MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Date of this version: September 22, 2019

Contents

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 Sections 2 and 3, 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, theorems and proofs

Basically, a ***proposition*** is something that can be true or false and can be the object of belief.

In other words: ***a proposition is an expression P such that it makes sense to ask the questions:***

- ***Is P true?***
- ***Is P false?***
- ***Do you believe that P?***

A ***fact*** is a true proposition.
For example,

- the following are true propositions:
  - George Washington was the first president of the United States,
  - Paris is the capital of France,
  - electrons are negatively charged particles,
  - two plus two equals four,
  - if a, b are real numbers then $(a+b)^2 = a^2 + 2ab + b^2$;
- the following are false propositions:
  - John Adams was the first president of the United States,
  - Paris is the capital of Spain,
  - electrons are positively charged particles,
  - two plus two equals five,
  - if a, b are real numbers then $(a+b)^2 = a^2 + b^2$;
- the following are propositions that I don't know if they are true or false:
  - Lee Harvey Oswald was part of a conspiracy to kill President Kennedy,
  - there is intelligent extraterrestrial life,
  - every even natural number n such that $n \geq 4$ is the sum of two prime numbers[1];
- and the following are ***not*** propositions:
  - John Adams,
  - is the capital of Spain,
  - Mount Everest,
  - the book that I bought yesterday,
  - two plus two,
  - if a, b are real numbers.

A ***proof*** of a proposition P is a logical argument[2] 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***.

For example, let us consider the proof, given on page 18, of Euclid's theorem, that the set of prime numbers is infinite: this proof consists of

[1] This proposition is called "the Goldbach conjecture"; it is an unsolved problem in Mathematics.

[2] 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.

several ***steps***, and the very last of these steps, i.e. the conclusion, says precisely what we were trying to prove, i.e., that *the set of prime nunbers is infinite*.

Proofs can by written in a ***language***, such as English, French, Chinese, Japanese, Spanish, etc. But in addition, there is a particular language which is prefectly suited for writing mathematical proofs: ***formal mathematical language***.

Formal mathematical language involves ***formulas***, rather than words. For example, "$2+2=4$" is an expression in formal language, i.e., a formula.

Most of our proofs will be written in a mixture of formal mathematical language and English. For example, we will write expressions such as

(#) If a and b are real numbers then $a^2 - b^2 = (a+b)(a-b)$.

But we will also explain how to write proofs in purely formal mathematical language. (And we will discuss why having a purely mathematical language is important: one of the main reasons is that ***formal mathematical language is a universal language***, that is, a language understandable by all the mathematicallu educated people in the world[3]. Another reason is that ***formal mathematical language is completely precise***: you cannot say vague things such as "the distance between A and B is small", and this is fine, because nobody knows what "small" means, so it is better if we are not allowed to say it.)

In order to write proofs in formal language, we will have to ***learn formal language***, i.e., we will have to learn to say in formal language everthing that we now say in English or in a mixture of English and formal language. For example, the sentence (#) that we wrote above will become, in formal language,

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

Why are proofs important? Again, this is an issue that will be taken up later, but let me sketch the answer right away:

> ***A mathematical proof of a proposition P absolutely guarantees, with complete certainty, that P is true.***

[3]For example, the formula "$2+2=4$" is the same in English, French, Chinese, or any other language.

This is so for a simple reason:

> ***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*[4].

Furthermore, ***there is no other way to know for sure that a mathematical statement is true.***

For example, consider the statement of the first theorem in this course, that the set of prime numbers is infinite. There is no way to know for sure that this is true, other than by proving it. Computing lots of prime numbers will not do, because no matter how many millions or billions or trillions of primes you may compute, you will only have computed a finite number of them, and you will never never know whether these are all the primes, or whether there are more. The proof given below shows you that, no matter how long a list of primes numbers may be, there is always at least one prime that is not on the list. And this guarantees that there are infinitely mamy primes.

[4]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.

2 An example of a proof: Euclid's proof of the infinitude of the set of prime numbers

Our first example of a proof will be Euclid's proof that there are infinitely many prime numbers. This proof is found in Euclid's *Elements* (Book IX, Proposition 20). Euclid (who was probably born in 325 BCE and died in 270 BCE) was the first mathematician to write a large treatise where mathematics is presented as a collection of definitions, postulates, propositions (i.e., theorems and constructions) and mathematical proofs of the propositions.

2.1 What Euclid's proof is about

You probably know what a "prime number" is. (If you do not know, do not worry; I will explain it to you pretty soon.) Here are the first few prime numbers:

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19\ \ldots$$

Does the list of primes stop there? Of course not. It goes on:

$$23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61\ \ldots$$

And it doesn't stop there either. It goes on:

$$67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97,\ 101,\ 103\ \ldots\ .$$

Does the list go on forever? If you go on computing primes, you would find more and more of them. And mathematicians have actually done this, and found an incredibly large number of primes.

The largest known prime

As of January, 2019, the largest known prime was

$$2^{82,589,933} - 1\,.$$

(That is, 2 multiplied by itself $82,589,933$ times, minus one.) This is a huge number! It has $24,862,048$ decimal digits.

Is it possible that the list of primes stops here, that is, that there are no primes larger than $2^{82,589,933} - 1$?

Before we answer this, just ask yourself: suppose it was indeed true that the list stops with this prime number. How would you know that? If you think about it for a minute, you will see that *there is no way to know.* You could go on looking at natural numbers larger than $2^{82,589,933} - 1$, and see if among these numbers you find one that is prime. But if you don't find any it doesn't mean there aren't any. It could just be that you haven't gone far enough in your computation, and if you went farther you would find one.

In fact, no matter how many primes you may compute, you will never know whether the largest prime you have found is indeed the largest prime there is, or there is a larger one.

Can we know in some way, other than by computing lots of primes, whether the list of primes goes on forever or there is a prime number which is the largest one?

It turns out that this question can be answered by means of **reasoning**. And, amazingly, the answer is "yes, the list of primes goes on forever"! This was discovered, in the year 300 B.C., approximately, by the great Greek mathematician Euclid. Euclid's 3,000-year old proof is a truly remarkable achievement, the first result of what we would now call "number theory", one of the most important areas of Mathematics.

Euclid's theorem says the following:

Theorem. *The set of prime numbers is infinite.*

In order to prove the theorem, we need to understand the precise meaning of the terms that occur in the statement. So I will begin by explaining the meaning of "prime number" and "infinite set".

And, in order to explain what a prime number is, we will have to explain first what we mean by "divisibility", and "factors".

2.2 Divisibility of integers; factors

If you have two integers a and b, you would like to "divide a by b", and obtain a "quotient" q, i.e., an integer q that multiplied by b gives you back a. For example, we can divide 6 by 2, and get the quotient 3. And we can divide 6 by 3, and get the quotient 2.

But it is not always possible to divide a by b. For example, if $a = 4$ and $b = 3$, then an integer q such that $3q = 4$ does not exist[5].

Since dividing a by b is sometimes possible and sometimes not, we will introduce some new words to describe those situations when division is possible.

Definition 1. Let a, b be integers.

1. We say that b <u>divides</u> a if there exists an integer k such that
$$a = bk\,.$$
2. We say that a is a <u>multiple</u> of b if b is a factor of a.
3. We say that b is a <u>factor</u> of a if b divides a.
4. We say that a is <u>divisible</u> by b if b divides a.
5. We write
$$b|a$$
to indicate that b divides a. □

Remark 1. As the previous definition indicates,

The following are five different ways of saying exactly the same thing:

- m divides n,
- m is a factor of n,
- n is a multiple of m,
- n is divisible by m,
- $m|n$.

□

[5]You may say that "the result of dividing 4 by 3 is the fraction $\frac{4}{3}$". That is indeed true, but $\frac{4}{3}$ ***is not an integer***, and so far we are working in a world in which there are integers and nothing else. If we want $\frac{4}{3}$ to exist, we have to invent new numbers—the fractions, or "rational numbers". We are going to do that pretty soon, but for the moment, since we are working with integers only, it is ***not*** possible to divide 4 by 3 and get a quotient which is an integer.

Reading statements with the "divides" symbol "|"

The symbol "|" is read as "divides", or "is a factor of".
For example, the statement "3|6" is read as "3 divides 6", or "3 is a factor of 6". And the statement "3|5" is read as "3 divides 5", or "3 is a factor of 5". (Naturally, "3|6" is true, but "3|5" is false.)
The vertical bar of "divides" has nothing to do with the bar used to write fractions. For example, " $3|6$ ***" is the statement*** [a] ***"*** 3 ***divides*** 6***', which is true. And "*** $\frac{3}{6}$ ***" is a noun phrase: it is one of the names of the number also known as "*** $\frac{1}{2}$ ***", or "*** 0.5 ***".***

[a] A statement is something we can say that is true or false. A noun phrase is something we can say that stands for a thing or person. For example, "Mount Everest", "New York City", "My friend Alice", "The movie I saw on Sunday", are noun phrases. "Mount Everest is very tall", "I live in New York City", "My friend Alice studied mathematics at Rutgers", and "The movie I saw on Sunday was very boring", are statements.

Example 1. Here are some examples illustrating the use of the word "divides" and the symbol "|":

- The following statements are true:
  1. 6 divides 6,
  2. 6|6,
  3. 6 divides 12,
  4. 6|12,
  5. 1 divides 5,
  6. 1|5,
  7. 13 divides 91,
  8. 13|91,
  9. 6 divides 0,
  10. 6|0,
  11. 6 divides -6,
  12. $6|-6$,

13. -6 divides 6,
14. $-6|6$,
15. 6 divides -12,
16. $-6|12$,
17. 6 divides 0,
18. $6|0$,
19. 0 divides 0,
20. $0|0$,

- and the following statements are false:

1. 6 divides 7,
2. $6|7$,
3. 0 divides 1,
4. $0|1$,
5. 12 divides 6,
6. $12|6$,
7. -5 divides 6,
8. $-5|6$,
9. $0|6$.

2.3 What is a "prime number"

Definition 2. A prime number is a natural number p such that

I. $p > 1$,

II. p is not divisible by any natural numbers other than 1 and p. □

And here is another way of saying the same thing, in case you do not want to talk about "divisibility".

Definition 3. A prime number is a natural number p such that

I. $p > 1$,

II. There do not exist natural numbers j, k such that $j > 1$, $k > 1$, and $p = jk$. □

2.3.1 Why isn't 1 prime?

If you look at the definition of "prime number", you will notice that, ***for a natural number*** p ***to qualify as a prime number, it has to satisfy*** $p > 1$. In other words, ***the number*** 1 ***is not prime.*** Isn't that weird? After all, the only natural number factor of 1 is 1, so the only factors of 1 are 1 and itself, and this seems to suggest that 1 *is* prime.

Well, if we had defined a number p to be prime if p has no natural number factors other than 1 and itself, then 1 *would* be prime. But we were *very* careful not to do that. Why?

The reason is, simply, that there is a very nice theorem called the "unique factorization theorem", that says that every natural number greater than 1 either is prime or can be written as a product of primes *in a unique way.* (For example: $6 = 2 \cdot 3$, $84 = 2 \cdot 2 \cdot 3 \cdot 7$, etc.)

If 1 was a prime, then the result would not be true as stated. (For example, here are two different ways to write 6 as a product of primes: $6 = 2 \cdot 3$ and $6 = 1 \cdot 2 \cdot 3$.) And mathematicians like the theorem to be true as stated, so we have decided not to call 1 a prime[6].

If you do not like this, just keep in mind that we can use words any way we like, as long as we all agree on what they are going to mean. If we decide that 1 is not prime, then 1 is not prime, and that's it. If you think that for you 1 is really prime, just ask yourself why and you will see that you do not have a proof that 1 is prime.

2.3.2 The prime factorization theorem

In our proof of Euclid's theorem, we are going to use the fact that every natural number (except 1) can be written as a product of prime numbers. This is a very important result in arithmetic[7], and we are going to prove it later.

The precise statement is as follows:

Theorem. (The prime factorization theorem.) *Every natural number n such that $n \geq 2$ is a product of primes.* □

[6]This is exactly the same kind of reason why Pluto is not a planet. Pluto is not a planet because astronomers have decided not to call Pluto a planet. Similarly, mathematicians have decided not to call 1 prime, and that's why 1 is not prime.

[7]Actually, many mathematicians call "The Fundamental Theorem of Arithmetic".

2.3.3 Clarification: What is a "product of primes"?

Like all mathematical ideas, even something as simple as "product of primes" requires a precise definition. Without a precise definition, it would not be clear, for example, whether a single prime such as 2 or 3 or 5 is a "product of primes".

Definition 4. A natural number n is a product of primes if there exist

1. a natural number k,

and

2. a finite list[8]
$$\mathbf{p} = (p_1, \ldots, p_k)$$
of prime numbers,

such that
$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k \,. \tag{2.1}$$
(If you are familiar with the product "$\prod$" notation, formula (2.1) says that $n = \prod_{i=1}^{k} p_i$.)

Notice that k *can be equal to one.* That is, ***a single prime, such as*** 2***, or*** 3***, or*** 23***, is a product of primes in the sense of our definition.*** □

Definition 5. If n is a natural number, then a list $\mathbf{p} = (p_1, \ldots, p_k)$ of prime numbers such that (2.1) holds is called a prime factorization of n. □

Example 2. The following natural numbers are products of primes:

- 7 (because 7 is prime); the list (7) is a prime factorization of 7,
- 24; (the list $(2, 2, 2, 3)$ is a prime factorization of 24, because $24 = 2 \times 2 \times 2 \times 3$),
- 309; (the list $(3, 103)$ is a prime factorization of 309);
- $3,895,207,331,689$. Here it would really take a lot of work to find the natural number k and the prime numbers $p_1, p_2, \ldots, p_k$ such that
$$3,895,207,331,689 = p_1 \cdot p_2 \cdot \cdots \cdot p_k \,.$$
But the prime factorization theorem guarantees to us that $3,895,207,331,689$ is a product of primes. □

[8] Finite lists will be defined and discussed in great detail later in these notes.

2.4 Proofs by contradiction

Our proof if Euclid's theorem is going to be a ***proof 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.

And, ir order to explain that, I have to discuss how to *negate* a sentence.

2.4.1 Negation

To ***negate*** (or ***deny***) a statement A is to assert that A is false. (Any such statement is called a *denial* of A)

So, for example, a denial of "7 is a prime number" is "7 is not a prime number". (But there are many other ways to write a denial of "7 is a prime number." For example, we could write "it is not true that 7 is a prime number", or "it is not the case that 7 is a prime number".)

> **The symbol "$\sim$" ("it's not true that")**
>
> The symbol "$\sim$", put in front of a statement, is used to assert that the statement is false.
> So "$\sim$" stands for "it is not the case that", or "it is not true that".

Example 3. The following sentences are true:

- $\sim$ 6 is a prime number (that is, "6 is not a prime number"),
- $\sim$ 2 is an odd integer (that is, "2 is not an odd integer"),
- $\sim$(6 is even and 7 is even) (that is, "it's not true that 6 and 7 are both even").

The following sentences are false:

- $\sim$ 7 is a prime number (that is, "7 is not a prime number"),
- $\sim$ 3 is an odd integer (that is, "3 is not an odd integer"),
- $\sim$(6 is even or 7 is even) (that is, "it's not true that 6 is even or 7 is even"),
- $\sim$ 6 is even and 7 is even (that is, "6 is not even and 7 is even").

2.4.2 When is a negation true?

If A is a sentence, then

- $\sim A$ is true if A is false;
- $\sim A$ is false if A is true.

2.4.3 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, simplified definition of "contradiction": A contradiction is a statement of the form "A and $\sim A$", that is, "A is true and A is not true". □

Example 4.

- 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. □

2.4.4 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. Once you have done that, you are allowed to conclude that the statement you are trying to prove is true.

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 $2 \neq 1$.
> > And "$2 = 1$ and $2 \neq 1$" is a contradiction.
>
> So assuming that A is false has led us to a contradiction.
> Therefore A is true. **Q.E.D.**

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.

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 in the real world S must be true.

2.5 What is a finite set? What is an infinite set?

We now explain what a "finite set" is.

Definition 6. Let S be a set,

1. We say that S is finite if there exist a natural number n and a finite list[9]
$$\mathbf{a} = (a_1, a_2, \ldots, a_n)$$
with n entries which is a list of all the members of S. (This means: *every member of S occurs in the list*; that is, *for every member x of S there exists a natural number j such that $j \leq n$ and $x = p_j$.*)

2. We say that S is infinite if it is not finite. □

2.5.1 A simple lemma

A lemma is a statement that one proves in order to use it in the proof of a theorem. In our proof of Euclid's Theorem we are going to need the following lemma:

Lemma 1. *If a, b, c are integers, and c divides both a and b, then c divides $a + b$ and $a - b$.*

Proof. Since $c|a$ and $c|b$, we may write

$$a = cj \text{ and } b = ck\,, \tag{2.2}$$

[9]If you are wondering "what is a finite list?", then I can tell you two things: (1) you are asking a good question, (2) I will give you more information about "finite lists" later, on page 19.

where j and k are integers.

But then

$$a + b = c(j + k) \text{ and } a - b = c(j - k)\,, \tag{2.3}$$

and $j + k$ and $j - k$ are integers. So $c|a + b$ and $c|a - b$. **Q.E.D.**

2.6 The proof of Euclid's Theorem

The proof I am going to present here is not exactly Euclid's, but is based essentially on the same idea.

First, here is Euclid's result, again:

Theorem 1. *The set of prime numbers is infinite.*

And here is the proof.

Let S be the set of all prime numbers.
We want to prove that S is an infinite set.
We will prove this by contradiction.

Suppose S is not infinite.
Then S is a finite set.
Since S is finite, we may write a finite list

$$\mathbf{p} = (p_1, p_2, \ldots, p_n)$$

of all the members of S, i.e., of all the prime numbers.

Let $N = p_1.p_2.\cdots.p_n$. (That is, N is the product of all the entries of the list $\mathbf{p}$.)
Let $M = N + 1$.
Then $M \geq 2$, so by the prime factorization theorem (in section 2.3.2) M is a product $q_1.q_2.\cdots.q_k$ of prime numbers.
Then q_1 is a prime number[10], and $\boxed{q_1 \text{ divides } M}$ (because $M = q_1 u$, if $u = q_2.q_3.\cdots.q_k$).

[10] All we need here is to have a prime number that divides M. We choose q_1, but we could equally well have chosen q_2, or any of the other q_j.

On the other hand, since **p** is a list of all the prime numbers, and q_1 is a prime number, we can conclude that q_1 is one of the entries $p_1, p_2, \ldots, p_n$ of the list **p**.
So we may write

$$q_1 = p_j \,,$$

where j is one of the nmbers $1, 2, \ldots, n$.
It follows that $\boxed{q_1 \text{ divides } N}$ (because p_j divides N and $q_1 = p_j$).
Since q_1 divides M and q_1 divides N, it follows that q_1 divides $M - N$, by Lemma 1.
But $M - N = 1$. So $\boxed{q_1 \text{ divides } 1}$.
On the other hand, q_1 is prime. It then follows from the definition of "prime number" (Definition 2, on page 10) that $q_1 > 1$.
Hence $q_1 \neq 1$.
But then $\boxed{q_1 \text{ does not divide } 1}$, because the only natural number that divides 1 is 1.
So $\boxed{q_1 \text{ divides } 1 \text{ and } q_1 \text{ does not divide } 1}$, which is a contradiction.

Hence the assumption that S is not an infinite set has led us to a contradiction.
Therefore $\boxed{S \text{ is an infinite set}}$. **Q.E.D.**

2.6.1 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.

Appendix: Finite lists

Finite lists have ***entries***. Sets have ***members***.
We can write[11] finite lists as follows:

1. First we write a left parenthesis, i.e., the symbol "(".

[11] I am saying "we can write" rather than "we write" because there are other ways to write lists and sets. We will discuss those ways later.

2. Then we write the names of the entries of the list, in order, beginning with entry number 1, then entry number 2, and so on. The entries must be separated by commas.
3. Then, finally, write a right parenthesis, i.e., the symbol ")".

And we can write finite sets as follows:

1. First we write a left brace, i.e., the symbol "{".
2. Then we write the names of the members of the set, in some order, separated by commas.
3. Then, finally, we write a right brace, i.e., the symbol "}".

WARNING

Be careful with the distinction between ***sets***, written with braces ("{" and "}") and ***lists***, written with parentheses ("(" and ")"). For example, the sentence

$$(1, 2, 3) = (3, 1, 2)$$

is false, but the sentence

$$\{1, 2, 3\} = \{3, 1, 2\}$$

is true.

Example 5.

- Here is the list **a** of the first ten natural numbers, in increasing order:

$$\mathbf{a} = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)\,. \tag{2.4}$$

- Here is the list **b** of the first ten natural numbers, in decreasing order:

$$\mathbf{b} = (10, 0, 8, 7, 6, 5, 4, 3, 2, 1)\,. \tag{2.5}$$

  And here is a list **c** of the first ten natural numbers, in a different order:

$$\mathbf{c} = (10, 1, 5, 8, 3, 2, 4, 9, 6, 7)\,. \tag{2.6}$$

These three lists are different. For example, the second entry of **a** is 2, whereas the second entry of **b** is 9 and that of **c** is 1.

Now let S be the set whose members are the first ten natural numbers. Then we can write

$$S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, \tag{2.7}$$

or

$$S = \{10, 9, 8, 7, 6, 5, 4, 3, 2, 1\}, \tag{2.8}$$

or, for example,

$$S = \{1, 3, 5, 7, 9, 2, 4, 6, 8, 10\}, \tag{2.9}$$

or

$$S = \{4, 2, 7, 8, 10, 1, 9, 3, 5, 6\}, \tag{2.10}$$

or even

$$S = \{4, 4, 2, 7, 7, 7, 5, 5, 5, 8, 10, 1, 9, 4, 3, 5, 6\}. \tag{2.11}$$

The sets S given by equations (2.7), (2.8), (2.9), (2.10), (2.11), are all the same set, even though the formulas describing them are different. What the formulas do is tell us who the members of the set are. So, for example, according to formula (2.7), 1 is a member of S, and 23 is not. And the other formulas also say that 1 is a member of S, and 23 is not.

The key facts are these:

- Two sets S, T are the same set if they have the same members, that is, if every member of S is a member of T and every member of T is member of S.
- Two lists **a**, **b** are the same if the first entry of **a** is the same as the first entry of **b**, the second entry of **a** is the same as the second entry of **b**, and so on. That is, $\mathbf{a} = \mathbf{b}$ if the j-th entry of **a** is the same as the j-th entry of **b** for every j.

Example 6. Let S be the set whose members are all the presidents of the United States, from George Washington to Donald Trump.

Let **a** be the list of all the presidents of the United States, from George Washington to Donald Trump, in chronological order, so

$$\mathbf{a} = (a_1, a_2, \ldots, a_{45}),$$

where, for $j = 1, 2, \ldots, 45$, a_j is the j-th U.S. president.

Then **a** has 45 entries. How many members does S have?

If you think that the answer is 45, think again!

It turns out that Grover Cleveland served two nonconsecutive terms as president, from 1885 to 1889 and from 1893 to 1897, and Congress decided that Cleveland would count as both the 22nd and the 24th president of the United States. So in the list **a**, the 22nd entry a_{22} and the 24th entry a_{24} are equal. So the set S has in fact 44 members, even though the list **a** has 5 entries. □

2.7 An analogy: twin primes

Let me tell you about another problem, very similar to the one we have just discussed, for which the situation is completely different.

Definition 7. A twin prime is a prime number p such that $p + 2$ is also prime. □

Example 7. Here are the first few twin primes:

$$3,\ 5,\ 11,\ 17,\ 29,\ 41,\ 59,\ 71,\ 101,\ 107\ . \qquad \square$$

Now we can ask the same question that we asked for primes: does the list go on forever, or does it stop at some largest pair of twin primes?

In other words,

Are there infinitely many twin primes?

This looks very similar to the question whether there are infinitely many primes. And yet, the situation in this case is completely different:

Nobody knows whether there are infinitely twin primes. Mathematicians have been trying for more than 2,000 years to solve this problem, by proving that there are infinitely many twin primes, or that that there aren't, and so far they haven't been successful.

The twin prime conjecture is the statement that there are infinitely many pairs of twin primes. It was formulated by Euclid, about 2,300 years ago, and it is still an open problem.

THE LARGEST KNOWN TWIN PRIME

According to *Wikipedia*, as of September 2018, the current largest twin prime known was $2996863034895 \times 2^{1290000} - 1$, with $388,342$ decimal digits. It was discovered in September 2016. (The fact that the number $2996863034895 \times 2^{1290000} - 1$ is a twin prime means that it is prime, and the number $2996863034895 \times 2^{1290000} + 1$ is also prime.)

2.8 A surprising fact: non-twin primes

How about primes that are *not* twin?

Definition 8. A non-twin prime is a prime number p such that $p + 2$ is not prime. □

Example 8. Here are the first few non-twin primes:

2, 7, 13, 19, 23, 31, 37, 43, 47, 53,
61, 67, 73, 79, 83, 89, 97, 103 . □

And now we can ask, again, the same question that we asked for primes and for twin primes: does the list go on forever, or does it stop at some largest pair of twin primes?

In other words,

Are there infinitely many non-twin primes?

This looks very similar to the question whether there are infinitely many twin primes. And yet, the situation in this case is completely different: it is very easy to prove the following:

Theorem 2. *The set of non-twin primes is infinite.*

(I am asking you to do this proof. See Problem 8 below.)

2.9 Problems

Problem 1. Using the definition of "divides" (Definition 1), explain precisely why the statements "1 divides 5", "6 divides -6", "6 divides 0", and "0 divides 0" are true, and the statements "$5|6$" and "$0|6$" are false. □

Problem 2. Indicate which of the statements in the following list are true and which ones are false, and explain why. (That is, prove that the true statements are true and the false ones are false.)

1. Every integer is divisible by 1.
2. Every integer is divisible by 2.
3. Every integer is divisible by 0.
4. Every integer divides 1.
5. Every integer divides 2.
6. Every integer divides 0.

Problem 3. Express each of the following numbers

- 37,
- 28,
- 236,
- 2247,

as a product of prime numbers. □

Problem 4. Give a precise mathematical definition of "prime number". □

Problem 5. Give a precise mathematical definition of "twin prime". □

Problem 6. Give a precise mathematical definition of "finite set" and "infinite set". □

Problem 7. Give precise mathematical definitions of each of the following concepts:

- divides,
- is divisible by,
- factor (as in "is a factor of"),

- multiple (as in "is a multiple of"). □

Problem 8. ***Prove*** Theorem 2 (on page 23). □

Problem 9. ***Prove*** that if a, b, c are integers, $a|b$ and $b|c$, then $a|c$. □

Problem 10. ***Prove*** that if a, b are integers, $a|b$ and $b|a$, then $a = b$ or $a = -b$. □

Problem 11. The proof that was given in Section 2.6 of Euclid's Theorem uses the definition of "prime number" given on page 10. In this problem, we change the definition of "prime number" and use the following definition: *A prime number is a natural number p such that p is not divisible by any natural numbers other than 1 and p.* That is, we do not require p to be > 1. So according to this new definition 1 is now prime

Rewrite the proof of Euclid's Theorem given in Section 2.6 using the new definition of "prime number". (What you have to do is basically copy the proof, but making a few changes. For example, one of the steps of the proof given in Section 2.6 says "It follows from the definition of 'prime number' that $q_1 > 1$". This step is not valid now, because 1 is prime, so q_1 could be 1. You have to make some slight changes in the proof to adapt it to this new situation.) □

Problem 12. ***Prove*** that if p is a prime number and $p \neq 2$ then p is odd.

In the following problems, you may want to use the division theorem: ***If*** a, b ***are integers and*** $b \neq 0$***, then it is possible to write*** $a = bq + r$***, where*** q, r ***are integers such that*** $0 \leq r < |b|$**.** (For example: if a is an integer then we can write $a = 3q + r$ where $r = 0$ or $r = 1$ or $r = 2$.)

Problem 13. ***Prove*** that if p is a prime number such that $p + 2$ and $p + 4$ are also prime, then $p = 3$.

Problem 14.

1. ***Find*** at least ten different prime numbers p such that $p + 4$ is also prime.
2. ***Prove*** that the only prime number p such that $p+4$ and $p+8$ are also prime is $p = 3$.
3. ***Prove*** that there does not exist a prime number p such that $p + 4$, $p + 8$ and $p + 12$ are also prime.

Problem 15.

1. ***Find*** at least ten different prime numbers p such that $p + 6$ is also prime.
2. ***Find*** at least ten different prime numbers p such that $p+6$ and $p+12$ are also prime.
3. ***Find*** at least four[12] different prime numbers p such that $p + 6$, $p + 12$ and $p + 18$ are also prime.
4. ***Prove*** that there exists a unique prime number p such that $p + 6$, $p + 12$, $p + 18$ and $p + 24$ are also prime.
5. ***Prove*** that there does not exist a prime number p such that $p + 6$, $p + 12$, $p + 18$, $p + 24$ and $p + 30$ are also prime.

Problem 16.

1. ***Express*** the integer 28 as a difference of two squares of integers. (That is, ***find*** two integers m, n such that $m^2 - n^2 = 28$.)
2. ***Express*** the integer 29 as a difference of two squares of integers. (That is, ***find*** two integers m, n such that $m^2 - n^2 = 29$.)
3. ***Prove*** that it is not possible to express the integer 30 as a difference of two squares of integers. (That is, ***prove*** that there do not exist two integers m, n such that $m^2 - n^2 = 30$.) □

[12]There are many more. I am just asking you to find four because I don't want to make you work too hard.

3 More examples of proofs: irrationality of $\sqrt{2}$ and of other numbers

3.1 Numbers and number systems

There are several different kinds of numbers, i.e., several different number systems. It is convenient to give the number systems *names*, and to introduce mathematical symbols to represent them.

3.1.1 The most common types of numbers

Here are some examples of number systems:

- the symbol $\mathbb{N}$ stands for the set of *natural numbers*,
- the symbol $\mathbb{Z}$ stands for the set of *integers*,
- the symbol $\mathbb{Q}$ stands for the set of *rational numbers*,
- the symbol $\mathbb{R}$ stands for the set of *real numbers*,
- the symbol $\mathbb{C}$ stands for the set of *complex numbers*,
- there are sets $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, and, more generally, $\mathbb{Z}_n$—the set of *integers modulo* n—for every natural number n such that $n \geq 2$. (So, for example, there are the systems $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{5403}$.)

Some of the above kinds of numbers should be familiar to you, and others may be less so or not at all. Do not worry if you find on our list things that you have never heard of before: we will be coming back to the list later, and discussing all the items in much greater detail.

A number can belong to different number systems, in the same way as, say, a person can belong to different associations. (For example, somebody could be a member, say, of the American Association of University Professors, the Rutgers Alumni Association, and the Sierra Club. Similarly, the number 3 belongs to lots of different number systems, such as, for example, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.)

At this point, we will just discuss $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, and we will do so very briefly. We will talk much more about these systems later, and we will also discuss later other number systems such as $\mathbb{C}$, and the $\mathbb{Z}_n$.

The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, are *special mathematical symbols*. They are *not* the capital letters N, Z, Q, R, C.

(Why do we use these special symbols? It's because mathematicians need to use lots of letters in their proofs, so they do not want to take the letters C, R, for example, and declare once and for all that they stand for "the set of all complex numbers" and "the set of all real numbers". For example, if they are working with a circle, they want to have the freedom to call the circle "C", and to say "let R be the radius of C", and this would not be allowed if the symbols "C", "R" already stood for something else. So they invented the special symbols $\mathbb{C}$, $\mathbb{R}$ to stand for the set of complex numbers and the set of real numbers, so that the ordinary letters C, R, will be available to be used as variables.)

> Please do **not** say "$\mathbb{N}$ is the natural numbers", or "$\mathbb{Z}$ is the integers". When we group things together to create a set, that set is one thing, not many things. So $\mathbb{N}$ cannot be "the natural numbers". What you can, and should, say is: "$\mathbb{N}$ is the set of all natural numbers."

3.1.2 The symbol "$\in$"

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.

How to read the "$\in$" symbol

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 2. 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 bad English grammar to say "pick an a belongs to S". But "pick an a belonging to S", "pick an a in S", or "pick an a that belongs to S", are 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.

3.1.3 The natural numbers

The symbol $\mathbb{N}$ stands for the set of all *natural numbers*. (Natural numbers are also called "positive integers", or—sometimes—"whole numbers",

or "counting numbers".) The members of this set are the numbers $1, 2, 3 \ldots$.

More precisely:

> The **natural numbers** are the numbers obtained from the number 1 by adding 1 any number of times. So, for example, the numbers 1, $1+1$ (i.e., 2), $1+1+1$ (i.e., 3), $1+1+1+1$ (i.e., 4), are natural numbers. And so are the numbers $4,503$, $46,902,444,531,322$ and $10^{10^{10^{10^{10}}}}$.
> The symbol $\mathbb{N}$ stands for **the set of all natural numbers**.

3.1.4 The integers

The symbol $\mathbb{Z}$ stands for the set of all *integers*.

The members of $\mathbb{Z}$ (i.e., the integers) are the natural numbers as well as 0 and the negatives of natural numbers, i.e., the numbers -1, -2, -3, etc. So, to say that a number n is an integer, we can write "$n \in \mathbb{Z}$", which we read as "n belongs to the set of integers" or, even better, as "n is an integer".

So, for example, the following statements are true:

$$\begin{aligned} 35 &\in \mathbb{N} \\ 35 &\in \mathbb{Z} \\ \sim -35 &\in \mathbb{N} \\ -35 &\in \mathbb{Z} \\ 35 &\notin \mathbb{Z} \\ 0 &\in \mathbb{Z} \\ \sim 0 &\in \mathbb{N} \\ 0 &\notin \mathbb{N} \\ 0.37 &\notin \mathbb{Z} \\ \pi &\notin \mathbb{Z} \end{aligned} \quad .$$

3.1.5 The real numbers

The symbol $\mathbb{R}$ stands for the set of all *real numbers*.

The real numbers are those numbers that you have used in Calculus. They can be positive, negative, or zero.

The positive real numbers have an "integer part", and then a "decimal expansion" that may terminate after a finite number of steps or may continue

forever. (So, for example, the number 4.23 is a real number, and so is the number π. The decimal expansion of the number 4.23 terminates after two decimal figures, but the decimal expansion of π goes on forever. Here, for example, is the decimal expansion of π with 30 decimal digits:

$$3.14159265358979323846264338327\,9\,.$$

Using Google you can find π with one million digits. As of 2011, 10 trillion digits of π had been computed, and nobody has found any pattern! Even simple questions, such as whether every one of the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ appears infinitely many times, are unresolved.)

And the negative real numbers are the negatives of the positive real numbers. So, for example, -4.23 and $-\pi$ are negative real numbers.

3.1.6 Positive, negative, nonnegative, and nonpositive numbers

In this course, "positive" means "> 0" (i.e., "greater than zero"), and "nonnegative" means "≥ 0" ("greater than or equal to zero"). So, for example, 3 and 0.7 are positive (and nonnegative), and 0 is nonnegative but not positive.

Similarly, "negative" means "< 0", and "nonpositive" means "≤ 0". So, for example, -3 and -0.7 are negative (and nonpositive), 0 is nonpositive but not negative.

3.1.7 Subsets

Definition 9. A set A is a **subset** of a set B if every member of A is a member of B.
We write "$A \subseteq B$" to indicate that A is a subset of B.

For example,

a. If, for example, S is the set of all people in the world, and T is the set of all people who live in the United States, then T is a subset of S. So the sentence "$T \subseteq S$" is true.

b. If A is the set of all animals, and G is the set of all giraffes, then G is a subset of A, so the sentence "$G \subseteq A$" is true.

c. Let S be the set of all people who live in the United States, and let C be the set of all U.S. citizens. Is C a subset of S? The answer is

"no", because there are U.S. citizens who do not live in the U.S., so these people are members of C but not of S, so it's not true that every member of C belongs to S.

And here are some mathematical examples:

I. The following sentences are true:

$$\mathbb{N} \subseteq \mathbb{Z}\,,$$
$$\mathbb{N} \subseteq \mathbb{R}\,,$$
$$\mathbb{Z} \subseteq \mathbb{R}\,,$$

because every natural number is an integer, every natural number is a real number, and every integer is a real number.

II. And the following sentences are false:

$$\mathbb{Z} \subseteq \mathbb{N}\,,$$
$$\mathbb{R} \subseteq \mathbb{N}\,,$$
$$\mathbb{R} \subseteq \mathbb{Z}\,.$$

(For example, it is not true that $\mathbb{Z} \subseteq \mathbb{N}$, because not every integer is a natural number since, for example, $0 \in \mathbb{Z}$ but $0 \notin \mathbb{N}$.)

3.1.8 The word "number", in isolation, is too vague

As we have seen, there are different kinds of numbers. So, if you just say that something is a "number", without specifying what kind of number it is, then this is too vague. In other words,

Never say that something is a "number", unless you have made it clear in some way what kind of "number" you are talking about.

For example, suppose you are asked to define "divisible", and you write:

> A number a is divisible by a number b if we can write $a = bc$ for some number c.

This is too vague! What kind of "numbers" are we talking about? Could they be real numbers?. If this was the case, then 3 would be divisible by 5, because $3 = 5.z$, if we take $z = 3/5$. But we do not want 3 to be divisible by 5. And we want the "numbers: we are talking about to be integers.

So here is a correct definition of "divisible":

Divisibility of integers: We say that an integer a is divisible by an integer b (or that a is a multiple of b, or that b is a factor of a, or that b divides a), if we can write

$$a = bc$$

for some integer c. □

For example, the following sentences are true:

$$\begin{gathered} 3 \text{ divides } 6\,, \\ -3 \text{ divides } 6\,, \\ 6 \text{ is divisible by } 3\,, \\ 6 \text{ is a multiple of } 3\,, \\ 3 \text{ is a factor of } 6\,. \end{gathered}$$

3.2 Existential statements

In the definition of divisibility given above, we have used the words "we can write". This language makes it sound as though, in order to decide whether, say, 3 divides 6, we need to have somebody there who "can write" things. This should not be necessary: "3 divides 6" would be a true sentence even if there was nobody around to do any writing. So it is much better to use a more impersonal language:

Divisibility of integers

DEFINITION. An integer a is divisible by an integer b (or a is a multiple of b, or b is a factor of a, or b divides a), if there exists an integer c such that

$$a = bc\,.$$

The sentence "there exists an integer c such that $a = bc$" is an example of nn **existential sentence**, i.e., a sentence that asserts that an object of a certain kind exists. Later, when we learn to write mathematics in formal language (that is, using only formulas), we will see that this sentence can be written as follows:

$$(\exists c \in \mathbb{Z})a = bc\,. \tag{3.12}$$

The symbol "$\exists$" is the **existential quantifier symbol**, and the expression "$(\exists c \in \mathbb{Z})$" is an **existential quantifier**, and is read as "there exists an integer c such that".

So Sentence (3.12) is read as "there exists an integer c such that $a = bc$". And it can also be read as "$a = bc$ for some integer c", or "it is possible to pick an integer c such that $a = bc$". (I recommend the "it is possible to pick ..." reading.)

3.2.1 The rule for using existential statements (Rule $\exists_{use}$)

Suppose you know that cows exist, that is that

$$(\exists x)x \text{ is a cow}\,. \tag{3.13}$$

Then the rule for using existential statements says that we can introduce into our conversation a cow, and give her name, by saying something like "pick a cow and call her Suzy".

In general,

- For a sentence $(\exists x)P(x)$, a witness is an object a such that $P(a)$. (For example: for the sentence (3.13), a witness is any a such that a is a cow, that is, any cow.)
- For a sentence $(\exists x \in S)P(x)$, a witness is an object a which belongs to S and is suchthat $P(a)$. (For example, if C is the set of all cows, then a witness for the sentence $(\exists x \in C)x$ is brown is any brown cow.)

The ***rule for using existential statements*** (Rule $\exists_{use}$) says that, ***if you know that an existential statement is true, then you can "pick a witness and give it a name".***

For example: suppose you know that a natural number n is not prime and is > 1. Then you know that the following is true: $(\exists m \in \mathbb{N})(m|n$ and $m \neq 1$ and $m \neq n)$. (That is, n has a factor which is a natural number and is not

equal to 1 or n.) Then Rule $\exists_{use}$ says that we can pick a witness and call it a, that is, we can pick a natural number a such that $a|n$, $a \neq 1$ and $a \neq n$.

Rule $\exists_{use}$

- From
$$(\exists x)P(x)$$
you can go to "Let w be a witness for $(\exists x)P(x)$, so $P(w)$," or "Pick a witness for $(\exists x)P(x)$ and call it w", or "Pick a w such that $P(w)$."

- From
$$(\exists x \in S)P(x)$$
you can go to "Let w be a witness for $(\exists x \in S)P(x)$, so $w \in S$ and $P(w)$," or "Pick a witness for $(\exists x \in S)P(x)$ and call it w", or "Pick a w such that $w \in S$ and $P(w)$."

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 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[13], "a".

[13]Can you call this solution x? This is a complicated issue. Think of this as follows:

3.3 Pythagoras' Theorem and two of its proofs

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 3. (Pythagoras' Theorem) *If T is a right triangle*[14]*, c is the length of the hypothenuse*[15] *of T, and a, b are the lengths of the other two sides, then*

$$a^2 + b^2 = c^2 \,. \tag{3.14}$$

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[16] of T as shown in the picture.

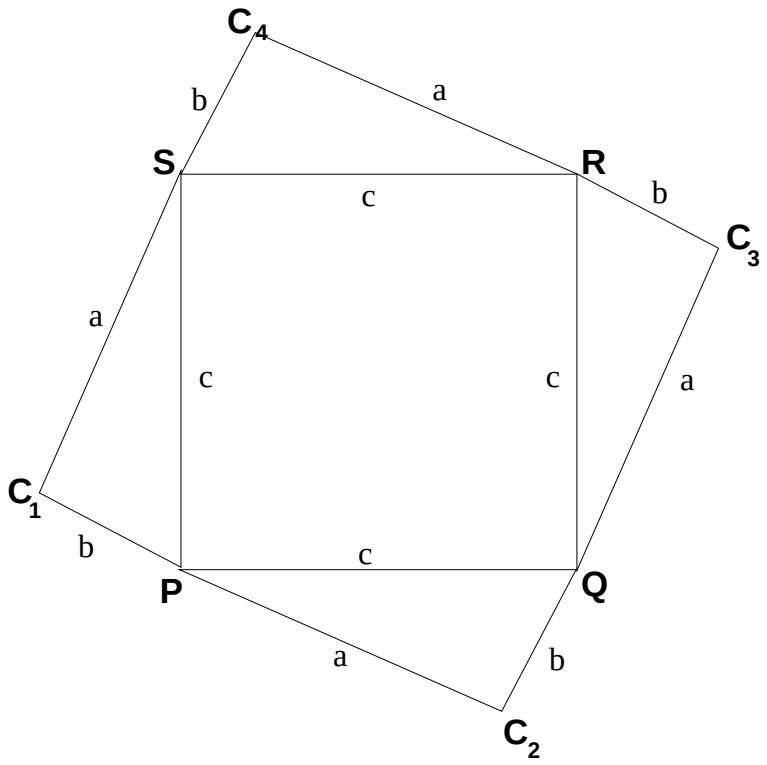
---

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 $\clubsuit$).

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

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

[16] 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

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

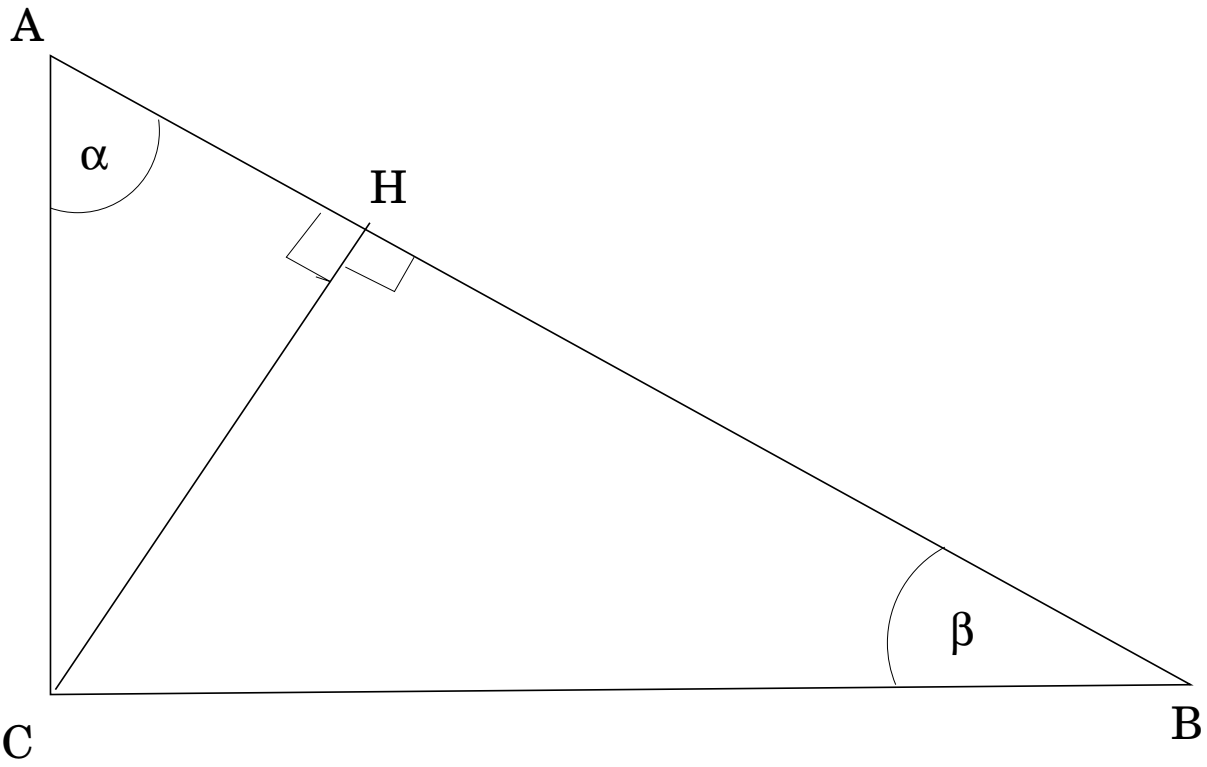
Subtracting $2ab$ from both sides, we get

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

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.**

3.4 Rational and 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 3.4.4.)

3.4.1 What are "numbers"?

We have already been talking quite a bot about "numbers", but I never told you what a "number" is. The question "what is a number?" is not an easy one 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 10.153098341832189504 82 ounces; and so on[17]. At no time did the amount of water "jump"[18] from some value u to some larger value v.
- they ***can be subdivided indefinitely***: for example

[17]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, 10.153098341832189504 82, 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 rigorously and precisely we must get rid of it.

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

- 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[19].

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

[19]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 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.

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 10.

- 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.

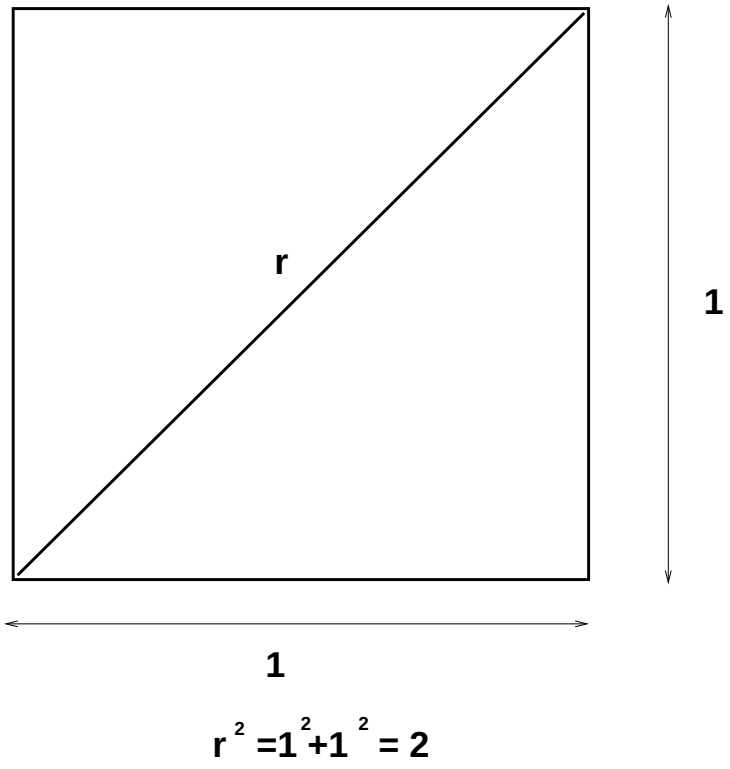
But then a momentous discovery of far-reaching consequences was made:

There are incommensurable lenghts.

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

Precisely: it is possible to construct geometrically[20] a segment whose length r satisfies $r^2 = 2$. For example, if we draw a square whose sides have length 1, then the length r of the diagonal of the square will satisfy $r^2 = 2$, by Pythagoras' theorem.

[20]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".)



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[21] numbers", are real numbers, but many real numbers are "irrational" numbers, that is, numbers that are not rational.
- Actually, most[22] 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.

3.4.2 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[23]. 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.)

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

---

[21]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 irrationality 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.

[22]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.

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

> 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.

3.4.3 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.

3.4.4 The most important number systems: real numbers vs. integers and natural numbers; definition of "rational number"

Now let us look at the main number systems[24] 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 the following key definition:

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

Definition 11.

- A rational number is a real number r such that there exist integers m, n for which:
  (a) $n \neq 0$
  (b) $r = \frac{m}{n}$.
- The set of all rational numbers is called $\mathbb{Q}$. (So "$x \in \mathbb{Q}$" is a way of saying "x is a rational number".)
- In formal language: If $r \in \mathbb{R}$, then $r \in \mathbb{Q}$ if[a]

$$(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})\left(n \neq 0 \text{ and } r = \frac{m}{n}\right). \qquad (3.15)$$

- An irrational number is a real number r which is not rational.

[a] Formula (3.15) is not yet completely formal, because it contains the word "and". Soon we are going to leanr the symbol "$\wedge$" for "and", and then we will be able to rewrite (3.15) as $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})\left(n \neq 0 \wedge r = \frac{m}{n}\right)$.

3.4.5 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, although 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 17. For each of the following formulas,

(a) translate the formula into English,
(b) indicate whether it is true or false.

Give the best, most natural English translation. For example, the formula "$1 \in \mathbb{N}$*" could be translated as "*1 *belongs to the set of natural numbers", but this sounds very awkward. A much better way to say the same thing in English is "*1 *is a natural number", so this translation is to be preferred.*

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. $\pi \in \mathbb{Q}$.

3.4.6 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 "EVEN" AND "ODD" INTEGERS

Definition 12. Let a be an integer. We say that a is <u>even</u> if it is divisible by 2. And we say that a is <u>odd</u> 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 13.

- Let a, b be integers. We say that a and b are <u>coprime</u> if they do no have any nontrivial common factors.
- We write "$a \perp b$" to indicate that a and b are coprime.
- In formal language, if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a \perp b$ if

$$\sim (\exists k \in \mathbb{Z})(k|a \text{ and } k|b \text{ and } k \neq 1 \text{ and } k \neq -1)\,.$$

Example 9. 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. □

3.5 The proof of the irrationality of $\sqrt{2}$

Now, finally, we are ready to prove that $\sqrt{2}$ is irrational.

We are going to use two facts:

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.*

Example 10. Here are some examples to illustrate what Fact 1 means:

- let $a = \frac{-36}{22}$. The integers -36 and 22 are not coprime, because they are both divisible by 2. But we can factor out the 2, and get $a = \frac{-18}{11}$. Now the numerator -18 and the denominator 11 are coprime.
- let $a = \frac{630}{840}$. The natural numbers 630 and 840 are not coprime, because they are both divisible, for example, by 2. We can factor out the 2, and get $a = \frac{315}{420}$. The numerator 315 and the denominator 420 are not yet coprime, because they are both divisible, for example, by 3. We can factor out the 3, and get $a = \frac{105}{140}$. The numerator 105 and the denominator 140 are not yet coprime, because they are both divisible, for example, by 5. We can factor out the 5, and get $a = \frac{21}{28}$. The numerator 21 and the denominator 28 are not yet coprime, because they are both divisible by 7. We can factor the common factor 7 and we get, finally, $a = \frac{3}{4}$. And now the numerator 3 and the denominator 4 *are* coprime. □

Theorem 4. *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. (Here we are using Rule $\exists_{use}$.)

Using the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that

(1) $n \neq 0$,

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

(Here we are using again Rule $\exists_{use}$.)

Using Fact 1, we may actually choose m, n such that

(3) m and n are coprime.

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[25] 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.)

Since m is even, m is divisible by 2, that is, $(\exists k \in \mathbb{Z})m = 2k$.

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[26] 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.)

[25] Notice that we have a proof by contradiction within our main proof by contradiction.
[26] Another proof by 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.

Hence $\boxed{m \text{ and } n \text{ are not coprime}}$.

But $\boxed{m \text{ and } n \text{ are coprime}}$

So $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, which is 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**.

3.6 More irrationality proofs

We now use the same technique 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.)

Theorem 5. *There does not exist a rational number r such that $r^2 = 3$.*

Proof. We want to prove that $\sim (\exists r \in \mathbb{Q}) r^2 = 2$. We will do a proof by contradiction .

Assume that $(\exists r \in \mathbb{Q}) r^2 = 2$, i.e., there exists a rational number r such that $r^2 = 3$.

Pick one such number and call it r.

Using the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that

(1) $n \neq 0$,

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

Then, using Fact 1, we can actually choose m, n so that

(3) m and n are coprime.

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

$$n^2 = 3k^2 \,. \tag{3.16}$$

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.

So m and n are not coprime.

But m and n are coprime.

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

3.6.1 What happens when you make a mistake in a proof

Can we do the same that we did before to prove the following theorem?

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

$$n^2 = 3k^2 \,. \tag{3.17}$$

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.

So m and n are not coprime.

But m and n are coprime.

Therefore $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, 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 $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 4}$.**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[27] 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 is not prime.

[27]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.***

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.

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

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

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 the fact that $r \in \mathbb{Q}$, we may pick integers m, n such that

(1) $n \neq 0$,

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

Then, using Fact 1, we may pick m, n such that

(3) m and n are coprime.

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

$$4n^2 = 3k^2 \,. \tag{3.18}$$

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.

So m and n are not coprime.

But m and n are coprime.

Therefore $\boxed{m \text{ and } n \text{ are coprime and } m \text{ and } n \text{ are not coprime}}$, 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 $\boxed{\text{there does not exist a rational number } r \text{ such that } r^2 = 12}$.**Q.E.D.**

Problem 18. ***Prove*** that each of the following numbers is irrational:

1. $\sqrt{5}$,
2. $\sqrt[3]{5}$,
3. $\sqrt[3]{9}$,
4. $\sqrt{28}$,
5. $\sqrt{2+\sqrt{2}}$,
6. $\sqrt{\frac{2}{3}}$,
7. $\sqrt{\frac{27}{31}}$. □

Problem 19. ***Prove or disprove***[28] 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 an irrational number.
4. The product of two irrational numbers is an irrational number.
5. The sum of two irrational numbers is a rational number.
6. The product of two irrational numbers is a rational number.
7. The sum of a rational number and an irrational number is an irrational number.
8. The product of a rational number and an irrational number is an irrational number. □

Problem 20.

I. ***Explain*** why the following "proofs" that $\sqrt{2}+\sqrt{3}$ and $\sqrt{6}$ are irrational (in which we are allowed to use the facts that $\sqrt{2}$ and $\sqrt{3}$ are irrational) are wrong:

[28]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".

1. *Proof that* $\sqrt{2}+\sqrt{3}$ *is irrational:*

   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. *Proof that* $\sqrt{6}$ *is irrational:*

   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.**

II. ***Give correct proofs*** that $\sqrt{2}+\sqrt{3}$ and $\sqrt{6}$ are irrational. □

Problem 21. ***Prove*** that $\sqrt{2}+\sqrt[3]{2}$ is irrational. □

Problem 22. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is irrational. (NOTE: This requires some hard thinking on your part.) □

Problem 23. ***Prove*** that $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is irrational. (NOTE: This requires ***quite a lot*** of thinking on your part.) □

Problem 24. ***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.) □

3.7 A general theorem on irrationality of square roots

After having proved that various numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{28}$, $\sqrt{\frac{2}{3}}$, $\sqrt{\frac{27}{31}}$ are irrational, can we prove once and for all a general theorem that will include all these cases? The answer is "yes", and here is the theorem. Notice that all the irrationality results about square roots that we have proved before follow easily from this theorem. (For example: if $r = 2$, then $r = \frac{2}{1}$ and $2 \perp 1$, so Theorem 7 tells us that $\sqrt{r}$ is irrational, because 2 is not the square of an integer; similarly, if $r = \frac{2}{3}$, then Theorem 7 tells us that $\sqrt{r}$ is irrational, because $2 \perp 3$ and 2 and 3 are not squarea of integers.)

Theorem 7. *Let r be a rational number written as a quotient $\frac{m}{n}$, where m and n are coprime integers and $n > 0$. Then either $\sqrt{r}$ is irrational or both m, n are squares of integers.*

The key fact that will be used in this proof is the following

Fact 4. *If a, b, c are integers such that $c|ab$ and $c \perp b$, then $c|a$. (That is, if c divides ab and is coprime with b, then c divides a.*

Rough idea of the proof of Fact 4. We can write a, b, c as products of primes: $a = p_1.p_2.\cdots.p_n$, $b = q_1.q_2.\cdots.q_m$, $c = r_1.r_2.\cdots.r_k$. Then the expression of ab as a product of primes is

$$ab = p_1.p_2.\cdots.p_n.q_1.q_2.\cdots.q_m\,. \tag{3.19}$$

Since $c|ab$, all the primes r_j occur in the right-hand side of (3.19). But $c \perp b$, so none of the r_j is a q_j. It follows that all the r_j are p's i.e., factors of a, so $c|a$.

This argument is not completely rigorous. I will give you a rigorous—and much more elegant—proof later.

Proof of Theorem 7:

We will prove that if $\sqrt{r}$ is rational then both m, n are squares of integers.

Assume $\sqrt{r} \in \mathbb{Q}$.

Then we can write $\sqrt{r} = \frac{p}{q}$, where p, q are integers, and $q \neq 0$.

Furthermore, in view of Fact 1, we can actually choose p and q to be coprime.

We then have

$$\frac{p^2}{q^2} = \frac{m}{n}\,,$$

so

$$p^2 n = mq^2\,.$$

So $n|mq^2$. But $n \perp m$, so by Fact 7 $n|q^2$.

Also, $q^2|p^2n$.

But $q^2 \perp p^2$. (Reason: Suppose q^2 and p^2 were not coprime. Then they would have a common factor k such that $k > 1$. And k would have a prime factor u. Then u is prime and divides both q^2 and p^2. By Fact 3, u divides q and u divides p, so p and q are not coprime. But p and q are coprime, so we get a contradiction.)

Since $q^2|p^2n$ and $q^2 \perp p^2$, it follows that $q^2|n$.

So q^2 divides n, n divides n are natural numbers.

Therefore $n = q^2$.

Since $n = q^2$ and $p^2 n = mq^2$, it follows that $p^2 n = mn$.

So $p^2 = m$.

We have shown that $m = p^2$ and $n = q^2$. Hence both m and n are squares of integers.

We have shown that if $\sqrt{r}$ is rational then m and n must be squares of integers. So either m and n are squares of integers or r is irrational. **Q.E.D.**

4 What is a proof, really?

THIS SECTION IS STILL BEING WRITTEN. WHEN IT IS FINISHED IT WILL BE INCLUDED IN THESE NOTES.

4.1 Analysis of the proof of Theorem 1

THIS SECTION IS STILL BEING WRITTEN. WHEN IT IS FINISHED IT WILL BE INCLUDED IN THESE NOTES.

5 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

from the facts that 2+2 = 4 and 4+2 = 6 we deduce that (2+2)+2 = 6 (5.20)

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

des faits que 2+2 = 4 et 4+2 = 6 on deduit que (2+2)+2 = 6 . (5.21)

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 (5.20) would become, in purely

formal language:

$$(2+2=4 \wedge 4+2=6) \Longrightarrow (2+2)+2=6\,. \quad (5.22)$$

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 11. 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[29]

$$\text{if } p \in \mathbb{N}\,, \text{then } p \text{ is } \underline{\text{prime}} \text{ if } (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\,. \tag{5.23}$$

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 (5.23) 1 is prime.

But we can make it right by writing:

$$\text{if } p \in \mathbb{N}\,, \text{then } p \text{ is } \underline{\text{prime}} \text{ if } p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big) \tag{5.24}$$

5.1 Things and their names

In any language, whether it is English, French, Russian, Spanish, Chinese, or formal or semiformal mathematical

[29] 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: $(\forall p \in \mathbb{N})\Big(P(p) \Longleftrightarrow (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\Big)$. This is not yet a correct definition of "prime number" but at least it is pefectly clear.

language, we talk about ***things*** (objects, entities), and in order to do that we give them ***names***.

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

5.1.1 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!

5.1.2 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 12. 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[30].). □

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 13. 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

[30]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.

to refer to a new defendant when a new trial begins. □

Example 14 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. □

5.1.3 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,

- 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.

5.1.4 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[31] (Φ, Ψ, Σ, etc.).

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

[31] 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.

- 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 $=$, $<$, $\leq$, $>$, $\geq$, $+$, $\times$, $\to$, $\Rightarrow$, $\wedge$, $\vee$, $\Leftrightarrow$, 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 4 The symbols π and e stand for the well known real numbers 3.14159265358979323 . . . and 2.71828182845904523 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[32]. □

5.1.5 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.

[32]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.

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:

(*) $x^2 = 1 + x\,.$

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

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

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.)

5.1.6 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.

Example 15. 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 16. 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 $m < n$. □

5.1.7 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 7, on page 95.)

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 7.5, on page 115 below.

Problem 25. 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. $(\forall m \in \mathbb{Z})(n < m \implies n^2 < m^2)$.
12. $(\forall m \in \mathbb{Z})(n > m \implies n^2 > m^2)$.
13. $(\forall m \in \mathbb{Z})(n = m \implies n^2 = m^2)$.
14. $(\forall m \in \mathbb{Z})(n^2 = m^2 \implies n = m)$.

6 Dealing with equality

Throughout these notes, the symbols "=" and "≠" will be used.

- The symbol "=" is read as "is equal to".
- The symbol "≠" 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 17.

- 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. □

6.1 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 18. 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 19. 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[33]
4. $\pi = \pi$.
5. My uncle Billy=My uncle Billy. □

[33]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!

6.2 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:

$$\text{for every } x\,, \quad x = x\,. \tag{6.25}$$

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

$$\text{for every } x\,, y\,, \quad \text{if } x = y \text{ then } y = x\,. \tag{6.26}$$

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

$$\text{for every } x\,, y\,, z\,, \quad \text{if } x = y \text{ and } y = z \text{ then } x = z \tag{6.27}$$

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,

$$\text{for every } x\,, y\,, z\,, \quad \text{if } x = z \text{ and } y = z \text{ then } x = y\,. \tag{6.28}$$

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 8. *Facts I, II, III, and IV above follow from the two basic facts about equality described in the box on page 90 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

$$\text{if } x = y \text{ then } y = x\,. \tag{6.29}$$

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

Since we have proved (6.29) for arbitrary x, y, it follows that

$$\text{For all } x, y, \text{ if } x = y \text{ then } y = x\,. \tag{6.30}$$

(This is because of Rule $\forall_{prove}$, discussed later in these notes in section 7.5 on page 115.) This completes our proof. **Q.E.D.**

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

Problem 26. Write proofs of Fact III and Fact IV, following the model of the proof given here for Fact II.□

7 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

every natural number is either even or odd (7.31)

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[34].
- Every real number has a cube root[35].
- If n is any natural number then n is even or odd. $\square$
- Every cow has four legs.
- Every cow has nine legs[36].
- All humans are thinking beings.
- All giraffes have a long neck.

[34] False!

[35] True!

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

- Every giraffe has a long neck.
- Every real number is positive[37].
- Every natural number can be written as the sum of three squares of integers[38].
- Every natural number can be written as the sum of four squares of integers[39].
- Every integer is even[40].
- 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 (7.31) says

If n is an arbitrary natural number then n is either even or odd. (7.32)

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".)

[37] This one is false.

[38] False again!

[39] 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".

[40] Also false.

Precisely, the symbol is used as follows:

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

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

  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

$$(\forall x),$$

  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 $P(x)$.

7.1 How to read universal sentences

7.1.1 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[41],

or as

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

or as

[41] See Remark 5 below.

- 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 $P(x)$.

7.1.2 Sentences with restricted universal quantifiers

The universal sentence

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

can be read as follows:

- for every x, $P(x)$ is true[42],

or as

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

or as

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

or as

[42] See Remark 5 below.

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

or as

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

or as

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

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

"all animals are made of cells" is true (7.33)

is just another way of saying

all animals are made of cells . (7.34)

Similarly, saying

$P(n)$ is true (7.35)

is just another way of saying

$$P(n)\,. \tag{7.36}$$

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 $P(n)$". □

7.2 Using the universal quantifier symbol to write universal statements

7.2.1 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

$$2 + 2 = 4\,. \tag{7.37}$$

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

$$b|a \tag{7.38}$$

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:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big((2|a \wedge 2|b) \Longrightarrow 2|a+b\Big)\,. \tag{7.39}$$

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 ***semi-formal language***: they are a mixture of formal language and ordinary English.

These statements are universal sentences. And now you have learned how to ***formalize***[43] universal statements. So you can write

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

or

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

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

7.2.2 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.

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

Example 20. Suppose you wanted to say "every natural number is positive". You can write

$$(\forall n \in \mathbb{N}) n > 0\,. \tag{7.40}$$

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

Example 21. 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 22. 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:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big(\text{if } a|b \text{ and } a|c \text{ then } a|b{+}c\Big)\,, \tag{7.41}$$

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 (7.41) in fully formal language, as follows:

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

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(a|b \iff (\exists k \in \mathbb{Z})b = ak)\,. \tag{7.42}$$

- We can translate (7.41) into fully formal language as

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big((a|b \wedge a|c) \implies a|b{+}c\Big)\,, \tag{7.43}$$

7.3 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 23. 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. □

7.4 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 24 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". □

7.4.1 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(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(Alice, Jim, Bill, 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(Alice, Jim, Bill, 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(Alice, Jim, Bill, 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 $P(x, y,$ Jim, Mary).

7.4.2 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 25. Suppose you have written, in a proof:

$$(\forall n \in \mathbb{Z}) n(n+1) \text{ is even}. \tag{7.44}$$

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 (7.44), 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 (7.44) to

$$(\forall n \in \mathbb{Z}) n + n^2 \text{ is even}. \tag{7.45}$$

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. □

7.5 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 $\forall$?"*

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 26. 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 27. 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. □.

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.

7.6 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 9. *If x is a positive*[44] *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

[44] 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".

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

$$x + \frac{1}{x} \geq 2\,. \tag{7.46}$$

We will prove this by contradiction.

Assume that (7.46) is not true.

Then

$$x + \frac{1}{x} < 2\,. \tag{7.47}$$

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:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})\Big((a < b \wedge c > 0) \Longrightarrow ac < bc\Big)\,. \tag{7.48}$$

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 (7.48), and get*

$$\Big(x + \frac{1}{x} < 2 \wedge x > 0\Big) \Longrightarrow \Big(x + \frac{1}{x}\Big)x < 2x\,. \tag{7.49}$$

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 (7.47) by x, getting

$$x^2 + 1 < 2x\,. \tag{7.50}$$

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:

$$(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall c \in \mathbb{R})(a < b \Longrightarrow a+c < b+c)\,. \tag{7.51}$$

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 (7.51), and get*

$$x^2 + 1 - 2x < 2x - 2x, . \tag{7.52}$$

Since $2x - 2x = 0$*, we can conclude that* $x^2 + 1 - 2x < 0$*. Summarizing:*
We add $-2x$ to both sides, and get

$$x^2 + 1 - 2x < 0\,. \tag{7.53}$$

But $x^2 + 1 - 2x = (x - 1)^2$.
(This is easy to prove it. Try to do it.)
So

$$(x - 1)^2 < 0\,. \tag{7.54}$$

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

$$(\forall u \in \mathbb{R}) u^2 \geq 0\,. \tag{7.55}$$

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

$$(x - 1)^2 \geq 0\,. \tag{7.56}$$

Next, we use a fourth fact from real number arithmetic, namely, that if a real number is

nonnegative then it it is not negative[45], that is:

$$(\forall u \in \mathbb{R})(u \geq 0 \Longrightarrow \sim u < 0)\,. \qquad (7.57)$$

It then follows from (7.56) that

$$\sim (x-1)^2 < 0\,. \qquad (7.58)$$

From (7.54) and (7.58), we get

$$(x-1)^2 < 0 \wedge \Big(\sim (x-1)^2 < 0 \Big)\,. \qquad (7.59)$$

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

$$x > 0 \Longrightarrow x + \frac{1}{x} \geq 2\,. \qquad (7.60)$$

Finally, we have proved (7.60) for an arbitrary real number x. Hence

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \qquad (7.61)$$

Q.E.D.

[45]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

$$x + \frac{1}{x} \geq 2\,. \tag{7.62}$$

Assume that (7.62) is not true.

Then

$$x + \frac{1}{x} < 2\,. \tag{7.63}$$

Since $x > 0$, we can multiply both sides of (7.63) by x, getting

$$x^2 + 1 < 2x\,. \tag{7.64}$$

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

$$x^2 + 1 - 2x < 0\,. \tag{7.65}$$

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

$$(x-1)^2 < 0\,. \tag{7.66}$$

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

$$(\forall u \in \mathbb{R}) u^2 \geq 0\,. \tag{7.67}$$

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

$$(x-1)^2 \geq 0\,. \tag{7.68}$$

Then

$$\sim (x-1)^2 < 0\,. \tag{7.69}$$

From (7.66) and (7.69), we get

$$(x-1)^2 < 0 \wedge \Big(\sim (x-1)^2 < 0 \Big)\,. \tag{7.70}$$

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

$$x > 0 \Longrightarrow x + \frac{1}{x} \geq 2\,. \tag{7.71}$$

Finally, we have proved (7.69) for an arbitrary real number x. Hence

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \tag{7.72}$$

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

$$x + \frac{1}{x} \geq 2\,. \tag{7.73}$$

Assume that (7.73) is not true. Then

$$x + \frac{1}{x} < 2\,. \tag{7.74}$$

Since $x > 0$, (7.74) impliues

$$x^2 + 1 < 2x\,. \tag{7.75}$$

Therefore

$$x^2 + 1 - 2x < 0\,. \tag{7.76}$$

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

$$(x-1)^2 < 0\,. \tag{7.77}$$

On the other hand.

$$(x-1)^2 \geq 0\,. \tag{7.78}$$

Clearly, (7.77) and (7.78) lead to a contradiction.

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

Therefore

$$(\forall x \in \mathbb{R})(x > 0 \Longrightarrow x + \frac{1}{x} \geq 2)\,. \tag{7.79}$$

Q.E.D.

7.6.1 A few more examples of proofs involving universal sentences

Theorem 10. *If a, b are real numbers, then*

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

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

PROOF. YOU DO IT

Problem 27. Prove Theorem 10.

Problem 28. Explain what is wrong with the following proof of Theorem 10.

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

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

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

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

Theorem 11. *If x, α, β are positive real numbers then*

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

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

I am going to give you two proofs. The first one follows the same pattern as the proof of Theorem 9. The second one, much shorter, uses Theorem 9.

FIRST PROOF.

Let α, β, x be arbitrary positive real numbers[46].

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

[46]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 $x > 0$.

But

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

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 $p\left(u+\frac{1}{u}\right)$ 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

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

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

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

Q.E.D.

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

Theorem 12. *Let a and b be positive real numbers, and let n be a positive integer. Then*

$$ab \leq \frac{1}{n}\Big(a^n + (n-1)b^{\frac{n}{n-1}}\Big)\,. \tag{7.80}$$

Remark 6. For $n = 2$, inequality (7.80) says that

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

which is Theorem 10.

So (7.80) is a generalization of Theorem 10. □

Proof of Theorem 12. 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

$$f(x) \geq f(c) \text{ for all } x \in \mathbb{R} \text{ such that } x > 0. \tag{7.81}$$

We now prove (7.81) 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 (7.81) is true.

It follows from (7.81) that for every positive $x \in \mathbb{R}$ we have $f(x) \geq f(c)$, that is,

$$\frac{x^n}{n} - bx \geq \frac{c^n}{n} - bc\,. \tag{7.82}$$

Since (7.82) holds for every positive x, we can use it for $x = a$, thereby obtaining

$$\frac{a^n}{n} - ab \geq \frac{c^n}{n} - bc\,. \tag{7.83}$$

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 (7.83), we get

$$\frac{a^n}{n} - ab \geq -\frac{n-1}{n} b^{\frac{n}{n-1}} , \tag{7.84}$$

that is,

$$\frac{a^n}{n} - ab + \frac{n-1}{n} b^{\frac{n}{n-1}} \geq 0 , \tag{7.85}$$

from which it follows that

$$ab \leq \frac{a^n}{n} + \frac{n-1}{n} b^{\frac{n}{n-1}} , \tag{7.86}$$

that is,

$$ab \leq \frac{1}{n}\Big(a^n + (n-1) b^{\frac{n}{n-1}}\Big) , \tag{7.87}$$

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

8 Existential sentences

8.1 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 28. The sentence

$$(\exists x \in \mathbb{R}) x^2 = 2 \tag{8.88}$$

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 (8.88) as:

It is possible to pick a real number x 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 $\exists_{use}$ □

8.1.1 How not to read existential quantifiers

Students sometimes read an existential sentence such as

$$(\exists x \in \mathbb{R})x^2 = 2) \tag{8.89}$$

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 (8.89) as "there exists a real number x and $x^2 = 2$", then you give the impression that (8.89) makes two assertions:

1. that there exists a real number,
2. that $x^2 = 2$.

- But (8.89) 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 (8.89) 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 (8.89) 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,

8.1.2 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.

8.2 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 $\exists_{use}$.

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

$$(\exists x \in C)P(x)\,, \tag{8.90}$$

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 (8.90, so Suzy is a grass-eating cow.

or

> Let Suzy be a grass-eating cow.

Example 30. Suppose you have a real number x and you know that

$$(\exists y \in \mathbb{R}) y^5 - y^3 = x\,. \tag{8.91}$$

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

> Pick a witness for (8.91) 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 7. 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, $\diamond$, ♣, 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 31. 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[47] 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.

8.2.2 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***;

[47] 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(Suzy) is the sentence "Suzy eats grass". If $P(x)$ is the sentence "$x + 3y = x^2$", then $P(a)$ is the sentence "$a + 3y = a^2$".

- ***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 32. 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 $(\exists x)x^2 + 3 \cdot x = 10$. $\square$

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.***

8.3 Examples of proofs involving existential sentences

8.3.1 Some simple examples

Problem 29. Consider the sentence

$$(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x^2 - y^2 = 17\,. \tag{8.92}$$

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 (8.92) 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 (8.92). By Rule $\exists_{prove}$, this proves (8.92). **Q.E.D.**

Problem 30. Consider the sentence

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})n < m\,. \tag{8.93}$$

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 (8.93) 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 31. Consider the sentence

$$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N}) n < m\,. \tag{8.94}$$

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 (8.94) is false. Here is a proof.

> Asssume (8.94) 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 (8.94) is false.

Problem 32. Consider the sentence

$$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z}) n < m\,. \tag{8.95}$$

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 (8.95) is false. Here is a proof of its negation, that is, of

$$\sim (\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z}) n < m\,. \tag{8.96}$$

We are going to prove (8.96) by contradiction .

Assume that

$$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z}) n < m\,. \tag{8.97}$$

Pick a witness for Statement (8.97), 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 (8.97). Hence, by the proof-by-contradiction rule, (8.97) is false, that is, (8.96) is true. **Q.E.D.**

Problem 33. 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).

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{N}) n > m\,, \tag{8.98}$$
$$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N}) n < m\,, \tag{8.99}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{Z}) n < m\,, \tag{8.100}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N}) n < m\,, \tag{8.101}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N}) n \leq m\,, \tag{8.102}$$
$$(\exists x \in \mathbb{R})(\forall m \in \mathbb{N}) x < m\,. \tag{8.103}$$

8.3.2 A detailed proof of an inequality with lots of comments

Problem 34 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

$$\sim (\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2+(y-1)^2 = R^2 \wedge y = x+4 \Big)\,. \tag{8.104}$$

Assume (8.104) isn't true.

Then

$$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2+(y-1)^2 = R^2 \wedge y = x+4 \Big)\,. \tag{8.105}$$

Pick witnesses for (8.105) 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

$$(x-5)^2 + (y-1)^2 = R^2 \wedge y = x+4\,. \tag{8.106}$$

In particular,

$$(x-5)^2 + (y-1)^2 = R^2\,. \tag{8.107}$$

And also

$$y = x+4\,. \tag{8.108}$$

COMMENT: How did we go from (8.106) to (8.107) and (8.108)? 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 (8.106) to (8.107) and (8.108), 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 (8.106) to (8.107) and (8.108) 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 (8.107), and get

$$(x - 5)^2 + (x + 4 - 1)^2 = R^2\,, \qquad (8.109)$$

that is

$$(x-5)^2 + (x+3)^2 = R^2\,. \tag{8.110}$$

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

$$(x-5)^2 + (x+3)^2 \geq 32\,. \tag{8.111}$$

But

$$(x-5)^2 + (x+3)^2 = R^2\,. \tag{8.112}$$

So

$$R^2 \geq 32\,. \tag{8.113}$$

COMMENT: How did we go from (8.111) and (8.112) to (8.113)? 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 (8.111) and (8.112) to (8.113), 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 (8.111) and (8.112) to (8.113) 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 (8.104) is proved. **Q.E.D.**

8.3.3 The same proof without the comments

Proof. Let R be the radius of C.

Assume that $R < 5$.

We want to prove that

$$\sim (\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2+(y-1)^2 = R^2 \wedge y = x+4 \Big) . \tag{8.114}$$

Assume (8.114) isn't true. Then

$$(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})\Big((x-5)^2+(y-1)^2 = R^2 \wedge y = x+4\Big)\,. \tag{8.115}$$

Pick witnesses for (8.115) and call them x, y.

Then $(x-5)^2 + (y-1)^2 = R^2 \wedge y = x+4$, so in particular,

$$(x-5)^2 + (y-1)^2 = R^2\,. \tag{8.116}$$

Since $y = x+4$, we can substitute $x+4$ for y in (8.116), and get $(x-5)^2 + (x+4-1)^2 = R^2$, that is

$$(x-5)^2 + (x+3)^2 = R^2\,. \tag{8.117}$$

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

$$(x-5)^2 + (x+3)^2 \geq 32\,. \tag{8.118}$$

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 (8.114) is proved. **Q.E.D.**

8.4 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:

$$(\exists! x)P(x) \iff$$
$$\Big((\exists x)P(x) \wedge \Big((\forall x_1)(\forall x_2)(P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2 \Big) \Big) .$$

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
$$(\exists x)P(x) \tag{8.119}$$
and
$$(\forall x_1)(\forall x_2)\Big((P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2 \Big) . \tag{8.120}$$
(Formula (8.119) is the existence assertion, and Formula (8.120) is the uniqueness assertion.)

Example 33. "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 $u = v$.) □

8.4.1 Examples of proofs of existence and uniqueness

Problem 35. 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 36. 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. □