggests a general idea:

- Sentences have a "form". (For example, the sentences "All men are mortal", "All men are immortal", "All Klingons are mortal", 'All borogoves are mimsy", are all of the form "All X are Y".)
- The validity of many inferences just depends on the form of the sentences involved.

This idea leads to a program for developing the science of logic: try to find and list all the valid inference forms. (An 'inference form" is the specification of one or two or three "forms of premises" and a "form of the conclusion". A valid inference form is an inference form such that, if we plug in actual sentences for the sentence forms involved, then the conclusion istrue if thee premises are true. For example, the inference form (*) is valid because, if we plug in actual sentences

And there are inferences that are valid just by virtue of the form of the sentences involved.

In classical Greece and the Middle Ages, logicians and philosophers singled out several forms of "syllogisms" (i.e., inferences in which a conclusion follows from two premises by virtue of the ***form*** of the sentences involved, and gave them various names such as *Barbara*, *Celarent*, *Darii*, *Ferioque*, *Baroco*, *Bocardo*, *Barbari*, *Celaront*, *Camestros*, *Felapton*, *Darapti.*

[62] Unless you have read Lewis Carroll's *Alice* books

In the Nineteenth Centtury, it became clear that this list of valid inferences was insuficient to capture the needs of mathematical reasoning, and a new form of logic, called the "predicate calculus", was developed.

This is the logic we have been presenting gradually in these notes. The equivalent for us of the classical syllogisms are our logical rules.

For example, take the *Modus Ponens Rule* , i.e., Rule $\Longrightarrow_{use}$:

$$\begin{array}{lll} (\Longrightarrow_{use}) & & P \\ & & P \Longrightarrow Q \\ & \text{Therefore} & Q \end{array}$$

and the *Specialization Rule*, i.e., Rule $\forall_{use}$:

$$\begin{array}{lll} (\forall_{use}) & & (\forall x \in S)P(x) \\ & & a \in S \\ & \text{Therefore} & P(a) \end{array}$$

These infereences are valid *no matter* which sentences P, Q, predicate $P(x)$, set S, and object a we plug in.

Using this, we can do complicated proofs using only logic, without bringing in any details about the actual sentences involved.

In order to make this apparent, we introduce the notion of ***sentence form***: a sentence form is an expression such as $A \wedge (\forall x \in S)P(x)$, or $(\forall x \in S)(\exists y \in T)P(x, y)$, in which A, $P(x)$, $P(x, y)$ are just symbolic expressions for which one can plug in sentences or predicates. For example, in the sentence form $(\forall x \in S)(\exists y \in T)P(x, y)$, if we plug in for $P(x, y)$ the 2-variable predicate "y is x's mother" and we take S and T to be the set of all people, then we get the sentence "every person has a mother". If, on the other hand, we plug in for $P(x, y)$ the 2-variable predicate "y is a shoe size that fita x", we take S to be the set of all people, and T to be the set of all shoe sizes, then we get the sentence "for every person there is a shoe size that fits him/her".

So we say that ***the sentences "every person has a mother". and "for every person there is a shoe size that fits him/her" are of the form*** $(\forall x \in S)(\exists y \in T)P(x, y)$, in which A.

Using the rules of logic, one can prove certain sentence forms without plugging in particular predicates or sentences. Any sentence that can be proved that way is said to be logically valid. And, if you know that a certain sentence form is logically valid, then every sentence of that form is true.

Example 35. We are going to see soon that the sentence form

$$\Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \Longleftrightarrow (\forall x \in S)\Big(P(x) \wedge Q(x)\Big) \qquad (7.138)$$

is logically valid.

This means that if you plug in any set for S and any two one-variable predicates for $P(x)$ and $Q(x)$ then you get a true sentence.

And, indeed, the following sentences are true:

1. Everybody likes tea and everybody likes coffee if and only if everybody likes tea and coffee.

2. I work every day and I sleep every day if and only if I work and sleep every day.

3. All borogoves are mimsy and all borogoves are slippy[63] if and only if all borogoves are mimsy and slippy.

And here is the proof that (7.138) is a logically valid sentence form.

Theorem 11. *The sentence form (7.138) is logically valid.*

1. Assume $(\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)$.
2. Let $u \in S$ be arbitrary.
3. $(\forall x \in S)P(x)$. [Rule $\wedge_{use}$, from step 1]
4. $(\forall x \in S)Q(x)$. [Rule $\wedge_{use}$, from step 1]
5. $P(u)$. [Rule $\forall_{use}$, from step 3]
6. $Q(u)$. [Rule $\forall_{use}$, from step 4]
7. $P(u) \wedge Q(u)$. [Rule $\wedge_{prove}$, from steps 5,6]
8. $(\forall u \in S)\Big(P(u) \wedge Q(u)\Big)$. [Rule $\forall_{prove}$, from steps 2,7]
9. $(\forall x \in S)\Big(P(x) \wedge Q(x)\Big)$. [Change of variables]
10. $\Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \Longrightarrow (\forall x \in S)\Big(P(x) \wedge Q(x)\Big)$.[Rule $\Longrightarrow_{use}$] from steps 1,9]
11. Assume $(\forall x \in S)\Big(P(x) \wedge Q(x)\Big)$.
12. Let u be arbitrary.
13. $P(u) \wedge Q(u)$. [Rule $\forall_{use}$, from step 11]

[63] If you don't know what "slippy" means, don't worry. I don't either. But it does no matter: the sentence is true.

14. $P(u)$. [Rule $\wedge_{use}$, from step 13]
15. $(\forall u \in S)P(u)$. [Rule $\forall_{prove}$, from steps 12,14]
15. $(\forall x \in S)P(x)$. [Change of variables]
16. Let u be arbitrary.
17. $P(u) \wedge Q(u)$. [Rule $\forall_{use}$, from step 11]
18. $Q(u)$. [Rule $\wedge_{use}$, from step 17]
19. $(\forall u \in S)Q(u)$. [Rule $\forall_{prove}$, from steps 16,17]
20. $(\forall x \in S)Q(x)$. [Change of variables]
21. $(\forall x \in S)P(x) \wedge (\forall x)Q(x)$. [Rule $\wedge_{prove}$, from steps 15,20]
22. $(\forall x \in S)\Big(P(x) \wedge Q(x)\Big) \Longrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)$. [Rule $\Longrightarrow_{prove}$, from steps 11,21]
23. $\Big((\forall x \in S)P(x) \wedge (\forall x)Q(x)\Big) \Longleftrightarrow (\forall x \in S)\Big(P(x) \wedge Q(x)\Big)$. [Rule $\Longleftrightarrow_{prove}$, from steps 10,22]

Q.E.D.

On the other hand, there are lots of sentences that are not true. If A is such a sentence, and S is a sentence form such that A is of the form S, then S cannot be provable, because if S could be proved then every sentence of the form S, including A, would have to be true.

This suggests a method for proving that a sentence form F is not logically valid: find a sentence of the form F which is not true.

Here is an example,

Theorem 12. *The sentence form*

$$\Big((\forall x)P(x) \vee (\forall x)Q(x)\Big) \Longleftrightarrow (\forall x)\Big(P(x) \vee Q(x)\Big) \tag{7.139}$$

is not logically valid.

Proof. To prove that (7.139) is not logically valid, it suffices to exhibit examples of one-variable predicates $p(x)$, $q(x)$ for which the sentence

$$\Big((\forall x \in S)p(x) \vee (\forall x \in S)q(x)\Big) \Longleftrightarrow (\forall x \in S)\Big(p(x) \vee q(x)\Big) \tag{7.140}$$

is not true.

Let us take $p(x)$ to be the sentence "x is a Democrat", and $q(x)$ to be the sentence "x is a Republican", and let S be the set of all U.S. Representatives.

Then the sentence "$(\forall x \in S)p(x) \vee (\forall x \in S)q(x)$" says "either all the representatives are Democrats or they are all Republicans", which is false. And the sentence "$(\forall x \in S)\Big(p(x) \vee q(x)\Big)$"says "every representative is a Democrat or a Republican", which is true. So the biconditional sentence (7.140) is false.

Now let us give a mathematical example. Let us take $p(x)$ to be the sentence "x is even", and $q(x)$ to be the sentence "x is odd", and let S be the set of all integers.

Then the sentence "$(\forall x \in S)p(x) \vee (\forall x \in S)q(x)$" says "either all the integers are even or they are all odd", which is false. And the sentence "$(\forall x \in S)\Big(p(x) \vee q(x)\Big)$" says "every integer is even or odd", which is true. So the biconditional sentence (7.140) is false.

Theorem 13. *The sentence form*

$$(\forall x \in S)(P(x) \Longrightarrow Q(x)) \Longrightarrow \Big((\forall x \in S)P(x) \Longrightarrow (\forall x \in S)Q(x)\Big) \quad (7.141)$$

is logically valid.

An example. Suppose S is the set of all people, $P(x)$ stands for "x likes tea" and $Q(x)$ stands for "x likes coffee".

Then

- "$P(x) \Longrightarrow Q(x)$" says "if x likes tea then x likes coffee".
- "$(\forall x \in S)(P(x) \Longrightarrow Q(x))$" says every person who likes tea likes coffee".
- "$(\forall x \in S)P(x)$" says "everybody likes tea".
- "$(\forall x \in S)Q(x)$" says "everybody likes coffee"
- "$(\forall x \in S)P(x) \Longrightarrow (\forall x \in S)Q(x)$" says "if everybody likes tea then everybdy likes coffee".
- sentence (7.141) says "if everybody who likes tea likes coffee, then if everybody likes tea then everybody likes coffee". which is clearly treu.

Proof.

1. Assume $(\forall x \in S)(P(x) \Longrightarrow Q(x))$.

2. Assume $(\forall x \in S)P(x)$.
3. Let $u \in S$ be arbitrary.
4. $P(u) \Longrightarrow Q(u)$. [Rule $\forall_{use}$, from step 1]
5. $P(u)$. [Rule $\forall_{use}$, from step 2]
6. $Q(u)$. [Rule $\Longrightarrow_{use}$, from steps 4,5]
7. $(\forall u \in S)Q(u)$. [Rule $\forall_{prove}$, from steps 3,6]
8. $(\forall x \in S)Q(x)$. [Change of variables]
9. $(\forall x \in S)P(x) \Longrightarrow (\forall x \in S)Q(x)$. [Rule $\Longrightarrow_{prove}$, from steps 2,8[
10. $(\forall x \in S)(P(x) \Longrightarrow Q(x)) \Longrightarrow \Big((\forall x \in S)P(x) \Longrightarrow (\forall x \in S)Q(x)\Big)$.
[Rule $\Longrightarrow_{prove}$, from steps 1,9[

Q.E.D.

Theorem 14. *The sentence form*

$$\Big((\forall x \in S)P(x) \Longrightarrow (\forall x \in S)Q(x)\Big) \Longrightarrow (\forall x \in S)(P(x) \Longrightarrow Q(x)) \quad (7.142)$$

is not logically valid.

Proof. To prove that (7.142) is not logically valid, it suffices to exhibit examples of one-variable predicates $p(x)$, $q(x)$ for which the sentence

$$\Big((\forall x \in S)p(x) \Longrightarrow (\forall x \in S)q(x)\Big) \Longrightarrow (\forall x \in S)(p(x) \Longrightarrow q(x)) \quad (7.143)$$

is not true.

Take S to be the set of all people. Let $p(x)$ stand for "x likes tea", and let $q(x)$ stand for "x likes coffee". Then

- "$(\forall x \in S)p(x)$" says "everybody likes tea", which is clearly false.
- "$(\forall x \in S)q(x)$" says "everybody likes coffee", which is also false.
- the implication "$(\forall x \in S)p(x) \Longrightarrow (\forall x \in S)q(x)$" says "if everybody likes tea then everybody likes coffee", which is clearly true, because it is an implication with a false premise.
- For a particular x, the open sentence $p(x) \Longrightarrow q(x)$ says "if x likes tea then x likes coffee". This is true of some people, but is not true of all people. (For example, if a is any person who likes tea but not coffee, then "$p(x) \Longrightarrow q(x)$" is false for $x = a$.)

- Therefore the sentence "$(\forall x \in S)(p(x) \Longrightarrow q(x))$" is false.
- So the sentence (7.143) is an implication whose premise is true and whose conclusion is false.
- Hence (7.143) is false.

7.3 A very important example: the order of the quantifiers matters

When we write formulas involving several different quantifiers, does the order of the quantifiers matter? For example, if a formula contains quantifiers $(\exists x \in S)$ and $(\forall y \in S)$, does it matter which one comes first?

The answer is ***it matters a lot.***

Here is an example:

Theorem 15. *The sentence forms* $(\forall x \in S)(\exists y \in S)P(x,y)$ *and* $(\exists y \in S)(\forall x \in S)P(x,y)$ *are not logically equivalent.*

Proof. We give an example of a two-argument predicate $p(x,y)$ such that $(\forall x \in S)(\exists y \in S)p(x,y)$ is true by $(\exists y \in S)(\forall x \in S)p(x,y)$ is false.

Let S be the set of all people, and let $p(x,y)$ stand for 'y is x's mother". Then

- "$(\forall x \in S)(\exists y \in S)P(x,y)$" says "everybody has a mother",
- "$(\exists y \in S)(\forall x \in S)P(x,y)$" says 'there is one person who is everybody's mother".

Clearly, "$(\forall x \in S)(\exists y \in S)P(x,y)$" is true, but "$(\exists y \in S)(\forall x \in S)P(x,y)$" is false. So the sentences are not logically equiva;ent. **Q.E.D.**

7.4 Examples of real proofs written fully in formal language

In this section we show some examples of true proofs, written completely in formal language, and not skipping any steps.

As you will see from these examples, a true proof, written in formal language, without skipping steps, can be extremely long. For that reason, once we know what a true formal proof really is, we never write true formal proofs. What we write is ***narratives*** in natural language (English, French, Chinese, Spanish, Italian, whatever) that tell the reader how you would go about writing a real proof.

These narratives are much shorter, but they have no value unless it is clear that behind the narrative there is a real proof.

If you write, for example, a vague statement that I don't see how to turn it into a real proof, then I will ask you "write this in formal language" and if yoiu cannot do it then you don't have a proof.

7.4.1 Proving that $2 + 2 = 4$ in only 15 steps

In this section we will prove that $2+2 = 4$. We will use the following axioms and definitions:

Definition 7.

$$2 = 1 + 1\,.$$

Definition 8.

$$3 = 2 + 1\,.$$

Definition 9.

$$4 = 3 + 1\,.$$

AXIOM 1. $1 \in \mathbb{R}$.

AXIOM 2. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y \in \mathbb{R}\,.$

AXIOM 3. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x + (y + z) = (x + y) + z\,.$

Theorem 16. $2 + 2 = 4$.

Proof.

[1.] $1 \in \mathbb{R}$. [Axiom 1]

[2.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y \in \mathbb{R}\,.$ [Axiom 2]

[3.] $(\forall y \in \mathbb{R})1 + y \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,2]

[4.] $1 + 1 \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,3]

[5.] $2 = 1 + 1$. [Definition 7]

[6.] $2 \in \mathbb{R}$. [Rule SEE, from steps 4,5]

[7.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x + (y + z) = (x + y) + z\,.$ [Axiom 3]

[8.] $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})2 + (y + z) = (2 + y) + z\,.$[Rule $\forall_{use}$, from steps 6,7]

[9.] $(\forall z \in \mathbb{R})2 + (1 + z) = (2 + 1) + z\,.$ [Rule $\forall_{use}$, from steps 1,8]

[10.] $2 + (1 + 1) = (2 + 1) + 1\,.$ [Rule $\forall_{use}$, from steps 1,9]

[11.] $3 = 2 + 1$. [Definition 8]

[12.] $2 + (1 + 1) = 3 + 1\,.$ [Rule SEE, from steps 10,11]

[13.] $2 + 2 = 3 + 1\,.$ [Rule SEE, from steps 5,12]

[14.] $4 = 3 + 1$. [Definition 9]

[15.] $2 + 2 = 4$. [Rule SEE. from steps 13,14]

Q.E.D.

7.4.2 Proving that $2 \times 2 = 4$ in only 24 steps

AXIOM 4. $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x(y + z) = xy + xz\,.$

AXIOM 5. $(\forall x \in \mathbb{R})x \times 1 = x$.

Theorem 17. $2 \times 2 = 4$.

Proof.

[1.] $1 \in \mathbb{R}$. [Axiom 1]

[2.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y \in \mathbb{R}\,.$ [Axiom 2]

[3.] $(\forall y \in \mathbb{R})1 + y \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,2]

[4.] $1 + 1 \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,3]

[5.] $2 = 1 + 1.$ [Definition 7]

[6.] $2 \in \mathbb{R}$. [Rule SEE, from steps 4,5]

[7.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x + (y + z) = (x + y) + z\,.$ [Axiom 3]

[8.] $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})2 + (y + z) = (2 + y) + z\,.$[Rule $\forall_{use}$, from steps 6,7]

[9.] $(\forall z \in \mathbb{R})2 + (1 + z) = (2 + 1) + z\,.$ [Rule $\forall_{use}$, from steps 1,8]

[10.] $2 + (1 + 1) = (2 + 1) + 1\,.$ [Rule $\forall_{use}$, from steps 1,9]

[11.] $3 = 2 + 1.$ [Definition 8]

[12.] $2 + (1 + 1) = 3 + 1\,.$ [Rule SEE, from steps 10,11]

[13.] $2 + 2 = 3 + 1\,.$ [Rule SEE, from steps 5,12]

[14.] $4 = 3 + 1.$ [Definition 9]

[15.] $2 + 2 = 4.$ [Rule SEE. from steps 13,14]

[16.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x(y + z) = xy + xz\,.$ [Axiom 4]

[17.] $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})2(y + z) = 2y + 2z\,.$ [Rule $\forall_{use}$, from steps 6,16]

[18.] $(\forall z \in \mathbb{R})2(1 + z) = 2 \times 1 + 2z\,.$ [Rule $\forall_{use}$, from steps 1,17]

[19.] $2 \times (1 + 1) = 2 \times 1 + 2 \times 1\,.$ [Rule $\forall_{use}$, from steps 1,18]

[20.] $2 \times 2 = 2 \times 1 + 2 \times 1\,.$ [Rule SEE, from steps 6,19]

[21.] $(\forall x \in \mathbb{R})x \times 1 = x.$ [Axiom 5]

[22.] $2 \times 1 = 2.$ [Rule $\forall_{use}$, from steps 6,21]

[23.] $2 \times 2 = 2 + 2\,.$ [Rule SEE, from steps 20,22]

[24.] $2 \times 2 = 4\,.$ [Rule SEE, from steps 15,23]

Q.E.D.

7.4.3 Organizing the theorems into a systematic theory

In the previous two subsections we have seen how one can begin developing elementary arithmetic by proving a couple of simple theorems such as, for example, that $2 + 2 = 4$ and that $2 \times 2 = 4$.

But if you look at the proofs of Theorems 16 and 17, you see that these proofs are very long. And there are several reasons for it:

- In both proofs, we devote several steps (six, in fact) to proving that $2 \in \mathbb{R}$. Wouldn't it be better if we just proved this once, and then used it every time we need it, without having to reprove it again? In other words: we can make our proofs shorter by first proving as a separate theorem the fact that $2 \in \mathbb{R}$, so that then we can use it later.

- However, "$2 \in \mathbb{R}$" is not a particularly interesting or important result. We just prove it because we are going to need it in order to prove other things we *really* want to prove. A theorem like that, that we prove because we are going to use it later, is usually called a ***lemma***. So we are going to ptove as a lemma that $2 \in \mathbb{R}$.
- In the proof of Theorem 17, the first 15 steps are devoted to proving that $2 + 2 = 4$. But this is unnecessary, if we allow ourselves the right to ***use*** previously proved theorems.

So we reorganize the first few steps in the development of elementary arithmetic into one lemma and two theorems.

And we get the following.

Lemma 1. $2 \in \mathbb{R}$.

Proof.
[1.] $1 \in \mathbb{R}$. [Axiom 1]
[2.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})x + y \in \mathbb{R}\,.$ [Axiom 2]
[3.] $(\forall y \in \mathbb{R})x + y \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,2]
[4.] $1 + 1 \in \mathbb{R}\,.$ [Rule $\forall_{use}$, from steps 1,3
[5.] $2 = 1 + 1.$ [Definition 7]
[6.] $2 \in \mathbb{R}$. [Rule SEE, from steps 4,5]
Q.E.D.

Theorem 18. $2 + 2 = 4$.

Proof.
[1.] $1 \in \mathbb{R}$. [Axiom 1]
[2.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x + (y + z) = (x + y) + z\,.$ [Axiom 3]
[3.] $2 \in \mathbb{R} \wedge 3 \in \mathbb{R}$. [Lemma 1]
[4.] $2 = 1 + 1\,.$ [Definition 7]
[5.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x + (y + z) = (x + y) + z\,.$ [Axiom 3]
[6.] $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})2 + (y + z) = (2 + y) + z\,.$[Rule $\forall_{use}$, from steps 2,5]
[7.] $(\forall z \in \mathbb{R})2 + (1 + z) = (2 + 1) + z\,.$ [Rule $\forall_{use}$, from steps 1,6]

[8.] $2 + (1 + 1) = (2 + 1) + 1\,.$ [Rule $\forall_{use}$, from steps 1,9]

[9.] $3 = 2 + 1.$ [Definition 8]

[10.] $2 + (1 + 1) = 3 + 1\,.$ [Rule SEE, from steps 8,9]

[11.] $2 + 2 = 3 + 1\,.$ [Rule SEE, from steps 4,10]

[12.] $4 = 3 + 1.$ [Definition 9]

[13.] $2 + 2 = 4.$ [Rule SEE. from steps 13,14] **Q.E.D.**

Theorem 19. $2 \times 2 = 4.$

Proof.

[1.] $1 \in \mathbb{R}.$ [Axiom 1]

[2.] $2 = 1 + 1.$ [Definition 7]

[3.] $2 \in \mathbb{R}.$ [Lmma 1]

[4.] $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})x(y + z) = xy + xz\,.$ [Axiom 4]

[5.] $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})2(y + z) = 2y + 2z\,.$ [Rule $\forall_{use}$, from steps 3,4]

[6.] $(\forall z \in \mathbb{R})2(1 + z) = 2 \times 1 + 2z\,.$ [Rule $\forall_{use}$, from steps 1,57]

[7.] $2 \times (1 + 1) = 2 \times 1 + 2 \times 1\,.$ [Rule $\forall_{use}$, from steps 1,6]

[8.] $2 \times 2 = 2 \times 1 + 2 \times 1\,.$ [Rule SEE, from steps 2,79]

[9.] $(\forall x \in \mathbb{R})x \times 1 = x.$ [Axiom 5]

[10.] $2 \times 1 = 2.$ [Rule $\forall_{use}$, from steps 3,9]

[11.] $2 \times 2 = 2 + 2\,.$ [Rule SEE, from steps 8,10]

[12.] $2 + 2 = 4\,.$ [Theorem 18]

[13.] $2 \times 2 = 4\,.$ [Rule SEE, from steps 11,12]

Q.E.D.

7.4.4 Another example of a real proof: proof that if $a|b$ and $a|c$ then $a|b + c$

Theorem 20. *If a, b, c are integers and a and b are divisible by c, then $a + b$ is divisible by c.*

Proof. We want to prove

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big((c|a \wedge c|b) \Longrightarrow c|a + b\Big)\,. \qquad (7.144)$$

[1.] $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})\Big(x|y \iff (\exists k \in \mathbb{Z})y = xk\Big)$. [Definition of "|"]

[2.] Let a be an arbitrary integer. [Declaring a value]

[3.] Let b be an arbitrary integer. [Declaring a value]

[4.] Let c be an arbitrary integer. [Declaring a value]

[5.] Assume $c|a \wedge c|b$. [Assumption]

[6.] $c|a$. [Rule $\wedge_{use}$ from step 5

[7.] $c|b$. [Rule $\wedge_{use}$ from step 5]

[8.] $(\forall y \in \mathbb{Z})\Big(c|y \iff (\exists k \in \mathbb{Z})y = ck\Big)$. [Rule $\forall_{use}$ from step 1]

[9.] $c|a \iff (\exists k \in \mathbb{Z})a = ck$. [Rule $\forall_{use}$ from step 8]

[10.] $(\exists k \in \mathbb{Z})a = ck$. [Rule $\iff_{use}$ from steps 6,9]

[11.] Pick a witness for the sentence of step 10 and call it i, so $i \in \mathbb{Z} \wedge a = ci$. [Rule $\exists_{use}$]

[12.] $i \in \mathbb{Z}$. . [Rule $\wedge_{use}$ from step 11.]

[13.] $a = ci$. [Rule $\wedge_{use}$ from step 11.]

[14.] $c|b \iff (\exists k \in \mathbb{Z})b = ck$. [Ru;e ($\forall_{use}$ from step 8]

[15.] $(\exists k \in \mathbb{Z})b = ck$. [Ru;e ($\iff_{use}$ from steps 7, 14]

[16.] Pick a witness for the sentence of step 15 and call it j, so $j \in \mathbb{Z} \wedge b = cj$. [Rule $\exists_{use}$]

[17.] $j \in \mathbb{Z}$. [Rule $\wedge_{use}$ from step 16]

[18.] $b = cj$. [Rule $\wedge_{use}$ from step 16]

[19.] $(\forall x)x = x$. [Equality axiom]

[20.] $a + b = a + b$. [Rule $\forall_{use}$, from step 19]

[21.] $a + b = ci + b$. [Rule SEE, from steps 13,20]

[22.] $a + b = ci + cj$. [Rule SEE, from steps 18,21]

[23.] $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})x(y + z) = xy + xz$. [Axiom about the integers (distributive law)]

[24.] $(\forall y \in \mathbb{Z})(\forall z \in \mathbb{Z})c(y + z) = cy + cz$. [Rule $\forall_{use}$, from step 23]

[25.] $(\forall z \in \mathbb{Z})c(i + z) = ci + cz$. [Rule $\forall_{use}$, from step 24]

[26.] $c(i + j) = ci + cj$. [Rule $\forall_{use}$, from step 25]

[27.] $a + b = c(i + j)$. [Rule SEE, from steps 22,26]

[28.] Let $\ell = i + j$. [Declaring a value]

[29.] $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})x + y \in \mathbb{Z}$. [Axiom about the integers]

[30.] $(\forall y \in \mathbb{Z})i + y \in \mathbb{Z}$. [Rule $\forall_{use}$, from step 29]

[31.] $i + j \in \mathbb{Z}$. [Rule $\forall_{use}$, from step 30]

[32.] $\ell \in \mathbb{Z}$. [Rule SEE, from steps 28,31]

[33.] $a + b = c\ell$. [Rule SEE, from steps 27,28]

[34.] $\ell \in \mathbb{Z} \wedge a + b = c\ell$. [Rule $\wedge_{prove}$, from steps 32,33]

[35.] $(\exists k \in \mathbb{Z})a + b = ck$. [Rule $\exists_{prove}$, from step 34]

[36.] $(\forall y \in \mathbb{Z})\Big(c|y \iff (\exists k \in \mathbb{Z})y = ck\Big)$. [Step 8]

[37.] $c|a + b \iff (\exists k \in \mathbb{Z})a + b = ck$. [Rule $\forall_{use}$, from step 36]

[38.] $(\exists k \in \mathbb{Z})a + b = ck \Longrightarrow c|a + b$. [Rule $\iff_{use}$, from step 37]

[39.] $c|a + b$. [Rule $\Longrightarrow_{use}$, from steps 35,38]

[40.] $(c|a \wedge c|b) \Longrightarrow c|a + b$. [Rule $\Longrightarrow_{prove}$, from steps 5,39]

[41.] $(\forall c \in \mathbb{Z})\Big(c|a \wedge c|b) \Longrightarrow c|a + b\Big)$. [Rule $\Longrightarrow_{prove}$, from steps 4,40]

[42.] $(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big(c|a \wedge c|b) \Longrightarrow c|a + b\Big)$. [Rule $\Longrightarrow_{prove}$, from steps 3,41]

[43.]$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big(c|a \wedge c|b) \Longrightarrow c|a + b\Big)$. [Rule $\Longrightarrow_{prove}$, from steps 2,42]

Q.E.D.

7.4.5 The proof that $x.0 = 0$ for every x

Theorem 21. *If x is a real number, then $x.0 = 0$. (In formal language: $(\forall x \in \mathbb{R}))x.0 = 0$.*

Let us first write a narrative version, the kind of narrative that we often call a “proof”.

Proof. Let $x \in \mathbb{R}$ be arbitrary. Since $0 + 0 = 0$, we have $x.(0 + 0) = x.0$. But $x.(0 + 0) = x.0 + x.0$. Hence $x.0 + x.0 = x.0\,$.

Subtracting $x.0$ from both sides we get

$$x.0 = 0\,.$$

Q.E.D.

Most people will find this persuasive enough, and will accept that whoever wrote this narrative knows how to write a true proof, if necessary. But, just in case somebody doubts it, here is a true proof.

Proof. [1.] $0 \in \mathbb{R}$

[2.] Let $x \in \mathbb{R}$ be arbitrary.

[3.] $(\forall u)u = u.$

[4.] $x.0 = x.0$

[5.] $(\forall u \in \mathbb{R})u + 0 = u$

[6.] $0 + 0 = 0$

[7.] $x.(0 + 0) = x.0$

[8.] $(\forall u \in \mathbb{R})(\forall v \in \mathbb{R})(\forall w \in \mathbb{R})u.(v + w) = u.v + u.w$

[9.] $(\forall v \in \mathbb{R})(\forall w \in \mathbb{R})x.(v + w) = x.v + x.w$

[10.] $(\forall w \in \mathbb{R})x.(0 + w) = x.0 + x.w$

[11.] $x.(0 + 0) = x.0 + x.0$

[12.] $x.0 + x.0 = x.0$

[13.] $(\forall u \in \mathbb{R})(\forall v \in \mathbb{R})u.v \in \mathbb{R}.$

[14.] $(\forall v \in \mathbb{R})x.v \in \mathbb{R}.$

[15.] $x.0 \in \mathbb{R}.$

[16.] $(\forall u \in \mathbb{R})u + (-u) = 0$

[17.] $x.0 + (-x.0) = 0$

[18.] $(x.0 + x.0) + (-x.0) = 0$

[19.] $(\forall u \in \mathbb{R})(\forall v \in \mathbb{R})(\forall w \in \mathbb{R})u + (v + w) = (u + v) + w$

[20.] $(\forall v \in \mathbb{R})(\forall w \in \mathbb{R})(x.0) + (v + w) = (x.0 + v) + w$

[21.] $(\forall w \in \mathbb{R})(x.0) + (x.0 + w) = (x.0 + x.0) + w$

[22.] $x.0 + (x.0 + (-x.0)) = (x.0 + x.0) + (-x.0)$

[23.] $(\forall u \in \mathbb{R})u + 0 = u.$

[24.] $x.0 + (x.0 + (-x.0)) = 0.$

[25.] $x.0 + 0 = 0.$

[26.] $x.0 + 0 = x.0$

[27.] $\quad x.0 = 0.$
[28.] $(\forall x \in \mathbb{R})\, x.0 = 0.$

Q.E.D.

Problem 24. ***Provide the justifications*** for the steps of the proof of Theorem 21. Use as your model the justficiations we gave for the proofs of Theorems 16, 17, 18, 19, and 20. □

Part III

8 Sets

The language of ***sets*** was introduced into mathematics in the 19th century, when the great mathematician ***George Cantor*** (1845-1918) almost single-handedly created ***Set theory***.

You should read the article "A history of set theory", in MacTutor.

Today, set theory is not only an important branch of mathematics, but the foundational pillar on which all of mathematics rests. Most mathematicians no longer ask questions that they used to ask, such as "what is a natural numebr?", or "what is a real number?", or "what is a function?", because they think that all these objects are just special kinds of sets.

This does not mean that they have answered those questions. It just means that they have reduced those questions to just one question: what is a set? Once you know what a set is, then all the other questions are answered.

As for the fundamental question "what is a set?", I am not going to answer it here. What I am going to do is start telling you about sets, until you get used to working with them and talking about them. The question about the ultimate nature of sets will remain unanswered.

8.1 What kind of thing is a set?

Sets are things that we invent in order to combine several objects and form with them a single thing, so that we can talk about the objects as one thing, a "collective entity".

This "grouping" operation, of forming a single thing out of several things, is something we perform very often, using different words, called "collective nouns", to create these collective objects.

Here are some examples.

1. ***Crowds.*** When you see a number of people standing together and shouting something (say, "long live the Queen"), you create a single thing, called "the crowd", so that, instead of saying

   the people are shouting "long live the Queen"

   you can use the collective noun "crowd" and say

   the crowd is shouting "long live the Queen"

   *Notice that "the people" have become a single object, "the crowd". So, instead of using the verb in plural ("the people **are** shouting") when you talk about the people, you use the verb in singular ("the crowd **is** shouting") when we talk about the crowd.*

2. ***Flocka of birds.*** When we see a number of birds flying in formation, we create an entity called "the flock", so that, instead of saying

   I see several birds, and they are flying East,

   we can use the collective noun "flock" and say

   I see a flock of birds, and it is flying East.

   *Notice that "the birds" have become a single object, "the flock". So, instead of using the verb in plural ("the birds **are** flying") when we talk about the birds, we use the verb in singular ("the flock **is** flying") when we talk about the flock.*

3. ***Orchestras.*** When several musicians are playing together, we introduce into our discourse the collective noun "orchestra", so that, instead of saying

The musicians are playing

we can use the collective noun "orchestra" and say

The orchestra is playing.

Once again, "the musicians" have become a single object, "the band". So, instead of using the verb in plural ("the musicians ***are*** *playing") when we talk about the musicians, we use the verb in singular ("the orchestra* ***is*** *playing") when we talk about the orchestra.*

4. ***Juries.*** When several people are brought together to sit in judgemebnt and decide if a defendant is guilty, the people are called ***jurors***, and are said to be members of the ***jury***.

   And we say things like

   The jurors ***find*** the defendant guilty

   or

   The jury ***finds*** the defendant guilty.

   Once again, when we talk about "the jurors" we use the verb in plural ("find") but when we talk about "the jury" itself we use the verb in singular ("finds") because the jury is a single object.

5. ***The sets*** $\mathbb{N}$***,*** $\mathbb{Z}$***, and*** $\mathbb{R}$***.*** When numbers of a certain kind are discussed together, we create entities called $\mathbb{N}$ ("the set of all natural numbers"), $\mathbb{Z}$ ("the set of all natural integers"), $\mathbb{R}$ ("the set of all real numbers"), so that, instead of saying

   there are infinitely many natural numbers

   we can use the collective noun "$\mathbb{N}$" and say the set $\mathbb{N}$ is infinite.

Similarly, instead of saying

all integers are real numbers,

we can use the collective nouns "$\mathbb{N}$" and "$\mathbb{Z}$" and say

$\mathbb{Z}$ is a subset of $\mathbb{R}$.

And, instead of saying

the real numbers form a complete ordered field,

we can use the collective noun "$\mathbb{R}$" and say

$\mathbb{R}$ is a complete ordered field.

*Notice that "the natural numbers", "the integers", and "the real numbers" have become single objecta, "$\mathbb{N}$". "$\mathbb{Z}$". "$\mathbb{R}$". So, instead of using verbs in plural ("there **are** infinitely many natural numbers", "all integers **are** real numbers", "the real numbers **form**..."), when we talk about the numbers, we use verbs in singular ("the set $\mathbb{N}$ **is** infinite", "$\mathbb{Z}$ **is** a subset of $\mathbb{R}$", "$\mathbb{R}$ **is** a complete ordered field") when we talk about the sets.*

8.1.1 Sets with structure

Most of these collective entities have a ***structure***; that is,

1. The members are not all equal and interchangeable. On the contrary, some play special roles.
2. The pairs of members are not all equal and interchangeable. On the contrary, some pairs of members are different from others.

3. The triples of members are not all equal and interchangeable. On the contrary, some triples of members are different from others.

For example,

1. A flock of birds flying in formation has a special member, the ***leader***. And, even more importantly, each bird has ***neighbors***, that is, a few other birds that are right next to it, to the left or to the right or in front or behind, and the bird communicates with its neighbors. The flock stays in formation because each bird, knowing which way its neighbors are moving, tries to move in the same way. "Being neighbors" is what we have called in these notes a ***binary relation***. If we use "xNy" for "x is a neighbor of y", then the "neighbor" relation N singles out some pairs (x, y) of birds as different from other pairs.

2. A number system such as $\mathbb{N}$, or $\mathbb{Z}$, or $\mathbb{R}$ has

   - special members (1 for $\mathbb{N}$, 0 and 1 for $\mathbb{Z}$ and $\mathbb{R}$),
   - special sets of members (for example, for $\mathbb{Z}$ or for $\mathbb{R}$, the set of all positive members of the set),
   - special pairs of members of the set (for example, for $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{R}$, the pairs (x, y) such that $x < y$ are different from the other pairs),
   - special triples (x, y, z) of members. (For example, the triples (x, y, z) such that $z = x + y$ play a special role: they determine the operation of ***addition***, in the sense that if you know the set S of all the triples (x, y, z) such that $x + y = z$ then you know the operation of addition, because, if I give you numbers x, y, then you can compute x, y by looking in the set S until you find a triple (x, y, z) that is in S, and then the sum $x + y$ is z.)

8.1.2 How sets are different from other collective entities

Usually, you cannot form collective entities by putting together any objects you want, because the objects have to be related in some way. For example,

- You would never form a "crowd" consisting of yourself, the prime minister of Australia, and five people living in Wyoming.

- And you would never take a bunch of wolves living in Wyoming together with some other wolves who live in Sweden and call that a “pack”. To form a pack, the wolves have to be together, run together, and hunt together.

Sets are different, in that they are collective entities that can be formed to put together into a single object ***any objects you want***. The things you put together to form a set do not have to be related in any way. For example,

1. You can form a set whose members are all the wolves in Wyoming.

2. You can form a set whose members are all the wolves in Wyoming together with all the wolves in Sweden.

3. You can form a set whose members are three wolves you like who live in Wyoming, together with the musicians of the New York Philharmonic, your uncle Billy, the planets Earth, Mars and Jupiter, the numbers 5, 7 and 23, the numbers π and $3+\sqrt{5}$, and all the integers that are larger than 377.

The only thing you need in order to be able to form a set S, is a “membership criterion”, i.e., a sentence $C(x)$ that specifies the condition that an object x has to satisfy in order to qualify as a member of the set. And any sentence will do[64].

8.1.3 Terms and sentences with variables: a review

In mathematical writing, there are two kinds of meaningful phrases[65], namely, ***terms*** and ***sentences***.

[64] At least for now. Later we will se that we cannot allow absolutely any sentence, because if you do allow that serious trouble ensues, in the form of the “Russell paradox”. So we will have to put some limitations. But we are not there yet.

[65] A “phrase” in a particular language is, according to the dictionary, “a small group of words standing together as a conceptual unit”. (The “small group” could be just a single word. Most phrases are meaningless. For example, the words “Obama” and “Alice” and the longer phrases “Ronald Reagan”, “the table”, “the case where I put my sunglasses yesterday”, “cows eat grass”, “the planets move around the Sun”, “cows like to attack lions and fight them to death”, “$2+3$”, “$2+3=5$”, “$2+3=6$”, “every odd number is prime”, are all phrases.

- Terms are phrases that stand for things or people: for example, "Obama", "Alice", "Ronald Reagan", "the table", "the case where I put my sunglasses yesterday", "$2 + 3$", are terms, because they stand for specific things.[66]

- Sentences are phrases that make an assertion that can be true or false: for example, "cows eat grass", "I have no idea where I left the case where I put my sunglasses yesterday", "the planets move around the Sun", "cows like to attack lions and fight them to death", "$2+3 = 5$", "$2+3 = 6$, and "every odd number is prime") are sentences. (Actually, "cows eat grass" is true, "the planets move around the Sun" is true, "cows like to attack lions and fight them to death" is false, "$2+3 = 5$" is true, "$2 + 3 = 6$" is false, and "every odd number is prime" is true.)

Remark 7. Terms are basically the same as "noun phrases", that is, phrases that can serve as the subject of an "is" sentence. So, for example,

- In the sentence "$2 + 3$ is an odd number", the subject is "$2 + 2$", so "$2 + 2$" is a term.

- In the sentence "the case where I put my sunglasses yesterday is on the table", the subject is "the case where I put my sunglasses yesterday", so "the case where I put my sunglasses yesterday" is a term. □

Terms and sentence can contain variables, that is, letters or expressions that do not stand for a definite object, but represent ***slots*** where the name of a person or object can be inserted. Then, when you actually put specific names of persons or objects in the slots,

- A term has a ***value***, i.e., becomes the name of a specific object.

- A sentence has a ***truth value***, i.e., becomes true or false.

But if you leave some of the the slots unfilled (i.e., if you keep some "free variables") then the terms do not have a definite value and the sentences do not have a truth value. In that case, we say that he term or sentence is meaningless, because it does not stand for a specific object or assertion.

[66] These things may be concrete,material objects or people, or abstract entities such as numbers. For example, "$2 + 3$" stands for a number, that happens to be the number 5.

Example 36. The term (i.e., noun phrase) "his mother" contains the possessive adjective "his", which is a variable. If you plug in "Barack Obama" for "his" the term becomes "Barack Obama's mother", which stands for a definite person. (In mathematical language, we would talk about "x's mother". And, again, when we plug in "Barack Obama" for "x" the term becomes "Barack Obama's mother", which stands for a definite person.) □

Example 37. The sentence "he is a friend of mine" contains the pronoun "he". If you do not tell me who "he" is, then I don't know what you are talking about. But if you tell me who "he" is, that is, if you ***assign a value*** to the variable "he" (by saying, for example, that "he" stands for "Bill Clinton") then the sentence becomes "Bill Clinton is a friend of mine", which has a definite truth value. (In mathematical language, we would say "x is a friend of mine", and then, when we plug in "Bill Clinton" for "x", we get when we plug in "Barack Obama" for "x" the term becomes "Barack Obama's mother", which stands for a definite person.) □

Example 38. The term "$x + 3y$" contains the letters "x" and "y". If you do not tell me which numbers the letters x and y stand for, then I cannot make sense of which object (in this case, a number) this term stands for. If, on the other hand, you assign specific values to x and y then I can figure out the value of the term. (For example, if you let $x = 4$, $y = -6$, then I can tell that "$x + 3y$" has the value -14, i.e., that $x + 3y = -14$. □

Example 39. The sentence "$x+3y > 6$" contains the letters "x" and "y". If you do not tell me which numbers the letters x and y stand for, then I cannot make sense of which assertion the sentence is making, and cannot decide if it is true or false, If, on the other hand, you assign specific values to x and y then I can figure out the truth value of the sentence. (for example, if you let $x = 4$, $y = -6$, then I can tell that "$x + 3y = 6$" has the truth value "false", because $x + 3y = 4 - 3 \times 6 = -14$, and $\sim -14 > 6$. But if $x = 3$ and $y = 2$, then $x + 3y = 9$, and $9 > 6$, so "$x + 3y = 6$" is true.. □

8.1.4 Forming sets

As long as you can write a sentence $C(x)$ about a variable object x, you can form the set

$$\{x : C(x)\}$$

that is, the set of all x for which $C(x)$ is true. And you could give this set a name. For example, suppose you want to form the set $\{x : C(x)\}$ and give it the name S. You would do that by writing

$$\text{Let} \qquad S = \{x : C(x)\}.$$

Let us formulate this rule for forming sets as an axiom:

The naïve axiom of set formation

Given any sentence $C(x)$ having x as an open variable, we can form the set whose members are all the objects x for which $C(x)$ is true.

A name for such a set is

$$\{x : C(x)\} \, .$$

And we read this as

The set of all x such that $C(x)$.

Remark 8. Why did I call the set formation axiom "naïve"? The reason is this: in a few days, we will discover that the set formation axiom, as we have formulated it, causes serious problems that can only be solved by changing the statement of the axiom. Instead of a "naïve" axiom that allows us to take any sentence $C(x)$ whatsoever and form the ser $\{x : C(x)\}$, we will have to adopt a "sophisticated" axiom in which nto all sentences are permitted. □

8.1.5 The membership criterion

Suppose we use the sentence "x is a cow", to form a set S, so

$$S = \{\, x : x \text{ is a cow} \,\}$$

that is, S is "the set of all x such that x is a cow", or, in much better English, S ***is the set of all cows.***

Then we can decide whether or not an object a belongs to the set S (that is, whether or not $a \in S$) by applying the following simple test

1. Find out if a is a cow or not.
2. If a is a cow, then a belongs to S.
3. If a is not a cow, then a does not belong to S.

In other words, the sentence "x is a cow" is the ***membership criterion***, or ***membership condition***, for S. A particular object a belongs to the set $\{\, x : x \text{ is a cow} \,\}$ if a is a cow, and doesn't belong to the set of a is not a cow.

For a general sentence $C(x)$:

Suppose $C(x)$ is a sentence having x as an open variable, and you define a set S by writing

$$\text{Let} \qquad S = \{x : C(x)\}\,.$$

Then

- The sentence $C(x)$ is called the membership criterion, or membership condition, for the set S.
- An object a ***belongs*** to S if $C(a)$ is true, and ***doesn't belong*** to S if $C(a)$ is not true.

8.1.6 Forming sets of members of a given set

Suppose we want to form the set of all natural numbers n that are even, i.e., such that $2|n$, and we want to call this set A.

Then we can say:

$$\text{Let} \qquad A = \{n : n \in \mathbb{N} \wedge 2|n\}\,,$$

and we can also say

$$\text{Let} \qquad A = \{n \in \mathbb{N} : 2|n\}\,.$$

The first ssentence is read as "Let A be the set of all things that are natural numbers and are even", whereas the second sentence is read as "Let A be the set of all natural numbers that are even".

And, clearly, both define the same set.

Suppose U is a set, $C(x)$ is a sentence having x as an open variable, and you define a set S by writing

$$\text{Let} \qquad S = \{\, x : x \in U \wedge C(x)\,\}\,.$$

Then the membership criterion is the sentence "$x \in U \wedge C(x)$".

And you can also write

$$\text{Let} \qquad S = \{\, x \in U : C(x)\,\}\,.$$

Example 40. Suppose the membership criterion $C(x)$ is the sentence "x is a natural number that can be written as the sum of the squares of two natural numbers". Let

$$S = \{x : C(x)\}\,.$$

Clearly, $C(x)$ is the sentence

$$x \in \mathbb{N} \wedge (\exists m \in \mathbb{N})(\exists n \in \mathbb{N})x = m^2 + n^2\,,$$

so we could have written the definition of S as follows:

$$S = \{x : x \in \mathbb{N} \wedge (\exists m \in \mathbb{N})(\exists n \in \mathbb{N})x = m^2 + n^2\}\,,$$

or as

$$S = \{x \in \mathbb{N} : (\exists m \in \mathbb{N})(\exists n \in \mathbb{N})x = m^2 + n^2\}\,, \tag{8.145}$$

(We read this as "S is the set of all natural numbers x such that there exist natural numbers m, n for which $m^2 + n^2 = x$". And an even better reading is "S is the set of all natural numbers that are the sum of two squares of natural numbers".)

Let us consider several possible values of x, and in each case let us figure out whether this x belongs to the set S.

1. Suppose x is the Math 300 textbook. Then x is a book, not a natural number. So $x \notin S$, that is, x is not a member of S.

2. Suppose $x = 5$. Then x is a natural number. And x is the sum of the squares of two natural numbers, because $x = 2^2 + 1^2$. Therefore x satisfies the criterion for membership in S. So x is a member of S, that is, $x \in S$.

3. Suppose $x = -5$. Then x is not a natural number. So $C(x)$ is not true. That is, x does not satisfy the criterion for membership in S. So x is not a member of S.

4. Suppose $x = 7$. Then x is a natural number. Can x be written as the sum of the squares of two natural numbers? The answer is "no". How do we know that? Well, for example, we know that a number that is of the form $k + 3$, $k \in \mathbb{Z}$, is not the sum of two squares. And 7 is of the form $k + 3$, because $7 = 4 + 3$. So $x \notin S$. □

8.1.7 How to read the symbol “$\in$”

How to read the “$\in$” symbol

If S is a set and a is an object, we write

$$a \in S$$

to indicate that a is a member of S.

And we write

$$a \notin S$$

to indicate that a is not a member of S.
The expression “$a \in S$” is read in any of the following ways:

- a belongs to S,
- a is a member of S,
- a is in S.

The expression “$a \notin S$” is read in any of the following ways:

- a does not belong to S,
- a is not a member of S,
- a is not in S.

Remark 9. Sometimes, “$a \in S$” is read as “a belonging to S”, or “a in S”, rather than “a belongs to S”, or “a is in S.” For example, if we write

$$\text{Pick an } a \in S,$$

then it would be very bad to say “pick an a belongs to S”. But “pick an a belonging to S”, “pick an a in S”, is fine. □

Never read “$\in$” as “is contained in”, or ”is included in”. The words “contained” and “included” have different meanings, that will be discussed later.

8.2 When are two sets equal?

As we have explained, sets have ***members***. And, even more imprtantly, ***knowledge of the members of the set determines the set. Two sets that have the same members are the same set.***

Let us make this precise:

The axiom of set equality

Two sets are equal if and only if they have the same members.
In semiformal language:
If A, B are sets, then $A = B$ if and only if

$$(\forall x)(x \in A \Longleftrightarrow x \in B)\,.$$

And, in formal language,

$$(\forall A)(\forall B)\Big(A = B \Longleftrightarrow (\forall x)(x \in A \Longleftrightarrow x \in B)\Big)\,.$$

Example 41. Let

$$\begin{array}{rcl} A & = & \{x \in \mathbb{R} : x \geq 0\}\,, \\ B & = & \{x \in \mathbb{R} : (\exists y \in \mathbb{R}) y^2 = x\}\,. \end{array}$$

Let us prove that $A = B$.

To prove that $A = B$, we have to prove that $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

So, let x be arbitrary. We have to prove that $x \in A \Longleftrightarrow x \in B$.

To prove this, we have to prove that $x \in A \Longrightarrow x \in B$ and that $x \in B \Longrightarrow x \in A$.

Let us first prove that $x \in A \Longrightarrow x \in B$.

> Assume that $x \in A$.
>
> Then $x \in \mathbb{R}$ and $x \geq 0$. (Reason: "$x \in \mathbb{R} \wedge x \geq 0$" is the membership criterion for A.)
>
> But every nonnegative real number has a square root.
>
> So x has a square root. That is, $(\exists y \in \mathbb{R})y^2 = x$.
>
> So x satisfies the membership criterion for B.
>
> Hence $x \in B$.

Therefore $x \in A \Longrightarrow x \in B$.

We now prove that $x \in B \Longrightarrow x \in A$.

> Assume that $x \in B$.
>
> Then $x \in \mathbb{R}$ and $(\exists y \in \mathbb{R})y^2 = x$. (Reason: "$x \in \mathbb{R} \wedge (\exists y \in \mathbb{R})y^2 = x$" is the membership criterion for B.)
>
> Pick $y \in \mathbb{R}$ such that $y^2 = x$.
>
> Then $y^2 \geq 0$. (Reason: $(\forall u \in \mathbb{R})u^2 \geq 0$.)
>
> So $x \geq 0$.
>
> So x satisfies the membership criterion for A.
>
> Hence $x \in A$.

Therefore $x \in B \Longrightarrow x \in A$.

So $x \in A \Longleftrightarrow x \in B$. Since x is arbitrary, we can conclude that $(\forall x)(x \in A \Longleftrightarrow x \in B)$. Hence $A = B$. **Q.E.D.**

Example 42. Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : x > 0\}, \\ B &= \{x \in \mathbb{R} : (\exists y \in \mathbb{R})y^2 = x\}. \end{aligned}$$

Let us prove that $A \neq B$.

To prove that $A \neq B$, we have to prove that it is not true that $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

Suppose[67] $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

Then we can specialize to $x = 0$, and conclude that $0 \in A \Longleftrightarrow 0 \in B$.

But "$0 \in B$" means that "$(\exists y \in \mathbb{R})y^2 = 0$, which is true, because $7^2 = 0$.

On the other hand, "$0 \in A$" means that "$0 > 0$", which is false.

Hence it is not true that $0 \in A \Longleftrightarrow 0 \in B$.

So $(0 \in A \Longleftrightarrow 0 \in B) \wedge \Big(\sim (0 \in A \Longleftrightarrow 0 \in B)\Big)$, which is a contradiction .

Hence $A \neq B$. **Q.E.D.**

Example 43. Let $A = \{n \in \mathbb{Z} : 6|n\}$, and let $B = \{n \in \mathbb{Z} : 2|n \wedge 3|n\}$.

Let us prove that $A = B$.

To prove that $A = B$, we have to prove that $(\forall x)(x \in A \Longleftrightarrow x \in B)$.

So, let x be arbitrary. We have to prove that $x \in A \Longleftrightarrow x \in B$.

To prove this, we have to prove that $x \in A \Longrightarrow x \in B$ and that $x \in B \Longrightarrow x \in A$.

Let us first prove that $x \in A \Longrightarrow x \in B$.

Assume that $x \in A$.

Then $x \in \mathbb{Z}$ and $6|x$.

Since $6|x$, we may pick $k \in \mathbb{Z}$ such that $x = 6k$.

Then $x = 2 \times (3k)$, and $3k \in \mathbb{Z}$, so $2|x$.

Also, $x = 3 \times (2k)$, and $2k \in \mathbb{Z}$, so $3|x$.

Hence $2|x \wedge 3|x$.

So $x \in B$.

[67] A proof by contradiction , of course.

Therefore $x \in A \Longrightarrow x \in B$.

We now prove that $x \in B \Longrightarrow x \in A$.

Assume that $x \in B$.

Then $x \in \mathbb{Z}$, $2|x$, and $3|x$.

Since $2|x$, we may pick $j \in \mathbb{Z}$ such that $x = 2j$.

Since $3|x$, we may pick $k \in \mathbb{Z}$ such that $x = 3k$.

Then $x = 1.x = (3-2)x = 3x-2x = 3\times(2j)-2\times(3k) = 6(j-k)$.

So $6|x$.

Hence $x \in A$.

Therefore $x \in B \Longrightarrow x \in A$.

So $x \in A \Longleftrightarrow x \in B$. Since x is arbitrary, we can conclude that $(\forall x)(x \in A \Longleftrightarrow x \in B)$. Hence $A = B$. **Q.E.D.**

Problem 25. Let

$$\begin{array}{rcl} A & = & \{x \in \mathbb{R} : x^3 > x\}\,, \\ B & = & \{x \in \mathbb{R} : -1 < x < 0 \vee x > 1\} \\ C & = & \{x \in \mathbb{R} : -1 < x\}\,. \end{array}$$

Prove or disprove each of the following:

- $A = B$,
- $A = C$.

8.2.1 Subsets

Definition 10. Let A, B be sets. We say that A is a subset of B, and write

$$A \subseteq B\,,$$

if every member of A is a member of B.

In semiformal language, A is a subset of B if and only if

$$(\forall x)(x \in A \Longrightarrow x \in B)\,.$$

In completely formal language:

$$\boxed{(\forall A)(\forall B)\Big(A \subseteq B \Longleftrightarrow (\forall x)(x \in A \Longrightarrow x \in B)\Big)\,.}$$ □

Example 44. The following are true:

- $\mathbb{N} \subseteq \mathbb{Z}\,,$
- $\mathbb{Z} \subseteq \mathbb{Q}\,,$
- $\mathbb{Q} \subseteq \mathbb{R}\,,$
- $\{x \in \mathbb{R} : 0 < x < 1\} \subseteq \{x \in \mathbb{R} : 0 \le x \le 1\}$. □

Example 45.

The following are true:

- $\{x \in \mathbb{R} : -1 < x < 0\} \subseteq \{x \in \mathbb{R} : x^3 > x\}$.
- $\{n \in \mathbb{N} : n \text{ is prime} \wedge n \neq 2\} \subseteq \{n \in \mathbb{N} : 2|n-1\}$.
- $\{n \in \mathbb{Z} : 4|n\} \subseteq \{n \in \mathbb{Z} : 2|n\}\,,$
- $\{x \in \mathbb{R} : 0 < x < 1\} \subseteq \{x \in \mathbb{R} : 0 \le x \le 1\}\,,$ □

WARNING!

"is a subset of" is a ***binary relation***. It does not make sense to say things like "A is a subset". What does make sense is to say "A is a subset of B".

If, in an exam, I ask you to define "subset", and you say "a set A is a subset if ....", then that is completely wrong and you get zero credit[a]

The definition of "subset" must start with the words: "Let A, B be sets. We say that A is a subset of B if $\ldots$.

[a] And if your definition starts with horrendous words "subset is when . . ." then you lose $10,000,000$ points, on a sclae from 0 to 10.

ALWAYS UNDERLINE THE DEFINIENDUM

In a definition, the term being defined is called the definiendum. The definiendum must always be underlined, or highlighted in some way, in order to indicate that we are writing a definition of that term, not just making a true statement.
For example:

- If I write “elephants are four-legged animals”, then I am making a true statement about elephants.
- If, on the other hand, I write “elephants are four-legged animals”, then I am saying that I am defining the word “elephant” to mean “four-legged animal”, and this is of course wrong, because “elephant” does not mean “four-legged animal”: there are lots of four-legged animals that are not elephants.
- If I write “an even integer is an integer that is divisible by 2”, then I am making a true statement. but I am not saying that this is what “even integer” means.
- If I want to explain what “even integer” means, i.e., give a ***definition*** of “even integer”, then I have to say “an even integer is an integer that is divisible by 2”. By underlining “even integer” I am conveying the message that this is my definition of “even inteeger”.
- If in an exam you are asked to give a definition and you do not underline the definiendum, you will lose points.

Question 1. *In the first sentence of the previous box, why is the word "definiendum" underlined?* □

Problem 26. ***Prove*** the four statements of Example 45.
The structure of your proofs should be as follows:

We want to prove that $A \subseteq B$.

For that purpose, we prove that $(\forall x)(x \in A \Longrightarrow x \in B)$.

Let x be arbitrary. We want to prove "$x \in A \Longrightarrow x \in B$".

Assume $x \in A$.

$\vdots$

$x \in B$.

So $x \in A \Longrightarrow x \in B$.

Therefore $(\forall x)(x \in A \Longrightarrow x \in B)$.

So $A \subseteq B$. **Q.E.D.**

Problem 27. ***Prove*** that the binary relation "$\subseteq$" is reflexive, antisymmetric, and transitive. (In the definition of these properties given in the notes, a set S is mentioned. Here you may think of S as "the set of all sets", which means that you can forget about S. Then, for example, the property that "$\subseteq$" is antisymmetric means "$(\forall A)(\forall B)\Big((A \subseteq B \wedge B \subseteq A) \Longrightarrow A = B\Big)$".)

8.2.2 The empty set

An important example of a set is the ***empty set***, that is, the set that has no members at all.

The symbol for the empty set is

$$\emptyset\,.$$

One possible way to define this set is by the following formula:

$$\boxed{\emptyset = \{x : x \neq x\}\,.}$$

This means that the members of $\emptyset$ are the things x that satisfy $x \neq x$. But our Equality Axiom says that $(\forall x)x = x$. So "$x = x$" is true for every x. This means that no x can be a member of $\emptyset$. So, indeed. $\emptyset$ has no members.

Let us make this precise:

Theorem 22. *The empty set has no members. That is.*

$$(\forall x)x \notin \emptyset\,.$$

Proof.

Let x be arbitrary. We want to prove that $x \notin \emptyset$.

Assume[68] that $x \in \emptyset$.

Then x satisfies the membership criterion for $\emptyset$, i.e.,

$$x \neq x\,.$$

But $(\forall x)x = x$, by the Equality Axiom.

So $x = x$, by the rule for using universal sentences.

Therefore $x = x \wedge x \neq x$, which is a contradiction.

So $x \notin \emptyset$.

Therefore $(\forall x)x \notin \emptyset$. **Q.E.D.**

8.2.3 The empty set is a subset of every set

If you have a set A and a subset B of A, and you remove some members from B, producing a subset C of B, then it is clear that C is still a subset of A. This ought to be true even in the extreme case when you remove *all* the members of B, so that C is the empty set. In other words, the empty set should be a subset of A, for every set A.

Let us prove a precise theorem:

[68] A proof by contradiction !.

Theorem 23. *The empty set is a subset of every set. That is,*

$$(\forall A)\emptyset \subseteq A\,.$$

Proof.

Let A be an arbitrary set. We want to prove that $\emptyset \subseteq A$.

Assume[69] that $\emptyset$ is not a subset of A.

That is, assume that it is not true that every member of $\emptyset$ is in A.

That means that some members of $\emptyset$ are not in A.

In other words, there exists an object x such that $x \in \emptyset$ and $x \notin A$.

Pick one such object and call it a.

Then $a \in \emptyset$ and $a \notin A$.

So in particular $a \in \emptyset$.

But we know from Theorem 22 that $(\forall x)x \notin \emptyset$.

So $a \notin \emptyset$.

Hence $a \in \emptyset \wedge a \notin \emptyset$.

So we have proved a contradiction.

Therefore $\emptyset \subseteq A$.

So $(\forall A)\emptyset \subseteq A$. **Q.E.D.**

8.2.4 Sets with one, two, three or four members

If a is any thing, we can form a set that has a as a member, and no other members. This name of this set is

$$\boxed{\{a\}}\,,$$

which we read as "singleton of a."

The precise definition of $\{a\}$ is as follows.

[69] A proof by contradiction !

Definition 11. Let a be any object. Then the singleton of a is the set $\{a\}$ given by

$$\{a\} = \{x : x = a\}\,.$$

In other words: to be a member of the set $\{a\}$ you have to be a. If you are a then you are a member, and if you are not a then you are not a member.

We can do a similar thing with two objects, say a and b. We can form the set $\{a, b\}$ whose members are a, b, and nothing else. The set $\{a, b\}$ is the unordered pair of a and b.

Definition 12. Let a, b be any two objects. Then the unordered pair of a and b is the set $\{a, b\}$ given by

$$\{a, b\} = \{x : x = a \vee x = b\}\,.$$

Remark 10. ***Warning:*** The set $\{a, b\}$ is ***not*** necessarily a set with two members. That depends on who a and b are. For example; if a happens to be equal to b, then $\{a, b\}$ has only one member. □

Naturally, we can do the same thing with three, four, or any number of objects. For example:

Definition 13. Let a, b, c be any three objects. Then the unordered triple of a, b and c is the set $\{a, b, c\}$ given by

$$\{a, b, c\} = \{x : x = a \vee x = b \vee x = c\}\,.$$

Definition 14. Let a, b, c, d be any four objects.

Then the unordered quadruple of a, b, c and d is the set $\{a, b, c, d\}$ given by

$$\{a, b, c, d\} = \{x : x = a \vee x = b \vee x = c \vee x = d\}\,.$$

And, in principle, you could go on like this and define sets with five members, sets with 6 members, and so on.

But as soon as the number of members gets large, this way of constructing sets becomes very complicated, so it is better to do it differently.

Example 46. Suppose you want to define a set whose members are the first five presidents of the U.S., and call this set A. That's easy to do. We say:

Let $A = \{$George Washington,John Adams,Thomas Jefferson,James Madison,James Monroe$\}$.

Now suppose you want to define a set whose members are the first 30 U.S. presidents, and call this set B. That is going to be much more complicated right? And what if you do not know the names of all those presidents?

Hhere is how you can do it. You can say:

Let

$$B = \Big\{ x : (\exists j \in \mathbb{N})(j \leq 30 \wedge x = p_j) \Big\} ,$$

where, for each $j \in \mathbb{N}$, p_j is the j-th president of the U.S.

This works perfectly! Indeed, let us see what has to be true of an object x for x to qualify as a member of A. If you are given an object x, and you have to decide whether $x \in B$ or not, you have to find out if there exists a natural number j such that $j \leq 30$ and x is the j-th U.S. president. And that's exactly what we want! □

Problem 28. How many members does the set B of Example 46 have?

If you think that the answer is 30, think again! Go to a history book (or to a history Web site) and read about Grover Cleveland, who was both the 22nd and the 24th president of the United States. □

Problem 29. Let $A = \{1, 2, 3, 4\}$. Write a list of all the subsets of A. (HINT: There are 16 of them.) □

Problem 30. Write a definition, in the style of Example 46, of the set X whose members are the first 325 prime numbers p such that $p-3$ is divisible by 4. □

8.3 Operations on sets

There are several operations that enable us to construct new sets from given sets.

8.4 The power set of a set

Definition 15. Let A be a set. The power set of A is the set $\mathcal{P}(A)$ given by

$$\mathcal{P}(A) = \{X : X \subseteq A\}\,.$$

In other words, $\mathcal{P}(A)$ ***(read as "the power set of*** A***") is the set whose members are all the subsets of*** A***.***

The ***membership criterion*** for the power set $\mathcal{P}(A)$ is the sentence "$X \subseteq A$". That is, for an object X to quality as a member of $\mathcal{P}(A)$, it has to be shown that X is a subset of A.

Example 47. If $A = \{1, 2, 3\}$ then

$$\mathcal{P}(A) = \Big\{\,\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\,\Big\}\,. \qquad (8.146)$$

Notice that A *is a finite set with* 3 *members, and* $\mathcal{P}(A)$ *has turned out to be a finite set with* 8 *members.* ***This is not a coincidence. We will prove later that: if*** A ***is a finite set and*** A ***has*** n ***members, then the power set*** $\mathcal{P}(A)$ ***is a finite set with*** 2^n ***members.*** □

Problem 31. Let $A = \{1, 2, 3, 4\}$. Write a formula similar to (8.146) listing all the members of $\mathcal{P}(A)$.

Problem 32. Let $A = \{\,\emptyset, \{\emptyset\}\,\}$. Write a formula similar to (8.146) listing all the members of $\mathcal{P}\Big(\mathcal{P}(A)\Big)$.

8.5 The union of two sets

Definition 16. Let A, B be sets. The union of A and B is the set $A \cup B$ given by

$$A \cup B = \{x : x \in A \vee x \in B\}\,.$$

In other words, $A \cup B$ ***(read as "A union B") is the set whose members are all the members of A as well as all the members of B.***

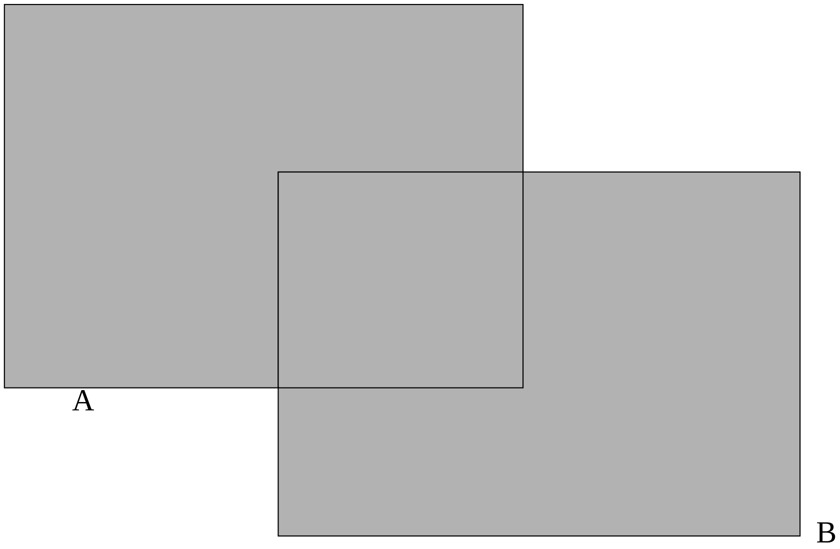
The ***membership criterion*** for $A \cup B$ is "$x \in A \vee x \in B$." That is, for an object x to quality as a member of $A \cup B$, it has to be shown that x is in A or that x is in B.

Example 48.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A \cup B = \{1, 2, 3, 4\}$.
- If $A = \{a, b, c\}$ and $B = \{d, e, f, g, h, i, j\}$ then $A \cup B = \{a, b, c, d, e, f, g, h, i, j\}$. *Notice that*

  1. *A is a finite set with 3 members,*
  2. *B is a finite set with 7 members,*
  3. *A and B have no memebrs in common (that is, using the terminology of the next section, $A \cap B = \emptyset$),*
  4. *and $A \cup B$ has turned out to be a finite set with 10 members.* ***This is not a coincidence. We will prove later that: if A, B are finite sets, A has m members, B has n members, and $A \cap B = \emptyset$, then the union $A \cup B$ is a finite set with $m + n$ members.***
  5. *If $A = \{n \in \mathbb{Z} : n > 0\}$ and $B = \{n \in \mathbb{Z} : n < 0\}$ then $A \cup B = \{n \in \mathbb{Z} : n \neq 0\}$.*
  6. *$\mathbb{N} \cup \{0\}$ is the set of all nonnegative integers, i.e., the set $\{n \in \mathbb{Z} : n \geq 0\}$.*
  7. *If $A = \{x \in \mathbb{R} : 0 < x < 1\}$ and $B = \{x \in \mathbb{R} : 1 \leq x < 2\}$ then $A \cup B = \{x \in \mathbb{R} : 0 < x < 2\}$.*
  8. *If $A = \{x \in \mathbb{R} : 0 < x < 1\}$ and $B = \{x \in \mathbb{R} : 1 < x < 2\}$ then $A \cup B = \{x \in \mathbb{R} : 0 < x < 2 \wedge x \neq 1\}$.* □

$$A \cup B:$$



(The shaded region is $A \cup B$)

8.6 The intersection of two sets

Definition 17. Let A, B be sets. The intersection of A and B is the set $A \cap B$ given by

$$A \cap B = \{x : x \in A \wedge x \in B\}\,.$$

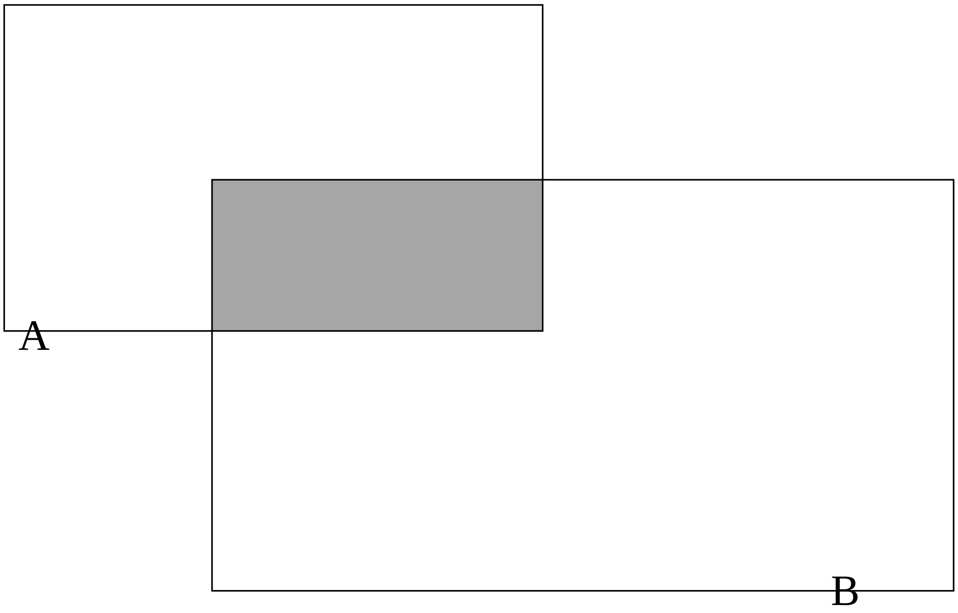
In other words, $A \cap B$ ***(read as "A intersection B") is the set whose members are all the things that belong both to A and to B.***

The ***membership criterion*** for $A \cap B$ is "$x \in A \wedge x \in B$." That is, for an object x to quality as a member of $A \cap B$, it has to be shown that x is in A and that x is in B.

Example 49.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A \cap B = \{2, 3\}$.
- If $A = \{n \in \mathbb{Z} : n > 0\}$ and $B = \{n \in \mathbb{Z} : n < 0\}$ then $A \cap B = \emptyset$.
- If $A = \{x \in \mathbb{R} : 0 < x < 2\}$ and $B = \{x \in \mathbb{R} : 1 < x < 3\}$ then $A \cap B = \{x \in \mathbb{R} : 1 < x < 2\}$.

$A \cap B$:



(The shaded region is $A \cap B$)

8.7 The difference of two sets

Definition 18. Let A, B be sets. The difference of A and B is the set $A - B$ given by

$$A - B = \{x : x \in A \land x \notin B\} .$$

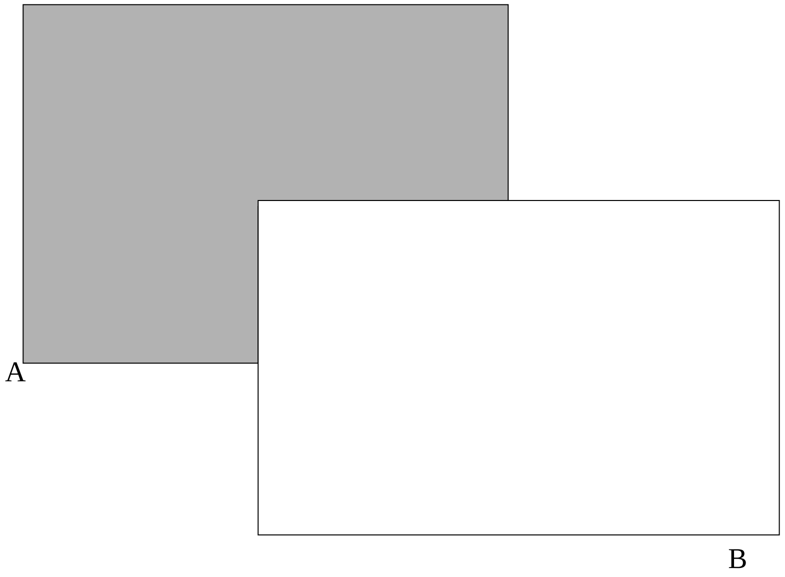
In other words, $A-B$ ***(read as "A minus B") is the set whose members are all the things that belong to A but do not belong to B.***

The ***membership criterion*** for $A - B$ is "$x \in A \land x \notin B$." That is, for an object x to quality as a member of $A - B$, it has to be shown that x is in A and that x is not in B.

Example 50.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A - B = \{1\}$.
- If $A = \mathbb{Z}$ and $B = \mathbb{N}$ then $A - B = \{n \in \mathbb{Z} : n \geq 0\}$.
- If $A = \{x \in \mathbb{R} : 0 < x < 2\}$ and $B = \{x \in \mathbb{R} : 1 < x < 3\}$ then $A - B = \{x \in \mathbb{R} : 0 < x \leq 1\}$.

$A - B$:



(The shaded region is $A - B$)

8.8 Complements

As you may have noticed, the operations of union and intersection are cloely related to the logical connectives $\vee$ and $\wedge$:

$A \cup B$ is the set of those x such that $x \in A \vee x \in B$

$A \cap B$ is the set of those x such that $x \in A \wedge x \in B$

Given this, which is rhe set operation that corresponds to the negation symbol $\sim$? Since $\sim$ is a unary connective (i.e., it can be applied to one sentence S to produce the sentence $\sim S$. the corresponding operation, let us call it #, should be a unary operation defined as follows:

$\#A$ is the set of those x such that $\sim x \in A$.

In other words, $\#A$ should be the set of all the things that are not members of A. This set $\#A$ could be called the "complement" of A, and would be defined by $\#A = \{x : x \notin A\}$.

Now, the set $\#A$ would be truly huge. For example, if $A = \{1, 2, 3, 4\}$, then $\#A$ would consist of all the things other than the numbers $1, 2, 3, 4$. So the members of $\#A$ would be the natural numbers other than $1, 2, 34$ (that is, $5, 6, 7$ and so on), as well as the integers that are not hantural numbers, all the real numbers other than $1, 2, 3, 4$, plus all the other things that are not the numbers $1, 2, 3, 4$, that is, all the cows, sheep, giraffes, people, rocks, tables, planets, stars, cells, viruses, molecules, atoms, electorns, protons, quarks, black holes, books, teeth, jackets, socks, cars, planes, forks, knives, and on and on and on.

Usually, when we are doing mathematics, we are studying a specific "universe" of mathematical objects. For example, when we do number theory we study the natural numbers or the integers, when we do Calculus we work with the real nunbers, and when we do Multivariable Calculus we work with $\mathbb{R}^2$, the set of pairs of real numbers)(i.e., the "xy plane") or $\mathbb{R}^3$ (the set of triples (x, y, z) of real numbers, i.e., "3-dimensional space"). If, for example, our "world" is $\mathbb{R}$, then when we have a set A of real numbers, i.e., a subset A of $\mathbb{R}$, we would be interested in the set of real numbers that are not in A. And this set is the difference $\mathbb{R} - A$. Se we give the following definition:

Definition 19. Suppose U is a set that we regard as the "universe", in the sense that we are only interested in sets that are subsets of U. Then the complement of a set A such that $A \subseteq U$ is the set A^c given by

$$A^c = U - A\,, \tag{8.147}$$

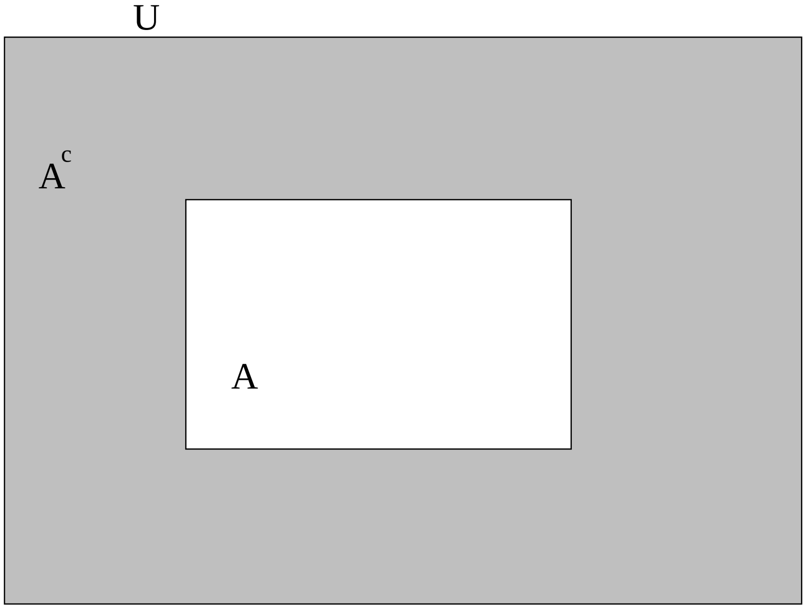
that is,

$$A^c = \{x : x \in U \wedge x \notin A\}\,. \tag{8.148}$$

Remark 11. Strictly speaking, it is inappropriate to define a set as we did in Definition 19 and call it "A^c". This set depends very much on who U is, so the right thing to do would be to call it the ***complement of*** A ***relative to*** A, and give it a name such as $A^{c,U}$, which shows that the set depends on U.

But, as long as we are working with a fixed "universe", and it is clear who U is, it is O.K. to use a notation such as A^c. □

$$A^c :$$



(The shaded region is A^c)

8.9 The symmetric difference of two sets

Definition 20. Let A, B be sets. The symmetric difference of A and B is the set $A\Delta B$ given by

$$A\Delta B = \{x : (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}\,.$$

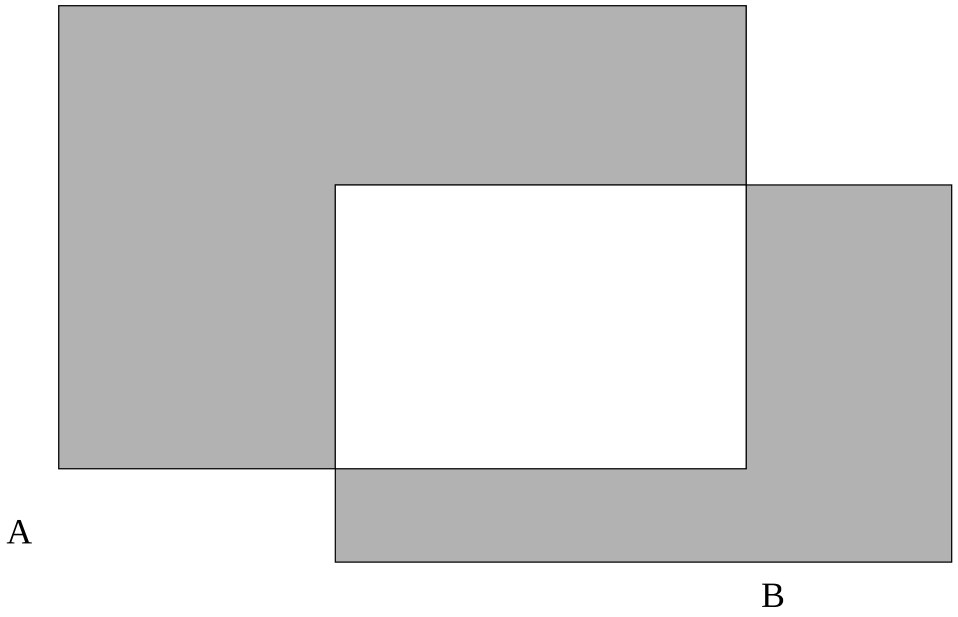
In other words, $A\Delta B$ ***(read as "the symmatric difference of*** A ***and*** B***") is the set whose members are all the things that belong to*** A

but do not belong to** B**, or belong to** B **but do not belomng to** A**.

That is, $A\Delta B$ ***is the set of all things that belong to one of the sets** A**,** B **but do not belong to both.***

The ***membership criterion*** for the symmetric difference $A\Delta B$ is the sentence "$(x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)$". That is, for an object x to quality as a member of $A - B$, it has to be shown that x is in A and that x is not in B, or that x is in B but not in A.

$A\Delta B$:



(The shaded region is $A\Delta B$)

Example 51.

- If $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then $A\Delta B = \{1, 4\}$.

- If $A = \{x \in \mathbb{R} : |x| > 4\}$ and $B = \{x \in \mathbb{R} : |x| < 10$ then $A \Delta B = \{x \in \mathbb{R} : |x| \geq 10 \vee |x| \leq 4\}$.

8.10 The Cartesian product of two sets

8.10.1 Ordered pairs

If a, b are any two objects, we would like to have a set, called "the ordered pair of a and b", such that wknowing this set would tell us who a is and who b is, so we would be able to say things such as "the first coordinate of (a, b) is a" and "the second coordinate of (a, b) is b".

For example, suppose we are doing plane geometry, using the standard procedure of drawing and "x axis" and a "y axis", and then representing each point P of the plane by a pair (a, b) of numbers, called the "coordinate pair" of P. Each point P then has, attached to it, a coordinate pair (a, b) of real numbers: the number a is the x ***coordinate*** (or "abscissa") and the number b is the y ***coordinate*** (or "ordinate") of P.

We would like the pair (a, b) to be a set, constructed somehow from a and b. And then the natural question is: which set is the pair (a, b)?

The most naïve idea is to let the pair (a, b) be the unordered pair $\{a, b\}$, that is, the set whose members are a and b.

But this will not do. If we take (a, b) to be $\{a, b\}$, then it cannot happen, for example, that the x-coordinate of $(1, 2)$ is 1, and the x-coordinate of $(2, 1)$ is 2, because, if $(1, 2) = \{1, 2\}$ and $(2, 1) = \{2, 1\}$, then $(1, 2) = (2, 1)$, so, if

(*) the x-coordinate of $(2, 1)$ is 2,

then it would also be true that

(**) the x-coordinate of $(1, 2)$ is 2,

(because $(1, 2) = (2, 1)$), but on the other hand

(***) the x-coordinate of $(1, 2)$ is 1,

so we would get $1 = 2$, which is definitely not true.

The only solution is to define the ordered pair to be something other than the unordered pair $\{a, b\}$. And then the question is, ***what set shall*** (a, b) ***be?***

There are many ways to answer this question, and it really makes no difference which one we use. So we shall choose one, but you must be warned that the specific way we make this choce is not important. What is important is that the following fact is true:

Theorem 24. *Let a, b, c, d be any objects. Then, if the pairs (a, b) and (c, d) are equal, that is, if $(a, b) = (c, d)$, it follows that $c = a$ and $d = b$.*

This is exactly the property that we need. For example, the pairs $(2, 1)$ and $(1, 2)$ are ***not*** equal. (Proof: Suppose $(2, 1) = (1, 2)$. Then Theorem 24 (with $a = 2$, $b = 1$, $c = 1$, and $d = 2$, would imply that $2 = 1$. But $2 \neq 1$. So $2 = 1 \wedge 2 \neq 1$, which is a contradiction. So $(2, 1) \neq (1, 2)$.)

Now we show how to define (a, b) in such a way that Theorem 24 is true.

Definition 21. Let a, b be any two objects. Then the <u>ordered pair</u> of a and b is the set (a, b) given by

$$(a, b) = \{\, \{a\}\, ,\, \{a, b\}\, \}\, . \tag{8.149}$$

Proof of Theorem 24. Suppose that $(a, b) = (c, d)$.
Let $p = (a, b)$, so p is also equal to (c, d) because we are assuming that $(a, b) = (c, d)$.
Since $p = \{\, \{a\}, \{a, b\}\, \}$, the set p has either two members (if $b \neq a$) or one member (if $a = b$, in which case $\{a, b\} = \{a\}$, so $\{\, \{a\}, \{a, b\}\, \} = \{\, \{a\}, \{a\}\, \} = \{\, \{a\}\, \}$).
But in either case, a is the only object that belongs to all the members of p.
And, since p is also equal to (c, d), it follows that c is the only object that belongs to all the members of p.
So $\boxed{\boxed{c = a}}$.
Next, let us prove that $d = b$.
We consider separately the two possible cases: $b = a$ and $b \neq a$.

> Assume that $b = a$.
>
> Then p has only one member, because, as explained before, $\{a, b\} = \{a\}$, so $p = \{\, \{a\}, \{a, b\}\, \} = \{\, \{a\}\, \}$.
>
> But then (c, d) also has only one member, because $(c, d) = p$. And this implies that $d = c$.
>
> So $d = c$ and $b = a$, and we already know that $c = a$.
>
> Hence $\boxed{d = b}$.
>
> Now assume that $b \neq a$.

Then the sets $\{a\}$ and $\{a,b\}$ are different, because $b \in \{a,b\}$ but $b \notin \{a\}$.

So p has two different members.

And b is the only object that belongs to one of the members of p but does not belong to both.

And, similarly, d is the only object that belongs to one of the members of p but does nto belong to both.

So $\boxed{d = b}$.

We have proved that $d = b$ in both cases, when $b = a$ and when $b \neq a$.
So $\boxed{\boxed{d = b}}$.

So we have proved that $\boxed{\boxed{\boxed{c = a \wedge d = b}}}$. **Q.E.D.**

8.10.2 The Cartesian product of two sets

Definition 22. Let A, B be sets. The <u>Cartesian product</u> of A and B is the set $A \times B$ given by

$$A \times B = \Big\{ u : (\exists a)(\exists b)(a \in A \wedge b \in B \wedge u = (a,b)) \Big\}.$$

In other words, $A \times B$ (read as "A times B") is the set of all objects u such that u is an ordered pair (a,b), with $a \in A$ and $b \in B$.

Or, more succintly and elegantly, $A \times B$ ***is the set of all ordered pairs*** (a,b) ***for which*** $a \in A$ ***and*** $b \in B$.

Example 52.

- Let $A == \{1,2,3\}$ and $B = \{2,3,4,5\}$. Then

$$\begin{aligned} A \times B \; = \; \Big\{ & (1,2),(1,3),(1,4),(1,5),(2,2),(2,3),(2,4),(2,5), \\ & (3,2),(3,3),(3,4),(3,5) \Big\}. \end{aligned}$$

Notice that A is a finite set with 3 members, B is a finite set with 4 members, and $A \times B$ is a finite set with 12 members. ***This is not a coincidence. We will prove later that: if A, B are finite sets, A has m members, and B has n members, then $A \times B$ is a finite set and $A \times B$ has mn members.***

- Let $A = \mathbb{R}$, $B = \mathbb{R}$. Then $A \times B$ is $\mathbb{R} \times \mathbb{R}$, that is, the set of all ordered pairs (x, y) such that x and y are real numbers. ***This is the "x-y plane" of plane Euclidean geometry. The members of $\mathbb{R} \times \mathbb{R}$ are the "points" of plane geometry.***

- Let

$$\begin{aligned} A &= \{x \in \mathbb{R} : 0 < x < 1\}\,, \\ B &= \{x \in \mathbb{R} : 1 < x < 3\}\,. \end{aligned}$$

Then A is the open interval $(0, 1)$ (***not to be confused with the ordered pair** $(0, 1)$**!***) and B is the open interval $(1, 3)$ (***not to be confused with the ordered pair** $(1, 3)$**!***). In this case, $A \times B$, that is, $(0, 1) \times (1, 3)$, is the set of all pairs (x, y) of real numbers such that $0 < xx < 1$ and $1 < y < 3$. In other words, $(0, 1) \times (1, 3)$ ***is the rectangle R characterized by the inequalities***

$$0 < x < 1 \qquad \text{and} \qquad 1 < y < 3\,.$$

8.11 Important facts about the set operations

So far, we have defined:

- One very special set (the empty set),
- One binary predicate (i.e., relation), about sets, namely, the predicate "is a subset of".
- Five binary operations on sets (union, intersection, difference, symmetric difference, and Cartesian product),
- One unary operation on sets (the power set).

By combining these nine things we can produce an enormous number of possible facts, some of which might be true, while others are not true. It would be pointless for me to give you a complete list and prove them all, because there are so many of them, and they are all so easy to prove (if true) or to disprove (if false).

And it would be pointless for you to memorize them all, because the list is so long. On the other hand, if you understand what yoiu are doing, you ought to be able, in each case, to figure out if the statement is true or false, and how to prove it (if it is true) or disprove it (if it is false).

So what I suggest is this: ***read carefully the list of facts, and pick a few of them and prove them or disprove them. Keep in mind that any of these facts could show up as a question in the exams.***

And here is the list:

1. If A is a set, then $\emptyset \subseteq A$. (True)

2. If A is a set, then $\emptyset \in A$. (False)

3. If A is a set, then $A \cup \emptyset = A$. (True)
   NOTE: If you think that $\emptyset$ is like the number 0, and the operation "$\cup$" is like addition, then this statement is analogous to the statement that $x + 0 = x$ for every real number x.

4. If A is a set, then $A \cup \emptyset = \emptyset$. (False)

5. If A is a set, then $A \cap \emptyset = A$. (False)

6. If A is a set, then $A \cap \emptyset = \emptyset$. (True)
   NOTE: If you think that $\emptyset$ is like the number 0, and the operation "$\cap$" is like multiplication, then this statement is analogous to the statement that $x.0 = 0$ for every real number x.

7. If A is a set, then $A \subseteq A$. (True)

8. If A, B are sets, then $A = B$ if and only if $A \subseteq B \wedge B \subseteq A$. (True)
   NOTE: This gives an another way to prove that two sets are equal: to prove that $A = B$, you prove that $A \subseteq B$ and that $B \subseteq A$.

9. If A is a set, then $A \cup A = A$. (True)

10. If A is a set, then $A \cap A = A$. (True)

11. If A, B are sets, then $A \subseteq A \cup B$. (True)

12. If A, B are sets, then $A \subseteq A \cap B$. (False)

13. If A, B are sets, then $A \cup B \subseteq A$. (False)

14. If A, B are sets, then $A \cap B \subseteq A$. (True)

15. If A is a set, then $A \subseteq A$. (True)
    NOTE: This aays that the binary relation "$\subseteq$" is reflexive.

16. If A, B are sets, $A \subseteq B$, and $B \subseteq A$, then $A = B$. (True)
    NOTE: This aays that the binary relation "$\subseteq$" is antisymmetric.

17. If A, B, C are sets, $A \subseteq B$, and $B \subseteq C$, then $A \subseteq C$. (True)
    NOTE: This aays that the binary relation "$\subseteq$" is transitive.

18. If A, B, C are sets, $A \subseteq B$, $B \subseteq C$, and $C \subseteq A$, then $A = B = C$. (True)

19. If A, B are sets, then $A \subseteq B$ if and only if $A \cup B = B$. (True)

20. If A, B are sets, then $A \subseteq B$ if and only if $A \cup B = A$. (False)

21. If A, B are sets, then $A \subseteq B$ if and only if $A \cap B = A$. (True)

22. If A, B are sets, then $A \subseteq B$ if and only if $A \cap B = B$. (False)

23. If A, B are sets, then $A \cup B = B \cup A$. (True)
    *NOTE: This is the **commutative law of the union operation**.*

24. If A, B are sets, then $A \cap B = B \cap A$. (True)
    *NOTE: This is the **commutative law of the intersection operation**.*

25. If A, B, C are sets, then $A \cup (B \cup C) = (A \cup B) \cup C$. (True)
    *NOTE: This is the **associative law of the union operation**.*

26. If A, B, C are sets, then $A \cap (B \cap C) = (A \cap B) \cap C$. (True)
    *NOTE: This is the **associative law of the intersection operation**.*

27. If A, B, C are sets, and $A \subseteq B$, then $A \cup C \subseteq B \cup C$. (True)

28. If A, B, C are sets, and $A \subseteq B$, then $A \cap C \subseteq B \cap C$. (True)

29. If A, B, C are sets, then $(A \cup B) \cap C = A \cup (B \cap C)$. (False)

30. If A, B, C are sets, then $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.(True)
NOTE: This is the ***distributive law of union with respect to intersection****.*

31. If A, B, C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.(True)
NOTE: This is the ***distributive law of intersection with respect to union****.*

    IMPORTANT NOTE: We have seen that union and intersection are in some ways like addition and multiplication: they obey commoutative and associative laws. and also $A \cap \emptyset = \emptyset$ (which is analogous to $x \cdot 0 = 0$) and $A \cup \emptyset = A$ (which is analgous to $x + 0 = x$). But ***the analogy should not be pushed too far:***

    - *there is a distributive law of union with respect to intersection (i.e., $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$),*
    - *and there is also a distributive law of intersection with respect to union (i.e., $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$),*
    - *but this is totally unlike what happens for addition and multiplication, because*
    - *there is a distributive law of multiplication with respect to addition (i.e., $x \cdot (y + z) = x \cdot y + x \cdot z$)*
    - *but there is no distributive law of addition with respect to multiplication (i.e., it is not true that $x + (y \cdot z) = (x + y) \cdot (x + z)$ since, for example, if we take $x = 1$, $y = 2$, $z = 3$, then $x + (y \cdot z) = 7$ and $(x + y) \cdot (x + z) = 12$).*

32. If A, B are sets, then $(A - B) \cup B = A$. (False)

33. If A, B are sets, then $(A - B) \cup B \subseteq A$. (False)

34. If A, B are sets, then $A \subseteq (A - B) \cup B$. (True)

35. If A, B, C are sets, then $A \cup (B - C) = (A \cup B) - (A \cup C)$. (False)

36. If A, B, C are sets, then $A \cap (B - C) = (A \cap B) - (A \cap C)$. (False)

    When we fix a "universe" U, then the complement of a subset A of U is defined to be the set $U - A$. The complement of A is denoted by "A^c".

37. If A, U are sets, and $A \subseteq U$, then $(A^c)^c = A$. (True)

38. If A, U are sets, and $A \subseteq U$, then $A \cup A^c = U$. (True)

39. If A, U are sets, and $A \subseteq U$, then $A \cap A^c == \emptyset$. (True)

40. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then

$$(A \cup B)^c = A^c \cap B^c\,. \tag{8.150}$$

    (This is true.)

41. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then

$$(A \cap B)^c = A^c \cup B^c\,. \tag{8.151}$$

    (This is true.)

    NOTE: Equations (8.150) and (8.151) are the famous ***De Morgan laws****. They say that*

    - ***the complement of the union of two sets is the intersection of the complements of the sets****,*

    and

    - ***the complement of the intersection of two sets is the union of the complements of the sets****.*

    I strongly recommend that you read the article on "De Morgab laws" in Wikipedia.

42. If A, B, U are sets, $A \subseteq U$, and $B \subseteq U$, then $A - B = A \cap B^c$. (True)

43. If A, B are sets, then $A - B = B - A$. (False)

44. If A, B, C are sets, then $A - (B - C) = (A - B) - C$. (False)

45. If A, B are sets, then $A\Delta B = (A \cup B) - (A \cap B)$. (True)

46. If A, B are sets, then $A\Delta B = B\Delta A$. (True)

47. If A, B, C are sets, then $A\Delta(B\Delta C) = (A\Delta B)\Delta C$. (True)

48. If A, B are sets, then $A \times B = B \times A$. (False)

49. If A, B, C, D are sets, then

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) .$$

(This is true.)

50. If A, B, C, D are sets, then

$$(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D) .$$

(This is false.)

51. If A is a set, then $A \in \mathcal{P}(A)$. (True)

52. If A is a set, then $A \subseteq \mathcal{P}(A)$. (False)

53. If A is a set, then $\emptyset \in \mathcal{P}(A)$. (True)

54. If A is a set, then $\emptyset \subseteq \mathcal{P}(A)$. (True)

55. If A, B are sets, then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. (True)

56. If A, B are sets, then $A = B$ if and only if $\mathcal{P}(A) = \mathcal{P}(B)$. (True)

57. If A, B are sets, then $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$. (False)

58. If A is a set, then $\emptyset \times A = \emptyset$ and $A \times \emptyset = \emptyset$. (True)

59. If A, B are sets, and $A \times B = B \times A$, then $A = B$. (False)

60. If A, B are nonempty sets, and $A \times B = B \times A$, then $A = B$. (True)

8.12 Some examples of proofs about sets

Let me give you the proofs of some of the results in the long list of the previous section.

8.12.1 Proof of one of the distributive laws

Theorem 25. *If A, B, C are sets, then*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\,. \tag{8.152}$$

Proof. To prove that the sets $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ are equal, we prove that they have the same members, that is, we prove that

$$(\forall x)\Big(x \in A \cup (B \cap C) \Longleftrightarrow x \in (A \cup B) \cap (A \cup C)\Big)\,. \tag{8.153}$$

Sentence (8.153) is a universal sentence, of the form $(\forall x)P(x)$. So, in order to prove it, we let x be an arbitrary object and prove $P(x)$.

Let x be arbitrary.

We want to prove

$$x \in A \cup (B \cap C) \Longleftrightarrow x \in (A \cup B) \cap (A \cup C)\,. \tag{8.154}$$

(1) The sentence "$x \in A \cup (B \cap C)$" is equivalent to "$x \in A \vee x \in B \cap C$". (Reason: if X, Y are sets, then the criterion for membership in $X \cup Y$ is "$x \in X \vee x \in Y$".)

(2) And "$x \in B \cap C$" is equivalent to "$x \in B \wedge x \in C$". (Reason: if X, Y are sets, then the criterion for membership in $X \cap Y$ is "$x \in X \wedge x \in Y$".)

(3) Hence "$x \in A \cup (B \cap C)$" is equivalent to "$x \in A \vee (x \in B \wedge x \in C)$".

(4) Also, "$x \in (A \cup B) \cap (A \cup C)$" is equivalent to "$x \in A \cup B \wedge x \in A \cup C$".

And

- "$x \in A \cup B$" is equivalent to "$x \in A \vee x \in B$".
- "$x \in A \cup C$" is equivalent to "$x \in A \vee x \in C$".

(5) So "$x \in (A \cup B) \cap (A \cup C)$" is equivalent to "$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$".

It follows from (3) and (6) that "$x \in A \cup (B \cap C) \Longleftrightarrow x \in (A \cup B) \cap (A \cup C)$", the sentence that we have to prove, is equivalent to

$$x \in A \vee (x \in B \wedge x \in C) \Longleftrightarrow \Big((x \in A \vee x \in B) \wedge (x \in A \vee x \in C)\Big)\,. \tag{8.155}$$

The sentence (8.155) is of the form

$$P \vee (Q \wedge R) \Longleftrightarrow \Big(P \vee Q) \wedge (P \vee R)\Big) , \tag{8.156}$$

where P stands for "$x \in A$", Q stands for "$x \in B$", and R stands for "$x \in C$".

We now prove that (8.156) is true.

Sentence (8.156) is a biconditional, of the form $\mathcal{L} \Longleftrightarrow \mathcal{M}$. And a biconditional $\mathcal{L} \Longleftrightarrow \mathcal{M}$ is true if and only if $\mathcal{L}$ and $\mathcal{M}$ have the same truth value, i.e., are both true or both false. So we are going to prove that $\mathcal{M}$ is true if $\mathcal{L}$ is true and $\mathcal{M}$ is false if $\mathcal{L}$ is false.

> Suppose that $P \vee (Q \wedge R)$ is true.
>
> Then either P is true or $Q \wedge R$ is true.
>
> > Suppose P is true.
> > Then both $P \vee Q$ and $P \vee R$ are true.
> > So $(P \vee Q) \wedge (P \vee R)$ is true.
> > Now suppose that $Q \wedge R$ is true.
> > Then both Q and R are true.
> > So $P \vee Q$ and $P \vee R$ are true.
> > And then $(P \vee Q) \wedge (P \vee R)$ is true.
>
> So $(P \vee Q) \wedge (P \vee R)$ is true in both cases, and then $(P \vee Q) \wedge (P \vee R)$ is true.

This proves that $(P \vee Q) \wedge (P \vee R)$ is true if $P \vee (Q \wedge R)$ is true.

> Now suppose that $P \vee (Q \wedge R)$ is false.
>
> Then both P and $Q \wedge R$ are false.
>
> Since $Q \wedge R$ is false, either Q is false or R is false.
>
> > Suppose Q is false.
> > Since P is false, $P \vee Q$ is false, because both P and Q are false.
> > Hence the conjunction $(P \vee Q) \wedge (P \vee R)$ is false.
> > Now suppose R is false.

Since P is false, $P \vee R$ is false, because both P and R are false.

Hence the conjunction $(P \vee Q) \wedge (P \vee R)$ is false.

So $(P \vee Q) \wedge (P \vee R)$ is false in both cases, and then $(P \vee Q) \wedge (P \vee R)$ is false.

This proves that $(P \vee Q) \wedge (P \vee R)$ is false if $P \vee (Q \wedge R)$ is false.

So we have proved that (8.155) is true, and this completes our proof, **Q.E.D.**

Problem 33. ***Prove*** the other distributive law: If A, B, C are sets, then

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) . \tag{8.157}$$

8.12.2 Proofs of the De Morgan laws

As we explained before, the De Morgan laws are the following two statements.

Theorem 26. *Let U be a set, and let A, B be subsets of U. Then*

$$(A \cup B)^c = A^c \cap B^c ,$$

and

Theorem 27. *Let U be a set, and let A, B be subsets of U. Then*

$$\begin{aligned}(A \cup B)^c &= A^c \cap B^c , \\ (A \cap B)^c &= A^c \cap B^c .\end{aligned}$$

I will give you a proof from first principles[70] of the first theorem, and then I will give you a short proof of the other using the first one, and ask you to give a proof from first principles of the second theorem.

[70] A bf*proof from first principles* is a proof in which you do not use any intermediate results proved before. For example, after we proved that $2 + 2 = 4$ from first principles we proved that $2 \times 2 = 4$ using the result that $2 + 2 = 4$. That was ***not*** a proof from first principles. In a proof from first principles, you would just have used the basic facts and the definitions, and no theorem proved before.

Proof. We want to prove that

$$DeMorgan(\forall x \in U)\Big(x \in (A \cup B)^c \Longleftrightarrow x \in A^c \cap B^c\Big)\,. \tag{8.158}$$

The sentence we want to prove is a universal sentence, of the form $(\forall x)P(x)$. So in order to prove it we let x be an arbitrary object and prove $P(x)$.

Let x be an arbitrary member of U.

We want to prove that

$$x \in (A \cup B)^c \Longleftrightarrow x \in A^c \cap B^c\,. \tag{8.159}$$

But, for $x \in U$, "$x \in (A \cup B)^c$ is equivalent to "$x \notin A \cup B$", i.e., to "$\sim x \in A \cup B$".

And "$x \in A \cup B$" is equiva;ent to "$x \in A \vee x \in B$".

So "$x \notin A \cup B$" is equivalent to "$\sim (x \in A \vee x \in B)$".

Therefore "$x \in (A \cup B)^c$" is equivalent to "$\sim (x \in A \vee x \in B)$".

On the other hand, "$x \in A^c \cap B^c$" is equiva;ent to "$x \in A^c \wedge x \in B^c$".

And the sentences "$x \in A^c$", "$x \in B^c$" are equivalent to "$\sim x \in A$" and "$\sim x \in B$".

So "$x \in A^c \cap B^c$" is equivalent to "$(\sim x \in A) \wedge (\sim x \in B)$".

Hence (8.159) is equivalent to

$$\Big(\sim (x \in A \vee x \in B)\Big) \Longleftrightarrow \Big((\sim x \in A) \wedge (\sim x \in B)\Big)\,. \tag{8.160}$$

If we use P to stand for "$x \in A$", and Q to stand for "$x \in B$", then (8.160) is the sentence

$$\Big(\sim (P \vee Q)\Big) \Longleftrightarrow \Big((\sim P) \wedge (\sim Q)\Big)\,. \tag{8.161}$$

The biconditional sentence (8.161) is of the form $\mathcal{L} \Longleftrightarrow \mathcal{M}$. And a biconditional $\mathcal{L} \Longleftrightarrow \mathcal{M}$ is true if and only if $\mathcal{L}$ and $\mathcal{M}$ have the same truth value, i.e., are both true or both false. So we are going to prove that $\mathcal{M}$ is true if $\mathcal{L}$ is true and $\mathcal{M}$ is false if $\mathcal{L}$ is false.

Proof that if $\sim(P \vee Q)$ *is true then* $(\sim P) \wedge (\sim Q)$ *is true.*

Suppose that $\boxed{\sim(P \vee Q) \text{ is true}}$.

Then $P \vee Q$ is false.

So both P and Q are false.

Hence $\sim P$ and $\sim Q$ are true.

So the conjunction $\boxed{(\sim P) \wedge (\sim Q) \text{ is true}}$.

Proof that if $\sim(P \vee Q)$ *is false then* $(\sim P) \wedge (\sim Q)$ *is false.*

Suppose that $\boxed{\sim(P \vee Q) \text{ is false}}$.

Then $P \vee Q$ is true.

So either P is true or Q is true.

Suppose that P is true.
Then $\sim P$ is false.
So the conjunction $(\sim P) \wedge (\sim Q)$ is false.
Now suppose that Q is true.
Then $\sim Q$ is false.
So the conjunction $(\sim P) \wedge (\sim Q)$ is false.

We have shown that $(\sim P) \wedge (\sim Q)$ is false in both cases, when P is true and when Q is true.

Hence $\boxed{(\sim P) \wedge (\sim Q) \text{ is false}}$.

So we have proved (8.159) for an arbitrary member x of U, and we can go to

$$(\forall x \in U)\Big(x \in (A \cup B)^c \Longleftrightarrow x \in A^c \cap B^c\Big)\,. \tag{8.162}$$

And (8.162) says that the sets $(A \cup B)^c$ and $(A \cap B)^c$ have rhe same members, so the sets are equal, that ism

$$(A \cup B)^c = A^c \cap B^c\,. \tag{8.163}$$

This is exactly what we wanted to prove. **Q.E.D.**

Now let us give a simple proof of Theorem 27 using Theorem 26.
Proof. We want to prove that $(A \cap B)^c = A^c \cup B^c$.

Theorem 26 says that, if X, Y are any subsets of U, then

$$(X \cup Y)^c = X^c \cap Y^c \,. \tag{8.164}$$

Apply this with $X = A^c$ and $B = Y^c$. We get

$$(A^c \cup B^c)^c = (A^c)^c \cap (B^c)^c \,. \tag{8.165}$$

But $(A^c)^c = A$, and $(B^c)^c = B$. So

$$(A^c \cup B^c)^c = A \cap B \,. \tag{8.166}$$

Now take the complement of both sides. We get

$$\Big((A^c \cup B^c)^c\Big)^c = (A \cap B)^c \,. \tag{8.167}$$

But $(X^c)^c = X$ for every subset X of U. Therefore

$$\Big((A^c \cup B^c)^c\Big)^c = A^c \cup B^c \tag{8.168}$$

Combining (8.167) and (8.168), we get

$$A^c \cup B^c c = (A \cap B)^c \,, \tag{8.169}$$

which is the formula we were trying to prove. **Q.E.D.**

Problem 34. Write a proof from first principles of Theorem 27. ***I strongly recommend that you use the same style as in the proof of Theorem 26. The proof of Theorem 26 is really very simple, and almost mechanical. It looks long because it was written on purpose to show you a proof written in a very precise, very detailed way, displaying the use of the rules of logic. Usually one does not write p;roofs like that, but I would like you to do it at least once, to show that you can do it.*** □

8.12.3 A proof involving the symmetric difference

Let us prove Fact 45 from our list. Recall that the ***symmetric difference*** of two sets A, B is the set $A\Delta B$ given by

$$A\Delta B = (A - B) \cup (B - A)\,.$$

In the proof, we are going to use the following facts, that are valid for arbitrary subsets X, Y, Z of a set U:

- $X - Y = X \cap Y^c$,
- $X \cup X^c = U$ and $X \cap X^c = \emptyset$,
- $X \cap U = X$ and $X \cap \emptyset = \emptyset$.
- $X \cup U = U$ and $X \cup \emptyset = X$.
- The commutative laws

$$\begin{array}{rcl} X \cup Y & = & Y \cup X\,, \\ X \cap Y & = & Y \cap X\,, \end{array}$$

- The associative laws

$$\begin{array}{rcl} X \cup (Y \cup Z) & = & (X \cup Y) \cup Z\,, \\ X \cap (Y \cap Z) & = & (X \cap Y) \cap Z\,, \end{array}$$

- The distributive laws

$$\begin{array}{rcl} X \cup (Y \cap Z) & = & (X \cup Y) \cap (X \cup Z)\,, \\ X \cap (Y \cup Z) & = & (X \cap Y) \cup (X \cap Z)\,, \end{array}$$

- The De Morgan laws

$$\begin{array}{rcl} X^c \cup Y^c & = & (X \cap Y)^c\,, \\ X^c \cap Y^c & = & (X \cup Y)^c\,. \end{array}$$

Theorem 28. *If A, B are sets, then $A\Delta B = (A \cup B) - (A \cap B)$.*

Proof. Choose as universe any set U such that $A \subseteq U$ and $B \subseteq U$. (For example, we could choose U to be $A \cup B$.)

Then

$$\begin{aligned}
A\Delta B &= (A-B)\cup(B-A) && (8.170)\\
&= (A\cap B^c)\cup(B\cap A^c) && (8.171)\\
&= \Big((A\cap B^c)\cup B\Big)\cap\Big((A\cap B^c)\cup A^c\Big) && (8.172)\\
&= \Big(B\cup(A\cap B^c)\Big)\cap\Big(A^c\cup(A\cap B^c)\Big) && (8.173)\\
&= \Big((B\cup A)\cap(B\cup B^c)\Big)\cap\Big((A^c\cup A)\cap(A^c\cup B^c)\Big) && (8.174)\\
&= \Big((B\cup A)\cap U\Big)\cap\Big(U\cap(A^c\cup B^c)\Big) && (8.175)\\
&= (B\cup A)\cap(A^c\cup B^c) && (8.176)\\
&= (A\cup B)\cap(A^c\cup B^c) && (8.177)\\
&= (A\cup B)\cap(A\cap B)^c\,. && (8.178)
\end{aligned}$$

So $A\Delta B = (A\cup B)-(A\cap B)$. **Q.E.D.**

Problem 35. Write the justfications of each of the nine steps (8.170), (8.171), (8.172), (8.173), (8.174), (8.175), (8.176), (8.177), (8.178) of the proof of Theorem 28. □

Problem 36. ***Prove or disprove*** each of the following distributive laws

1. *The distributive law of intersection with respect to symmetric difference.* If A, B, C are sets, then

$$A\cap(B\Delta C) = (A\cap B)\Delta(A\cap C)\,. \qquad (8.179)$$

2. *The distributive law of union with respect to symmetric difference.* If A, B, C are sets, then

$$A\cup(B\Delta C) = (A\cup B)\Delta(A\cup C)\,. \qquad (8.180)$$

9 Definitions: how you should write them and how you should not write them

9.1 An example of a correctly written definition

Suppose you don’t know what a prime number is. And suppose you are asked whether the numbers 1, 2, 6, 7, 10, 12, are “prime”. Then you will probably not be able to answer the question, because you don’t know what a “prime number” is. So you would answer with a question: *what is a prime number”*, or *what does it mean for a number to be prime?*

To answer such a question, you need to know the **definition** of “prime number”.

And here is the definition:

DEFINITION OF “PRIME NUMBER”

Let n be a natural number. We say that n is prime if $n \neq 1$ and the only natural numbers that are factors of n are 1 and n.

And here is another, equally correct, definition of “perfect number”:

DEFINITION OF “PRIME NUMBER”, VERSION II

A natural number n is prime if $n \neq 1$ and every natural number that is a factor of n is either equal to 1 or to n.

And here is a third, also completely correct, definition of “perfect number”:

DEFINITION OF "PRIME NUMBER", VERSION III

A natural number n is prime if $n \neq 1$ and $(\forall q \in \mathbb{N})\Big(q|n \Longrightarrow (q = 1 \vee q = n)\Big)$.

And, finally, here is a fourth completely correct definition of "perfect number":

DEFINITION OF "PRIME NUMBER", VERSION IV:

An integer n is a prime number if $n > 1$ and $(\forall q \in \mathbb{N})\Big(q|n \Longrightarrow (q = 1 \vee q = n)\Big)$.

9.2 How not to write a definition

Let us look now at some bad ways of writing the definition "prime number".

The examples I am going to give you are representative of things students often write in exams. ***You should read these examples carefully, and then read the explanation of why these definitions are bad, so that you will learn not to write that way.***

Some of the definitions below are truly horrendous (and would get zero points on a scale from 0 to 10), while others are not 100% wrong but are not entirely correct either, and may get 5 points on a 0-10 scale, or maybe in some cases even 6 or 7. But ***you should understand why those definitions are bad, so you can learn how to write definitions correctly and get* 10 *points otu of* 10*.***

Bad Definition 1. Prime number is when you cannot divide by any number other than by the number itself. □

Bad Definition 2. A prime number is a number that cannot be divided by any number other than 1 and itself. □

Bad Definition 3. A prime number is a natural number that cannot be divided by any number other than 1 and itself. □

Bad Definition 4. A prime number is a natural number such that the only factors of the number are 1 and the number itself. □

Bad Definition 5. A prime number is a natural number such that the only factors of n are 1 and n. □

Bad Definition 6. A prime number is a natural number such that the only natural numbers that are factors of n are 1 and n. □

Bad Definition 7. A prime number is a natural number such that $n > 1$ and the only natural numbers that are factors of n are 1 and n. □

Bad Definition 8. A prime number is a natural number n such that $n > 1$ and the only natural numbers that are factors of n are 1 and n. □

9.2.1 Analysis of bad definitions

Let us analyze our eight "bad definitions" and explain why they are bad.

The main question that we will ask, and the question that you should always ask, is: ***using this definition, can I tell correctly if an object is what the definition says it is supposed to be?*** (In this case, ***can I tell correctly if an object is a prime number or not?***)

Notice that this question really amounts to two questions:

(I) ***Can I tell?***, that is, *does the definition tell me precisely what to do in order to find out if the answer is "yes" or "no"?*

(II) Can I tell ***correctly***?, that is, *when I do what the definition tells me to do, do I get the right answers?*

Question (I) is the ***precision and clarity*** question: does the definition tell me cearly and precisely what I am supposed to do in order to find out the answer?

Question (II) is the ***correctenss*** question: If I do what the definition tells me to do, do I get the right answer?

These two questions are different. For example, if I were to define "prime number" as follows:

Bad Definition 9. A <u>prime number</u> is a natural number that is divisible by 2. □

Then this definition is completely clear and precise. It tells me that in order to find out if a number is prime, I have to see if it is divisible by 2. The problem with this definition is that it does not satisfy the ***correctness*** condition: if I apply the definition, say, to the number 6, I find that 6 is divisible by 2, so according to this definition 6 is prime, which is not true.

To assess a definition, you should always ask these two questions: is the definition clear and precise, so that when I want to apply it I know exactly what to do? And is it correct, in the sense that it gives me the right answers?

And, in order to answer the correctness question, you should ***test*** your definition by applying it to several examples and seeng whether it gives the right answer.

The simplest and most convincing way to establish that a definition is wrong is to give an example of something for which the definition gives thw rong answer. This is what we did when we disucssed the

You should always ask these two questions, ***especially about definitions you have written yourself.*** And if what you wrote does not meet the two requirements of (1) precision and clarity and (2) correctness, then your definition is not acceptable and you must work on it until you get it right.

Now let us look at the eight bad definitions in our list.

1. Bad Definition 1 says: *Prime number is when you cannot divide by any number other than by the number itself.*

   This is truly atrocious. Let us see why.

   – First of all, when you say “prime number is”, you are suggesting that “prime number” is a condition of the world, such as “chaos”, or “peace”. You can say something like “peace is when people are not fighting”, or “chaos is when there is utter confusion”. Even these sentences are very bad English, but you can more or less figure out what they mean. (For example, when you see that people are fighting, you would say that “there is no peace here”, and when people stop fighting, you would say “now there is peace”.) Much better ways to say these things would be: “Peace is the absence of war or other hostilities", or "Peace is a state of affairs in which people are not fighting".

- But in the case of "prime number", the "prime number is when" construction does not make sense. Being a prime number is not some kind of state of affairs. It is a property of a specific kind of object, namely, numbers. So one has to use much more precise language, and start the definition with "A prime number is", or "A number is prime if".

If a definition starts with "such and such is when..." you can be sure it is wrong:

- *"Prime number is when..." is wrong.*
- *"Divisible is when..." is wrong.*
- *"Even number is when..." is wrong.*
- *"Power set is when..." is wrong.*
- *"Subset is when..." is wrong.*
- *"Intersection is when..." is wrong.*

A correct definition of “prime number” should start in one of the following ways:

- “A prime number is a natural number n such that”
- “Let n be a natural number. Then n is a prime number if”
- “Let n be a natural number. We say that n is prime if”
- “A natural number n is prime if”

In other words: ***at the beginning of the definition you have to introduce the object or objects that you will be talking about.*** In this example, you do this by indicating that you will be talking about a natural number, not about a real number or a cow or a fish or a river. And you may give that natural number a name, such as n.

2. Bad Definitions 1 and 2 talk about “numbers”. We have already quoted Bad Definition 1, and Bad definition 2 says: *A pime number is a number that cannot be divided by any number other than* 1 *and itself.*

   This definition does not pass the “can I tell?” test. It tells me that to be a prime number an object has to be a “number”.

   But ***“number” is a vague concept***, because there are lots of different kinds of “numbers”, so when you say “number” you could mean “natural number” (that is, the kind of number that you are used to calling “whole number”), “integer”, “rational number”, “real number”, “complex number”, or lots of other kinds of numbers that exist.

Never say “number” unless it is clear what kind of “number” you are talking about.

If I want to follow Bad Definition 2, the, when I am given a thing and want to find out if that thing is a prime number, the first I thing I have to do is find out if it is a “number”. But I cannot do that because I don’t know what a “number” is. So the definition fails the “can I tell?” test.

In a correct, intelligible definition, when you talk about a ‘number”, you have to make it clear what you mean by “‘number”.

This can be made clear in at least three ways:

- You can just say what kind of number your number is supposed to be. (For example, you could say “let n be a natural number”, or “let n be an integer”, or “let n be a rational number”, or “let n be a real number”.)
- You can make it clear at the beginning of your text that the word “number” is always going to mean “integer”, or “real number”, or whatever. If you do so, then you don’t need to repeat that you mean “integer”, or “real number”, or whatever, every time you say “number”.
- You may want to talk about different kinds of numbers simultaneously. And, in order to do that, you may declare, at the beginning of your text, that, for example, “in this chapter, the letters m, n, p, q will always stand for natural numbers, and the letters x, y, z, u, v, w will stand for real numbers”.

3. Bad definitions 1, 2, and 3, talk about “dividing by numbers”, and tell me that a number is prime if it cannot be divided by certain numbers. But this is very confusing.

   - Actually, ***any number can be divided by any number (except zero)***. For example, I can divide 7 by 5, getting as a result the number $\frac{7}{5}$.
   - So the issue is not whether “we can divide”, because wwe can almost always do that, but ***what kind of result we get when we divide***.
   - When Bad Definition 3 tells me that I should see if a number “can be divided by numbers other that 1 and the number itself”, then I could try to apply the definition, for example, to the number 3, and I would immediately see that 3 can be divided by lots of numbers other than 1 and 3: I can divide 3 by 2 (and the result is $\frac{3}{2}$), I can divide 3 by 7 (and the result is $\frac{3}{7}$), I can divide 3 by 29 (and the result is $\frac{3}{29}$), and so on.

4. Bad Definitions 4 and 5 are a little bit better. Rather than talk about "dividing", they talk about "factors", which is more precise. because we have a precise definition of "factor".

   But that is not good enough. According to the definition of "factor", a factor of an integer a is an integer b such that there exists an integer k for which $a = bk$. So, when Bad Definition 5 says that

   > *A prime number is a natural number such that the only factors of n are 1 and n.*

   then ***this definition fails the correctness test***: ***according to this definition* 2 *is not prime***, becauuse 2 as other factors in addition to 1 and 2. Indeed, -1 and -2 are factors of 2 as well, since $2 = (-1) \times (-2)$ and $2 = (-2) \times (-12)$.

5. Bad Definition 6 is much better. It says that

   > *A prime number is a natural number such that the only natural numbers that are factors of n are 1 and n.*

   This is quite close, but ***this definition still fails the correctness test, because it gives us wrong answers***. Indeed, according to this definition 1 is prime. But this is wrong: 1 is not prime[71].

6. With Bad Definition 7 we enter, for the first time, the "partial credit" zone. This definition is essentially correct, but it is not well written. It says that

   > *A prime number is a natural number such that $n > 1$ and the only natural numbers that are factors of n are 1 and n.*

   The problem with this is that the defintion talks about "n" but does not tell us who this "n" is. ***In a mathematical text, when you refer to an object using a letter name, this name has to be introduced first.***

[71] Why is 1 not prime? For the same reason why Pluto is not a planet. Mathematicians have decided not to call 1 "prime", exactly as astronomers have decided not to call Pluto a planet. But this decision was made for good reasons, that will be discussed later in this course.

7. Bad Definition 8 does this: the symbol "n" is properly introduced when we are told that

   > *A prime number is a natural number n such that $n > 1$ and the only natural numbers that are factors of n are 1 and n.*

8. So Bad Ddefinition 8 is nearly perfect. What is missing? Only one thing: ***in a definition, the word or phrase being defined must be highlighted is some way, to indicate that we are defining that word or phrase.*** And when we write by hand the way we highlight is by underlining. So, for example, in a definition of "'prime number" the words "prime numebr" have to be underlined. And if we do that we get a correct definition. *A <u>prime number</u> is a natural number n such that $n > 1$ and the only natural numbers that are factors of n are 1 and n.*

9.2.2 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. But when we write by hand, it is hard to do Italics or Boldface, so we use underlining.

Look, for example, at any definitions you want in our textboook. Just open the book at random, at any page, and look at the definitions on that page. And, for each definition, ask yourself "what is this definition the definition of?" And, invariably, you will see that the term or phrase being defined is in **boldface**. (This is not just a peculiarity of our textbook. It's done in every Mathematics book.) In my lecture notes, I use underlining rather than boldface. And when you write your homework or your exams, or when I write on the blackboard, it's hard to do italics or boldface, so I use underlining instead, and you should do the same.

9.3 The general formats for definitions

In a definition, the word, symbol or phrase whose meanign we are trying to define is called the <u>definiendum</u>.

9.3.1 Step 1: Find out if the definiendum is a term or a sentence, and what its arguments are

In order to know how to write a definition of something, we first have to figure out two things:

1. Whether the definiendum is a ***term*** or a ***sentence***.
2. What the ***arguments*** of the definiendum are.

Recall that

- A ***term*** is a word or symbol or phrase that stands for a thing. Terms are essentially the same things that in your English or linguistics classes you may have called "noun phrases".
- A ***sentence*** is a word or symbol or phrase that makes an assertion that can be true or false. Sentences are essentially the same things as "predicates", or "statements".
- Terms and sentences have ***values***.
- The value of a term is the thing the term stands for. For example the term "New York City" is New York City.
- The value of a sentence is its truth value. For example, the sentence "New York City is the capital of New York State" has the truth value "false", because it is not true, but the sentence "Albany is the capital of New York State" has the truth value "true", because it is true.
- If a term or sentence contains variables, then the term or sentence only has a value, or truth value, is the variables that occur in it have been assigned values. For example,
  - the term "$x + y$" contains two variables, x and y. If we assign values to these variables, by saying something like "let $x = 5$, $y = 3$", then the term "$x + y$" has the value 8.
  - the sentence '$x + y = z$" contains three variables, x, y, and z. If we assign values to these variables, by saying something like "let $x = 5$, $y = 3$, $z = 4$", then the sentence "$x + y = z$" has the truth value "false", because $5 + 3$ is not equal to 4.

9.4 Step 2: Introduce the arguments

You must start your definition by introducing the arguments.

For example:

- If you want to define "prime number". then you will see, first of all, that the definiendum is a sentence, "something is a prime number". And it has one argument, because we say things such as "n is a prime number". What you want to explain to the readers is how to tell what the truth value of the definiendum is for any given value or values of the arguments. That is, you want to tell the readers under what conditions they should call a number n "prime", that is, when they should say "n is prime". So you definition must start by saying something like "Let n be an integer", or "let n be a natural number", or "let n be a real number". (Eventually, n will turn out to be a natural number anyhow. So you could start your definition by requiring n to be a natural number. But you can also require n to be an integer, and let the second part of the definition force n to be a natural number, for example by putting the requirement that $n > 1$. And you could even start by requiring n to be a real number, and then say later: "we say that n is a a prime number if it is a natural number such that ...".)

- "Divisible" is a two-argument sentence, because we say things such as "m is divisible by n", and these things are true or false. So in the definition of "divisible" you want to tell the readers under what conditions they should say of two numbers m, n that "m is divisible by n". And you must start by introducing the two numbers m and n, by saying something like "Let m, n be integers".

- "Union" is a two-argument term, because we talk about "the union of two sets A, B", and that union is a thing, namely, a set. So in the definition of "union" you want to tell the readers who the set $A \cup B$ is, if we are given two sets A, B. So you must start by introducing the two sets A and B, by saying something like "Let A, B be sets".

- "Subset" is a two-argument sentence, because we say things such as "A is a subset of B", and this sentence is true or false. So in the definition of "subset" you want to tell the readers under what conditions they should say that "$A \subseteq B$" is true, if we are given two sets A, B. And you must start by introducing the two sets A and B, by saying something like "Let A, B be sets".

- "Power set" is a one-argument term, because we talk about "the power set of a set A", and that power set is a thing, namely, a set. So in the definition of "power set" you want to tell the readers who the set $\mathcal{P}(A)$ is, if we are given a set A. So you must start by introducing the set A, by saying something like "Let A be a set".
- "Derivative" is more complicated, because there are two different concepts of derivative:
  - We talk about "the derivative of a function f at a point a." This is a two-argument term: the derivative of f at a is a real number. So your definition of "derivative of a function at a point" must start by saying something like "Let f be a function and let a be a real number".
  - We talk about "the derivative of a function f." This is a one-argument term: the derivative of a function f is another function, usually called f'. So your definition of "derivative of a function" must start by saying something like "Let f be a function".
- "married" is also complicated, like "derivative". because there are two different concepts of "married":
  - We talk about "two people begin married to each other." This is a two-argument sentence: if x and y are people, then "x and y are married to each other" can be true or false. So your definition of "x and y are married to each other" must start by saying something like "Let x, y be two persons".
  - We talk about one person being married, and say things like "x is married." This is a one-argument sentence. So your definition of "married" must start by saying something like "Let x be a person".

9.5 Step 3: Tell the readers how to find the value of the definiendum

Now that you have introduced the arguments, you have to tell your readers how they can determine the value of the definiendum for those arguments. That value will be a thing if the definiendum is a term, and a truth value if the definiendum is a sentence.

For example:

- In the definition of "prime number", after you have said, for example, "Let n be a natural number", you have to tell the readers how to figure out the value of the definiendum, for n. In this case, the definiendum is the sentence "n is prime", so you you have to tell the readers what has to happen that will make that sentence true. You can say, for example: "We say that n is a $\underline{\text{prime number}}$ if $n \neq 1$ and $(\forall m \in \mathbb{N})\Big(m|n \Longrightarrow (m = 1 \vee m = n)\Big)$".
- In the definition of "divisible". after you have said "Let m, n be integers", you have to tell the readers how to figure out the value of the definiendum, for m and n. In this case, the definiendum is the sentence "m is divisible by n", so you have to tell the readers what has to happen that will make them say that the sentence is true. You can say, for example: "We say that m is $\underline{\text{divisible}}$ by n if $(\exists k \in \mathbb{Z})m = nk$.".
- In the definition of "union". after you have said "Let A, B be sets", you have to tell the readers how to figure out the value of the definiendum, for A and B. In this case, the definiendum is the term "$A \cup B$", which is the name of a set. So you you have to tell the readers who that set is, by saying, for example: "the $\underline{\text{union}}$ of A and B is the set $A \cup B$ given by $A \cup B = \{x : x \in A \vee x \in B\}$."
- In the definition of "power set". after you have said "Let A be a set", you have to tell the readers how to figure out the value of the definiendum, for the set A. In this case, the definiendum is the term "$\mathcal{P}(A)$", which is the name of a set. So you you have to tell the readers who that set is, by saying, for example: "the $\underline{\text{power set}}$ of A is the set $\mathcal{P}(A)$ given by $\mathcal{P}(A) = \{X : X \subseteq A\}$."

Problem 37. ***Analyze critically*** (and, in particular, assign a grade on a scale from[72] 0 to 10) each of the following definitions:

1. *Definition of "union"*: The union of two sets is what you get when you combine the sets.

2. *Definition of "union"*: The union of two sets is all combined members of the sets.

3. *Definition of "union"*: Let A, B be sets. Then $A \cup B = \{x : x \in A \vee x \in B\}$.

4. *Definition of "divisible"*: A number n is divisible if it can be divided evenly into many parts.

5. *Definition of "divisible"*: Let m, n be integers. We say that m is divisible by n if $\frac{m}{n}$ is an integer

6. *Definition of "prime number"*: A prime number is a number that is not divisible by anything.

7. *Definition of "prime number"*: A prime number is a natural number n such that n has exactly two positive integer factors.

[72] You are allowed to give negative grades like -300 for particularly atrocious definitions. And, since the authors of these definitions are just figments of my imagination, you don't have to worry about the danger that you might hurt their feelings, and should feel free to be very harsh