MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Date of this version: November 10, 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.

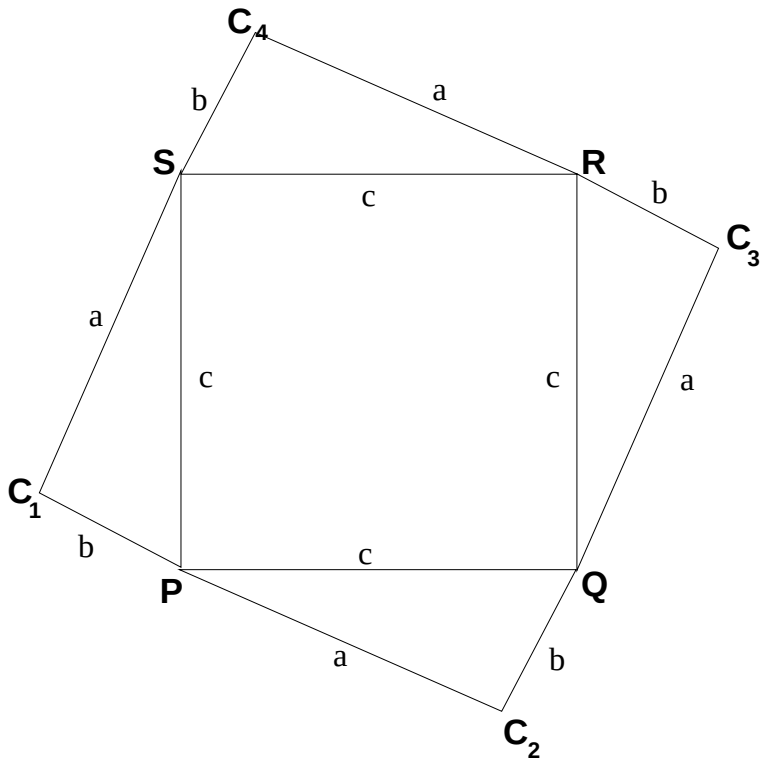
---

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

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

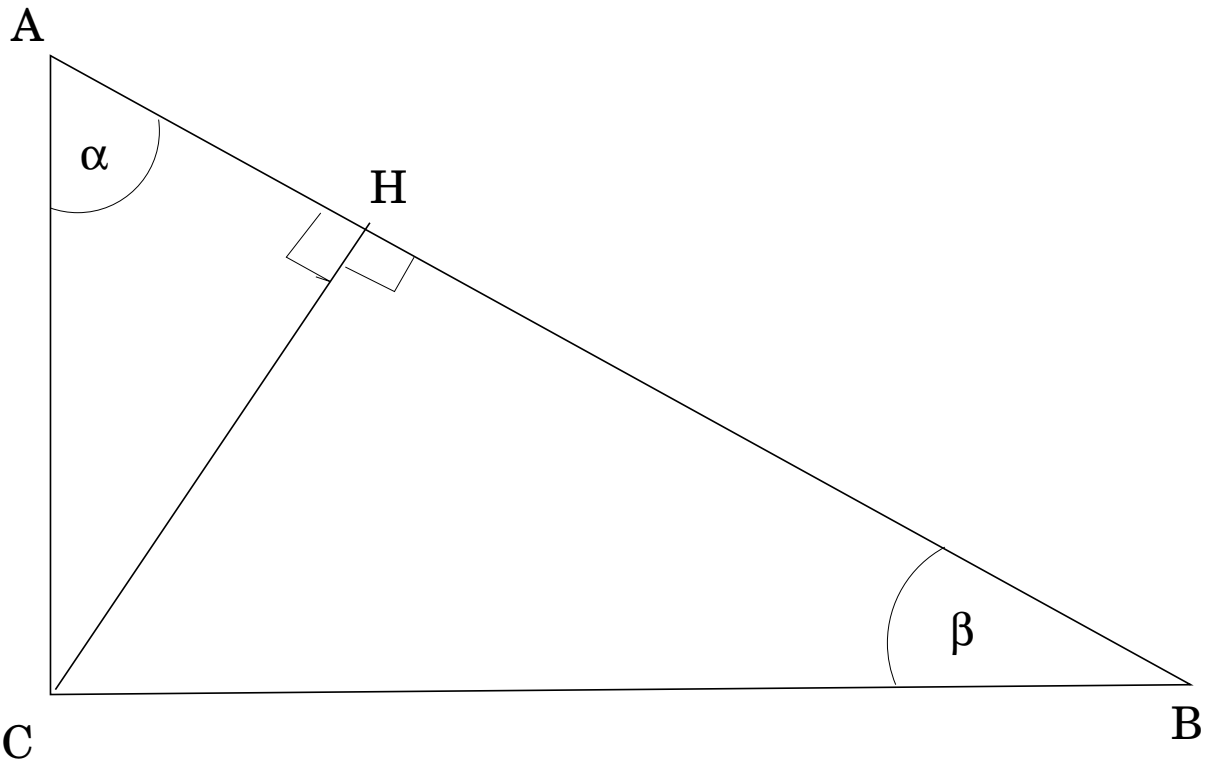
Subtracting $2ab$ from both sides, we get

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

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.

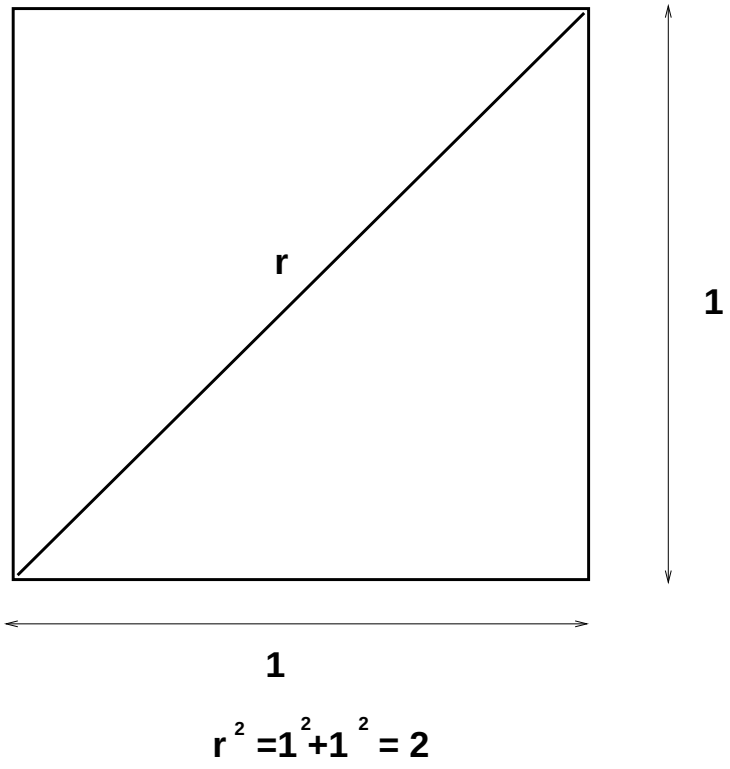
But then a momentous discovery of far-reaching consequences was made:

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 (&) and (&&) 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(Suzy) is the sentence "Suzy eats grass". And (&) says

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

whereas (&&) says

(&&') Suzy $\in C$.

So we are precisely in the situation where we can apply the rule for using universal sentences, and conclude that P(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. □

9 A summary of Logic

9.1 Terms and sentences

9.1.1 Nouns and noun phrases in English

- According to *Wikipedia*, a noun is "a word that functions as the name of some specific thing or set of things, such as living creatures, objects, places, actions, qualities, states of existence, or ideas".
- A noun phrase "is a phrase that has a noun (or indefinite pronoun) as its head or performs the same grammatical function as such a phrase".

So, for example, here is a list of noun phrases:

1. George Washington,
2. the first president of the United States,
3. the man who succeeded George Washington as prsdient of the United States,
4. this table,
5. the table,
6. the table that I bought yesterday,
7. the table that I bought yesterday at Walmart's and then brought home in a truck that I had borrowed from my very good friend Alice,
8. I,

9. you,
10. she,
11. he,
12. the news,
13. the number five,
14. the number that results from adding two plus three,

15. the product of two and three,
16. the number that results from adding two plus three and then multiplying the result by four,
17. the number that results from adding two plus three, multiplying the result by four, and then dividing the result of the multiplication by the product of six times seven,
18. the sum of the cubes of all the natural numbers from eight to forty-seven.

9.1.2 The "use-mention" distinction

Consider the following two sentences:

> Clarabelle is a cow.
>
> "Clarabelle" is a ten-letter word.

The first sentence talks about an animal and makes an assertion about that animal: it tells us that that animal is a cow.

The second sentence does not talk about an animal. It does not say anything about the animal called Clarabelle. It makes an assertion about a ***word***: it tells us that the word "Clarabelle" has ten letters.

The first sentence talks about the animal, so it ***mentions*** Clarabelle, And, in order to mention (i.e., talk about) Clarabelle it ***uses*** the word "Clarabelle".

The second sentence talks about the word, so it ***mentions*** the word "Clarabelle".

So the first sentence ***uses*** the word "Clarabelle" and the second sentence ***mentions*** it.

The distinction between use and mention is very important, and it is useful to understand it in order to avoid making mistakes in writing that sometimes might be confusing to the reader.

Let us be precise: word and groups of words are things, and like all other things words and groups of words can be given names. ***the name of a word or group of words is the word or groups of words enclosed in quotation marks***.

So, for example, the following are correct statements:

- Clarabelle is an animal.
- The name of Clarabelle is "Clarabelle".
- "Clarabelle" is a word.
- "Clarabelle" is a French name, not a cow.

- Clarabelle is a cow, not a French name;
- Clarabelle eats grass.
- "Clarabelle" does not eat grass.
- The name of the word "Clarabelle" is " "Clarabelle" ".

- The name of the first president of the United States was "George Washington". (If you had written instead "the name of the first president of the United States was George Washington", then, since George Washington was a general, it would follow that the name of the first president of the United States was a general, which is quite ridiculous, since a name is a word or group of words, and cannot be a general.)
- The name of George Washington is[48] "George Washington".
- If I say "the name of that cow over there is Clarabelle", then I am saying among other things that the name of that cow over there is a cow, which is not what I probably want to say[49]. I probably want to say that that the name of that cow over there is the

[48]So, strictly speaking, it is wrong to write: "my name is Alexander Hamilton", or "my name is Asher Lev", or "my name is Eminem". One should write "my name is "Alexander Hamilton" ", or "my name is "Asher Lev" ", or "my name is "Eminem" ". But this mistake is so common that nobody pays attention to it.

[49]For example: Clarabelle eats grass. So, if the name of that cow over there is Clarabelle, it follows that the name of that cow over there eats grass. And this is nonsense, of course: *cows* eat grass, *names* do not.

word "Clarabelle", so I must say: the name of that cow over there is "Clarabelle".

When you say something about Clarabelle, the cow, you ***use*** the word "Clarabelle" to talk about the cow, and by doing so you ***mention*** (i.e., talk about) the cow.

When you say something about "Clarabelle", the word, you ***mention*** (i.e., talk about) the word "Clarabelle", but you are not using the word to talk about the animal.

> When you ***use*** a word or group of words to talk about the thing that the word stands for, you do not enclose the word or group of words in quotation marks.
> When you ***mention*** a word or groups of words (i.e.,. talk about the word or gourp of words), you ***must*** enclose the word or group of words in quotation marks.

When writing mathematics, it is important to keep the distinction between use and mention, by using quotation marks when appropriate.

For example,

- we can write

  $$\text{I will prove that } 2 + 2 = 4$$

  in the same was as we would write

  $$\text{Alice said that she likes coffee.}$$

- but we should not write

$$\text{I will prove } 2 + 2 = 4$$

in the same was as we would not write

$$\text{Alice said I like coffee.}$$

We must write

$$\text{Alice said “I like coffee”.}$$

and

$$\text{I will prove “}2 + 2 = 4\text{”,}$$

or

$$\text{I will prove that “}2 + 2 = 4\text{” is true,}$$

or

$$\text{I will prove that the sentence “}2 + 2 = 4\text{” is true,}$$

or

$$\text{I will prove the sentence “}2 + 2 = 4\text{”.}$$

9.1.3 Terms in mathematical language

The noun phrases that we use in formal mathematical language are called ***terms***.

So a ***term*** is an expression that is the name of a thing. For example[50] the terms “four”, “4”, “two plus two”,

[50]Notice the use of the quotation marks, in keeping with the *use vs. mention* distinction explained in subsection 9.1.2. We can say correctly that 4 is a number, that $2 + 2$ is a number, that the term “4” has the value 4, that the term “$2 + 2$” has the value 4, that $2 + 2 = 4$ (meaning that both terms “$2 + 2$” and “4” have the same value). But it would be incorrect to write “4” = “$2 + 2$” because this says that the two terms “4” and “$2 + 2$” are the same, which is not true. (For example, the term “4” consists of just one character, whereas the term “$2+2$” consists of three characters, so they are manifestly not the same.)

"$2+2$" , "three plus one", $3+1$" all have the same value, namely, the number 4.

And usually mathematical terms are written with ***formulas***, that is, very concise expressions using special symbols. For example,

- instead of "the number five", we write "5";
- instead of "the number that results from adding two plus three", we write "$2+3$";
- instead of "the product of two and three", we write "2×3";
- instead of "the number that results from adding two plus three and then multiplying the result by four", we write "$(2+3) \times 4$";
- instead of "the number that results from adding two plus three, multiplying the result by four, and then dividing the result by the sum of twenty-three and the product of six times seven"; we write "$\frac{(2+3)\times 4}{23+6\times 7}$";
- instead of "the sum of the cubes of all the natural numbers from five to ten" we write "$\sum_{i=5}^{10}$".

9.1.4 Examples of terms and sentences

Example 34 The following expressions are terms:

- New York City;
- Mount Everest;
- the table;
- the student who asked why an implication is true when the premise is false;
- 2,
- $2 + 2$,
- $2 + x$,
- $x + y$,
- $(x + y)^2 + 3x + 5$,
- $\sum_{k=1}^{n}(k^3 + 1)$

But the following expressions are sentences, not terms:

- $2 + 2 = 4$,
- $2 + x = 4$,
- $x + y = 0$,
- $x + y = 0$,
- $x + y > 0$,
- $(\exists y \in \mathbb{R})x + y = 0$,

- $(\exists y \in \mathbb{R})x + y < 0$,
- $(\forall y \in \mathbb{R})x + y = 0$,
- $(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})y + z = x$.
- $(\forall x \in \mathbb{R})x.0 = 0$,
- $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})x + y > 0$,
- $(\forall x \in \mathbb{R})x^2 \geq 0$,
- $\sum_{x=1}^{5} x^2 = y$.
- $(\forall x \in \mathbb{R})x.0 = 0$,
- $\sum_{x=1} 5x^2 = y$.

9.1.5 The value of a term

A term has a ***value***, which is the thing that the term stands for. For example,

- the value of the term "5" is the natural number 5, and we indicate this by writing "$5 = 5$";
- the value of the term "$2 + 3$" is the natural number 5, and we indicate this by writing "$2 + 3 = 5$";
- the value of the term "2×3" is the natural number 6, and we indicate this by writing "$2 \times 3 = 6''$;

- the value of the term "$(2 + 3) \times 4$" is the natural number 20, and we indicate this by writing "$(2 + 3) \times 4 = 20$";
- the value of the term "$\frac{(2+3)\times 4}{23+6\times 7}$" is the rational number (i.e., fraction) $\frac{20}{65}$, and we indicate this by writing "$\frac{(2+3)\times 4}{23+6\times 7} = \frac{20}{65}$"; furthermore, the number $\frac{20}{65}$ is the same as the number $\frac{4}{13}$, so we could also written "$\frac{(2+3)\times 4}{23+6\times 7} = \frac{4}{13}$";
- the value of the term "$\sum_{i=5}^{10} i^3$" is the natural number $2,955$, and we indicate this by writing the equality "$\sum_{i=5}^{10} i^3 = 2,955$".

The values of terms can be all kinds of mathematical objects. Since the mathematical objects that you are most familiar with are numbers (natural numbers, integers, real numbers, complex numbers, etc.), you are probably used to terms whose values are numbers. But there are millions of other kinds of mathematical objects, and we can write terms with values of any of those kinds.

For example:

- The expression

$$\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix}$$

is a term whose value is a 2 by 2 matrix. The actual value of the term is the matrix $\begin{bmatrix} 3 & 4 \\ 2 & 4 \end{bmatrix}$, and we indicate this by writing:

$$\begin{bmatrix} 1 & 2 \\ -1 & 3 \end{bmatrix} + \begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 2 & 4 \end{bmatrix}$$

- ***Functions***[51] can be added (in some cases), and composed (in some cases). If f and g are functions then the name of the sum of f and g is "$f + g$", the name of the product of f and g is "$f \cdot g$", and the name of the composite "g followed by f" is "$f \circ g$". So, for example, if f, g, h are three functions, then the expression "$((f + g) \cdot g) \circ h$" is a term whose value is a function.

- ***Sets***[52] can be combined in various ways. For example, of A and B are sets, then we can form the sets $A \cup B$ (the *union* of A and B), $A \cap B$ (the *intersection* of A and B), $A \times B$ (the *Cartesian product* of A and B). Then the value of the term "$(\mathbb{R} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{R})$" is a set, namely, the intersection of the Cartesian product of $\mathbb{R}$ and $\mathbb{Z}$ with the Cartesian product of $\mathbb{Z}$ and $\mathbb{R}$.

[51] We will talk about functions later in the course.
[52] We will discuss sets in detail later later in the course.

9.1.6 Terms as instructions for a computation, i.e., as programs

You should think of a mathematical term as a computing device that executes a program, i.e., follows with a list of instructions for computing a result, called the ***value***. For example,

- the term "2+3" is a device that executes the following program: "add the number 3 to the number 2 and write down the result";
- the term "2×3" is a device that executes the following program: "multiply the number 2 by the number 3 and write down the result";
- the term "$(2 + 3) \times 4$" is a device that executes the following program: "add the number 3 to the number 2, multiply the result by the number 4, and write down the result";
- the term "$\frac{(2+3)\times 4}{23+6\times 7}$"; is a device that executes the following program: "add the number 2 to the number 3, multiply the result by the number 4, and divide the result by the number you get when you add to the number twenty-three the product of six times seven, and write down the result";
- the term "$\sum_{i=5}^{10}(i^3 + 3i^2 + 5)$" is a device that executes the following program:

    1. Look at all the natural numbers from 5 to 10.

2. For each such natural number, do the following:
   (a) Call the number i.
   (b) Compute $(i^3 + 3i^2 + 5)^2$.
3. Add up all the results of the computation of $(i^3 + 3i^2 + 5)^2$ for all values of i.
4. Write the result of this sum as the final result of the computation.

9.1.7 Letter variables in terms

A term can contain ***variables***, i.e. symbols that are not the names of definite objects, but could be used to stand for different objects.

For example: The term "$x + 3$", contains the letter variable x; it corresponds to the program: "add 3 to x and write down the result". When asked to compute $x + 3$, the term does not know what to do, because it does not know who x is. But if you give x a specific value, for example by saying "Let $x = 2$", then the term knows what to do: it gives x the value 2, and becomes the term $2 + 3$, which then know what to, and compues the value 5.

In other words: if a term t contains a variable x, then it is possible to give a value to the variable, and the term then can compute a value.

You should think of a variable as a "slot" that can be filled by plugging in a value. For example, the term "$x + 3$" consists of (1) a slot that can be filled in with a number; (2) the + sign, (3) the number 3.

A term may contain several variables. For example, the term

$$(x + y + 3x^2)y + y^2(z^2 + 3xz) + ye^x$$

contains the variables x, y, and z. The term has 10 slots. You can give a value to each of the three variables. The term then instructs us to fill in the first, third, seventh and tenth slots (the "x-slots") with the value we have chosen for x, the second, fourth, fifth and ninth slots (the "y-slots") with the value we have chosen for y, and and the sixth and eight slots (the "z-slots") with the value we have chosen for z. We can do this by writing, for example:

Let $x = 3\,,\ \ y = -1\,,\ \ z = 4\,.$

Then $(x + y + 3x^2)y + y^2(z^2 + 3xz) + ye^x \ = \ 33 - e^3\,.$

or

$$\Big((x+y+3x^2)y+y^2(z^2+3xz)+ye^x\Big)_{x=3,y=-1,z=4} \ = \ 33-e^3\,.$$

In a term t, a letter variable that has no value declared within the term and represents a slot that can be filled in by giving it values is called a free variable, or open variable.

9.1.8 Bound (dummy, closed) variables in terms

One of the main purposes of writing terms and sentences in formal language, with symbols, rather than phrases with lots of words, is to be able to say things much more ***concisely***[53]. (This is quite clear: "$2 + 2 = 4$" is much shorter than "two plus two equals four". And try to say "$(a + b)^2 = a^2 + 2ab + b^2$" with words, rather than symbols, and you'll se how much longer it gets.)

Further conciseness can be achieved by using letters to stand for expressions that appear repeatedly in a term

[53]This is ***not*** the only purpose. ***Another purpose*** is ***precision***: for example, if I say "two plus three times five", then this is ambiguous, because it could mean "two plus the product of three and five", or "the sum of three plus two, multiplied by five". In formal language, we write "$(2 + 3) \times 4$" or "$2 + (3 \times 5)$", and each of these two expressions has a clear and precise meaning. The ambigüity has disappeared. Furthermore, we agreed on the convention that when a product such as 3×4 is combined with another term by a "+" the parentheses surrounding the product can be omitted. So when we think we ought to write "$2 + (3 \times 4)$" we write instead "$2 + 3 \times 4$", and it is completely clear what that means, because if we had wanted to say "$(2 + 3) \times 4$" we would have had to enclose "$2 + 3$" in parenthees. A ***third purpose*** is ***universality***: to say "two plus two equals four" in Spanish you have to say "dos más dos es igual a cuatro", and in French you have to say "deux plus deux égale quatre". But in formal mathematical language you write "$2 + 2 = 4$", and this is understood by everybody, whether they speak English or Spanish or French or Chinese or any other language.

and are very long. For example, the term

$$32+5\frac{1+\sqrt{5}}{2}-23\left(\frac{1+\sqrt{5}}{2}\right)^2++7\left(\frac{1+\sqrt{5}}{2}\right)^3+19\left(\frac{1+\sqrt{5}}{2}\right)^4 \qquad (9.121)$$

can be written as

$$\left(32+5x-23x^2+7x^3+x^4\right)_{x=\frac{1+\sqrt{5}}{2}} \ , \qquad (9.122)$$

which we read as the computing instruction "give x the value $\frac{1+\sqrt{5}}{2}$, then compute $32+5x-23x^2+7x^3+x^4$, and write down the result".

Another example is the term

$$1^3+2^3+3^3+4^3+5^3+6^3+7^3+8^3+9^3+10^3\,, \qquad (9.123)$$

that can be written as

$$\sum_{k=1}^{10} k^3\,, \qquad (9.124)$$

which we read as the computing instruction

1. Look at all the natural number values between 1 and 10.
2. For each such value, do the following:
   (a) Call your number k.
   (b) Compute k^3.
3. Add up the results of these computations, for all natural numbers between 1 and 10.

As you can see, the term (9.122) is much shorter than the term (9.121), and the term (9.124) is much shorter than the term (9.123). And the difference becomes even more dramatic if consider very long terms, in which there is a computation that is repeated over and over. For example, suppose you want to talk about the sum of the cubes of the first $10,000$ natural numbers: using letters, we can write

$$\sum_{k=1}^{10,000} k^3 \,. \tag{9.125}$$

If you wanted to write this without using the $\sum$ notation, you would have to write a sum of $10,000$ terms, which would of course be enormously long[54].

It is clear that:

- In (9.122), we could have used any other letter instead of x, and the resulting term would execute exactly the same computation. So, for example, if we had written

  $$(32 + 5u - 23u^2 + 7u^3 + u^4)_{u=\frac{1+\sqrt{5}}{2}} \,, \tag{9.126}$$

  this would describe exactly the same computationas (9.126), and the term would have exactly the same

[54]Can you figure out what the value of this sum is? The answer is: $5,001,000,050,000,000$. Can you figure this out without having to compute $10,000$ cubes and then add them? Later in the course we will see how to figure this out and get the answer fairly fast.

value and (9.122).

- Similarly, in (9.124), we could have used any other letter instead of k, and the resulting term would execute exactly the same computation. So, for example, if we had written

$$\sum_{i=1}^{10} i^3 \text{ , or } \sum_{j=1}^{10} j^3 \text{ , or } \sum_{x=1}^{10} x^3 \text{ , or } \sum_{\alpha=1}^{10} \alpha^3 \text{ , or } \sum_{\diamond=1}^{10} \diamond^3 ,$$

  the resulting term would correspond to exactly the same computation and have the same value[55].

- Actually, in the term "$\sum_{k=1}^{10} k^3$" the letter k "isn't there", in the sense that we could describe the term without ever mentioning "k". For example, I could ask you to compute the value of this term without mentioning k: by saying "compute the sum of the cubes of all the natural numbers from 1 to 10", and you would know exactly what to do.

- A similar situation arises for the term

$$\left(32 + 5x - 23x^2 + 7x^3 + x^4\right)_{x=\frac{1+\sqrt{5}}{2}} .$$

  The letter x "isn't there", in the sense that we could describe the term without ever mentioning "x". For

[55] Using "x" here is not something one would normally do, because mathematicians usually prefer to use "x" for real numbers rather than natural numbers; but it is not forbidden to use x for a natural number.

examle, I could ask you to compute the value of this term without mentioning x: by saying

a. Add the following five numbers:
   1. the number 32,
   2. the number $5 \times \frac{1+\sqrt{5}}{2}$,
   3. the number $(-23) \times \left(\frac{1+\sqrt{5}}{2}\right)^2$,
   4. the number $7 \times \left(\frac{1+\sqrt{5}}{2}\right)^3$,
   5. the number $\left(\frac{1+\sqrt{5}}{2}\right)^4$.

b. Then write down the result.

9.1.9 What is a dummy (free, open) variable?

In a term t, a letter variable whose values are generated within the term itself, so that we do not need to ask the outside world what the value of that variable is in order to be able to compute the value of the term, is called a bound variable, or closed variable, or dummy variable.

The three clear signs that a variable is dummy

The following are three obvious signs that a variable in an expression T is a dummy variable:

(I) It is possible to substitute for the variable any other letter without changing the value of the expression. Indeed, the terms

$$\sum_{j=1}^{N} j^2\,, \tag{9.127}$$

$$\sum_{x=1}^{N} x^2\,, \tag{9.128}$$

$$\sum_{q=1}^{N} q^2\,, \tag{9.129}$$

all have the same value as "$\sum_{k=1}^{N} k^2$", and this is a sign that in the term "$\sum_{k=1}^{N} k^2$" the letter k is a dummy variable.

(II) If you ask somebody to execute the computation described by the expression T then this person does not need to be told what the value of the variable is, because the computation itself generates the value or values it needs for the variable. For example, if I ask you to compute the value of "$\sum_{k=1}^{N} k^2$", then you have to do this: you give k all natural number values between 1 and N, for each such value you compute its square, and then you add all the results. In order to be able to do this, you have to ask "who is N?", but ***you do not have to ask "who is k?"***, because you yourself, in the process of doing the computation, are going to generate the values of k. This is a second sign that in the term "$\sum_{k=1}^{N} k^2$" the letter k is a dummy variable.

(III) The expression T is equal or equivalent to another expression not involving the variable at all. For example, "$\sum_{k=1}^{N} k^2$" is equal to $\frac{(2N+1)N(N+1)}{6}$, an expression that does not contain k. And this is a third sign that in the term "$\sum_{k=1}^{N} k^2$" the letter k is a dummy variable.

9.1.10 Other examples of dummy variables in terms

The two examples of dummy variables that you probably know from previous courses are those occurring in expressions such as "$\sum_{k=a}^{b} \ldots$" and "$\prod_{k=a}^{b} \ldots$".

For example, the term "$\sum_{k=1}^{5} k^2$" executes the following computation: look at all the natural numbers from 1 to 45, for each such number compute its square, add all the results and write down the sum".

And the term "$\prod_{k=1}^{5}(k+1)^2$" executes the following computation: look at all the natural numbers from 1 to 45, for each such number compute the square of the sum of one plus the number, multiply all the results and write down the sum".

In both cases, the letter k is a dummy variable. You do not need to ask "who is k'?" is order to carry out the computation. If you are asked to compute $\sum_{k=1}^{25} k^3$ or $\prod_{k=1}^{25}(k+1)$, then you do not have to ask "who is k?". You yourself generate all the values of k from 1 to 25 and for each value compute something (k^3 in the first case, $k+1$ oin the second case), and then do something with the results (add them all up in the first case, multiply them in the second case).

Variables of integration. Another important example of a dummy variable is a ***variable of integration***.

If I ask you to tell me what the value of the integral

$$\int_a^b x^2\,dx$$

is, you have to ask me "who are a and b" but you don't have to ask "who is x?". That's because x is a dummy variable. This is precisely the second of the three "signs that a variable is a dummy variable".

Let us look at the first sign: "It is possible to substitute the letter for any other letter, without changing the value of the term". This is indeed true: if, instead of "$\int_a^b (x+1)^2\,dx$" I write "$\int_a^b (y+1)^2\,dy$", or "$\int_a^b (u+1)^2\,du$", or "$\int_a^b (q+1)^2\,dq$", or "$\int_a^b (\alpha+1)^2\,d\alpha$", then all those integrals are exactly the same.

Finally, let us look at the third sign: "The term T is equal to another expression not involving the variable at all." And this is indeed true: the integral $\int_a^b (x+1)^2\,dx$ is equal to $\frac{(b+1)^3}{3} - \frac{(a+1)^3}{3}$. And the expression "$\frac{(b+1)^3}{3} - \frac{(a+1)^3}{3}$" does not contain x at all.

So, clearly, ***in the term "$\int_a^b x^2\,dx$", the variable x is a dummy variable.*** This means that ***the integral $\int_a^b x^2 dx$ does not depend on x; it depends on a and b but not on x, in the sense that if you want me to give you a specific value for the term then you have to tell me who a and***

b ***are, but not whi*** x ***is***.

Variables in the definition of a function We will be discussing ***functions*** later. But let me tell you the basic facts:

- A ***function*** assigns to each object x belonging to a certain set S another object, called the ***value*** of the function at x. If f is a name of the function, then we use $f(x)$ to denote the value of f at x.
- The set S is called the ***domain*** of the function.
- In order to introduce and describe a function f, we can do this: we explain how, for each member of the domain S, the value of f at this member is computed or determined. To do this, we write things like

$$\text{the function } \mathbb{R} \ni x \mapsto 3(x+1)^4 + e^x\,, \qquad (9.130)$$

  which says that (a) the domain of the function is the set $\mathbb{R}$, (b) for each member of the domain $\mathbb{R}$, if we call that member x, then the value $f(x)$ is the number $3(x+1)^4 + e^x$.

Notice that "x" is a name that we introduce in order to explain how to compute $f(x)$. We could equally well have written:

$$\text{the function } \mathbb{R} \ni u \mapsto 3(u+1)^4 + e^u,$$

and that would be exactly the same function.

So ***the variable x in a function definition such as (9.130) is dummy.***

Remark 8. An expression such as "the function $\mathbb{R} \ni x \mapsto x^2$" is a term. Its value is a function, namely, the function that takes each real number and squares it. The term "the function $\mathbb{R} \ni x \mapsto x^2$" contains the variable x but, as we just explained, x is a dummy variable, because (a) the term is equal to another term that does nto contain x at all (namely, the term "the function that for each real number produces as value the square of the number", or "the function that takes each real number and suares it"); (b) if we substitute another letter for x we get the same function. (For example, "the function $\mathbb{R} \ni u \mapsto u^2$" is exactly the same function: it's "the function that takes each real number and squares it".)

The expressions "the function $\mathbb{R} \ni x \mapsto x^2$" and "the function $\mathbb{R} \ni x \mapsto (x+1)^2 - 2x - 1$" are terms. Each of these terms has a value, which is a function. Furthermore, those two functions are the same function, because for every real number x the numbers x^2 and $(x+1)^2 - 2x - 1$ are equal. So the terms "the function $\mathbb{R} \ni x \mapsto x^2$" and "the function $\mathbb{R} \ni x \mapsto (x+1)^2 - 2x - 1$" have the same value, and we can assert that

$$\text{The function } \mathbb{R} \ni x \mapsto x^2 \ = \text{the function } \mathbb{R} \ni x \mapsto (x+1)^2 - 2x - 1.$$

NOTE: It would be incorrect to write

$$\text{“The function } \mathbb{R} \ni x \mapsto x^2\text{”} \ = \text{“the function } \mathbb{R} \ni x \mapsto (x+1)^2 - 2x - 1\text{”},$$

because this asserts that the two terms are the same, which is manifestly not the case. If this is not clear tou consider the following examples:

$$\text{Bill Clinton} = \text{William Jefferson Clinton}$$

and

$$\text{“Bill Clinton”} = \text{“William Jefferson Clinton”}.$$

The first one says that that the values of the terms “Bill Clinton” and “William Jefferson Clinton” are the same, i.e., that the person whose name is “Bill Clinton” is the same as the person whose name is “William Jefferson Clinton”.

But the seond one says that the names “Bill Clinton” and “William Jefferson Clinton” are the same, i.e. that they conist of exactly the same letters in the same order. nd this is clearly false. (For example, the name “William Jefferson Clinton” contains a W and a J, but the name “Bill Clinton” does not. $\square$

9.1.11 Bound (dummy, closed) variables in sentences

Sentences are very similar to terms. Like terns, sentences have ***values***. The one big difference between terms and sentences is that ***the value of a term is a thing and the value of a sentence is a truth value, i.e., "true" or "false".***

Example 35.

1. The expression "$2 + 2$" is a term. Its value is the number 4.

2. The expressions "$2 + 2 = 4$" and "$2 + 2 = 5$" are sentences. They are both propositions, because they contain no open variables. So they both have a truth value. The value of "$2 + 2 = 4$" is "true". The value of "$2 + 2 = 5$" is "false".

3. The expression "$(\forall n \in \mathbb{Z})(2|n \implies 4|n^2)$" is a sentence. It contains the variable n . But this variable is dummy (closed, bound), because it satisfies all the three signs for dummy variables that we saw before:

   (I) *It is possible to substitute for the letter n any other letter, without changing the value of the*

expression. Indeed, the sentences

$$(\forall m \in \mathbb{Z})(2|m \Longrightarrow 4|m^2)\,, \quad (9.131)$$

$$(\forall q \in \mathbb{Z})(2|q \Longrightarrow 4|q^2)\,, \quad (9.132)$$

$$(\forall u \in \mathbb{Z})(2|u \Longrightarrow 4|u^2)\,, \quad (9.133)$$

are all equivalent to "$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2)$".

(II) *If you ask somebody to execute the computation described by this sentence, then this person does not need to be told what the value of the variable n, is, because the computation itself generates the value or values it needs for the variable.* (Indeed, to execute the computation described by the sentence "$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2)$", the person doing the computation has to do the following:

(a) look at all the integers, and for each integer do the following:
   i. call the integer n,
   ii. determine if "$2|n \implies 4|n^2$ is true,

(b) then look at all the results of the computations, for all the integers. If the are all "true" write "true". If one of the results is "false", write 'false".

The key point here is that ***the person doing the computation does need to ask***

"who is n?" because they themselves will generate the values of n to be looked at.

(III) *The sentence "$(\forall n \in \mathbb{Z})(2|n \implies 4|n^2)$" is equivalent to another sentence not involving the variable n at all.* Indeed: "$(\forall n \in \mathbb{Z})(2|n \implies 4|n^2)$" is equivalent to "if an integer is even then its square is divisible by 4".

Since the only variable that occurs in this sentence is bound, the sentence contains no open variables. So it is a proposition. It has a definite truth value, which turns oiut to be "true".

4. The expression "$(\forall n \in \mathbb{Z})(a|n \implies b|n^2)$" is a sentence. It contains the variables n, a, b . But b variable is dummy (closed, bound), because it satisfies all the three signs for dummy variables that we saw before:

   (I) *It is possible to substitute for the letter n any other letter, without changing the value of the expression.* Indeed, the sentences

$$(\forall m \in \mathbb{Z})(a|m \implies b|m^2)\,, \quad (9.134)$$
$$(\forall q \in \mathbb{Z})(a|q \implies b|q^2)\,, \quad (9.135)$$
$$(\forall u \in \mathbb{Z})(a|u \implies b|u^2)\,, \quad (9.136)$$

are all equivalent to "$(\forall n \in \mathbb{Z})(a|n \Longrightarrow b|n^2)$".

(II) *If you ask somebody to execute the computation described by this sentence, then this person does not need to be told what the value of the variable n, is, because the computation itself generates the value or values it needs for the variable.* (Indeed, to execute the computation described by the sentence "$(\forall n \in \mathbb{Z})(a|n \Longrightarrow b|n^2)$", the person doing the computation has to do the following:

(a) look at all the integers, and for each integer do the following:

i. call the integer n,

ii. determine if "$a|n \implies b|n^2$ is true,

(b) then look at all the results of the computations, for all the integers. If the are all "true" write "true". If one of the results is "false", write 'false".

The key point here is that ***the persons doing the computation does need to ask "who is n?" because they themselves will generate the values of n to be looked at.***

This is to be contrasted with a and b. The per-

son doing the computation cannot do anything without asking first ""who are a and b?". So a and b are free variables.

(III) *The sentence "*$(\forall n \in \mathbb{Z})(a|n \implies b|n^2)$*" is equivalent to another sentence not involving the variable* n *at all.* Indeed: "$(\forall n \in \mathbb{Z})(a|n \implies b|n^2)$" is equivalent to "if an integer is divisible a, then its square is divisible by b". And you can see that this sentence contains a and b but not n.

5. The expression

$$p \in \mathbb{Z} \wedge p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(jk = p \implies (j = 1 \vee k = 1)\Big) \quad (9.137)$$

is a sentence. It contains three variables, namely, p, j, and k. The variable p is free, but j and k are bound. So it should be possible to find an equivalent sentence that does not contain j and k at all. And, indeed, here is the sentence: "p is a prime number". This is not a proposition: its truth value depends on p. The sentence is true for p if p is a prime number, and is false if p is not a prime number.

6. The sentence

$$(\forall p \in \mathbb{Z})\left(p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(jk = p \implies (j = 1 \vee k = 1)\Big)\right) \quad (9.138)$$

contains three variables, namely, p, j, and k. They are all bound. So the sentence is a proposition, and

has a definite truth value. The sentence says "every integer is prime", which is of course false.

Important remark. Many students, when asked to define "prime number", answer by writing[56] (9.138). This, of course, is wrong. The students want to say "p is prime if and only if (9.137) holds", but instead they end up saying "every integer is prime", without understanding the difference. ***Please do not do that in your exam.*** □

Example 36. In each of the following sentences, the variable n is bound:

- "$(\forall n \in \mathbb{Z})n^2 - n$ is even". (In this case, the sentence itself says: "give n all possible integer values; for each such value, compute $n^2 - n$, see if it is even, and if the answer is "yes" for all value of n, then say "true"; otherwise say "false".)
- "$(\exists n \in \mathbb{Z})n^2 = 9$". (In this case, the sentence itself says: "give n all possible integer values; for each such value, compute n^2, and see if it is equal to 9; and if the answer is "yes" for at least one value of n, then say "true"; otherwise say "false".)

[56] If you don't believe me, I can show you exams in which several students wrote exactly that. I don't understand why this happens, but it does.

- "$\sum_{n=1}^{m} n^3 = \left(\frac{m(m+1)}{2}\right)^2$". (In this case, the sentence says: give n all possible integer values between 1 and m; for each such value, compute n^3; then add all the results, and see it the sum is equal to $\left(\frac{m(m+1)}{2}\right)^2$; if it is, say "true"; otherwise say "false". NOTE: In order to execute these instructions, you need to know who m is. So m is ***not*** a bound variable; the sentence does not generate a value for m. We have to tell the sentence who m is. So m is a ***free*** variable.)

- "$(\forall m \in \mathbb{N}) \sum_{n=1}^{m} n^3 = \left(\frac{m(m+1)}{2}\right)^2$". (In this case, the sentence says: give m all possible natural number values; for each such value, do what was described in the previous example, to decide if "$\sum_{n=1}^{m} n^3 = \left(\frac{m(m+1)}{2}\right)^2$" is true or not. If if the answer is "true" for all values of m, then say "true"; otherwise say "false".) So in this sentence m is also a bound variable.

Example 37. The same letter variable can occur in a sentence as both bound and free. So we really should not talk about a ***variable*** being free or being bound in a sentence: we should tall about an ***occurrence*** of a variable being free or bound.

For example, let S be the sentence

$$(\forall n \in \mathbb{Z})2|n \wedge n = 7$$

This very weird sentence says "every integer is even, and n is equal to 7." The letter n occurs three times in it, so ***there are three occurrences of*** n ***in*** S**.** The first two are bound, and the third one is free. □

9.1.12 A convention about naming sentences: the expression $P(x)$

Sentences, like anything else, can be given letter names. And for sentences we will usually use capital letters. So, for example, a sentence could be called A, or B, or P, or Q, or X. But it will be convenient to sometimes use more complicated names, such as $P(x)$, or $P(x, y)$.

And we will adopt the following very useful convention:

> We are allowed[a] to call a sentence $P(x)$, if x is free (i.e., not bound) in the sentence, that is, if the sentence does not contain an x-quantifier or any other expression (such as $\sum_{x=1} N$, or $\prod_{x=1}^{N}$) that assigns values to x.
> Similarly, we are allowed to call a sentence $P(x, y)$, if the variables x and y are free (i.e., not bound) in the sentence, that is, if the sentence does not contain an x-quantifier or a y-quantifier or any other expression (such as $\sum_{x=1}^{N}$, or $\sum_{y=1}^{N}$, or $\prod_{x=1}^{N}$, $\prod_{y=1}^{N}$), that assigns values to x or y.
>
> [a] I am saying "we are allowed to" rather "we have to". ***If a sentence has*** x ***as an open variable, we don't have to call it*** $P(x)$. We can call it P, if we want to.

Example 38.

- The following sentences can be called $P(x)$:
  1. $2 + 2 = 4$,
  2. $x > 5$,
  3. $(x + 2)^2 = 7x - 3$,
  4. $(y - x)^2 \geq 0$,
  5. $y + 3 + y^2$,
  6. $(\forall y \in \mathbb{R})(y - x)^2 \geq 0$,
  7. $(\forall y \in \mathbb{R})y^2 \geq 0$,
  8. $(x + y)^2 = x^2 + 2xy + y^2$,
  9. $(\exists y \in \mathbb{R})x + y = 0$,
  10. $(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})y + z = x$.
- and the following sentences cannot be called $P(x)$:
  1. $(\forall x \in \mathbb{R})(x + 1)^2 = x^2 + 2x + 1$,
  2. $\sum_{x=1}^{5} x^2 = 55$,
  3. $(\forall x \in \mathbb{R})x.0 = 0$.
- The following sentences can be called $P(x, y)$:
  1. $2 + 2 = 4$,
  2. $x > 5$,
  3. $(x + 2)^2 = 7x - 3$,

4. $(y - x)^2 \geq 0$,
5. $y + 3 + y^2$,
6. $(x + y)^2 = x^2 + 2xy + y^2$.

- and the following sentences cannot be called $P(x, y)$:
- $(\forall y \in \mathbb{R})(y - x)^2 \geq 0$,
- $(\forall y \in \mathbb{R})y^2 \geq 0$,
- $(\forall y \in \mathbb{R})x + y = 0$,
- $(\forall x \in \mathbb{R})(x + 1)^2 = x^2 + 2x + 1$,
- $\sum_{x=1}^{5} x^2 = 55$,
- $(\exists y \in \mathbb{R})x + y = 0$,
- $(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})y + z = x$.

(NOTE: If it bothers you that we are allowing using the name $P(x)$ for "$2 + 2 = 4$" and "$y + 3 + y^2$", even though these sentences have no x in them, the reason is very simple: all that matters is that x is not bound in these sentences. Whether it appears in them or not is irrelevant.)

9.1.13 Some problems

Problem 37. ***Prove*** each of the following propositions:

1. $(\forall n \in \mathbb{N})\Big(\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \Longrightarrow \sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}\Big)$.
2. $(\forall n \in \mathbb{N})\Big(\sum_{k=1}^{n} k^2 = \frac{(2n+1)n(n+1)}{6} \Longrightarrow \sum_{k=1}^{n+1} k^2 = \frac{(2n+3)(n+1)(n+2)}{6}\Big)$.
3. $(\forall n \in \mathbb{N})\left(\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 \Longrightarrow \sum_{k=1}^{n+1} k^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2\right)$.
4. $(\forall n \in \mathbb{N})(n < 2^n \Longrightarrow n+1 < 2^{n+1})$.
5. $(\forall n \in \mathbb{N})\Big(n^2 < 2^n + 2 \Longrightarrow (n+1)^2 < 2^{n+1} + 2\Big)$.
6. $(\forall n \in \mathbb{N})\Big(n^3 < 2^n + 257 \Longrightarrow (n+1)^3 < 2^{n+1} + 257\Big)$.

9.2 Substitution

Substitution

- If $P(x)$ is a sentence and t is a term, then the sentence obtained from $P(x)$ by substituting t for x is called $P(t)$.

  Example. If $P(x)$ is the sentence "$2 + 2 = 2 + x$", and t is the term "$1 + 1$", then $P(t)$ is the sentence "$2 + 2 = 2 + (1 + 1)$".

- ***We only allow the substitution of*** t ***for*** x ***in*** $P(x)$ ***when*** t ***is is free in*** $P(x)$***, in the sense that*** $P(x)$ ***does not contain a quantifier or any other expression that assigns values to any of the variables occurring in*** t.

Example. If $P(x)$ is the sentence "$(\exists y \in \mathbb{R})y = x$" (which is a sentence that contains x as an open variable, so we are allowed to call this sentence "$P(x)$"), and t is the term "y", then we are ***not*** allowed to substitute t for x in $P(x)$ and call the resulting sentence $P(y)$. □

In the following example, I will show you why the restriction on term substitution that we have just imposed in the box on "Substitution" is necessary.

Example 39. One of the rules of logic is Rule $\forall_{use}$,

which says that

($\forall_{use}$) *If we have proved* $(\forall x \in S)P(x)$*, and* t *is a term, then we can go to* $P(t)$*.*

Suppose we allowed this for any sentence $P(x)$ and any term t, with no restictions. Then we would be able to take $P(x)$ to be the sentence "$(\exists y \in \mathbb{R})y = x$" and t to be the term "$y + 1$".

The sentence "$(\forall x \in \mathbb{R})P(x)$" says

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})y = x\,.$$

It is easy to see that this sentence is in fact a true proposition. And it is easy to prove it. (Proof: Let x be an arbitrary real number. Pick y to be x. Then y is a witness for $(\exists y \in \mathbb{R})y = x$. So by Rule $\exists_{prove}$ we have proved $(\exists y \in \mathbb{R})y = x$ for arbirary $x \in \mathbb{R}$. Hence by Rule $\forall_{prove}$ we have proved that $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})y = x$.)

Now that we have proved "$(\forall x \in \mathbb{R})P(x)$", if we had no restriction on substitutions, we would be able to substitute the term t for x in $P(x)$, thus getting the sentence $P(t)$, that is, "$(\exists y \in \mathbb{R})y = y + 1$". But this sentence is clearly false. So we do not want to be able to prove it from a true sentence. The only way to solve this problem is to avoid this kind of substitution. □

This is why, in order to avoid the problem that we presented in Example 39, we impose the restriction explained earlier: ***in a sentence*** $P(x)$ ***we can only substitute for*** x ***a term*** t ***that does not contain any variables that are bound in*** $P(x)$.

So, for example, we can conclude from the sentence "$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})y \neq x$" that "$(\exists y \in \mathbb{R})y \neq 5$", or "$(\exists y \in \mathbb{R})y \neq x$", or "$(\exists y \in \mathbb{R})y \neq x^2 + z + 35$", but not "$(\exists y \in \mathbb{R})y \neq y$".

9.3 Forming sentences: the grammar of formal language

The English language has a ***grammar***, i.e., a set of rules that restrict what combinations of words are acceptable ("grammatically correct") sentences. For example, "cows eats grass" is not a grammatically correct English sentence, because the subject is the noun "cows", which is plural, and the verb is "eats", which is singular[57]

English grammar is very complicated, with lots of rules, an enormous number of exceptions, and many cases where it is unclear whether something is a grammatically cor-

[57]English grammar is crazy! Most nouns form their plural by adding an "s" at end, so the plurals of "cow", "duck", "table" are "cows", "ducks", "tables". But for most verbs it's the other way around: the singular ends with an "s" (as in "eats", "swims", "walks") and the plural is without the "s" (as in "eat", "swim", "walk"), so "cows eat grass" and "ducks swim" are grammatically correct, but "cows eats grass" and "ducks swims" are not. Go figure!

rect sentence. (For example, people argue about whether a sentence such as "He is determined to completely destroy the evidence", containing a split infinitive, is correct or not.)

Formal mathematical language has a very simple grammar. Here is the part of formal language grammar that has to do with the formation of sentences. (There is another part that deals with the formation of atomic sentences. That will be discussed later.)

- Sentences are formed by combining atomic sentences, connectives, and parentheses.
- Atomic sentences are sentences.
- If A, B are sentences, then we can form the sentences $A \wedge B$, $A \vee B$, $A \Longrightarrow B$, and $A \Longleftrightarrow B$.
- If A is a sentence, then we can form the sentence $\sim A$, the ***negation*** of A,
- If A is a sentence and Q is a quantifier, then we can form the sentence QA, known as an *existential quantification of* A, if Q is an existential quantifier, and as a *universal quantification of* A, if Q is a universal quantifier[58]

[58] ***Quantifers*** were discussed in Section 9.4.2, on page 203. Recall that: the symbols "$\forall$" and "$\exists$" are the ***quantifier symbols***. Using these symbols, we can form expressions such as "$(\forall x)$" and "$(\exists x)$", called ***unrestricted quantifiers***, and "$(\forall x \in S)$" and "$(\exists x \in S)$", called ***restricted quantifiers***.

- When a sentence A is combined with other sentences or connectives to form another sentence, then: if A is of the form $P \implies Q$, or $P \wedge Q$, or $P \vee Q$, or $P \iff Q$, then A has to be enclosed in parentheses before we form the combination.

Example 40. Let us say that "if n is an integer then if n is even then $n+1$ is odd". To say this, we use the atomic sentences "$2|n$" ("n is even") and "$2|n+1$" ("$n+1$ is even") and the connectives "$\sim$" and "$(\forall n \in \mathbb{Z})$". We negate "$2|n+1$" to form the sentence "$\sim 2|n+1$", which says "$n+1$ is odd". Then we combine "$2|n$" and "$\sim 2|n+1$" using the connective "$\implies$", and form the sentence "$2|n \implies \sim 2|n+1$" ("if n is even then $n+1$ is odd"). Finally, in order to assert that "$2|n \implies \sim 2|n+1$" is true for every integer n, we quantify "$2|n \implies \sim 2|n+1$" by writing the quantifier "$(\forall n \in \mathbb{Z})$" to its left. But before we do that, since the sentence "$2|n \implies \sim 2|n+1$" is of the form $A \implies B$, we enclosed it in parentheses, by writing "$(2|n \implies \sim 2|n+1)$" . The final result is the sentence

$$(\forall n \in \mathbb{Z})(2|n \implies \sim 2|n+1)\,.$$

This sentence says precisely what we want, i.e., that the statement "if n is even then $n+1$ is odd" is true for every integer n.

Example 41. Suppose we want to say

> if a natural number p has the property that whenever two integers a, b are such that p divides ab it follows that p divides a or p divides b, then p is a prime number or $p = 1$

in formal language.

We observe first that sentence clearly says that something is true for every natural number p, so the sentence is of the form "$(\forall n \in \mathbb{N})A$". Now, A is of the form $B \implies C$, where B is the sentence "p has the property that whenever two integers a, b are such that p divides ab it follows that p divides a or p divides b", and C is the sentence "p is a prime number or $p = 1$".

Then, if formal language, A says

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(p|ab \implies (p|a \vee p|b)\Big)\,,$$

and B says

$$p = \text{is a prime number } \vee p = 1\,.$$

So our sentence says

$$(\forall p \in \mathbb{N})\Bigg((\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(p|ab \implies (p|a \vee p|b)\Big) \implies (p \text{ is a prime number} \vee p = 1)\Bigg)\,.$$

This is not yet a completely formal sentence, because it has the words "is a prime number". In order to get a

completely formal sentence, we can substitute for "p is a prime number" the meaning of "p is a prime number" in formal language, that is,

$$(\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big) .$$

The result is

$$(\forall p \in \mathbb{N})\Bigg((\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(p|ab \Longrightarrow (p|a \vee p|b)\Big)$$

$$\Longrightarrow \Big((\forall k \in \mathbb{N})\big(k|p \Longrightarrow (k = 1 \vee k = p)\big) \vee p = 1\Big)\Bigg) .$$

Notice that this sentence contains several letter variables, namely, p, a, b, and k, but they are all bound variables, so the sentence is a proposition. And we can see this by rephrasing the sentence without using any letter variables at all. as follows:

> if a natural number has the property that whenever it divides the product of two integers it follows that it divides one of them, then the natural number is either one or a prime number.

9.4 How sentences are constucted

9.4.1 The seven logical connective symbols

There are ***seven*** logical connectives[a]. They are:

1. $\sim$: negation ("it's not the case that"),
2. $\wedge$: conjunction ("and"),
3. $\vee$: disjunction ("or"),
4. $\Longrightarrow$: implication ("implies", "if $\cdots$ then"),
5. $\Longleftrightarrow$: biconditionsl ("if and only if"),
6. universal quantifiers,
7. existential quantifiers.

[a] A Logical connective is a symbol that is used to combine sentences to form new sentences.

9.4.2 The quantifiers

- A quantifier is an expression

  $$(\forall x) \quad \text{or} \quad (\forall x \in S) \quad \text{or} \quad (\exists x) \quad \text{or} \quad (\exists x \in S)\,.$$

  where x is a variable and S is a set.
- The symbol "$\forall$" is called the universal quantifier symbol.
- The symbol "$\exists$" is called the existential quantifier symbol.
- "$(\forall x)$" is an unrestricted universal quantifier,

- "$(\forall x \in S)$" is a restricted universal quantifier.
- "$(\exists x)$" is an unrestricted existential quantifier,
- "$(\exists x \in S)$" is a restricted existential quantifier,

9.4.3 Sentence types

Every mathematical sentence is of one, and only one, of the following eight types:

1. atomic,
2. negation ("$\sim A$"),
3. conjunction ("$A \wedge B$"),
4. disjunction ("$A \vee B$"),
5. implication ("$A \Longrightarrow B$"),
6. biconditional ("$A \Longleftrightarrow B$"),
7. universal ("$(\forall x)P(x)$" or "$(\forall x \in S)P(x)$")
8. existential ("$(\exists x)P(x)$" or "$(\exists x \in S)P(x)$").

9.5 Forming sentences

- Sentences are formed by combining atomic sentences, connectives, and parentheses.
- Atomic sentences are sentences.

- If A, B are sentences, then we can form the sentences $A \wedge B$, $A \vee B$, $A \Longrightarrow B$, and $A \Longleftrightarrow B$.
- If A is a sentence, then we can form the sentence $\sim A$, the ***negation*** of A,
- If A is a sentence and Q is a quantifier, then we can form the sentence QA, known as an *existential quantification of* A, if Q is an existential quantifier, and as a *universal quantification of* A, if Q is a universal quantifier.
- When a sentence A is combined with other sentences or connectives to form another sentence, then: if A is of the form $P \Longrightarrow Q$, or $P \wedge Q$, or $P \vee Q$, or $P \Longleftrightarrow Q$, then A has to be enclosed in parentheses before we form the combination.

Example 42 Let us say that "if n is an integer then if n is even then $n+1$ is odd". To say this, we use the atomic sentences "$2|n$" ("n is even") and "$2|n+1$" ("$n+1$ is even") and the connectives "$\sim$" and "$(\forall n \in \mathbb{Z})$". We negate "$2|n+1$" to form the sentence "$\sim 2|n+1$", which says "$n+1$ is odd". Then we combine "$2|n$" and "$\sim 2|n+1$" using the connective "$\Longrightarrow$", and form the sentence "$2|n \Longrightarrow \sim 2|n+1$" ("if n is even then $n+1$ is odd"). Finally, in order to assert that "$2|n \Longrightarrow \sim 2|n+1$" is true

for every integer n, we quantify "$2|n \Longrightarrow\sim 2|n+1$" by writing the quantifier "$(\forall n \in \mathbb{Z})$" to its left. But before we do that, since the sentence "$2|n \Longrightarrow\sim 2|n+1$" is of the form $A \Longrightarrow B$, we enclosed it in parentheses, by writing "$(2|n \Longrightarrow\sim 2|n+1)$" . The final result is the sentence

$$(\forall n \in \mathbb{Z})(2|n \Longrightarrow\sim 2|n+1)\,.$$

This sentence says precisely what we want, i.e., that the statement "if n is even then $n+1$ is odd" is true for every integer n.

9.5.1 When do we put parentheses?

When a sentence A is combined with other sentences or connectives to form another sentence, then: if A is of the form $P \Longrightarrow Q$, or $P \wedge Q$, or $P \vee Q$, or $P \Longleftrightarrow Q$, then A has to be enclosed in parentheses before we form the combination.

Example 43. Suppose you want to say that

If an integer n is even, then n^2 is divisible by 4.

You start with the atomic sentences "$2|n$" ("n is even") and "$4|n^2$" ("n^2 is divisible by 4").

Then you combine these sentences using the implica-

tion connective, and get

$$2|n \Longrightarrow 4|n^2\,, \tag{9.139}$$

that is, "if n is even, then n^2 is divisible by 4".

Finally, it is clear that the sentence is intended to be an assertion for every integer n, so you quantify it with a universal quantifier. But before you quantify, you have to remember that (9.139) is an implication, that is, a sentence of the form $A \Longrightarrow B$. So ***before you quantify it, you have to enclose it in parentheses***.

The final result is the proposition

$$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2)\,. \tag{9.140}$$

What would have happened if you had not put the parentheses? You would have ended up with

$$(\forall n \in \mathbb{Z})2|n \Longrightarrow 4|n^2\,, \tag{9.141}$$

which is a completely different sentence! Sentence (9.141) says that the sentence "$(\forall n \in \mathbb{Z})2|n$" implies the sentence "$4|n^2$". In other words, (9.141) says: "if every integer is even, then n is divisible by 4". This is not even a proposition, because the third "n" is an open variable. □

9.6 The 14 logical rules

Here is the list of the fourteen logical rules.

1

Rule for using a conjunction (Rule $\wedge_{use}$)

If P, Q are sentences, and you have proved $P \wedge Q$, then you are allowed to go to P, and you are also allowed to go to Q.

2

Rule for proving a conjunction (Rule $\wedge_{prove}$)

If P, Q are sentences, and you have proved P and have proved Q, then you are allowed to go to $P \wedge Q$,

3

Rule for using an implication (Rule $\Longrightarrow_{use}$, a.k.a. Modus Ponens)

If P, Q are sentences, and you have proved $P \Longrightarrow Q$ and have proved P, then you are allowed to go to Q.

4

Rule for proving an implication (Rule $\Longrightarrow_{prove}$)

If P, Q are sentences, and you have proved Q assuming P, then you are allowed to go to $P \Longrightarrow Q$.

5

Rule for using a biconditional (Rule $\Longleftrightarrow_{use}$)

If P, Q are sentences, and you have proved $P \Longleftrightarrow Q$, then you can go to $P \Longrightarrow Q$ and to $Q \Longrightarrow P$.

6

Rule for proving a biconditional (Rule $\Longleftrightarrow_{prove}$)

If P, Q are sentences, and you have proved $P \Longrightarrow Q$ and $Q \Longrightarrow P$, then you are allowed to go to $P \Longleftrightarrow Q$.

7

Rule for using a disjunction (Rule $\vee_{use}$, a.k.a. the proof by cases rule)

If P, Q, R are sentences, and you have proved $P \vee Q$, $P \Longrightarrow R$, and $Q \Longrightarrow R$, then you can go to R.

8

Rule for proving a disjunction (Rule $\vee_{prove}$)

Suppose P and Q are sentences. Then, if you have proved $\sim P \Longrightarrow Q$ or $\sim Q \Longrightarrow P$ then you can go to $P \vee Q$.

9

The proof by contradiction rule

(I) If, assuming A, we prove C, which is a contradiction, then we can go to $\sim A$.

(II) If, assuming $\sim A$, we prove C, which is a contradiction, then we can go to A.

10

Rule for using universal sentences (Rule $\forall_{use}$, a.k.a. the "universal specialization rule")

If $P(x)$ is a sentence and t is a term that does not contain any variables that are bound in $P(x)$, then

- if you have proved $(\forall x)P(x)$, you can go to $P(t)$;
- If you have proved that $(\forall x \in S)P(x)$, and that $t \in S$, then you can go to $P(t)$.

11

Rule for proving universal sentences (Rule $\forall_{prove}$, a.k.a. the "universal generalization rule")

(I) If, starting with "Let x be arbitrary", you prove $P(x)$, then you are allowed to go to $(\forall x)P(x)$.

(II) If, starting with "Let $x \in S$ be arbitrary", or "Let x be an arbitrary member of S", you prove $P(x)$, then you are allowed to go to $(\forall x \in S)P(x)$.

12

Rule for using existential sentences (Rule $\exists_{use}$, a.k.a. the "existential specialization rule")

If $P(x)$ is a sentence, and the letter a is not in use as the name of anything, then:

- If you have proved $(\exists x)P(x)$, then you can introduce a witness for $(\exists x)P(x)$, and call it a, so that this new object will satisfy $P(a)$.
- 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.

13 **Rule for proving existential sentences, (Rule $\exists_{prove}$, a.k.a. the "existential generalization rule")**

Suppose $P(x)$ is a sentence and w is a term that does not contains any variables that are bound in $P(x)$. Then

(I) If w is a witness for $(\exists x)P(x)$ (i.e., if $P(w)$), then you can go to $(\exists x)P(x)$.

(II) If w is a witness for $(\exists x \in S)P(x)$ (i.e., if $w \in S$ and $P(w)$), then you can go to $(\exists x \in S)P(x)$.

14 **"Substitution of equals for equals" (Rule SEE)**

If $P(x)$ is a sentence, s and t are terms, and you have proved $s = t$ or $t = s$, and you have also proved $P(s)$, then you can go to $P(t)$.

9.7 Some problems, with solutions

Problem 38. For the sentence

$$(\forall n \in \mathbb{Z})(\exists m \in \mathbb{Z})m > n\,, \tag{9.142}$$

i. Translate the sentence into reasonable English.
ii. List all the variables that occur in the sentence, and indicate which ones are free (i.e. open) and which ones are bound (i.e., dummy, or closed). If a variable occcurs in the sentence more than once, it may happen that some of the occurrences are free and others are boiund. If this happens, say it.
iii. Indicate whether the sentence is a proposition (i.e., has no open variables) or not.
iv. If the sentence is a proposition, then
    a. ***indicate*** whether it is true or false,
    b. ***prove*** the assertion that you made to answer part a.

Solution.

i. Sentence (9.142) says: "for every integer n there exists an integer m such that $m > n$".
ii. The variables occurring in (9.142) are m and n. Both are bound. The sentence has no free variables.
iii. The sentence is a proposition.

iv.a The sentence is ***true***.

iv.b *Proof of (9.142):*

> Let $n \in \mathbb{Z}$ be arbitrary.
> *We want to prove "$(\exists m \in \mathbb{Z})m > n$", and for that purpose we are going to find a witness.*
> Chooe $w = n + 1$.
> *Why do I choose w this way? Because it works. How do I know it works? In this case, it is quite obvious: I need an integer greater than n, so $n + 1$ is a natural choice.*
> Then $w \in \mathbb{Z}$ and $w > n$.
> So w is a witness for "$(\exists m \in \mathbb{Z})m > n$".
> Hence $(\exists m \in \mathbb{Z})m > n$. [Rule $\exists_{prove}$]
>
> So we have proved "$(\exists m \in \mathbb{Z})m > n$" for arbitrary $n \in \mathbb{Z}$.

Hence $\boxed{(\forall n \in \mathbb{Z})(\exists m \in \mathbb{Z})m > n}$. [Rule $\forall_{prove}$] **Q.E.D.**

Problem 39. For the sentence

$$(\exists m \in \mathbb{Z})m > n\,, \tag{9.143}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.143) says: "there exists an integer m such that $m > n$".
ii. The variables occurring in (9.143) are m and n. The variable m is bound, and m is free.
iii. The sentence is a not a proposition.
iv.a,b Since the sentence is not a proposition, questions [iv.a] and [iv.b] do not apply.

Problem 40. For the sentence

$$(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n\,, \tag{9.144}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.144) says: "there exists an integer m such that m is larger than every integer".
ii. The variables occurring in (9.144) are m and n. Both are bound. The sentence has no free variables.

iii. The sentence is a proposition.
iv.a The sentence is ***false***.
iv.b *Proof that (9.144) is false:*

We want to prove that $\sim (\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n$.

We will do it by contradiction.

Assume that $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n$.

Pick a witness w, so $w \in \mathbb{Z}$ and $(\forall n \in \mathbb{Z})m > n$. [Rule $\exists_{use}$]

Then $w > w + 1$. [Rule $\forall_{use}$].

But $(\forall n \in \mathbb{Z})n \leq n + 1$.

So $w \leq w + 1$. [Rule $\forall_{use}$]

Hence $\sim w > w + 1$.

So $w > w + 1 \wedge \sim w > w + 1$ [Rule $\wedge_{prove}$]

And "$w > w + 1 \wedge \sim w > w + 1$" is a contradiction.

So we have proved a contradiction assuming that $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n$.

Therefore $\boxed{\sim (\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n}$. [Proof by contradiction rule] **Q.E.D.**

Problem 41. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2), \tag{9.145}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.145) says: "the square of every even integer is divisible by 4".
ii. The only variable occurring in (9.145) is n. And it is bound. The sentence has no free variables.
iii. The sentence is a proposition.
iv.a The sentence is ***true***.
iv.b *Proof of (9.145):*

We want to prove the universal sentence (9.145), and we are going to do it using Rule $\forall_{prove}$.

Let n be an arbitrary integer.

We want to prove that $2|n \Longrightarrow 4|n^2$. *And for that purpose we are going to use Rule* $\Longrightarrow_{prove}$.

Assume tbat $2|n$.

Then $(\exists k \in \mathbb{Z})n = 2k$.

Write $n = 2k$, $k \in \mathbb{Z}$. [Rule $\exists_{use}$]

Then $n^2 = (2k)^2 = 4k^2$.

Furthermore, $k^2 \in \mathbb{Z}$. [Reason: $k \in \mathbb{Z}$ and $(\forall k \in \mathbb{Z})k^2 \in \mathbb{Z}$.]

So k^2 is a witness for $(\exists k \in \mathbb{Z})n^2 = 4k$.

Therefore $(\exists k \in \mathbb{Z})n^2 = 4k$. [Rule $\exists_{prove}$]

So $4|n^2$. [Definition of "|"]

We have proved "$4|n^2$" assuming "$2|n$".

Hence $2|n \Longrightarrow 4|n^2$. [Rule $\Longrightarrow_{prove}$]

We have proved "$2|n \Longrightarrow 4|n^2$*" for arbitrary* $n \in \mathbb{Z}$.

Hence $\boxed{(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2)}$ [Rule $\forall_{prove}$]

Q.E.D.

Problem 42. For the sentence

$$(\forall n \in \mathbb{Z})2|n \Longrightarrow 4|n^2\,, \tag{9.146}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.146) says: "if every integer is even then n^2 is divisible by 4".

ii. The only variable occurring in (9.142ax) is n. This variable occurs in (9.146) three times; the first two occurrences are bound, and the third one is free.

iii. The sentence is a not a proposition.

iv.a,b Since the sentence is not a proposition, questions [iv.a] and [iv.b] do not apply.

Problem 43. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \wedge 4|n^2), \tag{9.147}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.147) says: "for every integer n, n is even and n^2 is divisible by 4".

ii. The only variable occurring in (9.145) is n. And it is bound. The sentence has no free variables.

iii. The sentence is a proposition.

iv.a The sentence is ***false***.

iv.b *Short proof that (9.147) is false:*

If "$(\forall n \in \mathbb{Z})(2|n \wedge 4|n^2)$" was true, then "$2|n \wedge 4|n^2$" would be true for every $n \in \mathbb{Z}$.

But "$2|n \wedge 4|n^2$" is false for $n = 1$.

So "$(\forall n \in \mathbb{Z})(2|n \wedge 4|n^2)$" is false.

Q.E.D.

Problem 44. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \vee 4|n^2), \tag{9.148}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.148) says: "for every integer n, n is even or n^2 is divisible by 4".

ii. The only variable occurring in (9.145) is n. And it is bound. The sentence has no free variables.

iii. The sentence is a proposition.

iv.a The sentence is ***false***.

iv.b *Short proof that (9.148) is false:*

If "$(\forall n \in \mathbb{Z})(2|n \vee 4|n^2)$" was true, then "$2|n \vee 4|n^2$" would be true for every $n \in \mathbb{Z}$.

But "$2|n \vee 4|n^2$" is false for $n = 1$.

So "$(\forall n \in \mathbb{Z})(2|n \vee 4|n^2)$" is false.

Q.E.D.

Problem 45. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \iff 4|n^2), \tag{9.149}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 38.

Solution.

i. Sentence (9.145) says: "for every even integer n, n is even if and only if n^2 is divisible by 4".

ii. The only variable occurring in (9.145) is n. And it is bound. The sentence has no free variables.

iii. The sentence is a proposition.

iv.a The sentence is ***true***.

Short proof of (9.149):

We want to prove the universal sentence (9.149). According to Rule $\forall_{prove}$*, we can do this by proving "*$(2|n \iff 4|n^2)$*" for an arbitarry integer* n*.*

Let n be an arbitrary integer.

We want to prove the biconditional sentence "$2|n \iff 4|n^2$*". According to Rule* $\iff_{prove}$*, we can do this by proving the implications "*$2|n \implies 4|n^2$*" and "*$4|n^2 \implies 2|n$*".*

Short proof of "$2|n \implies 4|n^2$*".*

We have already proved that $(\forall n \in \mathbb{Z})(2|n \implies 4|n^2)$ in our solution of problem 41.

So "$2|n \implies 4|n^2$" follows by Rule $\forall_{use}$.

Short proof of "$4|n^2 \implies 2|n$*".*

Assume $4|n^2$.

We will prove "$2|n$*" by contradiction.*

Assume $\sim 2|n$.
Then n is odd.
So n^2 is odd. [Reason: the product of two odd integers is odd]
That is, $\sim 2|n^2$.
But $4|n^2$, so n^2 is even.
That is, $2|n^2$.
Hence $2|n^2 \wedge \sim 2|n^2$, which is a contradiction.

Since we have proved a contradiction assuming $\sim 2|n$, we can conclude that $2|n$.

Since we have proved $2|n$ assuming $4|n^2$, we can conclude, thanks to Rule $\Longrightarrow_{prove}$, that $4|n^2 \Longrightarrow 2|n$.

Since we have proved "$2|n \Longrightarrow 4|n^2$" and "$4|n^2 \Longrightarrow 2|n$", we can conclude, thanks to Rule $\Longleftrightarrow_{prove}$, that $2|n \Longleftrightarrow 4|n^2$.

We have proved "$2|n \Longleftrightarrow 4|n^2$" for arbitrary $n \in \mathbb{Z}$.

Hence $\boxed{(\forall n \in \mathbb{Z})(2|n \Longleftrightarrow 4|n^2)}$ [Rule $\forall_{prove}$]

Q.E.D.

Problem 46. Let A, B, C be propositions. ***Prove***, using the rules of logic, that

$$\big(A \Longrightarrow (B \Longrightarrow C)\big) \Longleftrightarrow \Big((A \wedge B) \Longrightarrow C\Big)\,. \tag{9.150}$$

Solution.

We want to prove a biconditional sentence. For that purpose. we use Rule $\Longleftrightarrow_{prove}$: to prove $P \Longleftrightarrow Q$, prove $P \Longrightarrow Q$ and $Q \Longrightarrow P$.

Proof of "$\big(A \Longrightarrow (B \Longrightarrow C)\big) \Longrightarrow \Big((A \wedge B) \Longrightarrow C\Big)$".

Assume $\boxed{A \Longrightarrow (B \Longrightarrow C)}$. We want to prove $(A \wedge B) \Longrightarrow C$.

Assume $\boxed{A \wedge B}$. We want to prove C.
It follows from $A \wedge B$ that A. [Rule $\wedge_{use}$]
It follows from A and $A \Longrightarrow (B \Longrightarrow C)$ that $B \Longrightarrow C$. [Rule $\Longrightarrow_{use}$]
It follows from $A \wedge B$ that B, [Rule $\wedge_{use}$]
It follows from B and $B \Longrightarrow C$ that $\boxed{C}$. [Rule $\Longrightarrow_{use}$]

Since we have proved C assuming $A \wedge B$, we conclude that $\boxed{(A \wedge B) \Longrightarrow C}$.

[Rule $\Longrightarrow_{prove}$]

Since we have proved $(A \wedge B) \Longrightarrow C$ assuming $A \Longrightarrow (B \Longrightarrow C)$, we can go to

$$\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \Longrightarrow \big((A \wedge B) \Longrightarrow C\big)\,, \tag{9.151}$$

completing the proof of "$\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \Longrightarrow \big((A \wedge B) \Longrightarrow C\big)$".

Proof of "$\Big((A \wedge B) \Longrightarrow C\Big) \Longrightarrow \Big(A \Longrightarrow (B \Longrightarrow C)\Big)$".

Assume $\boxed{(A \wedge B) \Longrightarrow C}$. We want to prove $A \Longrightarrow (B \Longrightarrow C)$.

Assume $\boxed{A}$. We want to prove $B \Longrightarrow C$.

Assume $\boxed{B}$. *We want to prove* C.

Since we have A and B, we can go to $A \wedge B$. [Rule $\wedge_{prove}$]

Since we have $A \wedge B$ and $(A \wedge B) \Longrightarrow C$, we can go to $\boxed{C}$. [Rule $\Longrightarrow_{use}$]

Since we have proved C assuming B, we can go to $\boxed{B \Longrightarrow C}$. [Rule $\Longrightarrow_{use}$]

Since we have proved $B \Longrightarrow C$ assuming A, we can go to $\boxed{A \Longrightarrow (B \Longrightarrow C)}$.

[Rule $\Longrightarrow_{use}$]

Since we have proved $A \Longrightarrow (B \Longrightarrow C)$ assuming $(A \wedge B) \Longrightarrow C$, we can go to

$$\big((A \wedge B) \Longrightarrow C\big) \Longrightarrow \Big(A \Longrightarrow (B \Longrightarrow C)\Big), \tag{9.152}$$

completing the proof of "$\big((A \wedge B) \Longrightarrow C\big) \Longrightarrow \Big(A \Longrightarrow (B \Longrightarrow C)\Big)$".

Since we have proved both implications (9.151) and (9.152), we can conclude from Rule $\Longleftrightarrow_{prove}$ that

$$\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \Longleftrightarrow \big((A \wedge B) \Longrightarrow C\big), \tag{9.153}$$

Q.E.D.

Problem 47. Let $P(x)$, $Q(x)$, be one-variable predicates, and let S be a set.

1. ***Prove***, using the rules of logic, the sentence

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longleftrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \tag{9.154}$$

(Here is an example: suppose S is the set of all people, "$P(x)$" stands for "x likes tea" and "$Q(x)$" stands for "x likes coffee". Then the sentence "$(\forall x \in S)(P(x) \wedge Q(x))$" says "everybody likes tea and coffee", and the sentence "$(\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)$" says "everybody likes tea and everybody likes coffee". It is clear that both sentences say the same thing, so it is obvious that they are equivalent, so that the sentence (9.154) is true.)

2. ***Prove*** that the sentence

$$(\forall x \in S)(P(x) \vee Q(x)) \iff \Big((\forall x \in S)P(x) \vee (\forall x \in S)Q(x)\Big) \tag{9.155}$$

cannot be proved using the rules of logic. (HINT: Find an example of a pair of predicates $P(x)$, $Q(x)$ for which (9.155) is false.)

Solution. First, we prove (9.154).

Sentence (9.154) is a biconditional, of the form $P \iff Q$. So, in order to prove it, we will use Rule $\iff_{prove}$, and prove both $P \implies Q$ and $Q \implies P$.

Proof of "$(\forall x \in S)(P(x) \wedge Q(x)) \implies \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)$".

Assume

$$(\forall x \in S)(P(x) \wedge Q(x))\,. \tag{9.156}$$

We want to prove $(\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)$.

For this purpose, we will use Rule $\wedge_{prove}$, and prove the sentences $(\forall x \in S)P(x)$ and $(\forall x \in S)Q(x)$.

Proof of $(\forall x \in S)P(x)$:

Let u be an arbitrary member of S.

Then $P(u) \wedge Q(u)$. [Rule $\forall_{use}$, from (9.156)]

Therefore $P(u)$. [Rule $\wedge_{use}$, from $P(u) \wedge Q(u)$.

So we have proved $P(u)$ for an arbitary $u \in S$, and then $\boxed{(\forall x \in S)P(x)}$. [Rule $\forall_{prove}$]

Proof of $(\forall x \in S)Q(x)$:

Let u be an arbitrary member of S.

Then $P(u) \wedge Q(u)$. [Rule $\forall_{use}$, from (9.156)]

Therefore $Q(u)$. [Rule $\wedge_{use}$, from $P(u) \wedge Q(u)$.

So we have proved $Q(u)$ for an arbitary $u \in S$, and then $\boxed{(\forall x \in S)Q(x)}$. [Rule $\forall_{prove}$]

We have proved $(\forall x \in S)P(x)$ and $(\forall x \in S)Q(x)$. Therefore

$$(\forall x \in S)P(x) \wedge (\forall x \in S)P(x)\,, \tag{9.157}$$

by Rule $\wedge_{prove}$.

Since we have proved 9.157) assuming (9.156), we can go to

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)\,, \tag{9.158}$$

completing the proof of (9.158).

Proof of "$\Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \Longrightarrow (\forall x \in S)(P(x) \wedge Q(x))$"

Assume

$$(\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\,. \tag{9.159}$$

We want to prove $(\forall x \in S)(P(x) \wedge Q(x))$.

Let u be an arbitrary member of S.

It follows from (9.159) by Rule $\wedge_{use}$ that $(\forall x \in S)P(x)$.

And it also follows that $(\forall x \in S)Q(x)$.

Since $(\forall x \in S)P(x)$, and $u \in S$, it follows by Rule $\forall_{use}$ that $P(u)$.

Since $(\forall x \in S)Q(x)$, and $u \in S$, it follows by Rule $\forall_{use}$ that $Q(u)$.

Since we have proved $P(u)$ and $Q(u)$, it follows by Rule $\wedge_{prove}$ that $\boxed{P(u) \wedge Q(u)}$.

Since we have proved $P(u) \wedge Q(u)$ for arbitrary u in S, it follows by Rule $\forall_{prove}$ that

$$(\forall x \in S)(P(x) \wedge Q(x))\,. \tag{9.160}$$

Since we have proved (9.160) assuming (9.159), it follows from Rule $\Longrightarrow_{prove}$ that

$$\Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \Longrightarrow (\forall x \in S)(P(x) \wedge Q(x))\,. \tag{9.161}$$

completing the proof of (9.161).

Since we have proved (9.158) and (9.161), it follws by Rule $\Longleftrightarrow_{prove}$ that

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longleftrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)\,, \tag{9.162}$$

Q.E.D.

We now prove that (9.155) cannot be proved. We do this by exhibitng examples of a set S and predicates $P(x)$, $Q(x)$ for which (9.155) is false.

Let S be the set of all people. Let "$P(x)$" stand for "x likes tea" and "$Q(x)$" stand for "x likes coffee". Then the sentence "$(\forall x \in S)(P(x) \vee Q(x))$" says "everybody likes tea or coffee", and the sentence "$(\forall x \in S)P(x) \vee (\forall x \in S)Q(x)$" says

"everybody likes tea or everybody likes coffee". It is clear that both sentences say totally different things. The sentence "everybody likes tea or everybody likes coffee" is certainly false, because it is a disjunction "everybody likes tea $\vee$ everybody likes coffee", and both disjuncts ("everybody likes tea" and "everybody likes coffee") are false, so the disjunction is false.

10 A more detailed introduction to logic

10.1 First-order predicate calculus

The language most mathematicians use to talk about mathematical objects (numbers of various kinds, sets, functions, lists, points, lines, planes, curves of various kinds, spaces where we can do geometry, graphs, and millions of other things) is a ***first-order predicate calculus***.

So let us explain what this means.

- The language is a "predicate calculus" because we can use it to express predicates.

So let us review what "predicates" are.

10.1.1 Predicates

Remember that

> A ***predicate*** is a sentence[a] involving one or more (or zero) variables, in such a way that the sentence has a definite truth value[b] for each choice of values of the variables.
>
> [a] "Sentence" means the same as "statement", or "assertion".
>
> [b] The ***truth value*** of a sentence is "true" if the sentence is true and "false" if the sentence is false.

For example:

- "Alice likes Mark" is a zero-variables predicate. It is either true or false.

- "x likes Mark" is a one-variable predicate. It is true or false depending on who x is. For example, suppose that Alice likes Mark but Andrew does not like Mark. Then "x likes Mark" is true when x =Alice but "x likes Mark" is false when x =Andrew.

  If we call this predicate $P(x)$, then $P(Alice)$ is true and $P(Andrew)$ is false.

- "x likes y" is a two-variables predicate. It is true or false depending on who x and y are. For example, suppose that Alice likes Mark, Andrew does not like Mark, Andrew likes Alice, and Mark does not like Andrew. Then "x likes y" is true when x =Alice and y =Mark, and when x =Andrew and y =Alice, but "x likes y" is false when x =Andrew and y =Mark.

  If we call this predicate $P(x, y)$, then $P(Alice, Mark)$ is true but on the other hand $P(Mark, Andrew)$ is false.

- If S is the set of all people, then "$(\forall x \in S)x$ likes y" says "everybody likes y". This is a one-variable predicate. We could call this predicate $Q(y)$, and then

we could define $Q(y)$ as follows:

$$\text{if } y \in S \text{ then } Q(y) \text{ means } (\forall x \in S) P(x, y)\,, \tag{10.163}$$

or, in purely formal language:

$$(\forall y \in S)\Big(Q(y) \Longleftrightarrow (\forall x \in S) P(x, y)\Big) \tag{10.164}$$

- "x likes y more than x likes z" is a three-variables predicate.
- "$2 + 2 = 4$" and "$2 + 2 = 5$" are zero-variables predicates. They are either true or false. (And, of course, "$2 + 2 = 4$" is true and "$2 + 2 = 5$" is false.)
- "$x > 0$" and "$2|n$" are one-variable predicates. They are true or false depending on who x (or n) is. For example, "$x > 0$" is true $x = 3$ but is false for $x = -5$. And "$2|n$" is true for $n = 4$ but is false for $n = 5$.
- "$x > y$" and "$m|n$" are two-variables (i.e., binary) predicates. They are true or false depending on who x and y (or m and n) are. For example, "the sentence $x > y$" is true for $x = 5$ and $y = 4$, but is false for $x = 5$ and $y = 6$. And "$m|n$" is true for $m = 3$ and $y = 6$, but is not true for $m = 3$ and $y = 7$.

- "$x+y=z$", "$x+y>z$", and "$n|m+q^2$" are three-variables predicates. The predicate "$x+y=z$" is,true for $x=2$, $y=3$ and $z=5$, but is false for $x=2$, $y=3$ and $z=4$. The predicate "$x+y>z$" is true for $x=2$, $y=3$ and $z=4$. but is false for $x=2$, $y=3$ and $z=5$. The predicate "$n|m+q^2$" is true for $n=5$, $m=9$, and $q=6$, but is false $n=5$, $m=7$, and $q=6$.

- "$x+2y^2-z>u$" and "$a=bq+r$ and $0\leq r<|b|$" are four-variables predicates. The predicate "$x+2y^2-z>u$" is true for $x=2$, $y=4$. $z=3$, $u=4$, but is false for $x=2$, $y=1$. $z=3$, $u=3$, The predicate "$a=bq+r$ and $0\leq r<|b|$" is true for $a=23$, $b=5$, $q=4$ and $r=3$, but is false for $a=23$, $b=5$, $q=4$ and $r=2$.

10.2 Free and bound variables, quantifiers, and the number of variables of a predicate

As was explained in the previous section, in a predicate such as "$x>y$", the variables x, y are ***free variables***, that is, variables that are free to be given any value we want. We can plug in values for x and y, and for each choice of values the resulting sentence has a definite truth value, that is, is true or false.

You should think of a predicate as a ***processing device***, with several "input channels". The input channels are the ***open variables***. Each input channel is ***open***, in the sense that the entrance to the channel is open so you can can put things in, or ***free***, in the sense that we are free to put things in there. Once you have put in a value for, say, the variable x, then x is no longer open: it becomes ***closed***, or ***bound***.

Once you have put in values in all the input channels, the device processes these inputs, and produces a answer: true, or false.

If, on the other hand, the predicate "$x > y$" appears in a text after a statement such as

$$\text{Let } x = 5,\ y = 3.$$

then the variables x and y are no longer free: they are ***bound variables***[59], because they are "attached" to particular values.

We now look at another, very important way to turn free variables into bound variables.

Let us consider, for example, the predicates

$$(\forall y \in \mathbb{R})x + 2y^2 - z > u \tag{10.165}$$

[59]Bound variables are also called ***closed variables***, because they are not open: the "input channel" through which we can input values for the variables is closed.

and

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \text{ , and } 0 \leq r < |b|) \,. \tag{10.166}$$

You may think that these are four-variables predicates, because each one of them contains four variables. (Predicate (10.165) contains the variables x, y, z and u. Predicate (10.166) contains the variables a, b, a and r.)

But this is not right:

> ***(10.165) is a three-variables predicate***, and
> ***(10.166) is two-variables predicate.***.

Let me explain.

10.2.1 An example: a predicate with three free variables and one bound variable

We first look at the predicate

$$(\forall y \in \mathbb{R}) x + 2y^2 - z > u \,. \tag{10.167}$$

- The predicate (10.167) is built from the predicate "$x + 2y^2 - z > u$" by ***quantifying*** it, i.e., putting a universal quantifier $(\forall y \in \mathbb{R})$ in front.
- The unquantified predicate "$x + 2y^2 - z > u$" contains the variables x, y, z, u. These are four open variables.
- So, if you are asked the "truth question"

$$\text{Is} \quad \text{“}x + 2y^2 - z > u\text{”} \quad \text{true or false?}$$

then you have to reply with a question of your own:

$$\text{Who are } x, \, y, \, z \text{ and } u?$$

- But in the quantified predicate (10.167) ***the variable y is quantified***.
- So, if you are asked the “truth question”

$$\text{Is} \quad \text{“}(\forall y \in \mathbb{R})x + 2y^2 - z > u\text{”} \quad \text{true or false?}$$

then you have to reply with the question:

$$\text{Who are } x, \, z \text{ and } u?$$

- In the predicate “$x+2y^2-z > u$”, the four variables x, y, z and u are open variables, that is, “slots”, or “input channels”, where you can put in (or “plug in”) values for each of the variables.
- When you fill in the four slots by plugging in values for the variables, you get a ***proposition***, i.e., a sentence that has a definite truth value.

A ***proposition*** is a sentence with no open variables

So a proposition is just true or false, whereas a predicate with open variables is true or false depending on the values of the variables.

Example:

1. The sentence "$m \geq n$" has two open variables. It is true if, for example, $m = 3$ and $n = 1$, and it is false if, for example, $m = 3$ and $n = 4$.

2. The sentence "$(\forall m \in \mathbb{N})m \geq n$" is true if, for example, $n = 1$, and it is false if, for example, $n = 2$. So this sentence has one open variable, namely, n.

3. The sentences

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})m \geq n$$

and

$$(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})m \geq n$$

do not have any open variables. So they are propositions. The first one is true. (Reason: Take $n = 1$. Then for arbitrary $m \in \mathbb{N}$ $m \geq 1$.) The second one is false. (Reason: Take $m = 1$, $n = 2$. Then it is not true that $m \geq n$.)

- So, for example, if you plug in the values $x = 2$,

$y = 4$, $z = 3$, $u = 4$, into the sentence

$$x + 2y^2 - z > u$$

you get the proposition

$$19 > 4, ,$$

which is true.

- But in the quantified predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$", there is no y-slot. The three variables x, z and u are open variables, that is, slots or input channels where you can put in values. But y is not an open variable.
- When you fill in the slots by plugging in values for the three open variables, you get a proposition.
- So, for example, if you plug in the values $x = 2$, $z = -3$, $u = 4$, into the sentence

$$(\forall y \in \mathbb{R})x + 2y^2 - z > u$$

then you get the sentence

$$(\forall y \in \mathbb{R})2 + 2y^2 + 3 > 4$$

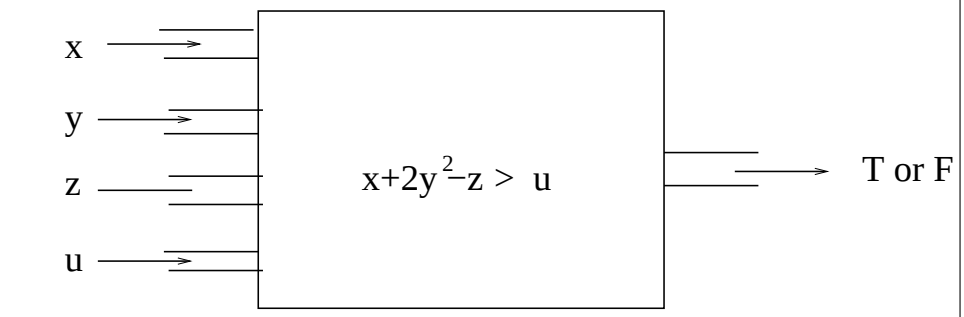
which is equivalent to the sentence

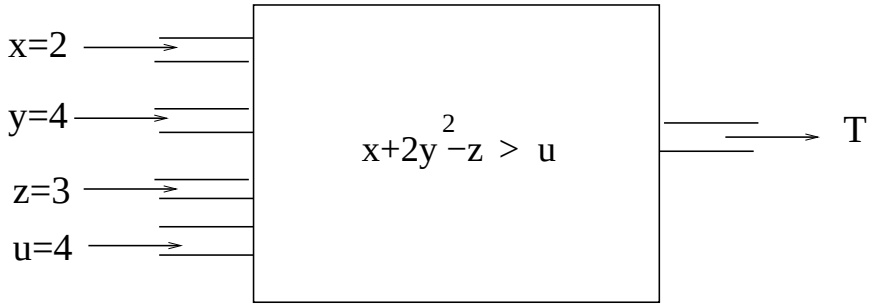
$$(\forall y \in \mathbb{R})2y^2 + 5 > 4\,.$$

And this sentence is true. (Proof: Let $y \in \mathbb{R}$ be arbitrary. Then $2y^2 \geq 0$. But $5 > 4$. So $2y^2 + 5 > 4$. Hence "$2y^2 + 5 > 0$" is true for arbitrary $y \in \mathbb{R}$. Therefore "$(\forall y \in \mathbb{R})2y^2 + 5 > 4$" is true.)

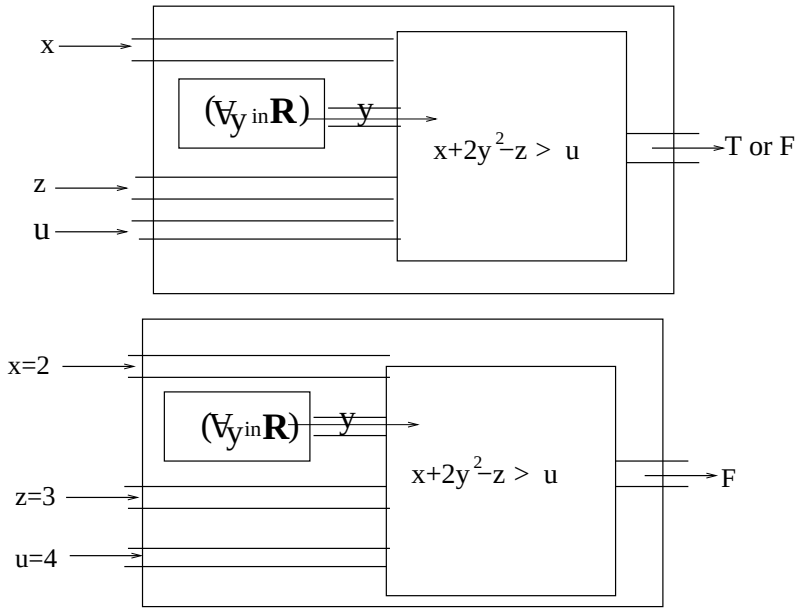
- The key point here is that ***the sentence "***$(\forall y \in \mathbb{R})x + 2y^2 - z > u$***" does not have a*** y***-slot where you can plug in a value of*** y***.*** That's because ***the sentence itself decides which value or values of*** y ***to plug in***. The quantifier $(\forall y \in \mathbb{R})$ says: "let y be an arbitrary real number". And then, with the values of x, z and u supplied by you, the truth value of the resulting sentence is determined. ***There is no need to ask "who is*** y***?"***

Another way to see this is as follows: when you universally quantify a sentence by putting in front of it the universal quantifier "$(\forall y \in \mathbb{R})$", this adds to the sentence a "generator of y-values", that is, a new component that tells the sentence what value of y to use. More precisely, the universal quantifier "$(\forall y \in \mathbb{R})$" says "Let y be an arbitrary real number". And this ***closes*** the y-input channel, so that it is no longer possible to plug a y-value into the sentence from outside.





The sentence $\boxed{x + 2y^2 - z > u}$ is a processing device that has four input channels: the x-channel, the y-channel, the z-channel, and the u-channel. When values for the four variables are inputted into the sentence, the sentence produces a truth value. The four variables x, y, z, u are ***open***, or ***free***. They are open, because the input channels are open so that values of the variables can be put into them. They are free, because the variables are not tied to any particular value.



The quantified sentence $(\forall y \in \mathbb{R})x + 2y^2 - z > u$ is a combination of two interconnected processing units: the original unquantified sentence "$x + 2y^2 - z > u$", and the quantifier "$(\forall y \in \mathbb{R})$". The quantifier generates a value for the quantified variable y (by saying "let y be an arbitrary real number") and, by doing so, it ***closes*** the y input channel, so that y is no longer free; we cannot choose a value for y and plug it in. The other three channels remain open. So in this sentence x, z and u are open variables. but y is ***closed***, or ***bound***.

The other three letter variables (x, z and u) remain open. So we can plug in values for them in order to obtain propositions that have a definite truth value.

Summarizing:

- Even though the predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" appears to contain four letter variables, only three of these variables (x, z and u) are open. The other variable, y, is ***bound***, or ***closed.***

- This means that the predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is a ***three variables***, or ***three arguments***, predicate. Therefore:
  - For each choice of values for x, z and u, the predicate becomes a proposition, i.e. a sentence with a definite truth value.
  - If we want to give a name to this predicate, then we can of course call it P, but if we want to indicate the names of the free variables, we should call it $P(x, z, u)$.
  - But ***we must not call it*** $P(x, y, z, u)$, because if we give it such a name we would erroneously be suggesting that this predicate has a "y-channel" where we can input values for the variable y.
- For example, "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is true for $x = 4$, $z = 2$, $u = 1$. (Proof: We want to prove that $(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$, that is, that $(\forall y \in \mathbb{R})2 + 2y^2 > 1$. Let $y \in \mathbb{R}$ be arbitrary. Then $y^2 \geq 0$, so $2y^2 \geq 0$, so $2 + 2y^2 \geq 2$, and $2 > 1$, so $2 + 2y^2 > 1$. Since "$2 + 2y^2 > 1$" has been proved to be true for arbitrary real y, it follows that $(\forall y \in \mathbb{R})2 + 2y^2 > 1$. Q.E.D.)

- The predicate "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is false for $x = 4$, $z = 2$, $u = 8$. (Proof: We want to prove that "$(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$" is not true, i.e., that "$(\forall y \in \mathbb{R})2 + 2y^2 > 8$" is not true. Take $y = 0$. Then "$2 + 2y^2 > 8$" is not true, because "$2 + 0 > 8$" is not true. So "$(\forall y \in \mathbb{R})4 + 2y^2 - 2 > 1$" is not true.Q.E.D.)

- The "truth question", i.e., the extra question we need to ask is order to be able to tell if "$(\forall y \in \mathbb{R})x + 2y^2 - z > u$" is true or false, is the question: ***"who are*** x***,*** z ***and*** u***?"***

- ***in order to have enough information to determine if the sentence "***$(\forall y \in \mathbb{R})x + 2y^2 - z > u$***" is true or false, we do not have to ask "who is*** y***?", because once you are given the values of*** x***,*** z ***and*** u***, the quantified sentence itself determines if it is true or false, because it is up to the sentence to decide if it's true for all*** y ***or not, and it's not up to you to choose a value for*** y***.***

10.2.2 A second example: a predicate with two free variables and two bound variables

We now look at the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,. \quad (10.168)$$

As I said before, on page 226, ***(10.166) is a two-variables predicate.***.

- Predicate (10.168) contains the variables a, b, q and r. But q ***and*** r ***are quantified***. So, if you are asked the "truth question"

  Is "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$" true or false?

  then you have to reply with a question of your own:

  Who are a and b?

  The variables a and b in (10.168) are "slots", or "input channels", where you can put in (or "plug in") a value for each of the variables, and then you get a proposition.

- So, for example, if you plug in the values $a = 23$, $b = 11$, into the sentence

  $$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

then you get the sentence

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)\,.$$

And this sentence is true. (Proof: To prove an existential statement we use rule $\exists_{use}$: we exhibit values of q and r for which the proposition "$23 = 11q + r \wedge 0 \leq r < 11$" is true. Take $q = 2$, $r = 1$. Then $23 = 11q + r$ and $0 \leq r < 11$. Hence "$23 = 11q + r \wedge 0 \leq r < 11$" is true for some $q, r \in \mathbb{Z}$. Therefore "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11$" is true.)

- The key point here is that ***the sentence***

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)$$

does not have a q-slot or an r-slot where you can plug in values for q and r. That's because ***the sentence itself decides which value or values of q and r to plug in***. The sentence itself[60] decides which values of q and r it has to look

[60]Remember: you must think of a sentence as a processing device. The unquantified sentence "$a = bq + r \wedge 0 \leq r < |b|$" does the following: once it has been fed values for a, b, q and r, it finds out if "$a = bq + r \wedge 0 \leq r < |b|$" is true or not; if it is true is says "yes"; if it is false it says "no". The quantified sentence "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(23 = 11q + r \wedge 0 \leq r < 11)$" does a much more complicated job: once it has been fed values for a and b, the sentence looks at all possible values of q and r, and sees whether it can find one choice of values of q and r for which "$23 = 11q + r \wedge 0 \leq r < 11$" is true; and then, if it find such values, it says "yes"; and if it cannot find any values of q and r for which "$23 = 11q + r \wedge 0 \leq r < 11$" is true, it says "no".

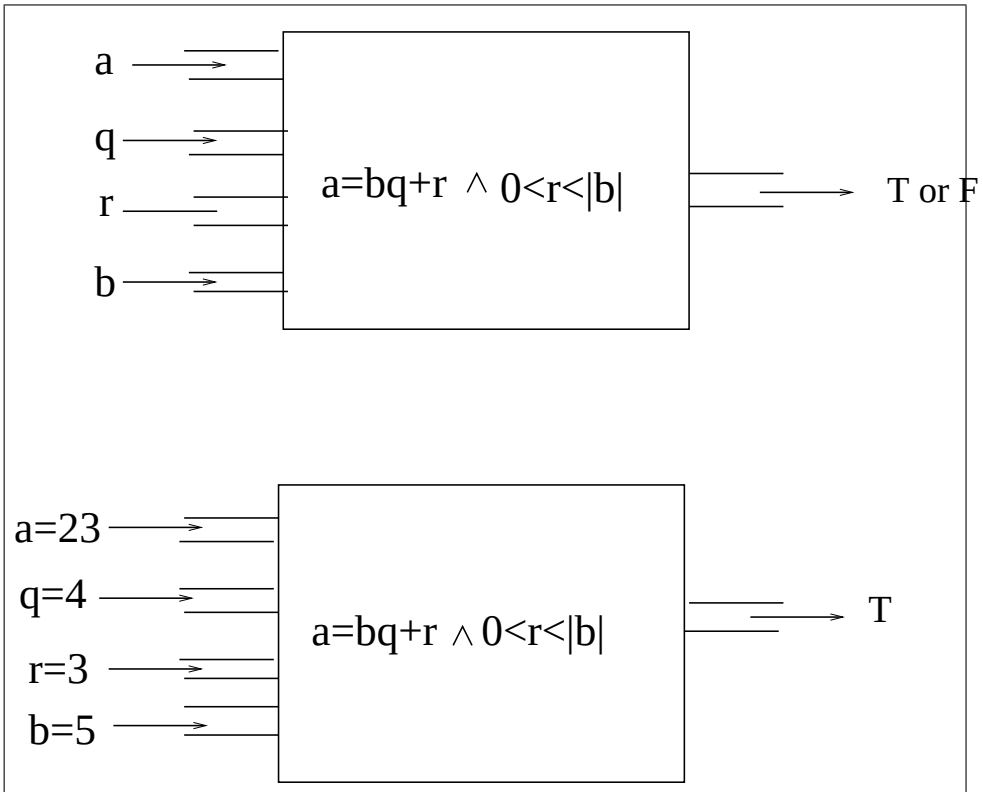
at, and then, with the values of a and b supplied by you, the truth value of the resulting sentence is determined.

- Another way to see this is as follows: the sentence "$a = bq + r \wedge 0 \leq r < |b|$" has four input channels that are open, or free, so you can put into each channel a value of the corresponding variable.

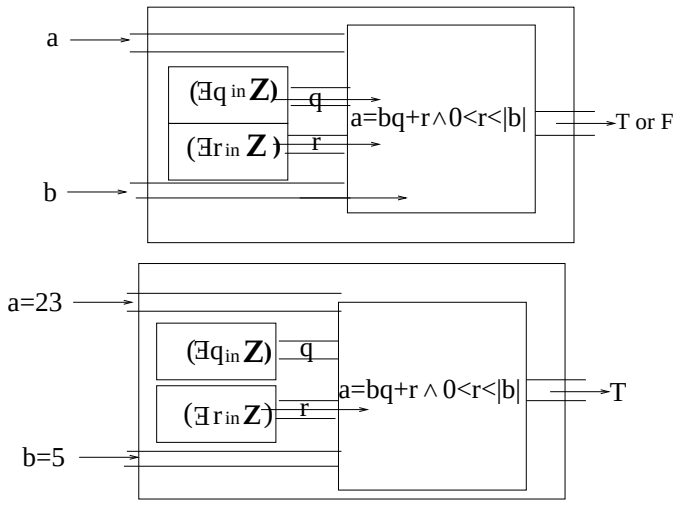
  But when you existentially quantify the sentence twice by putting in front of it the two existential quantifiera "$(\exists q \in \mathbb{Z})$" and "$(\exists r \in \mathbb{Z})$", this adds to the sentence a "generator of q-values" and a "generator of r-values", that is, two new components that tell the sentence what values of q and r to look at. More precisely, the existential quantifiers "$(\exists q \in \mathbb{R})$" and "$(\exists r \in \mathbb{R})$" do the following:

  - They look for a q-value and an r-value that make the sentence "$a = bq + r \wedge 0 \leq r < |b|$" true.
  - If they find such values, then they send to the sentence the message "yes, we have found values that make you true", and then the sentence produces the final verdict "yes, true".
  - If they do not find such values, then they send to the sentence the message "no, we have not

found values that make you true", and then the sentence produces the final verdict "no, not true".



The sentence $\boxed{a = bq + r \wedge 0 \leq r < |b|}$ is a processing device that has four input channels:the a-channel, the q-channel, the r-channel, and the b-channel. When values for the four variables are inputted into the sentence, the sentence produces a truth value. The four variables a, q, r, b are ***open***, or ***free***. They are open, because the input channels are open so that values of the variables can be put into them. They are free, because the variables are not tied to any particular value.



The quantified sentence $\boxed{(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)}$ is a combination of three interconnected processing units: the original unquantified sentence "$a = bq + r \wedge 0 \leq r < |b|)$", and the two quantifiers "$(\exists q \in \mathbb{Z}$", "$(\exists r \in \mathbb{Z}$". The quantifiers generate values for the quantified variablea q, r. (They look for values of q, r that will make "$a = bq + r \wedge 0 \leq r < |b|)$" true. If they find them, then they send one pair of such values to the main processing unit "$a = bq + r \wedge 0 \leq r < |b|)$", which then says "yes, true". If they do not find them, then they send some values to the main processing unit, but these values will not work, so the main processing unit wil say "no, not true".) By doing so, the quantifiers ***close*** the q and r input channels, so that q and f are no longer free; we cannot choose values for q and r and plug them in. The other two channels remain open. So in this sentence a and b are open variables. but q and r are ***closed***, or ***bound***.

The other two letter variables (a and b) remain open. So we can plug in values for them in order to obtain propositions that have a definite truth value.

Summarizing:

- Even though the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

appears to contain four letter variables, only two of these variables (a and b) are open. The other variables, q and r, are ***bound***, or ***closed.***

- This means that the predicate

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$$

is a ***two variables***, or ***two arguments***, predicate. Therefore:

  - For each choice of values for a and b, the predicate becomes a proposition, i.e. a sentence with a definite truth value. (And the Division Theorem tells us that the truth value is "true" for all choices of integers a and b such that $b \neq 0$, that is, that the proposition[61]

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(b \neq 0 \Longrightarrow (\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\Big) \tag{10.169}$$

is true.

[61] Notice that (10.169) is a proposition, i.e., a predicate with no open variables at all (or, if you prefer, with zero open variables), because in (10.169) all four variables that occur are quantified, so a, b, q and r are closed variables. For the sentence (10.169), if you are asked "is this true", you do not need to ask any "truth question", because you do not need values of any variables to determine if the sentence is true.

  - Suppose we want to give a name to the two-variables predicate

    $$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,.$$

    We can, of course, call it P. But if we want to indicate the names of the free variables, we should call it $P(a, b)$.
  - But ***we must not call it*** $P(a, b, q, r)$, because if we give it such a name we would erroneously be suggesting that this predicate has a "q-channel" and an "r-channel", where we can input values for the variables q, r.

- The "truth question", i.e., the extra question we need to ask is order to be able to tell if "$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$" is true or false, is the question: ***"who are*** a ***and*** b***?"***

- ***in order to have enough information to determine if the sentence "***$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)$***" is true or false, we do not have to ask "who are*** q ***and*** r***?", because once you are given the values of*** a ***and*** b***, the quantified sentence itself determines if it is true or false, because it is up to the sentence to decide if the required values of*** q ***and*** r ***exists or not, and***

it's not up to you to choose valuea for q ***and*** r***.***

10.2.3 Another example, illustrating the fact that only open variables really matter

Some natural numbers are products of two prime numbers; for example, $4 = 2 \times 2$, $6 = 2 \times 3$, $35 = 5 \times 7$, and so on, Other natural numbers are not products of two prime numbers; for example, $18 = 2 \times 3 \times 3$, and the Fundamental Theorem of Arithmetic tells us that that there is no other way to write 18 as a product of primes, so in particular 18 is not the product of two primes.

So we can consider the predicate "n is a product of two prime numbers". And we can call this predicate $A(n)$. (We could just have called is "A", but we choose the name "$A(n)$" to emphasize the fact that this predicate has the open variable n.) Then, according to the conventions we made before about naming predicates, $A(6)$ is the proposition "6 is the product of two primes", and $A(7)$ is the proposition "7 is the product of two primes", so $A(6)$ is true, and $A(7)$ is false.

You can think of the predicate $A(n)$ as a "black box": you input a value of n, the predicate does some work, and produces an answer: "true" or "false". (For example, for $n = 6$ $A(n)$ is true, and for $n = 7$ $A(n)$ is false.)

But we can also look inside the box, and analyze in more detail how this predicate works. That is, we can observe that $A(n)$ says that

There exist prime numbers p, q such that $n = pq$.

So now our predicate has three variables, p, q, and n!

How come? Has the number of variables of $A(n)$ suddenly changed? Has $A(n)$ become a three-variables predicate? You may think so, because now $A(n)$ seems to have three variables: p, q and n.

But the answer is: ***No!*** $A(n)$ ***is still a one-variable predicate!*** The variables p and q are ***bound***, because they are quantified. Precisely, $A(n)$ says, in semiformal (almost formal) language:

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p \text{ is prime} \wedge q \text{ is prime} \wedge n = pq)\,. \tag{10.170}$$

So, even though $A(n)$ appears to have three variables, namely, p, q and n, two of them are ***internal variables***[62], within the sentence (10.170). The sentence itself generates the values of p and q that it needs in order to answer its true-false question, and when the sentence ends p and q are free variables again. And, in particular,

[62] If you think of the sentence "$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p \text{ is prime})$" as a processing unit, you will see that it has two existential quantifiers that generate values of p and q. But outside the processing unit all one sees is that certain values of n are fed in and certain 'true"s and "false"s come out. The variables p and q are part of the internal operation of the device.

outside the sentence

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})(p \text{ is prime} \wedge q \text{ is prime} \wedge n = pq)$$

the variables p ***and*** q ***have no value.***

Another way to see that p and q have no value, is to observe that $A(n)$ can equally well be written as

$$(\exists x \in \mathbb{N})(\exists y \in \mathbb{N})(x \text{ is prime} \wedge y \text{ is prime} \wedge n = xy)\,, \tag{10.171}$$

or as

$$(\exists u \in \mathbb{N})(\exists v \in \mathbb{N})(u \text{ is prime} \wedge v \text{ is prime} \wedge n = uv)\,. \tag{10.172}$$

Sentences (10.170), (10.171), and (10.172) say exactly the same thing. The only difference is in the names of the variables that, inside the box, the sentence uses to process the inputs and produce an output.

From outside the box, we do not see these variables. ***That's why the letters*** p, q ***in (10.170), as well as the letters*** x, y ***in (10.171), and the letters*** u, v ***in (10.172), are internal variables, that have no value outside the sentence.***

And this is not the end of the story. "p is prime" is itself a complex predicate. In fact, "p is prine" stands for

$$p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\,. \tag{10.173}$$

This means that $A(n)$ can also be written as

$$(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})\Bigg(\Bigg(p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\Bigg) \wedge \Bigg(q > 1 \wedge (\forall k \in \mathbb{N})\Big(k|q \Longrightarrow (k = 1 \vee k = q)\Big)\Bigg) \wedge n = pq\Bigg) \quad (10.174)$$

Now one may think that $A(n)$ is a four-variables predicate, because it involves the variables n, p, q and k. But by now you know better: the new variable k is also bound, so the only open variable in (10.174)) is still n. That means that ***even if you write it in the form (10.174),*** $A(n)$ ***is still a one-variable predicate.***

Actually, the story doesn't end here either. "$k|p$" is also a complex preddcate with an internal structure of its own: is stands for "$(\exists j \in \mathbb{Z})p = kj$". So, if we substitute this for "$k|p$" in (10.174), we get an even more detalied

version of $A(n)$, namely,

$$\begin{aligned}&(\exists p \in \mathbb{N})(\exists q \in \mathbb{N})\\ &\quad\Bigg(\Bigg(p > 1 \wedge (\forall k \in \mathbb{N})\Big((\exists j \in \mathbb{Z})p = kj \Longrightarrow (k = 1 \vee k = p)\Big)\Bigg)\\ &\quad\wedge\Bigg(q > 1 \wedge (\forall k \in \mathbb{N})\Big((\exists j \in \mathbb{Z})q = kj \Longrightarrow (k = 1 \vee k = q)\Big)\Bigg)\\ &\quad\wedge n = pq\Bigg). \end{aligned} \tag{10.175}$$

Now $A(n)$ apears to involve five variables: n, p, q, k and j. But this time you will have no problem figuring out that $A(n)$ ***is still a one-variable predicate, because the only open variable in (10.175) is still*** n***, and all the other variables are bound***.

Problem 48. Draw a diagram of the sentence (10.175) as a processing unit, similar to the diagrams that appear on pages 232 and 239.

Make sure that your diagram shows that there is only only one input channel. □

10.2.4 Dummy variables

So far, we have seen that variables that appear in a sentence but are quantified are "internal variables", or

"closed variables", or "bound variables". If you think of a sentence as a "processing unit", or "processing device", that takes in certain inputs and produces "true-false" outputs, then the closed (or bound, or internal) variables are variables that the sentence itself generates and uses to do its processing work. So the sentence does not need to be fed the values of these variables, and does not produce values of those variables that an outside obsevrer can see.

There is another way in which a variable appearing in a sentence can be a closed (or bound, or internal) variable. The sentence may contain a part that generates values of some variable in order to do a computation.

Consider. for example, the sentence

$$\sum_{k=1}^{n}(a+r^k)=b\,, \tag{10.176}$$

This sentence contains five letter variables, namely, $a, r, b, k,$ and n.

Which ones of these five variables are open?

The best way to answer this question is by thinking of (10.176) as a processing device, opening it up to look into its internal structure, and figuring out what the device does.

Suppose you ask the device the truth question:

$$\text{Is it true that } \textstyle\sum_{k=1}^{n}(a+r^k)=b?$$

Then the device will not know what to do, because in order to get started the device needs to be given the values of a, b, r, and n. (Maybe we should think of (10.176) as an inteligent device, that can ask questions. Then if you ask the truth question, the device will answer with a question: ***who are*** a***,*** b***,*** r ***and*** n***?***)

Suppose you do feed the device by inputting values for a, b,r and n. Then the device will do the following:

1. First, the CPU (central procssing unit) will report to the summation component Σ—that is, the component that computes the summation $\sum_{k=1}^{n}(a+r^k)$—the values of a, b, r and n that it has received from you.

2. Then Σ will perform the following calculation:

   (a) First, it will write the list of all values of k, from 1 to n. (This is something it can do, because it knows who n is, since it has received this information from the CPU.)

   (b) Then it will compute $a+r^k$ for each of the values of k in the list. (Again, Σ knows how to do this, because it knows who a and r are.)

   (c) Then it will take all those values of $a+r^k$ that it has computed, and add them.

(d) Finally, it will report the result to the CPU. (Maybe, in order to facilitate communication between Σ and the CPU, they will introduce letter variables. For example, they may decide to call the result of the summation s, and then Σ will report the value of s to the CPU. But we need not concern ourselves with the variable s, because that's an internal variable used within the device for the various parts to communicate with each other.)

3. The CPU will then compare the result reported by the summation unit with b, and determine if they are equal.

4. If they are equal, the CPU will report to you the answer "true".

5. If they are not equal, the CPU will report to you the answer "false".

The main point of this is that k ***is an internal variable used by the sentence to perform its calculation. The values of*** k ***are generated by the sentence itself. So the sentence need not be given the value of*** k. And that's why

1. If asked the truth question, the sentence will ask "who are a, b, r and n"".

2. The sentence will not ask "who is k?", because ***the sentence itself generates the values of*** k ***it needs***.

3. k ***is not an open variable in (10.176)***

4. The open variables of (10.176) are a, b, r and n.

Let's just look at one more example. Let us analyze the following four sentences

$$(\forall n \in \mathbb{N})\Big((\exists m \in \mathbb{N}) \sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N}) n = p^2\Big), \tag{10.177}$$

$$(\forall n \in \mathbb{N})\Big((\exists m \in \mathbb{N}) \sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N}) n = p^3\Big), \tag{10.178}$$

$$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})\Big(\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N}) n = p^2\Big) \tag{10.179}$$

and

$$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})\Big(\sum_{k=1}^{m} k^3 = n \Longrightarrow (\exists p \in \mathbb{N}) n = p^3\Big) \tag{10.180}$$

Each of these sentences contains four variables, namely, n, m, k, and p.

And I am sure that this time you can see right away what is going on: ***all four variables are closed***. Three of them (n, m, and p) are quantified. and the variable k is also closed because the sentence itself generates the values of k that it needs to perfom its calculations.

So ***the sentences (10.177), (10.178), (10.179), and (10.180), are propositions***.

And then of course each of the sentences is true or false. Which leads me to a natural question, that I will ask you to answer.

Problem 49. Which of the propositions (10.177), (10.178), (10.179), (10.180), are true, and which ones are false?

NOTE: All these propositions are of the form $(\forall n \in \mathbb{N})P(n)$, where $P(n)$ is a one-variable predicate having n as the open variable.

If you want to prove that a sentence of this form is true, then you need a reasoned argument, starting with "Let n be an arbitrary natural number." (You may also try a proof by induction, but in this case I would not recommend that.) If you want to prove that it is false, then you need a counterexample, i.e., an example of an n for which the one-variable sentence $P(n)$ is false.

HINT: The answer to this problem is actually very easy. All you have to do is use the result of one of your ear-

lier homework problems. (I can narrow this down a bit further: *it's one of the problems in the third set of lecture notes.*) Using this, plus a little bit of logic (for example, truth values of implications), each of the four propositions should just require a couple of lines on your part.) □

A variable such as the k in $\sum_{k=1}^{n} t(k)$ (where $t(k)$ is some expression containing k, such as k, or k^2, or r^k, or $a + r^k$), is called a "dummy variable".

Let us define this term precisely. (The definition I am about to give is taken from Wolfram MathWorld.)

Definition 14 A dummy variable is ***a variable that appears in a calculation only as a placeholder and which disappears completely in the final result.*** □

And ***every dummy variable is bounded***.

Example 44 Naturally, summations are not the only type of expressions where some of the variables are bound variables

Examples of dummy variables are:

1. the k in a summation such as $\sum_{k=1}^{n} t(k)$,
2. the k in a product such as $\prod_{k=1}^{n} t(k)$,

3. the k in the name of a list, such as $(p_k)_{k=1}^n$,
4. the x in the name $\{x : P(x)\}$ of a set,
5. the x in an integral such as $\int_a^b f(x)dx$.
6. the x in a limit such as $\lim_{x\to a} f(x)$. □

Example 45. Let us look at the sentence

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{u \in \mathbb{R} : a \le u \le b\} \neq \emptyset \wedge \int_a^b x^2 dx = c\Big). \tag{10.181}$$

This sentence contains the letter variables a, b, u, x, and c.

Of these five letters, four are bound variables:

1. the variables a and b are bound because they are quantified;
2. the variable u is bound because it is a dummy variable, used as part of the name $\{u \in \mathbb{R} : a \le u \le b\}$ of a set;
3. the variable x is bound because it is a dummy variable, used as a variable of integration.

It follows from this analysis that

1. ***Sentence (10.181) defines a one-variable predicate.***

2. ***The open variable in sentence (10.181) is*** c.

3. If you think of sentence (10.181) as a processing device, then this device will take values of c as inputs, and produce a true-false answer as output.

4. If you ask the "truth question" ***is (10.181) true?***, then the device (10.181) cannot answer because it does not know who c is. So the device will answer your question with another question: ***who is*** c***?***

5. But, in order to be able to answer the truth question, the device does not need to ask "who is a?", or "who is b?" or "who is u?", or "who is x?". The device itself will generate the values of a, b, u and x it needs, and these values will be part of the calculations that (10.181) performs, and will not be seen by the outside world.

10.2.5 How to tell if a variable is dummy

Here are two ways to see that a variable is dummy.

1. The variable is dummy if "it isn't really there", in the sense that we can eliminate it completely. For example,

(a) The set $\{u \in \mathbb{R} : a \leq u \leq< b\}$ is an object very well known to all of us: it is none other than the closed interval $[a, b]$. So we can say the same thing as (10.181) by writing "$[a, b]$" instead of "$\{u \in \mathbb{R} : a \leq u \leq< b\}$". And we get

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge \int_a^b x^2 dx = c\Big), \tag{10.182}$$

which says exactly the same thing as (10.181). but now there is no "u" anymore.

(b) The definite integral $\int_a^b x^2 dx$ is a number that is completely determined by a and b. We do not need to ask "who is x?" in order to determine this number. Actually, the integral can be computed, and the result is $\frac{1}{3}(b^3 - a^3)$. So we can say the same thing as (10.182) by writing "$\frac{1}{3}(b^3 - a^3)$" instead of "$\int_a^b x^2 dx$", and we get

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge \frac{1}{3}(b^3 - a^3) = c\Big), \tag{10.183}$$

or, more nicely,

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big), \tag{10.184}$$

which say exactly the same thing as (10.182). but

now there is no "x" anymore.

2. A variable is dummy if it can be replaced by any other variable (except with variables that are already being used for something else) without changing the meaning of the sentence. For example,

   (a) If instead of the expression "$\{u \in \mathbb{R} : a \leq u \leq b\}$" we use a different letter and write something like "$\{v \in \mathbb{R} : a \leq v \leq b\}$", or "$\{z \in \mathbb{R} : a \leq z \leq b\}$", or maybe "$\{\alpha \in \mathbb{R} : a \leq \alpha \leq b\}$", or "$\{\diamond \in \mathbb{R} : a \leq \diamond \leq b\}$", nothing changes. So, for example, we can rewrite (10.181) as

   $$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{q \in \mathbb{R} : a \leq q \leq b\} \neq \emptyset \wedge \int_a^b x^2 dx = c\Big), \tag{10.185}$$

   which says exactly the same thing as (10.181). but now there is no u anymore.

   (b) If we replace the definite integral $\int_a^b x^2 dx$ by the expression $\int_a^b h^2 dh$, or $\int_a^b \sigma^2 d\sigma$, or $\int_a^b m^2 dm$, nothing changes. So, for example, we can rewrite (10.185) as

   $$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big(\{q \in \mathbb{R} : a \leq q \leq b\} \neq \emptyset \wedge \int_a^b k^2 dk = c\Big), \tag{10.186}$$

which says exactly the same thing as (10.181). but now there is no u and no x anymore.

Summarizing: Sentence (10.181) defines a ***one-variable predicate, with the open variable*** c. So we can call this predicate $P(c)$.

And then we may ask: can we tell what this predicate $P(c)$ is? Can we find a simpler expression for $P(c)$?

It turns out that, in this case, the answer is "yes, we can":

$\boxed{P(c) \textbf{ \textit{just says } ``}c \geq 0\textbf{''}}$.

Proof. We want to prove that $(\forall c \in \mathbb{R})(P(c) \iff c \geq 0)$.

Let $c \in \mathbb{R}$ be arbitrary.

We want to prove that $P(c) \iff c \geq 0$.

For that purpose, we will prove the implications $P(c) \implies c \geq 0$ and $c \geq 0 \implies P(c)$.

Proof that $P(c) \implies c \geq 0$.

Assume $P(c)$.

This means that

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big) .$$

Pick real numbers a, b such that $a, b] \neq \emptyset$ and $b^3 - a^3 = 3c$.

Since $a, b] \neq \emptyset$, it follows that $a \leq b$. (Reason: if $a > b$ then the set $[a, b]$, i.e., the set $\{u \in \mathbb{R} : a \leq u \leq b\}$, would be empty.)

Since $a \leq b$, we have $a^3 \leq b^3$.

So $b^3 - a^3 \geq 9$.

So $3c \geq 0$.

Hence $\boxed{c \geq 0}$.

Proof that $c \geq 0 \Longrightarrow P(c)$.

Assume that $c \geq 0$.

Let $a = 0$, $b = \sqrt[3]{3c}$.

Then $b \geq 0$.

So the closed interval $[a, b]$ (i.e., the interval $[0, b]$) is nonemtpy.

And $b^3 - a^3 = 3c$.

Hence $[a, b] \neq \emptyset \wedge b^3 - a^3 = 3c$.

So

$$(\exists a \in \mathbb{R})(\exists b \in \mathbb{R})\Big([a, b] \neq \emptyset \wedge b^3 - a^3 = 3c\Big) .$$

That is, $\boxed{P(c) \text{ holds.}}$

Since we gave proved that $P(c) \Longrightarrow c \geq 0$ and that $c \geq 0 \Longrightarrow P(c)$, we can conclude that $P(c) \Longleftrightarrow c \geq 0$.

Since we have proved that $P(c) \iff c \geq 0$ for arbitrary real c, we have proved that $(\forall c \in \mathbb{R})\Big(P(c) \iff c \geq 0)$. **Q.E.D.**

10.3 First-order predicate calculus

The language we use in mathematics is a ***predicate calculus*** because it enables us to predicates. And it is ***first-order*** because we can quantify variables, and write things such as "$(\forall x \in P)x$ likes Mark" (meaning, if P is the set of all people, "everybody likes Mark"), but we cannot quantify over predicates. That is,

- We cannot say things such as ""for every predicate $P(x)$ and every predicate $Q(x)$ if $(\forall x)P(x)$ is true and $(\forall x)Q(x))$ is true, then if $(\forall x)(P(x) \wedge Q(x))$ is true."
- We can say this for a particular pair of predicates $P(x)$, $Q(x)$ (for example, we can say "if everybody likes coffee and everybody likes milk then everybdoy likes coffee and milk", or we can say "if everybody studies and everybody reads books then everybdoy studies and reads books"), but we cannot say the same thing for arbitrary predicates $P(x)$, $Q(x)$.

It turns out that there are "second order" languages,

in which you can say things like "'for every predicate $P(x)$ and every predicate $Q(x)$ if $(\forall x)P(x)$ is true and $(\forall x)Q(x))$ is true, then if $(\forall x)(P(x) \wedge Q(x))$ is true." But the language we are using here is a ***first-order language***, in which those things cannot be said.

10.4 Logical connectives

In firts-order predicate calculus, one or more sentences can be combined to form other sentences. The symbols used to combine sentences are called the ***logical connectives.*** And there are exactly seven of them

10.4.1 The seven logical connectives

And here they are, in all their glory:

The seven logical connectives

1. The ***negation symbol*** $\sim$

   (meaning "no", "it's not the case that").

2. The ***conjunction symbol***, $\wedge$
   (meaning "and").

3. The ***disjunction symbol***, $\vee$
   (meaning "or").

4. The ***implication symbol***, $\Longrightarrow$
   (meaning "implies", or "if ... then").

5. The ***biconditional symbol***, $\Longleftrightarrow$
   (meaning "if and only if").

6. The ***existential quantifier symbol***, $\exists$
   (meaning "there exists ... such that", or "it is possible to pick ... such that").

7. The ***universal quantifier symbol***, $\forall$
   (meaning "for all",or "for avery", or "for an arbitrary").

10.4.2 How the seven logical connectives are used to form sentences

These seven symbols are used to form new sentences as follows:

1. The negation symbol $\sim$ is a ***one-argument connective***: it can be put in front of a sentence A to form the sentence $\sim A$ (meaning "no A", or "it's not the case that A"). For example: "$\sim 3|5$" means "3 does not divide 5".

2. The conjunction symbol $\wedge$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sentence $A \wedge B$, (meaning "A and B"). For example: "$(\sim 3|5) \wedge 3|6$" means "3 does not divide 5 and 3 divides 6".

3. The disjunction symbol $\wedge$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sentence $A \vee B$, (meaning "A or B"). For example: "$x > 0 \vee x < 0$" means "$x > 0$ or $x < 0$".

4. The implication symbol $\Longrightarrow$ is a ***binary connective***, or ***two-argument connective***: it can be put between two sentences A, B to form the sen-

tence $A \implies B$, (meaning "A implies B", or "if A then B"). For example: "$x \neq 0 \implies x^2 > 0$" means "if $x > 0$ then $x^2 > 0$".

5. The biconditional symbol $\iff$ is a ***two-argument connective***, that is ***binary connective***: it can be put between two sentences A, B to form the sentence $A \iff B$, (meaning "A if and only if B"). For example: "$(2|n \wedge 3|n) \iff 6|n$" means "2 divides n and 3 divides n if and only if 6 divides n".

6. The existential quantifier symbol $\exists$ has a more complicated grammar:

   (a) Using $\exists$ we can form ***existential quantifiers***.

   (b) There are two kinds of existential quantifiers:

      i. ***Unrestricted existential quantifiers*** are expressions
      $$(\exists x),$$
      that is: left parenthesis, $\exists$, variable, right parenthesis.

      ii. ***Restricted existential quantifiers*** are expressions
      $$(\exists x \in S),$$
      that is: left parenthesis, $\exists$, variable, $\in$, name of a set, right parenthesis.

(c) Then we can take a sentence A (or $A(x)$) and put a restricted or unrestricted existential quantifier in front, forming the sentences $(\exists x)A$ ("there exists x such that A", or "it is possible to pick x such that A") and $(\exists x \in S)A$ ("there exists x belonging to S such that A", or "it is possible to pick x belonging to S such that A").

7. The universal quantifier symbol $\forall$ has a grammar similar to that of the existential quantifier symbol:

   (a) Using $\forall$ we can form ***universal quantifiers***.

   (b) There are two kinds of universal quantifiers:

      i. ***Unrestricted universal quantifiers*** are expressions
      $$(\forall x),$$
      that is: left parenthesis, $\forall$, variable, right parenthesis.

      ii. ***Restricted universal quantifiers*** are expressions
      $$(\forall x \in S),$$
      that is: left parenthesis, $\forall$, variable, $\in$, name of a set, right parenthesis.

   (c) Then we can take a sentence A (or $A(x)$) and put a restricted or unrestricted universal quantifier in

front, forming the sentences $(\forall x)A$ ("for all x, A", or "A i strue for arbitrary x") and $(\forall x \in S)A$ ("for all x belonging to S, A", or "A is true for arbitrary x in S").

10.5 Conjunctions ("$\wedge$", i.e., "and")

The symbol

$$\wedge$$

is the ***conjunction symbol***, and means "and".

Hence,

- If P is the sentence

  Today is Friday

  and Q is the sentence

  Tomorrow is Saturday

  then "$P \wedge Q$" stands for the sentence

  Today is Friday and tomorrow is Saturday.

- A sentence of the form $P \wedge Q$ is a ***conjunction***.
- In a conjunction $P \wedge Q$, the sentences P, Q are the ***conjuncts***.

10.5.1 Proving a conjunction: a stupid but important rule

The rule for proving a conjunction (Rule $\wedge_{prove}$)

If P, Q are sentences, and you have proved P and you have proved Q, then you are allowed to go to $P \wedge Q$.

IMPORTANT REMARK. You may wonder "what is the point of such a rule?" But you cannot dispute that it is a reasonable rule! Of course, if you know that "today is Friday" and you also know that "tomorrow is Saturday", then you will have no doubt that "today is Friday and tomorrow is Saturday" is true. So you should have no problem accepting (and remembering) this rule. You may not understand why it is needed. So let me tell you why. Suppose it was a computer doing proofs, rather than a human being like you. Suppose the computer is told that today is Friday and then it is told that tomorrow is Saturday. How will the computer know that it can write "today is Friday and tomorrow is Saturday". It won't, unless you tell it. Computers do not "know" anything on their own. If you want the computer to "know" that once it knows that "today is Friday" and also that "tomorrow is Saturday", then it can write "today is Friday and tomorrow is Saturday", then you have to **tell** the computer. In other words, you have to input Rule $\wedge_{prove}$

into the computer. Proofs are mechanical manipulations of strings of symbols, and should therefore be doable by a computer. So Rule $\wedge_{prove}$ is needed.

And now let's go back to you, the human being. How do *you* know that, once you find out that "today is Friday" and also that "tomorrow is Saturday", then you can say (or write) "today is Friday and tomorrow is Saturday". **You know this because you know Rule** $\wedge_{prove}$. You know this rule so well, it is embedded so deeply in your mind, that you don't even realize that the rule is there. But **the rule is there!**

Here is another way to think about this. Suppose you didn't know any English at all. Then you would not know what the word "and" means, and you would not know that, if you have two sentences P and Q, then you can say or write "P and Q". As you learn English, at some point you would learn the meaning of the word "and" and then you would learn that when you have two sentences P and Q, then you can say or write "P and Q". (And I would even argue that this rule about that use of "and" is in fact what "and" means, but I will not pursue this now.) The point is: *there are* rules for using the word "and", and those rules have to be *learned*, and they only look obvious to you because you already learned them a long time ago and have grown accustomed to them.

What we are doing in Logic is **elucidating the laws of thought, making them explicit, bringing them to the surface, as it were**, so that we can, for example, pass them on from our minds to a computer: the computer does not "know" any of the things that you know, unless you tell the computer those things. And this applies even to the rules that you know so well that they are deeply embedded in your subconscious, so you take them for granted without even realizing that there is something to be known there.

Once you understand this, you will also see that **it is not an accident that modern Logic developed first, at the end of the 19th century and the beginning of the 20th century, and computers came into being soon afterwards.** □

10.5.2 Using a conjunction: another stupid but important rule

The rule for using a conjunction (Rule $\wedge_{use}$)

If P, Q are sentences, and you have proved $P \wedge Q$, then you are allowed to go to P, and you are also allowed to go to Q.

IMPORTANT REMARK. This looks like a very stupid rule. But you should reread the "Important Remark" on Page 266, where we talked about another "stupid

rule", namely, Rule $\wedge_{prove}$. That remark also applies to Rule $\wedge_{use}$. $\square$

10.6 Disjunctions ("$\vee$", i.e., "or")

The symbol

$$\vee$$

is the ***disjunction symbol***, and means "or".

So, for example,

- If P is the sentence

  today is Friday

  and Q is the sentence

  today is Saturday

  then "$P \vee Q$" stands for the sentence

  today is Friday or today is Saturday.

- A sentence of the form $P \vee Q$ is a ***disjunction***.
- In a disjunction $P \vee Q$, the sentences P, Q are the ***disjuncts***.

10.6.1 Using a disjunction: the "proof by cases" rule

The rule for using a disjunction, that we are going to call "Rule $\vee_{use}$", as you may have guessed, is extremely important. It is also called the "proof by cases rule", and is one of the most widely used rules in theorem proving.

Before I state the rule, let us look at an example.

Example 46. Suppose you want to prove that

$$(\forall x \in \mathbb{R})(x \neq 0 \Longrightarrow x^2 > 0)\,. \tag{10.187}$$

Then you could reason as follows. Since $x \neq 0$, there are two possibilities: $0 < x$ or $x < 0$. So

$$0 < x \ \vee x < 0\,. \tag{10.188}$$

Sincde we have the disjunction (10.188), we are in a position to use Rule $\vee_{use}$. To do this, we consider each of the two possibilities "$0 < x$" and "$x < 0$" separately.

> First we assume that $\boxed{0 < x.}$
>
> Then we use the fact that we can multiply both sides of an inequality by a positive number[63]. Since $0 < x$ (because we are assuming that $0 < x$), we can multiply both sides of "$0 < x$" by x, and get $x.0 < x.x$.

[63] This is one of the axioms of real number theory, that we will discuss later. The axiom says: $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})\Big((x < y \wedge 0 < z) \Longrightarrow xz < yz\Big)$.

But $x \cdot 0 = 0$ by a well-known theorem[64]

And $x \cdot x = x^2$. (This is because the definition of x^2 says that $x^2 = x \cdot x$.)

So $\boxed{0 < x^2}$.

Next we assume that $\boxed{x < 0.}$

Then we use the axiom that says that we can add a real number to both sides of an inequality and the result is an inequality going in the same direction[65]. So we add $-x$ to both sides of "$x < 0$" and get $0 < -x$.

Then we use the axiom about multiplication of both sides of an inequality by a positive number. Since $-x$ is positive, because we have proved that it is (under the assumption that $x < 0$), we can multiply both sides of "$0 < -x$" by $-x$, and get $(-x).0 < (-x).(-x)$.

But $x \cdot 0 = 0$.

And $(-x) \cdot (-x) = x \cdot x$.

So $0 < x \cdot x$.

[64] The theorem says that $(\forall x \in \mathbb{R})x.0 = 0$.

[65] Precisely, the axiom says: $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})(x < y \Longrightarrow x + z < y + z\Big)$.

And $x \cdot x = x^2$, by the definition of "square".

So $\boxed{0 < x^2}$ in this case as well.

So we have analyzed each of the two possibilities $0 < x$ and $x < 0$, and in each case we arrived a the same conclusion, namely, that $0 < x^2$.

Hence we have proved that $\boxed{\boxed{0 < x^2}}$.

What we have done in this example is this: we knew that a disjunction $A \vee B$ was true. (In our example, A was "$0 < x$" and B was "$x < 0$".) Then we proved that a ceartain conclusion C must hold if A is true, and also if B is true. (In our example, C was "$0 < x^2$".) Then we concluded that C must be true. And the reason is quite simple: one of A, B is true, and in either case C is true, so C is true.

This is exactly what the proof by cases rule says.

The rule for using a disjunction (Rule $\vee_{use}$, a.k.a. the proof by cases rule)

If P and Q are sentences, and you have proved $P \vee Q$ in a previous step, and then you prove another sentence R both assuming P and assuming Q, then you can go to R.

10.6.2 Proving a disjunction

The rule for proving a disjunction (Rule $\vee_{prove}$)

Suppose P and Q are sentences, and you want to prove $P \vee Q$. Here is what you can do. You look at the two possible cases, when P is true and when P is false. If P is true then of course $P \vee Q$ is true, so we are O.K. So all we have to do is look at the other case, when P is false, and prove that in that case Q is true.
So here is the rule:

I. If, assuming that P is false, you can prove Q, then you can go to $P \vee Q$.

II. If, assuming that Q is false, you can prove P, then you can go to $P \vee Q$.

Example 47. Let us prove that

$$(\forall n \in \mathbb{Z})(3|n \vee 3|n^2 - 1)\,. \tag{10.189}$$

Proof.

Let n be an arbitrary integer.

We want to prove that $3|n \vee 3|n^2 - 1$.

Assume that $\sim 3|n$, that is, 3 does not divide n.

We want to prove that $3|n^2 - 1$.

Clearly, $n^2 - 1 = (n-1)(n+1)$.

Furthermore, it is well known that if k, $k+1$ and $k+2$ are any three consecutive integers, then one of them must be divisible by 3.

Applying this with $k = n-1$, we see that one of the integers $n-1, n, n+1$ is divisible by 3.

But we are assuming that n is not divisible by 3.

Hence one of the numbers $n-1, n+1$ is divisible by 3.

So the product $(n-1)(n+1)$ is divisible by 3.

That is, $n^2 - 1$ is divisible by 3.

So we have proved that $3|n^2 - 1$, assuming that $\sim 3|n$.

By Rule $\vee_{prove}$, it follows that $3|n \vee 3|n^2 - 1$.

We have proved that $3|n \vee 3|n^2 - 1$ for an arbitrary integer n.

Therefore $(\forall n \in \mathbb{Z}) 3|n \vee 3|n^2 - 1$. **Q.E.D.**

10.7 Implications ("$\Longrightarrow$", i.e., "if ... then")

Implication: The symbol

$$\Longrightarrow$$

is the ***implication symbol***, and means "implies".

A sentence "$P \Longrightarrow Q$" is read as

$$P \text{ implies } Q$$

or as

$$\text{If } P \text{ then } Q\,.$$

Then

- If P is the sentence

  Today is Friday

  and Q is the sentence

  Tomorrow is Saturday

  then "$P \Longrightarrow Q$" stands for the sentence

  If today is Friday then tomorrow is Saturday.

- A sentence of the form $P \Longrightarrow Q$ is an ***implication***, or a ***conditional sentence***.

- In a conditional sentence $P \Longrightarrow Q$, P is the ***premiss*** (or ***antecedent***), and Q is the ***conclusion*** (or ***consequent***.

10.7.1 The rule for using an implication (Rule $\Longrightarrow_{use}$, a.k.a. "Modus Ponens")

We now come to one of the most important rules in Logic: the rule for using an implication. For us, this rule will be called— guess what!—"Rule $\Longrightarrow_{use}$", but it also has a couple of much more impressive names: **Modus Ponens**, and **implication elimination**[66]

The rule for using an implication (Rule $\Longrightarrow_{use}$, a.k.a. *Modus Ponens*)

Suppose P, Q are sentences. Suppose you have the sentences $P \Longrightarrow Q$" and "P" in previous steps of your proof. Then you can go to Q.

Example 48. Suppose you know that "If you are a student then you are entitled to a discount" and you also know that you are a student. Then you can conclude that you are entitled to a discount.

10.7.2 The "for all...implies" combination

One of the most important and widely used combinations of moves in proofs is what we may call ***the "for all...implies" combination***.

It works like this:

[66] "Modus Ponens" is an abbreviation of "modus ponendo ponens", which is Latin for "the way that affirms by affirming".

- First, you bring into your proof a statement S of the form "for every x of some kind, if something happens then something else happens". That is, $(\forall x)(A(x) \Longrightarrow B(x))$, or

$$(\forall x \in S)(A(x) \Longrightarrow B(x))\,. \tag{10.190}$$

- Then, you bring into your proof an object a for which you know that this object satisfies Property A, that is, you know that

$$A(a)\,. \tag{10.191}$$

- Then you derive the conclusion that $B(a)$ is true, in two steps:

  Step 1: Use the specialization rule to go from (10.190) to

$$A(a) \Longrightarrow B(a)\,. \tag{10.192}$$

  Step 2: Use Modus Ponens to go from (10.192) and (10.191) to

$$B(a)\,. \tag{10.193}$$

This combination is used all the time in proofs. The reason is that many theorems in Mathematics are of the form: "whenever something is true of an object, then something else is also true of that object", that is

$$(\forall x)(A(x) \Longrightarrow B(x))\,. \tag{10.194}$$

And what you often do in proofs is take one of those theorems and apply it to a particular situation. And this is exactly what the "for all...implies" combination does.

Here are some examples:

1. Take the statement that "Every positive real number has a real square root", which translates into

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

   This is exactly of the form (10.194), with "$x > 0$" in the role of $A(x)$, and "$(\exists y \in \mathbb{R}) y^2 = x$" in the role of $B(x)$.

   Then you can prove that 2 has a square root, by applying the "for all ... implies" combination, with $a = 2$, and getting "$(\exists y \in \mathbb{R}) y^2 = 2$".

2. Suppose you know that "If x is a positive real number then $x + \frac{1}{x} \geq 2$", that is, in formal language,

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

   (We will prove this later.) Suppose you have a real number a, and have proved that a is positive (that is, $a > 0$). Then you can draw the conclusion that $a + \frac{1}{a} \geq 2$ by using the "for all...implies" combination, as follows:

1. $(\forall x \in \mathbb{R})(x > 0 \implies x + \frac{1}{x} \geq 2)$ [Fact proven before]
2. $a > 0$.[Known]
3. $a > 0 \implies a + \frac{1}{a} \geq 2$.[Rule $\forall_{use}$, from Step 1]
4. $a + \frac{1}{a} \geq 2$.[Rule $\implies_{use}$, from Steps 2,3]

10.7.3 Proving an implication (Rule $\Longrightarrow_{prove}$)

The rule for proving an implication
(Rule $\Longrightarrow_{prove}$)

Suppose P, Q are sentences. Suppose you start a proof with "Assume P", and you prove Q. Then you can go to $P \Longrightarrow Q$.

Example 49. Say you are a Martian who just landed on Earth, you know nothing about the days of the week, and you want to prove that to your own satisfaction that "If today is Friday then tomorrow is Saturday". To apply Rule $\Longrightarrow_{prove}$, you would begin by "assuming that today is Friday." This means that you would imagine that today is Friday, and see what would happen in that case. For example, you could go to a public library and look at lots of newspapers published on a Friday, and you would see that every time such a paper talks about the following day it says something like "tomorrow is Saturday." Then you would be reasonably confident that the sentence "If today is Friday then tomorrow is Saturday" is true. And it would not matter whether today is Friday or not. □

10.7.4 The connectives "$\wedge$" and "$\Longrightarrow$" are very different

Students sometimes think that "If P then Q" is basically the same as "P and Q", or "P then Q". But this is very wrong and it important that you should understand the difference between "P and Q" and "If P then Q".

Take, for example, the sentences

Today is Friday and tomorrow is June 12.

and

If today is Friday then tomorrow is June 12.

Using "P" to represent the sentence "Today is Friday" and "Q" to represent the sentence "Tomorrow is June 2", the first sentence is $P \wedge Q$, and the second one is $P \Longrightarrow Q$.

What conditions have to be satisfied for $P \wedge Q$ to be true? What conditions have to be satisfied for $P \Longrightarrow Q$ to be true?

The sentence $P \wedge Q$ is true if both P and Q are true. In our example, the only way the sentence "Today is Friday and tomorrow is June 12" can be true is if today is Friday and tomorrow is June 12, So ***the sentence "Today is Friday and tomorrow is June 12" is true if today is Friday June 11, and in no other case***.

On the other hand, ***The sentence*** $P \Longrightarrow Q$ ***when*** Q ***is true, and also when*** P ***is false. And if neither one of these conditions hold (that is, if*** Q ***is false and*** P ***is true) then*** $P \Longrightarrow Q$ ***is false***. So, in our example, the only possible situation when "If today is Friday then tomorrow is June 12" would be false is if today is Friday but tomorrow is not June 12. So ***the sentence "If today is Friday then tomorrow is June 12" is true if today is not Friday, is also true if tomorrow is June 12, and is false if today is Friday but tomorrow is not June 12***.

We can summarize these observations by means of the following "truth tables" for the connectives "$\wedge$" and "$\Longrightarrow$":

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The first table gives you the truth value[67] of $P \wedge Q$

[67]Every sentence, when used correctly, has a ***truth value***: the truth value is T is the sentence is true, and F is the sentence is false. For example: the truth value of "$3 > 5$" is F, the truth value of "$3 < 5$" is T. How about the truth value of "$x < 5$". If you tell me that $x < 5$ without having told me who x is, then I do not knwo the truth value of "$x < 5$". But this would be an incorrect us of "$x < 5$". If you were writing a proof, then

in terms of the truth values of P and Q, and the second table gives you the truth value of $P \Longrightarrow Q$ in terms of the truth values of P and Q.

Notice that ***what makes the truth tables for "wedge" and "$\Longrightarrow$" is the last two lines***. In particuler:

> $P \Longrightarrow Q$ ***is always true when*** Q ***is true, no matter whether*** P ***is true or false***.

and

> $P \Longrightarrow Q$ ***is always true when*** P ***is false, no matter whether*** Q ***is true or false***.

So for example, the following sentences are true:

- If the Earth is a planet then 3 is a prime number.
- If the Earth is a comet then 3 is a prime number.
- If the Earth is a comet then 6 is a prime number.

The first one and the second one are true because the conclusion (that is, "3 is a prime number) is true. . (It does

you could never have "$x < 5$" as one of the steps, unless you have told the reader before, in some previous step, who x is, and once you have done that, the truth value of "$x < 5$" would be known. For example, if you said in a previous step "Let $x = \frac{1+\sqrt{5}}{2}$", then I would know that "$x < 5$" is true. (Proof: $\sqrt{5} < 5$. So $1 + \sqrt{5} < 6$. So $\frac{1+\sqrt{5}}{2} < 3$. Hence $\frac{1+\sqrt{5}}{2} < 5$. So $x < 5$.)

not matter, for the second sentence, that the premiss—"the Earth is a comet"— is false.)

And the second one and third one are true because the premiss ("the Earth in a comet" is false. (It does not matter whether for the second sentence, that the conclusion—"6 is a prime number"— is false.)

On the other hand, the sentence "If the Earth is a planet then 6 is a prime number" is false, because the premiss ("The Earth is a planet") is true, but the conclusion ("6 is a prime number") is false.

10.7.5 Isn't the truth table for $\Longrightarrow$ counterintuitive?

Students often ask questions about the implication connective $\Longrightarrow Q$ and in partuclar about the truth table for the implication.

One often raise question is "how can '$P \Longrightarrow Q$' be true if P and Q have nothing to do with each other?".

For example, we said that the sentence "If the Earth is a planet then 3 is a prime number" is true, but what does the fact that the Earth is a planet have to do with 3 being a prime number? That sounds like a good question, but let us think about it. I suggest that you do do this:

Think of "$P \implies Q$" as saying "it does not happen that P is true without Q also being true".

In other words: what "$P \implies Q$" does is exclude the possibility that you might ever run into a "bad situation", menaing, "a situation where P is true but Q is not". And this is the only possibilty excluded the implication. So, in particular,

- if P is false then you will not be in a bad situation, so "$P \implies Q$" is true.
- if Q is true then you will not be in a bad situation, so "$P \implies Q$" is true.

Once you understand this, you will see that it does not matter very much whether P and Q have something to do with each other. Maybe $P$and Q are totally unrelated, but if, for example, they both happen to be true then "$P \implies Q$" is true. And also, "$P \implies Q$" will be true if both P and Q are false, or if P is false and Q is true.

Example 50. Suppose a street sign says:

IF YOU ARE DRIVING AT MORE THAN 25MPH YOU WILL GET A FINE.

Supoose you want to prove to a friend of yours that the municipal government that put up the sign isn't really enforcing its own rule. What do you have to do to prove this?

Let "P" represent the premiss, i.e., "you are driving at more than 25mph", and let "Q" represent the conclusion, that is, "you will get a fine". Then the street sign asserts the implication "$P \Longrightarrow Q$".

Certainly,

- If you find someone driving at 20mph, that will do nothing to prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter whether that driver got a fine or not[68].

- If you find someone who got a fine, that will do nothing to prove your case. ***That's because in that case the implication "$P \Longrightarrow Q$" is true, according to the truth table for the implication.*** It does not matter whether that driver was driving at more than 25mph or not.[69].

[68] The driver may have been given a fine for some other reason, e.g., using a cell phone while driving.

[69] The driver may have been driving at 20mph but may have been given a fine for some other reason, e.g., using a cell phone while driving.

- The only way to prove that the injunction in the street sign is not being enforced is to find cases of drivers that were driving at more than 25mph but did not get a fine. ***That's because the onlt case when the implication "$P \implies Q$" is false, according to the truth table for the implication, is when the premiss is true but the conclusion is false.***

Example 51. Alice is a cashier at a department store, and she has to follow the rule that

> ***IF A CUSTOMER PAYS CASH FOR A PURCHASE THEN ALICE HAS TO PUT THE MONEY SHE COLLECTED IN A DRAWER.***

Suppose you are a detective and you want to prove that Alice is not obeying the rule. What do you have to do?

- If you find a situation when there was not customer at all, or there was customer that did not pay cash, then that will do nothing prove your case. ***That's because in that case the implication "$P \implies Q$" is true, according to the truth table for***

the implication. It does not matter whether Alice put money is the drawer or not[70].

- If you find a situation where Alice put cash in the drawer even though she did not collect any money from a customer, then that will do nothing to prove your case. ***That's because in that case the implication "$P \implies Q$" is true, according to the truth table for the implication.*** It does not matter that there was no customer poaying cash[71].

- The only way you can prove that Alice is violating the rules is by showing that a customer paid cash but Alice did notput themoney in the drawer. ***That's because the only case when the implication "$P \implies Q$" is false, according to the truth table for the implication, is when the premiss is true but the conclusion is false.***

Example 52. Suppose you have a natural number n, but you do not know which number it is. (For example, maybe someone gave you a sealed envelope containing

[70] Why would Alice have put money in the drawer if she did not collect any cash from the customer? Who knows?

[71] Again, why would Alice put money in the drawer even if she did not collect the money from a customer? Who knows? And who cares? The point is: ***even if she put money in the drawer when there had been no customer that paid her the money, so P was false but Q was true, she did not violate the rules.***

a card where the number is written. So the number is there, it's a fixed number, but you just do not knwo which specific number it is.)

Suppose you are asked to prove that

(*) If n is even then n^2 is divisible by 4.

Then you could ask: could (*) possibly be false? Could there be a possible value of n for which (*) is false. (Remember that you do not know who n is. So if you want be able to assert for sure that (*) is true you have to consider all possible values of n. If you find one value of n for which (*) is not true, then you cannot be sure that n is true, because the number that you have in the envelope could be the one you have found, the one for which (*) is false. But if you can make sure that no such number exists, then you can be sure that (*) is true, even though you do not know who n is.)

What would have to happen for (*) to be false? Well, according to our truth table, the only case when the implication (*) is false is when the premiss is true but the conclusion is not. So to make sure that (*) is true, you have to consider numbers n that are even, because if n is not even then (*) is true. You indicate that you are going to do that by writing:

Assume that n is even.

(In other words: ***you are allowed to assume that*** n ***is even because if*** n ***is not even then (*) is automatically true thanks to the truth table for the implication.***)

And then you move on to prove that n^2 is divisible by 4. (Since n is even, we can pick a natural number k such that $n = 2k$. Then $b^2 = 4k^2$, so n^2 is divisible by 4.)

And now you can be sure that (*) is true. The number n is even or odd, but in either case (*) is true, even though in each case it's true for a different reason: if n is not even, then (*) is true because of the truth table for the implication, and if n is even then (*) ia true because in that case we have proved that the conclusion (that is, "n^2 is divisible by 4") must be true.

Finally, we have prove that (*) must be true for any natural number, because we have proved for n, but n could be any number. So we can conclude that

$$(\forall n \in \mathbb{N})\Big(n \text{ is even} \Longrightarrow n^2 \text{ is divisible by } 4\Big),$$

or, if you prefer,

$$(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big).$$

So we can structure our proof as follows:

THEOREM. $(\forall n \in \mathbb{N})\Big(2|n \Longrightarrow 4|n^2\Big)$.

PROOF We want to prove that $(\forall n \in \mathbb{N})\Big(2|n \implies 4|n^2\Big)$.

Let $n \in \mathbb{N}$ be arbitrary.

We want to prove that $2|n \implies 4|n^2$.

Assume that $2|n$.

Then $(\exists k \in \mathbb{N})n = 2k$.

Pick one such k and call it k_*.

Then $k_* \in \mathbb{N}$ and $n = 2k_*$.

Then $n^2 = (2k_*) \cdot (2k_*) = 4k_*^2$.

Let $q = k_*^2$.

Then $n^2 = 4q$.

So $(\exists k)n^2 = 4k$.

Hence $4|n^2$.

We have proved that $4|n^2$ assuming that $2|n$. Hence

$$2|n \implies 4|n^2 \,.$$

We have proved that $2|n \implies 4|n^2$ for an arbitrary n. Therefore

$$(\forall n \in \mathbb{N})\Big(2|n \implies 4|n^2\Big) \,.$$

Q.E.D.

I hope that these remarks will suffice to clarify they way implication works. Implication will be discussed in great detail later.

10.8 Biconditionals ("$\Longleftrightarrow$", i.e., "if and only if")

The ***biconditional*** is the symbol

$$\Longleftrightarrow.$$

It is a *binary connective*, like $\wedge$, $\vee$, and $\Longrightarrow$. That means that $\Longleftrightarrow$ ***can be used to connect two sentences***.

If P and Q are sentences, the sentence "$P \Longleftrightarrow Q$" is read as

$$\boxed{P \text{ if and only if } Q}$$

or

$$\boxed{P \text{ is equivalent to } Q}.$$

And mathematicians often use "iff" as shorthand for "if and only if", so they write "P iff Q."

$$\boxed{P \text{ iff } Q}.$$

The precise meaning of "equivalence" will be explained later. But, if you want to know right away what it means, it's very simple:

When you know that P is equivalent to Q then you can pass freely from P to Q. That is, if you know that P is true then you can write Q, and if you know that Q is true then you can write P.

So for all practical purposes if "$P \iff Q$" is true then P and Q are interchangeable.

10.8.1 The meaning of "if and only if"

You should think of "P iff Q" as meaning

$$(P \iff Q) \wedge (Q \iff P)\,.$$

That is, "$P \iff Q$" means[72]

$$\text{If } P \text{ then } Q \text{ and if } Q \text{ then } P\,,$$

or

$$P \text{ implies } Q \text{ and } Q \text{ implies } P\,.$$

[72] *This note is only for philosophically minded nitpickers.* What does "means" mean? The point of view adopted here is that *the meaning of a word, phrase or symbol consists of the rules for the use of that word, phrase or symbol.* For example, the meaning of "and" is the specification that if P, Q are two sentences, then (i) if you have "P and Q" you can go to P and you can go to Q, and (ii) if you have P and you have Q then you can go to "P and Q." That is, *the meaning of "and" is captured by Rules $\wedge_{use}$ and $\wedge_{prove}$.* Naturally, this does not cover all the uses of "and" in our culture, such as, for example, to indicate a progression (as in "this is getting better and better"), or to indicate a causal relation, (as in "do that and I'll hit you"), or the literary use full of nuances (as 'in 'tomorrow and tomorrow and tomorrow"). And, most importantly for us, it does not cover the use of "and" to connect *nouns*, as in "slings and arrows". But it's what "and" means in logic and mathematics. If you want to program a computer so that it will know what "and" means, you have to tell the computer how to use "and". And this amounts to programming the computer to use rules $\wedge_{use}$ and $\wedge_{prove}$. And you don't need to tell the computer anything else. A similar situation arises with the biconditional. A computer that "knows" the rules $\iff_{use}$ and $\iff_{prove}$ "knows" all it needs to know to work with the biconditional, and for that reason I believe that knowing the meaning of "$\iff$" amounts to knowing the two rules for working with it.

In order to make this true, we will choose the rules for proving and using biconditional sentences as follows:

- *To prove "$P \iff Q$" you do exactly the same thing that you would do to prove* $(P \iff Q) \wedge (Q \iff P)$.
- *To use "$P \iff Q$" you do exactly the same thing that you would do to use* $(P \iff Q) \wedge (Q \iff P)$.

So, for example, suppose you want to prove that

$$(\forall x \in \mathbb{R})\Big(x^2 = 4 \iff (x = 2 \vee x = -2)\Big). \quad (10.195)$$

Then you would start by introducing into your proof an arbitrary real number called x, and then you would prove that

$$(x^2 = 4 \iff (x = 2 \vee x = -2). \quad (10.196)$$

And to prove (10.196), which is an "iff" sentence, you would prove both implications $x^2 = 4 \implies (x = 2 \vee x = -2)$ and $(x = 2 \vee x = -2) \implies x^2 = 4$.
(The proof of these two sentences is very simple: to prove that $x^2 = 4 \implies (x = 2 \vee x = -2)$, you use the fact that a positive real number r cannot have more than two square roots[73]. Since 2 and -2 are two distinct square roots of

[73]This was proved in the notes for Lectures 2,3,4 but, just in case, here is a quick proof: suppose r has three distinct square roots a, b, c. Then $a^2 = r$, $b^2 = r$ and $c^2 = r$. Hence $a^2 - b^2 = 0$. So $(a - b)(a + b) = 0$. Therefore $a - b = 0$ or $a + b = 0$. Since a and b are different, it cannot be the case that $a - b = 0$, so $a + b$ must be zero, and then $b = -a$. Now we can use exactly the same argument with c instead of b, and conclude that $c = -a$. But then $c = b$, contradicting the fact that $b \neq c$.

4, there cannot be a third square root. So, if $x^2 = 4$, so x is a square root of 4, it follows that x must be 2 or -2. So $x^2 = 4 \Longrightarrow (x = 2 \vee x = -2)$. To prove the other implication, i.e., that $(x = 2 \vee x = -2) \Longrightarrow x^2 = 4$, just observe that if $x = 2$ then $x^2 = 4$, and if $x = -2$ then $x^2 = 4$ as well,)

10.8.2 The rules for proving and using biconditionals

Now let us state explicitly the rules for proving and using biconditional sentences.

As I explained in the previous subsection, *these rules are designed so as to make "$P \Longleftrightarrow Q$" mean precisely what we want it to mean, that is "$(P \Longrightarrow Q) \wedge (Q \Longrightarrow P)$".*

The rules are as follows.

Rule $\iff$ *prove*

If P, Q are sentences, and you have proved the sentences

$$P \Longrightarrow Q$$

and

$$Q \Longrightarrow P\,,$$

then you can go to

$$P \iff Q\,.$$

Rule $\iff$ *use*

If P, Q are sentences, and you have proved the sentence

$$P \iff Q\,,$$

then you can go to

$$P \Longrightarrow Q$$

and you can also go to

$$Q \Longrightarrow P\,.$$

10.9 The other six rules

So far I have given you eight rules, two for each of the connectives $\wedge$, $\vee$, $\Longrightarrow$, and $\Longleftrightarrow$.

In addition, there are six more rules that we have already discussed:

1. Rule $\forall_{prove}$, the rule for proving a universal sentence. (This rule is sometimes called "universal generalization".)
2. Rule $\forall_{use}$, the rule for using a universal sentence. (This is sometimes called the "specialization rule".)
3. Rule $\exists_{prove}$, the rule for proving an existential sentence.. (This rule is sometimes called the "existential generalization rule".)
4. Rule $\exists_{use}$, the rule for using a universal sentence. (This rule is sometimes called the "existential specialization rule".)
5. The proof by contradiction rule.
6. Rule SEE, substitution of equals for equals (also called "Rule $=_{use}$").

So ***we now have all fourteen rules!***

10.10 Are the logical rules hard to understand and to learn and remember ?

Most of the logical rules are very simple and easy to remember. For example,

- The rules for using and proving $\wedge$ sentences are so stupid that you might object to having them because they are so obvious, but you certainly cannot find it hard to understand them.
- The rules for using and proving universal sentences are also natural:
  - if you know that all the items in this store cost 1 dollar, and you pick an item in this store, you can be sure that it costs 1 dollar. That's all that Rule $\forall_{use}$ says.
  - if you prove that a schmoo must be green, without using any information about that schmoo other than the fact that it is a schmoo, then you can conlude that all schmoos are green. And that's= all that Rule $\forall_{prove}$ says.
- And the rules for using and proving existential sentences are natural as well:
  - if you know that somewhere in this store there is a schmoo, then you can go and get a schmoo and call it any way you want, for example "my woderful schmoo". That's all that Rule $\exists_{use}$ says.
  - if you find a schmoo, then you can conclude that schmoos exist. And that's all that Rule $\exists_{prove}$ sats.

10.10.1 Proofwriting and rules for proofs

Writing proofs is like playing chess, checkers, or some other board game.

- There are rules that tell you which moves are allowed. (Notice that the rules for proofs never say "you ***have*** to do this". They say "you ***are allowed*** to do this". It's exactly like the moves you are allowed to make in a board game.)
- You have to obey the rules all the time.
- If you cheat, by violating the rules once, then you are out of the game.
- If you know how to play, you will never make a move that violates the rules.
- Once you know the moves, then the hard part begins: you have to figure out how to choose which moves to make in order to win. And that is where proofwriting becomes difficult and challenging: some people are better than others at figuring out how to win.
- From 1637 until 1995, many mathematicians tried very hard to prove Fermat's last theorem. Finally, Andrew Wiles suceeded in doing it in 1995.
- But the proofs we do in this course are not that hard.

11 Induction

11.1 Introduction to the Principle of Mathematical Induction

You know that the following is true:

(*) *Every integer is even or odd, and not both.*

How can we prove statement (*)?

First, we have to make it clear what we mean by "even" and "odd".

Definition 15.

1. An integer n is <u>even</u> if n is divisible by 2, that is, if there exists an integer k such that $n = 2k$.
2. An integer n is <u>odd</u> if $n - 1$ is even, that is, if there exists an integer k such that $n = 2k + 1$. □

Now that we know what it means for an integer to be "even" or "odd", we can try to prove some facts about even and odd integers. Here are some simple examples of theorems about even and odd numbers that are easy to prove:

Theorem 13. *If m and n are even integers, then $m+n$ is even. (That is, "the sum of two even integers is even".)*

Theorem 14. *If m and n are odd integers, then $m+n$ is even. (That is, "the sum of two odd integers is even".)*

Theorem 15. *If m and n are integers, m is even and n is odd, then $m+n$ is odd. (That is, "the sum of an even integer and an odd integer is odd".)*

Theorem 16. *If m and n are integers, and m or n is even, then $m.n$ is even. (That is, "the product of an even integer and an integer is an even integer".)*

Theorem 17. *If m and n are odd integers, then $m.n$ is odd. (That is, "the product of two odd integers is odd".)*

Theorem 18. *The integer 1 is odd and is not even.*

Theorem 19. *If an integer n is even, then the integers $n+1$ and $n-1$ are odd.*

Theorem 20. *If an integer n is odd, then the integers $n+1$ and $n-1$ are even.*

All these theorems are very easy to prove. I will do two of the proofs, and I will ask you to do all the others.

Proof of Theorem 14:

Let m, n be integers.

Assume m and n are odd.

We want to prove that $m + n$ is even.

Since m is odd, we can pick an integer j such that $m = 2j + 1$.

Since n is odd, we can pick an integer k such that $n = 2k + 1$.

Then $m + n = (2j + 1) + (2k + 1)$, so $m + n = 2j + 2k + 2$ and then $m + n = 2(j + k + 1)$.

Hence $(\exists i \in \mathbb{Z})m + n = 2i$.

So $m + n$ is even. **Q.E.D.**

Proof of Theorem 18: First, we show that 0 is even. To prove this, we observe that $0 = 2.0$, so $(\exists k \in \mathbb{Z})0 = 2k$, and then 0 is even.

It then follows immediately that 1 is odd, because the definition of "odd integer" says that "n is odd" means "$n - 1$ is even", so in particular "1 is odd" means "$1 - 1$ is even", and this is true, because $1 - 1 = 0$, and 0 is even.

Finally, we have to show that 1 is not even. For this purpose, we have to show that there is no integer k such that $2k = 1$. But there is only one real number k such that $2k = 1$, and that number is $\frac{1}{2}$, which is not an integer. So there is no integer k such that $2k = 1$. Hence 1 is not even. **Q.E.D.**

Problem 50. ***Prove*** Theorems 13, 15, 16, 17, 19, and 20.

WARNING: We have not proved yet that "odd" is equivalent to "not even". This will be proved later, in Theorem 25 in Section 11.3.3. But ***until we have proved it we cannot use it.*** So, for example, you are ***not*** allowed to prove that an integer n is even by contradiction, by saying "suppose n is not even, then n is odd." You cannot do that because we have not proved yet that "n is not even" is equivalent to "n is odd". □

What we actually want is to prove (*), i.e., to show that every integer is even or odd and not both.

Let us call an integer "good" if it is even or odd and not both even and odd. So we want to prove that

(**) *Every integer is good.*

We are going to prove first that every natural number is good, and then we will take the extra step of proving that every natual number is good.

So let us start by trying to prove that every natural number is good.

We already know that 1 is good. How about 2?

Theorem 21. *The number* 2 *is even and not odd. So* 2 *is good.*

Proof. 1 is odd, so by Theorem 20, $1+1$ is even, so 2 is even.

On the other hand, 2 cannot be odd, because if 2 was odd then $2-1$ would be even by Theorem 20.

So 2 is even and not odd, and then 2 is good. **Q.E.D.**

How about 3?

Theorem 22 *The number* 3 *is odd and not even. So* 3 *is good.*

Proof. 2 is even. So by Theorem 19, $2+1$ is odd, so 3 is odd.

On the other hand, 3 cannot be even, because if 3 was even then $3-1$ would be odd by Theorem 19, i.e., 2 would be odd.

So 3 is odd and not even, and then 3 is good. **Q.E.D.**

It is clear that we could go on the same way, and prove that 4 is good, 5 is good, 6 is good, *and so on.* And then we would conclude that every natural number is good.

However, saying "and so on" is not a rigorous way to ***prove*** that every natural number is good.

The key idea is this: we are going to prove that ***goodness is a property that is passed on from each natural number*** n ***to the number following it, i.e.,*** $n+1$.

Precisely, we are going to prove:

Theorem 23. *If n is natural number and n is good, then $n+1$ is good.*

Once we have proved Theorem 23, since we have already proved Theorem 18, which says that 1 is good, we will be able to reason as follows:
We know that

1. 1 ***is good***.
2. ***Goodness is passed on from each natural number n to its successor $n+1$.*** (That is: if $n \in \mathbb{N}$ and n is good, then $n+1$ is good.)

Then:

1. 2 is good, because 1 is good and 1 passes on the goodness property to 2,
2. 3 is good, because 2 is good and 2 passes on the goodness property to 3,
3. 4 is good, because 3 is good and 3 passes on the goodness property to 4,
4. 5 is good, because 4 is good and 4 passes on the goodness property to 5,

   ...

   and so on,
   so every natural number is good.

But it would be much better not to rely on vague phrases like "and so on", and to have instead a precise, rigorous way of doing the proof.

The key point is that ***all the natural numbers are eventually arrived at by counting***, so that, if we know that something is true for $n = 1$, and when we count (that is, go from 1 to 2, then from 2 to 3, then from 3 to 4, "and so on", each time passing from a natural

number n to its successor $n+1$), then at each step the goodness property will be passed on from n to $n+1$, and eventually every natural number n will be reached by our counting process, so n will be good.

This means that

> Every property that is true of the number 1 and is passed on from each natural number to its successor must be true of all natural numbers.

And ***this is exactly what the Principle of Mathematical Induction (PMI) says***.

Example 53. Suppose you decide to paint natural numbers green according to the following rule: first, you paint the number 1 green. And then every time you paint a number n green, you go to its successor $n+1$ and paint it green. Then the PMI guarantees that every natural number is painted green. □

Example 54. Suppose there is an infinitely long queue of people standing in line: person No. 1, then person No. 2, then person No. 3, then person No. 4, and so on[74]. Suppose you have a flyer with an announcement that you want all the people in the queue to read. (For

[74]Sure, I am talking about an infinitely long queue, with infinitely many people. And you may object that this is impossible in reality. I have two answers to that. ANSWER NO. 1: This may be impossible in reality, but you can certainly ***imagine*** it! It may be impossible in reality for a person to jump 50 feet high, but you can certainly imagine

example, a message saying something like "if you come to my restaurant after the show you will get a great meal with a 20% discount"). Suppose you want everybody to read the flyer, but you have only one copy. Then all you have to do is

(1) Give the flyer to person No. 1,

and

(2) Make sure that each person passes on the flyer to the person next in line after reading it[75].

The PMI says the obvious thing: if you do (1) and (2) then everybody will eventually get your flyer. □

11.2 The Principle of Mathematical Induction (PMI)

As explained in the previous section, the ***Principle of Mathematical Induction (PMI)*** captures as a precise mathematical statement the intuitively clear fact that when we count ***we get all the natural numbers***.

Wonder Woman doing it, so why not imagine an infinite queue? ANSWER 2: Suppose you only have a finite queue, say 40 people. Then you can consider the following property $P(n)$ of a natural number: "person n got the message or there is no person n". This makes sense of every natural number n. If you guarantee that $P(n)$ is true of every natural number n, this will imply that persons 1, 2, 3, and so on up to person 40, will get the message. Property $P(n)$ will be true of every n but for different reasons: for $n = 1, 2, 3, 4, \cdots$, up to $n = 40$, it will be true because person n gets the message. And for larger n it will be true because there is no person No. n.

[75]For example, you could include in the flyer, in big letters, the statement PLEASE PASS THIS ON TO THE PERSON NEXT IN LINE TO YOU.

Remark 9. There are other numbers (that is, people have invented other numbers), such as zero, the negative numbers -1, -2, etc., fractions such as $\frac{2}{3}$, $\frac{22}{7}$,$-\frac{5}{2}$, 2.75, -5.16, and even "irrational numbers", that cannot be expressed as fractions. But ***we do not get these numbers by the counting process***.

So, if you prove by induction that a statement $P(n)$ is true for all natural numbers, then it does ***not*** follow that it will be true for $n = 0$, because 0 is not a natural number, so if you count $1, 2, 3, 4, \ldots$ you will never get to 0.

And it does not follow either that $P(n)$ will be true for $n = \frac{1}{2}$, because $\frac{1}{2}$ is not a natural number, so if you count $1, 2, 3, 4, \ldots$ you will never get to $\frac{1}{2}$. □

Imagine that you have some statement $P(n)$ about natural numbers that could be true or not for each natural number n. (For example, the statement $P(n)$ could be "$n(n + 1)$ is even", or "n is even or odd", or "n is not both even and odd".) Suppose the following two facts are true:

I. The statement $P(n)$ is true for $n = 1$. (That is, $P(1)$ is true.)

II. Any time the statement $P(n)$ is true for one particular n, it follows that it is true for $n + 1$. (That is:

if $P(n)$ is true then $P(n+1)$ is true.)

The PMI says that, under these circumstances, $P(n)$ must be true for ***every*** natural number n.

THE PRINCIPLE OF MATHEMATICAL INDUCTION

Suppose $P(n)$ is any sentence in which n is an open variable.

Suppose, furthermore, that

I. $P(1)$ is true.

II. Any time $P(n)$ is true for one particular n, it follows that $P(n+1)$ is true.)

Then $P(n)$ is true for every natural number n.

Let us say the same thing in formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION (FORMAL LANGUAGE VERSION)

Suppose $P(n)$ is a sentence in which n is an open variable. Then

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\Big) \Longrightarrow (\forall n \in \mathbb{N})P(n)\,. \tag{11.197}$$

11.3 The proof by induction that every natural number is even or odd and not both

We are going to use Theorems 18 (which says that 1 is good) and 23 (which says that goodness is passed on from each natural number n to its successor $n+1$).

We have already proved Theorem 18, but we have not proved Theorem 23, so we have to do it now.

Proof of Theorem 23.

Let n be an arbitrary natural number.

Assume that $\boxed{n \text{ is good}}$.

We are going to prove that $n+1$ is good.

Since n is good, n is even or odd, and n is not both even and odd.

Assume that $\boxed{n \text{ is even}}$.

Then n is not odd, because n is good.

It then follows from Theorem 19 that $n+1$ is odd.

It also follows from Theorem 19 that $n+1$ is not even. (Reason: If $n+1$ was even, then $(n+1)-1$ would be odd, that is, n would be odd. But n isn't odd[76].)

So $n+1$ is odd and $n+1$ is not even.

So $\boxed{n+1 \text{ is good}}$.

So $\boxed{n \text{ is even} \implies n+1 \text{ is good}}$.

Now assume that $\boxed{n \text{ is odd}}$.

Then n is not even, because n is good.

It then follows from Theorem 20 that $n+1$ is even.

It also follows from Theorem 20 that $n+1$ is not odd. (Reason: If $n+1$ was odd, then $(n+1)-1$ would be even that is, n would be even. But n isn't even[77].)

So $n+1$ is even $n+1$ is not odd.

[76] Notice that this is a proof by contradiction

[77] Another proof by contradiction!

So $\boxed{n+1 \text{ is good}}$.

So $\boxed{n \text{ is odd} \implies n+1 \text{ is good}}$.

Since we have "n is even $\vee$ n is odd", "n is even $\implies$ $n+1$ is good", and "n is odd $\implies$ $n+1$ is good", it follows from Rule $\vee_{prove}$ that $\boxed{\boxed{n+1 \text{ is good}}}$.

Since we have proved "$n+1$ is good" assuming "n is good", it follows from Rule $\implies_{prove}$ that

$$n \text{ is good} \implies n+1 \text{ is good}. \qquad (11.198)$$

Since we have proved (11.198) for an arbitrary natural number n, it follows from Rule $\forall_{prove}$ that

$$(\forall n \in \mathbb{N})\Big(n \text{ is good} \implies n+1 \text{ is good}\Big). \quad (11.199)$$

We are now ready, finally, to prove the theorem that we had announced before, that every natural number is even or odd and not both.

We will prove this by induction.

THE FORMAT OF A PROOF BY INDUCTION

A proof by induction of a statement

$(\forall n \in \mathbb{N})XXXX$ should look like this:

Let $P(n)$ be the predicate XXXX.

Basis step. Proof of $P(1)$.

. . . . . .

$\boxed{P(1)}$.

Inductive step. We prove that $(\forall n \in \mathbb{N})\Big(P(n) \implies P(n+1)\Big)$.

Let $n \in \mathbb{N}$ be arbitrary. We want to prove $P(n) \implies P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.

. . . . . .

. . . . . .

$P(n+1)$.

So $P(n) \implies P(n+1)$. [Rule $\implies_{prove}$]

Hence $\boxed{(\forall n \in \mathbb{N})\Big(P(n) \implies P(n+1)\Big)}$

[Rule $\forall_{prove}$]

We have completed the basis step and the inductive step. Hence it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$.

That is, $(\forall n \in \mathbb{N})XXXX$. **Q.E.D.**

11.3.1 A remark on the importance of parentheses

PARENTHESES MATTER!!!

The sentence

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \qquad \text{(a)}$$

is not at all the same as the sentence

$$(\forall n \in \mathbb{N})P(n) \Longrightarrow P(n+1)\,. \qquad \text{(b)}$$

Sentence (a) says that the implication "$P(n) \Longrightarrow P(n+1)$" (that is, "$P$ is passed on from n to $n+1$") is true for every natural number n. So (a) says "every natural number passes on Property P to its successor".
Sentence (b) is totally different. It says: "if it is true that all natural numbers have P then $n+1$ has P". This is in fact meaningless, because n is an open variable.

11.3.2 Our first proof by induction: proof that every natural number is even or odd and not both

Theorem 24 *If n is a natural number, then*

1. *n is even (that is, $(\exists k \in \mathbb{Z})n = 2k$) or n is odd (that is, $(\exists k \in \mathbb{Z})n = 2k+1$);*

2. n is not both even and odd.

Proof. As we have been doing in previous sections, let us call an integer n "good" if n is even or odd and not both even and odd.

Let $P(n)$ be the sentence "n is good".

We want to prove that $(\forall n \in \mathbb{N})P(n)$.

Basis step. We have to prove $P(1)$, i.e., that 1 is good. But we already know, from Theorem 18 that 1 good. So $\boxed{P(1) \text{ is true}}$, and this completes the basis step.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\big(P(n) \Longrightarrow P(n+1)\big)\,.$$

But we have alrady proved this, in Theorem 23, on page 305, which says precisely that goodness is passed on from an integer n to its successor $n+1$.

Since we have proved both that $P(1)$ and that

$$(\forall n \in \mathbb{N})\big(P(n) \Longrightarrow P(n+1)\big)\,,$$

it follows from the PMI that

$$(\forall n \in \mathbb{N})G(n)\,, \tag{11.200}$$

i.e., every natural number is good. **Q.E.D.**

Finally, we need to prove that every integer is good. It is very easy to prove that if $n \in \mathbb{Z}$ and n is good then $-n$ is good. (**YOU DO THIS.**)

Now, let n be an arbitrary integer. Then either $n \in \mathbb{N}$ or $-n \in \mathbb{N}$ or $n = 0$, by Basic Fact BFN4.

If $n \in \mathbb{N}$ then we already know that n is good.

If $-n \in \mathbb{N}$ then $-n$ is good, and then n is good as well.

So we have proved that the nonzero integers are good. If $n = 0$, then n is good as well because, for example, we alreadyknow that -1 is good, and goodness is passed on from each integer to its successor.

So we have proved that every integer is good. **Q.E.D.**

11.3.3 Proof that every integer is even or odd and not both

We now want to prove that every integer is good. That is, we want to prove:

Theorem 25. *If n is an integer, then*

1. *n is even (that is, $(\exists k \in \mathbb{Z})n = 2k$) or n is odd (that is, $(\exists k \in \mathbb{Z})n = 2k + 1$);*
2. *n is not both even and odd.*

In order to prove this, we need two very simple theorems.

Theorem 26. *The integer 0 is even and not odd.*

Theorem 27. *If n is an integer then*

1. *If n is even then $-n$ is even.*

2. *If n is odd then $-n$ is odd.*

3. *If n is even and odd and not both, then $-n$ is even or odd and not both.*

Problem 51. ***Prove*** Theorems 26 and 27, using the theorems already proved in this section. □

Proof of Theorem 25.

As we have been doing in previous sections, let us call an integer n "good" if n is even or odd and not both even and odd.

We want to prove that every integer is good.

Let $n \in \mathbb{Z}$ be arbitrary.

Then either $n \in \mathbb{N}$, or $-n \in \mathbb{N}$, or $n = 0$.

If $n \in \mathbb{N}$, then n is good by Theorem 24.

If $-n \in \mathbb{N}$, then $-n$ is good by Theorem 24, and this implies that n is good by Theorem 27.

If $n = 0$ then n is good by Theorem 26.

So n is good. **Q.E.D.**

12 Examples of proofs by induction

12.1 Some divisibility theorems

Theorem 28. *If n is natural number, then $8^n - 5^n$ is divisible by 3.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N}) 3 | 8^n - 5^n \,. \tag{12.201}$$

Let $P(n)$ be the predicate "$3|8^n - 5^n$

.

We want to prove that $(\forall n \in \mathbb{N}) P(n)$.

We are going to prove this by induction.

Basis step:

We want to prove $P(1)$.

$P(1)$ aays "$3|8^1 - 5^1$".

And $8^1 = 8$, $5^1 = 5$, so $8^1 - 5^1 = 3$.

Therefore $3|8^1 - 5^1$, so $\boxed{P(1) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

Let $n \in \mathbb{N}$ be arbitrary.

Assume $P(n)$.

Then $3|8^n - 5^n$.
So we can write

$$8^n - 5^n = 3k\,, \quad k \in \mathbb{Z}\,.. \tag{12.202}$$

Then

$$8 \times (8^n - 5^n) = 3 \times 8k\,. \tag{12.203}$$

So

$$8^{n+1} - 8 \times 5^n = 3 \times 8k\,, \tag{12.204}$$

and then

$$8^{n+1} = 8 \times 5^n + 3 \times 8k\,, \tag{12.205}$$

But $8 = 5 + 3$, so

$$8 \times 5^n = 5 \times 5^n + 3 \times 5^n = 5^{n+1} + 3 \times 5^n\,, \tag{12.206}$$

so

$$8^{n+1} = 5^{n+1} + 3 \times 5^n + 3 \times 8k\,, \tag{12.207}$$

and then

$$8^{n+1} = 5^{n+1} + 3(5^n + 8k)\,, \tag{12.208}$$

so that

$$8^{n+1} - 5^{n+1} = 3(5^n + 8k)\,, \tag{12.209}$$

Let $j = 5^n + 8k$. Then $j \in \mathbb{Z}$ and

$$8^{n+1} - 5^{n+1} = 3j\,. \tag{12.210}$$

Hence $3|8^{n+1} - 5^{n+1}$. That is, $\boxed{P(n+1)}$.

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$(by Rule $\Longrightarrow_{prove}$).

So $\boxed{(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$ (by Rule $\forall_{prove}$).

This completes the inductive step.

Since we have proved $\boxed{P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$, it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$, that is,. $\boxed{(\forall n \in \mathbb{N})3|8^n - 5^n}$. **Q.E.D.**

Here are a few examples of theorems similar to Theorem 28

Theorem 29. *If n is natural number, then $11^n - 4^n$ is divisible by 7.*

Theorem 30. *If n is natural number, then $22^n - 10^n$ is divisible by 12.*

Theorem 31. *If n is natural number, then $31^n - 18^n$ is divisible by 13.*

Problem 52. ***Prove*** Theorem 29. □

Problem 53. ***Prove*** Theorem 30. □

Problem 54. ***Prove*** Theorem 31. □

Problem 55. *If, after reading the proof of Theorem 28 and solving Problems 52, 53, 54, you get the feeling that these are all the same thing,* ***try to prove*** *the following general theorem:*

Theorem 32. *If a, b are integers, then for every natural number n, $a^n - b^n$ is divisible by $a = b$.*

(This is done later, see Theorem 39 on page 349. But you shoud try to prove it by yourself before you look at the proof.) □

12.2 An inequality

Here is another example of a proof by induction.

Theorem 33. *If n is a natural number, then $2^n < n! + 3$.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N}) 2^n < n! + 3\,. \tag{12.211}$$

Let $P(n)$ be the predicate "$2^n < n! + 3$".

We want to prove that $(\forall n \in \mathbb{N}) P(n)$.

We are going to prove this by induction.

Basis step:

We want to prove $P(1)$.

$P(1)$ aays "$2^1 < 1! + 3$".

And $2^1 = 2$ and $1! + 3 = 4$.

Therefore $2^1 < 1! + 3$, so $\boxed{P(1) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

Let $n \in \mathbb{N}$ be arbitrary.

Assume $P(n)$. We want to prove $P(n+1)$.

Since $P(n)$ holds, we have

$$2^n < n! + 3\,. \tag{12.212}$$

Therefore, multiplying both sides of (12.212) by 2, we get

$$2^{n+1} < 2n! + 6\,. \tag{12.213}$$

On the other hand, $n + 1 = n - 1 + 2$, so

$$(n+1)! = (n+1)n! = (n-1)n! + 2n!\,. \tag{12.214}$$

We are going to treat separately the cases $n \geq 3$ and $n < 3$.

Assume that $n \geq 3$.

Then $n-1 \geq 2$ and $n! \geq 6$, so $(n-1)n! \geq 12$ and *a fortiori* $(n-1)n! > 3$.

∗ Since $(n+1)! = (n-1)n! + 2n!$, and $(n-1)n! > 3$, we have $(n+1)! > 2n! + 3$, that is

$$2n! + 3 < (n+1)! \,. \tag{12.215}$$

Since $2^{n+1} < 2n! + 6$, we have

$$\begin{aligned} 2^{n+1} &< 2n! + 6 \\ &= 2n! + 3 + 3 \\ &< (n+1)! + 3 \,, \end{aligned}$$

so $2^{n+1} < (n+1)! + 3$.

That is, $\boxed{P(n+1) \text{ holds.}}$

We now consider the case when $n < 3$.

Assume that $n < 3$.

Then $n = 1$ or $n = 2$,

If $n = 1$ then $P(n+1)$ says $2^2 < 2! + 3$, that is $4 < 5$. So $P(n+1)$ is true.

If $n = 2$ then $P(n+1)$ says $2^3 < 3! + 3$, that is $8 < 9$. So $P(n+1)$ is true.

So in both cases $\boxed{P(n+1) \text{ holds.}}$

We have proved that $P(n+1)$ holds in both case, when $n \geq 3$ and when $n < 3$. So $\boxed{\boxed{P(n+1).}}$

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$(by Rule $\Longrightarrow_{prove}$).

So $\boxed{(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$ (by Rule $\forall_{prove}$).

This completes the inductive step.

Since we have proved $\boxed{P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$, it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$, that is,. $\boxed{(\forall n \in \mathbb{N})2^n < n! + 3}$. **Q.E.D.**

Problem 56.

1. ***Prove*** that if n is a natural number then $3^n < n! + 124$.

2. Is it true that if n is a natural number then $3^n < n! + 123$?

12.3 More inequalities, with applications to the computation of some limits

Let us use induction to prove an inequality:

Theorem 34 *If x is a positive real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{12.216}$$

Proof. We want to prove that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{12.217}$$

Let x be an arbitrary real number.

We want to prove that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1+nx\Big)\,. \quad (12.218)$$

We prove this by induction.

Let $P(n)$ be the predicate "$x > 0 \Longrightarrow (1+x)^n \geq 1+nx$".

Base step. We have to prove $P(1)$.

But $P(1)$ says "$x > 0 \Longrightarrow 1+x \geq 1+x$", and this implication is obviously true, because its conclusion is true.

So $P(1)$ is true, and we are done with the base case.

Inductive step. We have to prove

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \quad (12.219)$$

Let n be an arbitrary natural number. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.

Then

$$x > 0 \Longrightarrow (1+x)^n \geq 1+nx\,. \quad (12.220)$$

We want to prove

$$x > 0 \Longrightarrow (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{12.221}$$

Assume $x > 0$.

Then it follows from (12.220) (by Rule $\Longrightarrow_{use}$) that

$$(1+x)^n \geq 1 + nx\,. \tag{12.222}$$

Multiplying both sides of (12.222) by $1 + x$ (which is possible because $1 + x > 0$), we get

$$(1+x)^{n+1} \geq (1+x)(1+nx)\,. \tag{12.223}$$

But

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

(The fact that $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$ follows because $nx^2 \geq 0$ and then, adding $1 + (n+1)x$ to both sides, we get $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$.)

So

$$(1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{12.224}$$

Since we proved (12.224) under the assumption that $x > 0$, it follows that

$$x > 0 \Longrightarrow (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{12.225}$$

That is, $P(n+1)$ holds.

Since we have proved $P(n+1)$ assuming $P(n)$, Rule $\Longrightarrow_{prove}$ allows us to conclude that $P(n) \Longrightarrow P(n+1)$.

So we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary $n \in \mathbb{N}$, Rule $\forall_{prove}$ allows us to conclude that (12.219) holds.

This completes the inductive step.

Since we have also proved $P(1)$, we can use the PMI to conclude that (12.218) holds, i.e., that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1+nx\Big)\,. \tag{12.226}$$

Since we have proved for an arbitrary real number x, we can conclude that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1+nx\Big)\,, \tag{12.227}$$

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

Problem 57. In the proof of Theorem 34, we translated the statement to be proved into formal language as Formula (12.217) and then followed the rules of logic, plus the PMI, to prove it.

Suppose instead that we had translated the statement of Theorem 34 in a different way, as

$$(\forall n \in \mathbb{N})(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{12.228}$$

1. ***Prove that this translation is equivalent to Formula (12.217)***, as a matter of pure logic. That is, prove that no matter what the 2-variable predicate $A(x, n)$ is, and what the sets S, T are, the formulas

$$(\forall x \in S)(\forall n \in T)A(x, n)$$

and

$$(\forall n \in T)(\forall x \in S)A(x, n)$$

are equivalent. (Two formulas U, V are equivalent if $U \Longleftrightarrow V$ is true.)

2. ***Write a different proof*** of Theorem 34, using the translation (12.228) instead of (12.217).

Problem 58. By looking carefully at the proof of Theorem 34, ***prove*** the following stronger result:

Theorem 35. *If $x \in \mathbb{R}$ and $x \geq -1$, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{12.229}$$

With a little bit more work, it is possible to prove a result stronger than Theorem 34:

Theorem 36. *If x is a nonnegative real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2\,. \tag{12.230}$$

Proof.

YOU DO THIS ONE.

HINT. Just repeat the proof of Theorem 34 up to the point when you multiply by $1+x$, and at that point keep the x^2 term. □

Problem 59. ***Prove*** Theorem 36. □

12.3.1 An application of Theorem 36: computing $\lim_{n\to\infty} \sqrt[n]{n}$

In this section we use the notion of "limit of a sequence". All you need to know about limits of seuences is the following sandwiching theorem": If $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$, and $\{c_n\}_{n=1}^{\infty}$, are sequences of real numbers such that $a_n \leq b_n \leq c_n$ for every $n \in \mathbb{N}$, and L is a real number such that

$$\lim_{n\to\infty} a_n = L \quad \text{and} \quad \lim_{n\to\infty} c_n = L\,,$$

then $\lim_{n\to\infty} b_n$.

Let us prove that

$$\lim_{n\to\infty} \sqrt[n]{n} = 1\,. \tag{12.231}$$

Define

$$\alpha_n = \sqrt[n]{n} - 1\,.$$

To prove (12.231), we have to prove that

$$\lim_{n\to\infty} \alpha_n = 0\,. \tag{12.232}$$

It is clear that $\alpha_n \geq 0$. (Reason: $\sqrt[n]{n} \geq 1$, because if $\sqrt[n]{n}$ was < 1, it would follow that $\left(\sqrt[n]{n}\right)^n < 1$, but $\left(\sqrt[n]{n}\right)^n = n$, and $n \geq 1$.)

Also, $1 + \alpha_n = \sqrt[n]{n}$, so

$$(1+\alpha_n)^n = n\,. \tag{12.233}$$

Using the inequality of Theorem 36, we get

$$(1+\alpha_n)^n \geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2\,. \tag{12.234}$$

So

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

Hence

$$n \geq \frac{n(n-1)}{2}\alpha_n^2\,,$$

so

$$1 \geq \frac{n-1}{2}\alpha_n^2\,,$$

and then

$$\alpha_n^2 \leq \frac{2}{n-1}\,,$$

so

$$\alpha_n \leq \sqrt{\frac{2}{n-1}}\,.$$

Hence the numbers α_n satisfy

$$0 \leq \alpha_n \leq \sqrt{\frac{2}{n-1}}\,.$$

So the α_n are 'sandwiched" between two sequences that converge to 0. Hence $\lim_{n\to\infty} \alpha_n = 0$ by the sandwiching theorem.

Hence (12.231 is proved.

12.4 Some formulas for sums

In this section we use the notation "$\sum_{k=1}^{n} a_k$" for "$a_1 + a_2 + \cdots + a_n$". (A precise definition of "$\sum_{k=1}^{n} a_k$", without using $\cdots$, is given in section 12.5.3 on page 342.)

Theorem 37. *If n is an arbitrary natural number, then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,. \tag{12.235}$$

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

Proof. Let $P(n)$ be the statement "$\sum_{k=1}^{n} = \frac{n(n+1)}{2}$".

We prove $(\forall n \in \mathbb{N})P(n)$ by induction.

Base step. $P(1)$ says "$1 = \frac{1(1+1)}{2}$", which is obviously true. So $P(1)$ is true.

Inductive step.

We prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

Let n be an arbitrary natural number.

Assume that $P(n)$ is true.

Then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Therefore

$$\begin{aligned}\sum_{k=1}^{n+1} k &= (\sum_{k=1}^{n} k) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left[\frac{n}{2} + 1\right] \\ &= (n+1) \times \frac{n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

So

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

That is, $P(n+1)$ holds.

We have proved $P(n+1)$ assuming $P(n)$. Hence $\boxed{P(n) \Longrightarrow P(n+1)}$.

We have preved $P(n) \Longrightarrow P(n+1)$ for an arbitrary natural number n. Therefore $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$, which completes the inductive step.
Hence, by the PMI, $(\forall n \in \mathbb{N})P(n)$, that is,

$$(\forall n \in \mathbb{N}) \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Q.E.D.

Using the same method, many other formulas for sums can be proved. Here is an exmaple of a rather remarkable one:

Theorem 38. *If n is a natural number, then*

$$\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2, \tag{12.236}$$

that is:

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Proof. **YOU DO THIS ONE.**

Problem 60.

1. ***Compute*** the sum $\sum_{k=1}^{n} k^3$ for $n = 1, 2, 3, 4, 5$ and 6.

2. ***Verify*** that in each case the sum you got is a perfect square (i.e., the square of an integer).

3. ***Prove*** Theorem 38. □

Problem 61.

1. ***Compute*** the sum $\sum_{k=1}^{n} k^2$ for $n = 1, 2, 3, 4, 5$ and 6.

2. ***Verify*** that in each case the sum you got agrees with the formula

$$\sum_{k=1}^{n} k^2 = \frac{n + 3n^2 + 2n^3}{6}\,. \tag{12.237}$$

3. ***Prove*** that Formula (12.237) holds for every natural number n. □

Problem 62.

1. ***Compute*** the sum $\sum_{k=1}^{n} k$ for $n = 1, 2, 3, 4, 5$ and 6.

2. ***Verify*** that in each case the sum you got agrees with the formula

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,. \tag{12.238}$$

3. ***Prove*** that Formula (12.238) holds for every natural number n. □

Problem 63.

1. ***Compute*** the sum $\sum_{k=1}^{n}(2k-1)$ for $n = 1, 2, 3, 4, 5$ and 6.

2. ***Verify*** that in each case the sum you got agrees with the formula

$$\sum_{k=1}^{n}(2k-1) = n^2\,. \tag{12.239}$$

3. ***Prove*** that Formula (12.239) holds for every natural number n. □

Problem 64. ***Figure out*** a formula for the sum

$$\sum_{k=1}^{n}(2k-1)^2\,, \tag{12.240}$$

and ***prove*** that your formula holds for every natural number n. □

Problem 65. ***Figure out*** a formula for the sum

$$\sum_{k=1}^{n}(4k+3)^3\,, \tag{12.241}$$

and ***prove*** that your formula holds for every natural number n. □

12.5 Inductive definitions

In an earlier set of lectures, we defined "x^2", for a real number x, to mean "$x.x$". And we can define "x^3" to mean "$(x.x).x$", or, if you prefer, "$x^2.x$". But how can we define "x^n" for an arbitrary natural number n? One possibility would be to write something like this

$$x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ times}}$$

Similarly, we would like to define the "factorial" $n!$ of a natural number n by the formula

$$n! = 1 \times 2 \times 3 \times \cdots \times n\,.$$

And we would like to define summations such as

$$1 + 2 + 3 + \cdots + n$$

or

$$1^2 + 2^2 + 3^2 + \cdots + n^2\,,$$

or products such that

$$2 \times 4 \times 6 \times 8 \times \cdots \times 200\,.$$

With this notation, if we want to talk about the product of the first 20 prime numbers, i.e., the number

$$2\times3\times5\times7\times11\times13\times17\times19\times23\times29\times31\times37\times41\times43\times47\times53\times59\times61\times67\times71\,,$$

we could write

$$2 \times 3 \times \cdots \times 71\,. \tag{12.242}$$

But this is very unclear. I do not know what "$\cdots$" means, precisely (and if you think you do, please tell me!). For example, in the expression (12.242), how on Earth are we supposed to know which numbers should go in place of the $\cdots$? Take a simple example of a similar situation: suppose I write

$$3 \times 5 \times 7 \times \cdots \times 71\,. \tag{12.243}$$

Is this supposed to be "the product of all odd numbers from 3 to 71", or "the product of all prime numbers from 3 to 71", or "the product of all the odd numbers from 3 to 71 that do not end in a 9", or what?

Next, let us look at another example: suppose I write

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots.$$

What is the next number, after 377? Well, if you have guessed the pattern, then you will probably guess that each number, after the first two, is the sum of the two preceding ones, so what comes after 377 is $233+377$, that is, 610. But, why couldn't the pattern be this:

- Start with 1, and then another 1.
- Then each number is obtained by adding the two preceding ones.
- Yo go on like this until you get to 377, and then you switch to a different rule: each number is obtained by adding 100 to the previous one.

This is a perfectly legitimate rule for generating a sequence of numbers, and if you use this rule then the numbers that come after 377 are 477, 577, and so on. If you say "that's not a true pattern", then I will ask you to tell me what you mean by "a true pattern", and I will

also ask "Why not? What do you mean by 'pattern'?". "Why is this not a true pattern?".

One last example. If I write

$$27, 82, 41, 124, 61, 184, 92, 46, \cdots$$

what comes next? I'll let you think about this one.

The fact is: in general, "$\cdots$" is meaningless. So in mathematics we just do not use it.

And, in any case, once we develop fully our way of writing all of mathematics formally (that is, with formulas and no words), the symbol "$\cdots$" will not be there in the list of symbols we can use. So we do not want to use "$\cdots$" at all.

What we are going to do instead is use ***inductive definitions***.

12.5.1 The inductive definition of powers of a real number

The way to define the power "x^n" correctly is by means of an inductive definition: we first define x^1 to be x, and then define x^{n+1} to be $x^n.x$, for every n. That is, we write:

Definition 16. ***(Inductive definition of positive integer powers of a real number)*** For all $a \in \mathbb{R}$,

we set

$$\begin{aligned} a^1 &= a\,, \\ a^{n+1} &= a^n.a \quad \text{for } n \in \mathbb{N}\,. \end{aligned}$$

We also set $a^0 = 1$. □

Using this definition, we can write down what a^n is for any n.

Suppose, for example, that we want to know what a^5 is. By the second line of our inductive definition of a^n,

$$a^5 = a^4.a.$$

This answers our question about a^5, in terms of a^4. And what is a^4? Again, using the second line of the inductive definition, we find

$$a^4 = a^3.a.$$

So

$$a^5 = ((a^3).a).a.$$

And what is a^3? Once again, we can use the second line of the inductive definition, and find

$$a^3 = a^2.a$$

So

$$a^5 = (((a^2).a).a).a.$$

One more step yields

$$a^2 = a^1.a\,,$$

so

$$a^5 = (((a^1.a).a).a).a.$$

And, finally, the first line of the inductive definition, tells us that $a^1 = a$, so we end up with

$$a^5 = (((a.a).a).a).a.$$

Furthermore, since multiplication of real numbers has the associative property, we can omit the parentheses and just write:

$$a^5 = a.a.a.a.a.$$

12.5.2 The inductive definition of the factorial

The "factorial" of a natural number n is supposed to be the product $1 \times 2 \times 3 \times \cdots \times n$. That is, the factorial of n is the product of all the natural numbers from 1 to n. Here is the inductive definition:

Definition 17. The factorial of a natural number n is the number $n!$ given by

$$1! \;=\; 1\,, \tag{12.244}$$

$$(n+1)! \;=\; n! \times (n+1) \quad \text{for } \; n \in \mathbb{N}\,. \tag{12.245}$$

In addition, we define

$$0! = 1\,,$$

so $n!$ is defined for every nonnegative integer n. □

Example 55. Let us compute 7! using the inductive definition. Using (12.245) we get $7! = 7 \times 6!$. Then using (12.245) again we get $6! = 6 \times 5!$, so $7! = 7 \times 6 \times 5!$. Continuing in the same way we get $5! = 5 \times 4!$, so $7! = 7\times6\times5\times4!$, and then $4! = 4\times3!$, so $7! = 7\times6\times5\times4\times3!$. Then $3! = 3 \times 2!$, so $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2!$. And $2! = 2 \times 1!$, so $7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1!$. Finally, (12.244) tells us that $1! = 1$, so we end up with

$$7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1\,,$$

which is of course what 7! is supposed to be. □

12.5.3 The inductive definition of summation.

Definition 18. Suppose we have a natural number n, and a list

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

of n real numbers. We define the <u>sum</u> (or <u>summation</u>) of the list $\mathbf{a}$ (also called the sum of the a_j for j from 1 to

n) to be the number $\sum_{j=1}^{n} a_j$ determined as follows:

$$\sum_{j=1}^{1} a_j \;=\; a_1\,,$$
$$\sum_{j=1}^{n+1} a_j \;=\; \Big(\sum_{j=1}^{n} a_j\Big) + a_{n+1} \quad \text{for} \quad n \in \mathbb{N}\,.$$

And we also define $\sum_{j=1}^{0} a_j = 0$.

Example 56. Let us compute $\sum_{j=1}^{5} j^2$. We have

$$\begin{aligned}
\sum_{j=1}^{5} j^2 &= \Big(\sum_{j=1}^{4} j^2\Big) + 5^2 \\
&= \left(\Big(\sum_{j=1}^{3} j^2\Big) + 4^2\right) + 5^2 \\
&= \Big(\sum_{j=1}^{3} j^2\Big) + 4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{2} j^2\Big) + 3^+4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{1} j^2\Big) + 2^2 + 3^+4^2 + 5^2 \\
&= 1^2 + 2^2 + 3^+4^2 + 5^2 \\
&= 1 + 4 + 9 + 16 + 25 \\
&= 55\,.
\end{aligned}$$

12.5.4 Inductive definition of product.

Definition 19. For a natural number n, and a list $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ of n real numbers, we define the product of the a_j for j from 1 to n to be the number $\prod_{j=1}^{n} a_j$

determined as follows:

$$\prod_{j=1}^{1} a_j \;=\; a_1\,,$$
$$\prod_{j=1}^{n+1} a_j \;=\; \Big(\prod_{j=1}^{n} a_j\Big) \times a_{n+1} \quad \text{for} \quad n \in \mathbb{N}\,.$$

And we also define $\prod_{j=1}^{0} a_j = 1$.

Example 57. If you compare the inductive definition of a product with the inductive definition of the factorial, you can easily see that

$$n! = \prod_{j=1}^{n} j \qquad \text{for every } \; n \in \mathbb{N}\,.$$

12.5.5 A simple example of a proof by induction using inductive definitions

Here is a simple example of a proof of an inequality by induction. Notice how the proof uses the notion of "n-th power" of a real number exactly in the form of the inductive definition.

Proposition 1. *For all $n \in \mathbb{N}$, $n < 2^n$.*

Proof.
Let $P(n)$ be the statement "$n < 2^n$".

We are going to prove

$$(\forall n \in \mathbb{N})P(n) \tag{12.246}$$

by induction

Basis step. $P(1)$ is the statement "$1 < 2^1$". But $2^1 = 2$ by the inductive definition, so $P(1)$ says "$1 < 2$" which is clearly true. So $\boxed{P(1)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{12.247}$$

Let n be an arbitrary natural number.

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.

Then $n < 2^n$.

So $2n < 2^n \times 2 = 2^{n+1}$.

But $1 \leq n$, because n is a natural number. (Precisely: if $n = 1$ then $1 = n$, so $1 \leq n$. And if $n \neq 1$ then ny Basic Fact BFZ9, $n - 1 \in \mathbb{N}$, so $1 < n$, and then $1 \leq n$.)

So $n + 1 \leq n + n$, i.e., $n + 1 \leq 2n$.

Therefore $n + 1 < 2^{n+1}$.

So $P(n+1)$ is true.

Since we have proved $P(n+1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n+1)$.

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary n, it follows that (12.247) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (12.246 holds, that is, that $(\forall n \in \mathbb{N}) n < 2^n$. **Q.E.D.**

12.5.6 Another simple example of a proof by induction using inductive definitions

Here is a slightly more involved example of a proof of an inequality by induction. Notice how the proof uses the notion of "n-th power" of a real number and the notion of "factorial" exactly in the form of their inductive definitions.

We would like to prove the inequality "$2^n < n!$". This, however, isn't true for every natural number n. (For example, it is not true if $n = 1$ or $n = 2$ or $n = 3$.) But it is true for $n \geq 4$.

Proposition 2 *For all $n \in \mathbb{N}$, if $n \geq 4$ then $2^n < n!$.*

Proof.
Let $P(n)$ be the statement "$2^n < n!$".
We are going to prove

$$(\forall n \in \mathbb{N})(n \geq 4 \Longrightarrow P(n)) \,. \tag{12.248}$$

by induction. And we will start the induction at 4 rather than 1.

Basis step. $P(4)$ is the statement "$2^4 < 4!$". But $2^4 = 16$, and $4! = 24$. So $P(1)$ says "$16 < 24$', which is clearly true. So $\boxed{P(4)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)\,. \quad (12.249)$$

Let n be an arbitrary natural number such that $n \geq 4$..

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.
Then $2^n < n!$.
So $2 \times 2^n < 2n!$.
But $2 \times 2^n = 2^{n+1}$.
Hence $2^{n+1} < 2n!$.
Also, $2 < n + 1$.
So $2n! < (n + 1)n!$.
But $(n + 1)n! = (n + 1)!$ by the inductive definitionof "factorial".
Therefore $2n! < (n + 1)!$.
So, finally, $2^{n+1} < (n + 1)!$.
So $P(n + 1)$ is true.

Since we have proved $P(n + 1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n + 1)$.

Since we have proved $P(n) \implies P(n+1)$ for arbitrary n, it follows that (12.249) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (12.248) holds, that is, that $(\forall n \in \mathbb{N})\Big(n \geq 4 \implies (2^n < n!)\Big)$. **Q.E.D.**

12.5.7 Another simple example: divisibility by 3, 9, and 11

Let us prove

Theorem 39. *If a, b are arbitrary integers, then for every nonnegative integer*[78] *n the integer $a^n - b^n$ is divisible by $a - b$.*

Example 58. Here are some examples of what the theorem says:

1. Take $a = 8$, $b = 3$. Then the theorem says that $8^n - 3^n$ is divisible by 5 for every n. (And you can check this. For example, $8^3 = 512$, and $3^3 = 27$, so $8^3 - 3^3 = 512 - 27 = 495$, which is indeed divisible by 5.

2. Take $a = 10$, $b = 1$. Then the theorem says that $10^n - 1$ is divisible by 9, and you can check this. (For example, $10^1 - 1 = 9$, $10^2 - 1 = 99$, $10^3 - 1 = 999$, $10^4 - 1 = 9,999$, and so on.)

[78] Recall that the ***nonnegative integers*** are the natural numbers as well as zero.

3. Take $a = 10$, $b = -1$. Then the theorem says that $10^n - (-1)^n$ is divisible by 11. And you can check this: $10-(-1) = 11$, $10^2-(-1)^2 = 99$, $10^3-(-1)^3 = 1,001$, $10^4 - (-1)^4 9,999$, and all these are divisible by 11. □

Proof.

Let a, b be arbitrary integers.

We will prove that

$$(\forall n \in \mathbb{N}) a - b | a^n - b^n \,, \tag{12.250}$$

and also that "$a - b | a^n - b^n$" is true for $n = 0$.

First we prove (12.250) by induction.

Let $P(n)$ be the statement[79] "$a - b$ divides $a^n - b^n$".

Basis Step. $P(1)$ says "$a - b$ divides $a - b$", which is obviously true.

This completes the basis step.

Inductive Step. We want to rpove

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1)) \,. \tag{12.251}$$

[79] We do not have to worry about the quesion "who are a and b?", because we have fixed a and b earlier. They are fixed integers. Arbitrary, but fixed.

Let n be an arbitrary natural number.

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.

Then $a - b$ divides $a^n - b^n$.

So we may pick an integer k such that

$$a^n - b^n = (a-b)k\,. \tag{12.252}$$

Then

$$\begin{aligned} a^{n+1} - b^{n+1} &= a^{n+1} - ab^n + ab^n - b^{n+1} \\ &= aa^n - ab^n + ab^n - bb^n \\ &= a(a^n - b^n) + (a-b)b^n \\ &= a(a-b)k + (a-b)b^n \\ &= (a-b)\big(ak + b^n\big)\,. \end{aligned}$$

Hence $a^{n+1} - b^{n+1} = (a-b)\big(ak + b^n\big)$.

Clearly, $ak + b^n$ is an integer[80].

Therefore $a - b$ divides $a^{n+1} - b^{n+1}$.

So $P(n+1)$ is true.

Since we have proved $P(n+1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n+1)$.

[80]Strictly speaking even a stupid, trivial, obvious statement like this needs proof. On the other hand, it is so obvous that nobody would actually insult the reader's intelligence by putting in the proof. On the other hand, at this point we are just getting started with proofs, so you shousl knwo how to prove this. So I am going to ask you to write down the proof, as a homework problem. ***Sorry!***.

Since we have proved $P(n) \implies P(n+1)$ for arbitrary n, it follows that (12.251) holds.

So we have completed the basis step and the inductive step, and then the PMI tells us that (12.250 holds, that is, that if n is an arbitrary natural number, then $a - b$ divides $a^n - b^n$.

This almost completes our proof. But there is a minor missing detail: we also have to prove that $a - b$ divides $a^n - b^n$ when $n = 0$.

But if $n = 0$ then $a^n - b^n$ is equal to zero, because the inductive definition of the powers tells us that $a^0 = 1$ and $b^0 = 1$.

And 0 is divisible by any integer.

So $a - b$ divides $a^n - b^n$ also when $n = 0$.

We have now proved that $a - b | a^n - b^n$ for every nonnegative integer n.

And this has been proved for arbitrary integers a, b. So our proof is complete. **Q.E.D.**

Problem 66.

1. ***Provide a detailed proof*** of the step that we skipped in the proof of Theorem 39, namely, that

$ak + b^n$ is an integer. (This will require proving that if $b \in \mathbb{Z}$ then $b^n \in \mathbb{Z}$ for every nonnegative integer n, and the only way to do that is by induction, using the inductive definition of the powers.)

2. ***Provide an alternative proof*** of Theorem 39, in which you do not treat separately the cases $n \in \mathbb{N}$ and $n = 0$, but do the whole thing in one swoop, using the PMI starting at 0 rather than at 1.

3. ***Explain*** how you would answer the following objection that somebody studying these notes might raise: *In the theorem, you do not assume that $a \neq b$, and you talk about "divisibility by $a - b$". But if $a = b$ then $a - b$ is zero, and we cannot divide by zero, so how come you allow a to be equal to b? How can you say that "0 is divisible by 0", given that $\frac{0}{0}$ is not defined?* □

Problem 67. One of the consequences of Theorem 39 is that $10^n - 1$ is divisible by 9 for each nonnegative integer n. So, for example, if you look at the number 438, and let $s = 4 + 3 + 8$, so $s = 15$, it follows that $438 - s$ is

divisible by 9, because:

$$\begin{aligned} & 438 - s \\ &= 4 \times 100 + 3 \times 10 + 4 \times 1 - (4 + 3 + 8) \\ &= 4 \times 10^2 - 4 + 3 \times 10 - 3 + 4 \times 1 - 1 \\ &= 4 \times (10^2 - 1) + 3 \times (10 - 1) + 4 \times (1 - 1)\,, \end{aligned}$$

which is clearly divisible by 9.

1. ***Explain*** how this fact leads to the following two divisibility criteria:

   Criterion for divisibilitly by 9***:*** A natural number n is divisible by 9 if and only if the sum of its decimal figures is divisible by 9. (For example: $572,265$ is divisible by 9 because $5+7+2+2+6+5 = 27$, which is divisible by 9. And $772,265$ is not divisible by 9 because $7+7+2+2+6+5 = 29$, which is not divisible by 9.)

   Criterion for divisibilitly by 3***:*** A natural number n is divisible by 3 if and only if the sum of its decimal figures is divisible by 3. (For example: $572,265$ is divisible by 3 because $5+7+2+2+6+5 = 27$, which is divisible by 3. And $772,265$ is not divisible by 3 because $7+7+2+2+6+5 = 29$, which is not divisible by 3.)

2. Explain, in a similar way, how the fact that $10^n - (-1)^n$ is divisible by 11 leads to the following divisibility criterion:

   Criterion for divisibilitly by 11***:*** A natural number n is divisible by 11 if and only if the alternating sum[81] of its decimal figures is divisible by 11. (For example: $572,473$ is divisible by 11 because $5 - 7 + 2 - 4 + 7 - 3 = 0$, which is divisible by 11. And $772,463$ is not divisible by 11 because $7 - 7 + 2 - 4 + 6 - 3 = 1$, which is not divisible by 11.) □

12.5.8 Some problems

Problem 68. ***Prove***, using the inductive definition of the powers a^n, that

1. $(\forall a \in \mathbb{R})(\forall b \in \mathbb{R})(\forall n \in \mathbb{N})(ab)^n = a^n b^n$,
2. $(\forall a \in \mathbb{R})(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})a^{m+n} = a^m a^n$. □

Problem 69. ***Prove***, using the inductive definition of summation, that if $n \in \mathbb{N}$ and $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$, are finite lists of natural numbers of length

[81] That is, the sum with alternating signs: first figure minus second figureplus third figure minus fourth figure, etc, etc.

n, then

$$\sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k = \sum_{k=1}^{n} (a_k + b_k) \,. \tag{12.253}$$

13 Other forms of induction

13.1 Induction with a different starting point (sometimes called "generalized induction")

The PMI says that, if a property is true of 1, and is passed on to the right, so each natural number n passes it on to its successor $n+1$, then the property will hold of all the numbers that we reach by counting starting at 1.

It is clear that the same thing should be true if we start counting at some other starting point s_*, that is, some other integer such as, for example, 3, or 7, or 0, or -5, or -372. The general result is the following rather trivial theorem:

THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH A GENERAL STARTING POINT

Theorem 40. *Let $P(n)$ be a statement about a variable integer n. Suppose we fix an integer s_*. Let $\mathbb{Z}_{\geq s_*}$ denote the set of all integers n such that $n \geq s_*$. Suppose, furthermore, that*

I. $P(s_*)$ is true.

II. Any time $P(n)$ is true for one particular $n \in \mathbb{Z}_{\geq s_*}$, it follows that $P(n+1)$ is true.

Then $P(n)$ is true for every integer n belonging to $\mathbb{Z}_{s_*}$.

And we can say the same thing in more formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH A GENERAL STARTING POINT (FORMAL LANGUAGE VERSION)

Theorem 40. Let $P(n)$ be a statement about a variable integer n. Suppose we fix an integer s_*. Let $\mathbb{Z}_{\geq s_*}$ denote the set of all integers n such that $n \geq s_*$. Suppose, furthermore, that

$$P(s_*) \tag{13.254}$$

and

$$(\forall n \in \mathbb{Z}_{\geq s_*})\big(P(n) \Longrightarrow P(n+1)\big)\,. \tag{13.255}$$

Then

$$(\forall n \in \mathbb{Z}_{\geq s_*})P(n)\,. \tag{13.256}$$

And we can say the same thing in even more formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION
WITH A GENERAL STARTING POINT
(VERY FORMAL LANGUAGE VERSION)

Theorem 40. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$, and let

$$\mathbb{Z}_{\geq s_*} = \{n \in \mathbb{Z} : n \geq s_*\}\,. \tag{13.257}$$

Then

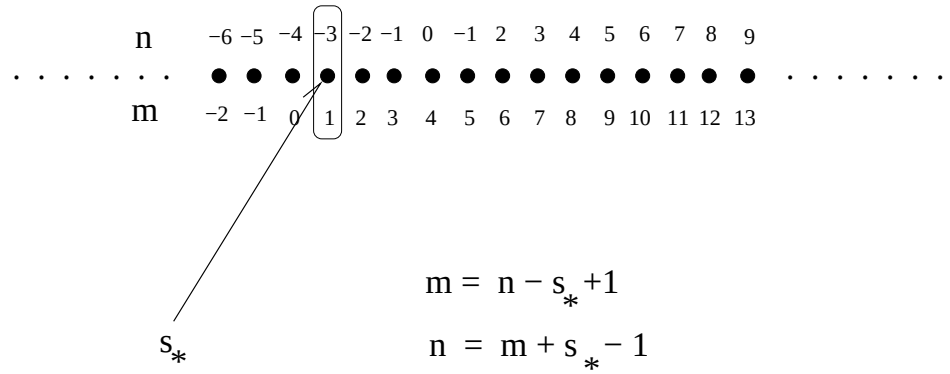
$$\Big(P(s_*) \wedge (\forall n \in \mathbb{Z}_{s_*})\big(P(n) \Longrightarrow P(n+1)\big)\Big) \Longrightarrow (\forall n \in \mathbb{Z}_{s_*})P(n)\,. \tag{13.258}$$

Proof of Theorem 40.

Assume that $P(n)$ is a 1-variable predicate and s_* is an arbitrary integer. We want to prove that if (13.254) and (13.255) hold, then (13.256) holds.

So we assume that (13.254) and (13.255) hold, and we try to prove that (13.256) holds.

We do the proof by "changing coordinates". That is, we relabel the integers so that s_* becomes 1, $s_* + 1$ becomes 2, and so on.



Changing coordinates on $\mathbb{Z}$ so that
$n = s_*$ becomes $m = 1$

(In the picture, s_* is -3.)

Precisely, we introduce a new variable m related to n by

$$m = n + 1 - s_* \,. \tag{13.259}$$

(That is: $n = s_*$ corresponds to $m = 1$, $n = s_* + 1$ corresponds to $m = 2$, and, in general, $n = s_* + k$ corresponds to $m = k$.)

We can express n in terms of m as follows:

$$n = m + s_* - 1 \,. \tag{13.260}$$

We let $Q(m)$ be $P(n)$ expressed in terms of m. That is, we let $Q(m)$ stand for $P(m + s_* - 1)$. Then $Q(1)$ is $P(s_*)$, $Q(2)$ is $P(s_* + 1)$, $Q(3)$ is $P(s_* + 2)$, and so on.

We want to prove that $P(s_*)$, $P(s_* + 1)$, $P(s_* + 2)$, ..., are all true. But this amounts to proving that $Q(1)$, $Q(2)$, $Q(3)$, ... are true, i.e. that $(\forall m \in \mathbb{N})Q(m)$.

We prove this by induction. $Q(1)$ is true because $Q(1)$ is the same as $P(s_*)$, which we are assuming is true.

And $Q(m) \implies Q(m+1)$ is true for every $m \in \mathbb{N}$, because "$Q(m) \implies Q(m+1)$" is equivalent to "$P(m + s_* - 1) \implies P(m + s_*)$", which is also true because $m + s_* - 1$ is to the right of s_*, so $P(m + s_* - 1)$ implies that the successor $m + s_*$ also has property P.

So $Q(m)$ satisfies all the conditions of the ordinary PMI, and we can conclude that $Q(m)$ is true for every $m \in \mathbb{N}$. And this says that $P(m + s_* - 1)$ is true for all $m \in \mathbb{N}$. Hence $P(n)$ is true for all n such that $n = m + s_* - 1$ for some $m \in \mathbb{N}$. But "$n = m + s_* - 1$ for some $m \in \mathbb{N}$" is equivalent to "$n \geq s_*$"

Hence $P(n)$ is true for all $n \in \mathbb{Z}_{s_*}$, and our proof is complete. **Q.E.D.**

Remark 10. Theorem 40 is a generalization of the PMI in the following precise sense: according to our definition, the set $\mathbb{Z}_{\geq 1}$ is precisely $\mathbb{N}$. So Theorem 40, if we take s_* to be 1, is exactly the PMI. □

Example 59. Let us prove the following:

Theorem 41. *If n is an integer such that $n \geq 4$, then*

$2^n < n!$.

Proof. We want to prove that

$$(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow 2^n < n!)\,. \tag{13.261}$$

Let $P(n)$ be the predicate "$2^n < n!$".

We want to prove that $(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow P(n))$.

We are going to prove this by induction, using the PMI with a general starting point.

And we are going to take the starting point s_* to be 4.

Basis step:

We want to prove $P(4)$.
$P(4)$ says "$2^4 < 4!$".
And $2^4 = 16$, $4! = 24$, so $2^4 < 4!$.
Therefore $\boxed{P(4) \text{ is true}}$

Inductive step:

We want to prove that

$$(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big)\,. \tag{13.262}$$

Let $n \in \mathbb{Z}$ be arbitrary.
We want to prove that

$$n \geq 4 \Longrightarrow (P(b) \Longrightarrow P(n+1))\,. \tag{13.263}$$

Assume that $n \geq 4$. We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.

The inductive hypothesis $P(n)$ tells us that $2^n < n!$.
Then

$$2^{n+1} < 2n! \,. \tag{13.264}$$

But $2 \leq n+1$, so $2n! \leq (n+1)n! = (n+1)!$.

Then $2^{n+1} < (n+1)!$.
So $\boxed{P(n+1) \text{ holds}}$.

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$ (Rule $\Longrightarrow_{prove}$).

So $\boxed{n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))}$ (Rule $\Longrightarrow_{prove}$).

Hence $\boxed{(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)}$ (by Rule $\forall_{use}$).

This completes the inductive step.

Since we have proved that

$$\boxed{P(4) \wedge (\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)},$$

it follows from the PMI with general starting point that $(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow P(n))$, that is,

$\boxed{(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow 2^n < n!)}$. **Q.E.D.**

13.2 Induction going forward and backward

The PMI says that, if a property P is true of 1, and is passed on to the right, so each natural number n passes it on to its successor $n + 1$, then the property will hold of all the numbers that we reach by counting starting at 1. And the "generalized" form says that the same is true for integers if you start at any integer s_*.

It is clear that if in addition to being passed on to the right property P is also passed on to the left, (that is, if the implication $P(n + 1) \implies P(n)$ holds for every $n \in \mathbb{Z}$), then $P(n)$ will be true for every integer n.

INDUCTION GOING FORWARD AND BACKWARD

Theorem 42. *Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that*

I. $P(s_*)$ is true.

II. Any time $P(n)$ is true for one particular integer n, it follows that $P(n+1)$ is true.

III. Any time $P(n+1)$ is true for one particular integer n, it follows that $P(n)$ is true.

Then $P(n)$ is true for every integer n.

And we can say the same thing in more formal language:

INDUCTION GOING FORWARD AND BACKWARD

(FORMAL LANGUAGE VERSION)

Theorem 42. Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that

$$P(s_*) \tag{13.265}$$

and

$$(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)\,. \tag{13.266}$$

Then

$$(\forall n \in \mathbb{Z})P(n)\,. \tag{13.267}$$

And we can say the same thing in even more formal language:

INDUCTION GOING FORWARD AND BACKWARD

(VERY FORMAL LANGUAGE VERSION)

Theorem 42. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$. Then

$$\Big(P(s_*) \wedge (\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)\Big) \implies (\forall n \in \mathbb{Z})P(n)\,. \tag{13.268}$$

Problem 70. ***Prove*** Theorem 42. □

13.3 Examples of proofs using induction going forward and backward

13.3.1 A very simple example

Here is a simple example of a proof using indcuction going forwad and backward.

First let us review a fact that we already know:

(D3) *if* $n \in \mathbb{Z}$*, then* $n^3 - n$ *is divisible by* 3.

(This is easy to prove: we have

$$n^3 - n = n(n^2 - 1) = n(n-1)(n+1) = (n-1)n(n+1)\,,$$

so $n^3 - n$ is the product of three consecutive integers. One of these integers must be divisible by 3, so the product is divisible by 3. Actually, it is also true that $n^3 - n$ must be even, that is, divisible by 2, and then, since 2 and 3 are coprime, it follows that a stronger result is true: $n^3 - n$ *is divisible by* 6.)

In view of (D3), we may conjecture that a similar statement may be true for 4 instead of 3:

(D4) *if* $n \in \mathbb{Z}$*, then* $n^4 - n$ *is divisible by* 4.

This, however, is not true. (Proof: (D4) is a universal sentence; it says that for all integers n 4 divides $n^3 -$

n. To prove that (D4) is not true, it suffices to give a counterexample. Let us just take $n = 2$. Then $2^4 = 16$, so $2^4 - 2 = 14$, which is not divisible by 4.)

How about (D5)? This one turns out to be true, and we can prove it using induction going backward and forward.

Theorem 43. *If n is an integer, then $n^5 - n$ is divisible by 5.*

Proof. We are going to use the binomial formula for the fifth power of a sum:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\,, \tag{13.269}$$

which is valid for all integers a, b. (And also for real numbers or, more generally, members of any commutative ring with identity.)

Using this formula we can write, for $n \in \mathbb{Z}$,

$$\begin{aligned} (n+1)^5 &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 \\ (n+1)^5 - n^5 - 1 &= 5n^4 + 10n^3 + 10n^2 + 5n \\ &= 5(n^4 + 2n^3 + 2n^2 + n)\,, \end{aligned}$$

so $(n+1)^5 - n^5 - 1$ is divisible by 5.

But

$$(n+1)^5 - (n+1) = ((n+1)^5 - n^5 - 1) + n^5 - n\,.$$

This implies that, for all $n \in \mathbb{Z}$,

$$5|(n+1)^5 - (n+1) \iff 5|n^5 - n\,. \qquad (13.270)$$

In other words, the predicate "5 divides $n^5 - n$" is passed on forward (from n to $n+1$) and backward (from $n+1$ to n). This means that we are in a perfect situation to do induction going forward and backward.

Let $P(n)$ be the predicate "5 divides $n^5 - n$". We will prove the statement "$(\forall n \in \mathbb{Z})P(n)$" by induction going forward and backward. We choose the starting point s_0 to be 0.

Basis step. $P(0)$ says "5 divides 0", which is true because every integer divides 0. So $\boxed{P(0) \text{ is true}}$.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{Z})\Big(P(n) \iff P(n+1)\Big)\,.$$

But Formula (13.270) says precisely that for every $n \in \mathbb{Z}$ $P(n) \iff P(n+1)$

This completes the inductive step. **Q.E.D.**

Problem 71. ***Prove or disprove*** each of the following statements:

1. If n is an integer, then $n^6 - n$ is divisible by 6.
2. If n is an integer, then $n^7 - n$ is divisible by 7.

3. If n is an integer, then $n^8 - n$ is divisible by 8.
4. If n is an integer, then $n^9 - n$ is divisible by 9.
5. If n is an integer, then $n^{10} - n$ is divisible by 10.
6. If n is an integer, then $n^{11} - n$ is divisible by 11.

You may find the following binomial formulas useful:

$$\begin{aligned}(a+b)^7 &= a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 \\ &\quad +21a^2b^5 + 7ab^6 + b^7 \\ (a+b)^{11} &= a^{11} + 11a^{10}b + 55a^9b^2 + 165a^8b^3 + 330a^7b^4 \\ &\quad +462a^6b^4 + 462a^5b^6 + 330s^4b^7 \\ &\quad +165a^3b^8 + 55a^2b^9 + 11ab^{10} + b^{11}\,.\end{aligned}$$

Remark 11. If you have done problem 71 you will have discovered the cases $p = 3, 6, 7$ and 11 of ***Fermat's little theorem:*** *If p is a prime numbet and n is an arbitrary integer then $n^p - n$ is divisible by p.* (And the case $p = 2$ is trivial, because if $n \in \mathbb{Z}$ then $n^2 - n$ is always even.) □

13.3.2 Divisibility properties of products of consecutive integers

We now discuss several theorems on divisibility of a product of consecutive integers:

1. It is easy to prove that a product $n(n+1)$ of two consecutive integers must be divisible by 2.

2. We will then look at the product $n(n+1)(n+2)$ of three consecutive integers, and prove that such a product is divisible by 6.

3. Then we will look at the product $n(n+1)(n+2)(n+3)$ of four consecutive integers, and prove that such a product is divisible by 24.

4. Since $2 = 2 \times 1 = 2!$, $6 = 3 \times 2 \times 1 = 3!$, and $24 = 4 \times 3 \times 2 \times 1 = 4!$, this will clearly be a good indication that there is a general pattern, namely, that for every natural number k the product of k consecutive integers is divisible by $k!$. (Recall the inductive definition of the factorial $n!$ of a natural number: $1! = 1$ and $(n+1)! = n! \times (n+1)$ for $n \in \mathbb{N}$.) In other words, the general result should be that

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z}) k! \,\Big|\, n(n+1)(n+2)\cdots(n+k-1) \tag{13.271}$$

or, using a notation without the mysterious and incomprehensible symbol "$\cdots$":

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z}) k! \,\Big|\, \prod_{j=1}^{k}(n+j-1) \tag{13.272}$$

5. And we will indeed prove (13.272) eventually, but the proof will be little but harder than other proofs we

have done so far, because it will use a ***double induction***: we will prove (13.272) by induction with respect to k, and for each k we will need induction with respect to n.

First let us start with the trivial result for $k = 2$:

Theorem 44 *If n is an integer, then $n(n+1)$ is even, i.e., divisible by 2. That is,*

$$(\forall n \in \mathbb{N})2|n(n+1)\,. \tag{13.273}$$

Proof. As I said earlier, this result is trivial.

Let n be an arbitrary integer.

We know that n is either even or odd.

If n is even then $\boxed{n(n+1) \text{ is even}}$.

And if n is odd then $n+1$ is even so $\boxed{n(n+1) \text{ is even}}$.

So we have proved that $n(n+1)$ is even in both cases, when n is even and when n is odd. And we know that one of these two cases must occur. So $\boxed{\boxed{n(n+1) \text{ is even}}}$.

So we have proved that $n(n+1)$ is even for an arbitrary integer n.

Hence $\boxed{\boxed{\boxed{(\forall n \in \mathbb{Z})n(n+1) \text{ is even}}}}$. **Q.E.D.**

We now want to prove that the product $n(n+1)(n+2)$ of three consecutive integers is divisible by 6. And the strategy is going to be to prove the result by induction going forward and backward.

Here is the result:

Theorem 45. *If n is an integer, then $n(n+1)(n+2)$ is divisible by 6. That is,*

$$(\forall n \in \mathbb{Z})6|n(n+1)(n+2)\,. \tag{13.274}$$

Proof. Let $P(n)$ be the statement "$6|n(n+1)(n+2)$"

We prove that $(\forall n \in \mathbb{Z})P(n)$ by induction going forward and backward.

Basis step. If $n = 0$, then $n(n+1)(n+2) = 0$, so $P(0)$ is the statement "$6|0$", which is obviously true. So $\boxed{P(0)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)\,. \tag{13.275}$$

Let n be an arbitrary integer.

We want to prove that $P(n) \iff P(n+1)$.

We already know that $n(n+1)$ is even. So we can write

$$n(n+1) = 2k\,, \quad k \in \mathbb{Z}\,.$$

Then

$$\begin{aligned}(n+1)(n+2)(n+3) &= (n+3)(n+1)(n+2)\\ &= n(n+1)(n+2)\\ &\quad +3(n+1)(n+2)\\ &= n(n+1)(n+2)+3\times 2k\\ &= n(n+1)(n+2)+6k\,.\end{aligned}$$

If 6 divides $n(n+1)(n+2)$, then $(n+1)(n+2)(n+3)$ is the sum of two integers that are divisible by 6. So 6 divides $(n+1)(n+2)(n+3)$.

If 6 divides $(n+1)(n+2)(n+3)$, then $n(n+1)(n+2)$ is the difference of two integers that are divisible by 6. So 6 divides $n(n+1)(n+2)$.

We have shown that

$$6|(n+1)(n+2)(n+3) \Longleftrightarrow 6|n(n+1)(n+2)\,,$$

i.e., that $P(n) \Longleftrightarrow P(n+1)$.

Since we have shown that $P(n) \Longleftrightarrow P(n+1)$ for an arbitrary integer n, it follows that

$$(\forall n \in \mathbb{Z})\big(P(n) \Longleftrightarrow P(n+1)\big)\,,$$

and this completes the inductive step.

It the follows from Theorem 42 that $P(n)$ is true for all integers n. That is, (13.274) holds. **Q.E.D.**

In the proof of Theorem 45 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)$ is divisible by 2. Similarly, to prove that $(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)$, the proof should use the result that $(\forall n \in \mathbb{Z})6|n(n+1)(n+2)$.

Similar results can be proved for the products of four and five consecutive integers.

Theorem 46. *If n is an integer, then the product $n(n+1)(n+2)(n+3)$ is divisible by 24. That is,*

$$(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)\,. \qquad (13.276)$$

Proof. **YOU DO THIS ONE.**

In the proof of Theorem 45 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)$ is divisible by 2.

Similarly, to prove that

$$(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)\,,$$

the proof should use the result of Theorem 45, that is, that $(\forall n \in \mathbb{Z})6|n(n+1)(n+2)$.

Problem 72. ***Prove*** Theorem 46. You are ***not*** allowed to use Theorem 48.

NOTE: Theorem 46 is a special case of Theorem 48, for $k = 4$. But I want you to prove Theorem 46 directly, without using Theorem 48. □

Theorem 47. *If n is an integer, then the product $n(n+1)(n+2)(n+3)(n+4)$ is divisible by 120. That is,*

$$(\forall n \in \mathbb{Z})120|n(n+1)(n+2)(n+3)(n+4)\,. \quad (13.277)$$

Proof. **YOU DO THIS ONE.**

In the proof of Theorem 46 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)(n+2)$ is divisible by 6. Similarly, to prove that $(\forall n \in \mathbb{Z})120|n(n+1)(n+2)(n+3)(n+4)$, the proof should use the result that

$$(\forall n \in \mathbb{Z})24|n(n+1)(n+2)\,.$$

Problem 73. ***Prove*** Theorem 47. You are ***not*** allowed to use Theorem 48.

NOTE: Theorem 47 is a special case of Theorem 48, for $k = 5$. But I want you to prove Theorem 47 directly, without using Theorem 48. □

What we have done so far is clearly the beginning of a proof by induction. We have proved the following:

(*) *for $k = 1, 2, 3, 4, 5$ the product of k consecurive integers is divisible by $k!$.*

This makes it natural to make the following

Conjecture. *For every natural number k the product of k consecutive integers is divisible by $k!$.*

But, of course, knowing that something is true for a few values of k in no way proves that it is true for all k, If we want to be sure that a statement about k is true for all k, we have to prove it.

So let us prove it.

Theorem 48. *If k is a natural number then every product of k consecutive integers is divisible by $k!$.*

Proof. As usual, our first task is to rewrite the statement we want to prove in precise formal language. And for that purpose we need to write a formula for the product of k consecutive integers.

If we start with an integer n, then the k consecutive integers starting at n are n, $n+1$, $n+2$, ..., up to $n+k-1$. And the product of these k integers is $\prod_{j=1}^{k}(n+j-1)$. (For example, for $k=3$, the product is $n(n+1)(n+2)$. The first factor is n, that is $n+j-1$ with $j=1$, and the last factor is $n+2$, that is, $n+j-1$ with $j=3$.)

Let us call this product $a_{n,k}$, so

$$a_{n,k} = \prod_{j=1}^{k}(n+j-1)\,, \tag{13.278}$$

or, if you prefer,

$$a_{n,k} = n \times (n+1) \times (n+2) \times \cdots \times (n+k-1)\,. \quad (13.279)$$

So, for example,

$$\begin{aligned} a_{2,3} &= 2 \times 3 \times 4\,, \\ a_{-5,7} &= (-5) \times (-4) \times (-3) \times (-2) \times (-1) \times 0 \times 1\,, \\ a_{4,9} &= 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12\,. \end{aligned}$$

Then what we want to prove is the following statement:

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\; k! \,\Big|\, a_{n,k}\,. \quad (13.280)$$

In order to prove this, we will use induction.

We let $P(k)$ be the predicate "for every integer n, the product of k consecutive integers starting with n is divisible by $k!$". That, $P(k)$ is the predicate

$$(\forall n \in \mathbb{Z})\; k! \,\Big|\, a_{n,k}\,. \quad (13.281)$$

Basis step of the induction. We want to prove that $P(1)$ is true. And $P(1)$ is true, for trivial reasons: $P(1)$ says "$(\forall n \in \mathbb{Z})1! \,\Big|\, a_{n,1}$", i.e., "$(\forall n \in \mathbb{Z})1 \,\Big|\, n$", and this is true because every integer is divisible by 1. So we have proved $\boxed{P(1)}$.

Inductive step. We want to prove that

$$(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)\,. \quad (13.282)$$

Let $k \in \mathbb{N}$ be arbitrary. We want to prove that

$$P(k) \Longrightarrow P(k+1)\,. \tag{13.283}$$

Assume $P(k)$. That is, we assume that the product of k consecutive integers is divisible by $k!$.

We want to prove $P(k+1)$. That is, we want to prove

$$(\forall n \in \mathbb{Z})\,(k+1)! \,\Big|\, a_{n,k+1}\,. \tag{13.284}$$

We are going to prove this by induction going forward and backward. This means that

* We are going to do a second induction proof, with respect to n, within the main proof by induction with respect to to k.
* We are going to call this "the n-induction", to distinguish it from the main induction, the "k-induction".

So at this point

* we are within the k-induction,
* we are about to do the n-induction,
* we are assuming that $P(k)$ is true,
* and we are trying to prove that $P(k+1)$ is true, that is, we are trying to prove that (13.284) is true,

∗ and, since (13.284) is a universal sentence about "all integers n", we are going to do the proof by induction going forward and backward.

We let $Q(n)$ be the predicate

$$(k+1)! \,\Big|\, a_{n,k}\,. \tag{13.285}$$

We choose the starting point s_* of our induction to be 0.

Basis step of the n-induction. We want to prove that $Q(0)$ is true. But $Q(0)$ says

$$(k+1)! \,\Big|\, a_{0,k+1}\,.$$

And $a_{0,k+1} = 0$, because $a_{0,k+1}$ is a product of numbers the first one of which is 0. So $Q(0)$ says "$(k+1)!\Big|0$", and this is true, because 0 is divisible by every integer. So we have proved $\boxed{Q(0)"}$.

Inductive step of the n-induction. We want to prove that

$$(\forall n \in \mathbb{Z})\big(Q(n) \iff Q(n+1)\big)\,. \tag{13.286}$$

Let $n \in \mathbb{Z}$ be arbitrary. We want to prove

$$Q(n) \iff Q(n+1)\,. \tag{13.287}$$

$Q(n)$ says that $(k+1)!$ divides $a_{n,k+1}$.

And $Q(n{+}1)$ says that $(k{+}1)!$ divides $a_{n+1,k+1}$.
We are going to prove that

$$(k{+}1)! \text{ divides } a_{n+1,k+1} - a_{n,k+1}\,. \quad (13.288)$$

Before we do that, let me explain why this is a significant fact.

Suppose that we have proved (13.288).

We are going to prove the two implicatios $Q(n) \Longrightarrow Q(n+1)$ and $Q(n+1) \Longrightarrow Q(n)$.

First, assume that $Q(n)$ holds.

Then $a_{n,k+1}$ is divisible by $(k+1)!$.

Since $a_{n+1,k+1} - a_{n,k+1}$ is also divisible by $(k+1)!$, we can conclude that the sum $a_{n,k+1} + \big(a_{n+1,k+1} - a_{n,k+1}\big)$ is divisible by $(k+1)!$.

But this sum is equal to $a_{n+1,k+1}$, So $a_{n+1,k+1}$ is divisible by $(k+1)!$.

That says that $Q(n+1)$ holds.

Hence $Q(n) \Longrightarrow Q(n+1)$.

Conversely, assume $Q(n+1)$ holds. Then $a_{n+1,k+1}$ is divisible by $(k+1)!$.

Since the difference $a_{n+1,k+1} - a_{n,k+1}$ is divisible by $(k+1)!$, we can conclude that $a_{n+1,k+1} - \big(a_{n+1,k+1} - a_{n,k+1}\big)$ is divisible by $(k+1)!$.

But

$$a_{n+1,k+1} - \big(a_{n+1,k+1} - a_{n,k+1}\big) = a_{n,k+1}\,.$$

So $a_{n,k+1}$ is divisible by $(k+1)!$.

That says that $Q(n)$ holds.

So $Q(n+1) \Longrightarrow Q(n)$.

Summarizing, we have shown that, if the assertion (13.288) is true, then both implications "$Q(n) \Longrightarrow Q(n+1)$" and "$Q(n+1) \Longrightarrow Q(n)$" hold, so $Q(n) \Longleftrightarrow Q(n+1)$, which is exactly what we are trying to prove to complete the n-induction.

In other words: *all we need to do is prove (13.288) and that will complete our proof.*

We now prove (13.288).

The number $a_{n,k+1}$ is the product of $k+1$ consecutive integers starting with n and ending with $n+k$. That is,

$$a_{n,k+1} = n \times (n+1) \times (n+2) \times \cdots \times (n+k-1) \times (n+k)\,.$$

And then

$$a_{n,k+1} = n \times \Big((n+1) \times (n+2) \times \cdots \times (n+k-1) \times (n+k)\Big)\,,$$

so $a_{n,k+1}$ is equal to n times the product $(n+1)\times(n+2)\times\cdots\times(n+k-1)\times(n+k)$ of k consecutive integers starting with $n+1$. That is,

$$a_{n,k+1} = n \times a_{n+1,k}\,. \tag{13.289}$$

Similarly, the number $a_{n+1,k+1}$ is the product of $k+1$ consecutive integers starting with $n+1$ and ending with $n+k+1$. That is,

$$a_{n+1,k+1} = (n+1) \times (n+2) \times \cdots \times (n+k) \times (n+k+1)\,.$$

So

$$a_{n+1,k+1} = \Big((n+1) \times (n+2) \times \cdots \times (n+k)\Big) \times (n+k+1)\,.$$

In other words, $a_{n+1,k+1}$ is equal to the product of k consecutive integers starting with $n+1$, multiplied by $n+k+1$. That is,

$$a_{n+1,k+1} = a_{n+1,k} \times (n+1+k)\,. \quad (13.290)$$

Therefore

$$\begin{aligned} & a_{n+1,k+1} - a_{n,k+1} \\ &= a_{n+1,k} \times (n+1+k) - n \times a_{n+1,k} \\ &= (n+k+1) \times a_{n+1,k} - n \times a_{n+1,k} \\ &= \big((n+k+1) - n\big) \times a_{n+1,k} \\ &= (k+1) \times a_{n+1,k}\,. \end{aligned}$$

So we get the key formula

$$a_{n+1,k+1} - a_{n,k+1} = (k+1) \times a_{n+1,k}\,. \quad (13.291)$$

(see the example in the box below to get a better understanding of this formula).

THE FORMULA $a_{n+1,k+1} - a_{,k+1} = (k+1) \times a_{n+1,k}$: AN EXAMPLE

Take $n = 11$, $k = 5$. Then

$$\begin{aligned} a_{11,6} &= 11 \times 12 \times 13 \times 12 \times 15 \times 16\,, \\ a_{12,6} &= 12 \times 13 \times 12 \times 15 \times 16 \times 17\,, \\ a_{11,6} &= 11 \times \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \\ &= 11 \times a_{12,5} \\ a_{12,6} &= \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \times 17 \\ &= 17 \times \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \\ &= 17 \times a_{12,5}\,, \end{aligned}$$

so

$$\begin{aligned} a_{12,6} - a_{11,6} &= (17 - 11) \times a_{12,5} \\ &= 6 \times a_{12,5}\,. \end{aligned}$$

That is,

$$\boxed{a_{n+1,k+1} - a_{n,k+1} = (k+1) \times a_{n+1,k}}.$$

Now comes ***the crucial point of the proof:*** remember that we are within the k-induction. We are assuming $P(k)$ and trying to prove $P(k+1)$. So at this point we are allowed to

use $P(k)$. And $P(k)$ says that

$$(\forall n \in \mathbb{Z})\, k! \Big| a_{n,k}\,. \tag{13.292}$$

So we can use (13.292).

Then $k!$ divides $a_{n+1,k}$, so we can write

$$a_{n,k} = m \times k!$$

for some $m \in \mathbb{Z}$. Then

$$\begin{aligned} a_{n+1,k+1} - a_{n,k+1} &= (k+1) \times k! \times m \\ &= (k+1)! \times m\,, \end{aligned}$$

so $(k+1)!$ divides $a_{n+1,k+1} - a_{n,k+1}$.

That is, we have proved (13.288) and, as was explained before, it follows from this that $\boxed{Q(n) \Longleftrightarrow Q(n+1)}$.

Since we have proved that $Q(n) \Longleftrightarrow Q(n+1)$ for an arbitrary integer n, we can conclude that $\boxed{(\forall n \in \mathbb{Z})\big(Q(n) \Longleftrightarrow Q(n+1)\big)}$.

This completes the inductive step of the n-induction.

We have proved that $Q(0)$ and also that $(\forall n \in \mathbb{Z})\big(Q(n) \Longleftrightarrow Q(n+1)\big)$. By the PMI Going Forward and Backward, it follows that

$$(\forall n \in \mathbb{Z}) Q(n)\,. \tag{13.293}$$

Since $Q(n)$ is the predicate "$(k+1)!\Big|a_{n,k+1}$", we have proved

$$(\forall n \in \mathbb{Z})(k+1)!\Big|a_{n,k+1}\,, \tag{13.294}$$

that is, we have proved $P(k+1)$.

Since we have proved $P(k+1)$ assuming $P(k)$, it follows that

$$P(k) \Longrightarrow P(k+1)\,. \tag{13.295}$$

Since we have proved (13.295) for an arbitrary natural numebr k, it follows that

$$(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)\,. \tag{13.296}$$

So we have proved $P(1)$, and we have also proved that $(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)$. It follows from the PMI that

$$(\forall k \in \mathbb{N})P(k)\,. \tag{13.297}$$

But $P(k)$ is the predicate "$(\forall n \in \mathbb{Z})\, k!\Big|a_{n,k}$".

So we have proved

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\, k!\Big|a_{n,k}\,, \tag{13.298}$$

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

13.4 An application of Theorem 48: integrality of the binomial coefficients

An important application of Theorem 48, on the divisibility of a product of k consecutive integers, is to give a second proof of Theorem 50, different from the one suggested in the hints for Problem 74.

13.4.1 The binomial coefficients

The binomial coefficients $\binom{n}{k}$ are defined as follows:

Definition 20. If n, k are nonnegative integers[82] such that $k \leq n$, then the binomial coefficient $\begin{pmatrix} n \\ k \end{pmatrix}$ is defined by the formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \tag{13.299}$$

Remark 12. One of the most important facts about the numbers $\begin{pmatrix} n \\ k \end{pmatrix}$ is that ***they are always integers***.

It is not obvious at all from Definition 20 that $\binom{n}{k}$ is always an integer.

[82] A nonnegative integer is an integer n such that $n \geq 0$. So the nonnegative integers are the natural numbers, together with the integer 0, which is not a natural number. The set of all nonnegative integers is denoted by the expression "$\mathbb{N} \cup \{0\}$". Therefore "$n \in \mathbb{N} \cup \{0\}$" is a way of saying that $n \in \mathbb{N} \vee n = 0$, i.e., that n is a nonnegative integer.

For example: ***why should*** $\binom{17}{9}$ ***be an integer? Why does*** $17!$ ***have to be divisible by*** $9! \times 8!$***?*** There is no doubt that $17!$ has to be divisible by $9!$, because $17! = 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9!$. But why is the quotient

$$\frac{17!}{9!} = 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10$$

divisible by $8!$? In this particular example, it is easy to do the cancellations, and get

$$\begin{aligned}
\frac{17!}{8!9!} &= \frac{17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10}{8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2} \\
&= \frac{17 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10}{7 \times 6 \times 5 \times 4 \times 3} \\
&= \frac{17 \times 14 \times 13 \times 12 \times 11 \times 10}{7 \times 6 \times 4} \\
&= \frac{17 \times 14 \times 13 \times 12 \times 11 \times 5}{7 \times 6 \times 2} \\
&= \frac{17 \times 13 \times 12 \times 11 \times 5}{6} \\
&= 17 \times 13 \times 2 \times 11 \times 5\,.
\end{aligned}$$

So in this particular case it is clear that $\left(\begin{array}{c} 17 \\ 9 \end{array} \right)$ is an integer, but ***it is not clear yet why it should be true in general that*** $\left(\begin{array}{c} n \\ k \end{array} \right)$ ***is an integer for all*** $n, k \in \mathbb{N} \cup \{0\}$ ***such that*** $k \leq n$.

The following two theorems give one answer to this question. □

Theorem 49. *Let $n, k \in \mathbb{N} \cup \{0\}$ be such that $1 \leq k \leq n$. Then*

$$\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k-1 \end{pmatrix} + \begin{pmatrix} n \\ k \end{pmatrix}. \tag{13.300}$$

Proof. **YOU DO IT.**

Theorem 50. *If n, k are nonnegative integers such that $k \leq n$, then the binomial coefficient $\begin{pmatrix} n \\ k \end{pmatrix}$ is an integer.*

Proof. **YOU DO IT.**

Problem 74. ***Prove*** Theorems 49 and 50.

The proof of Theorem 49 should be very easy: you just add the fractions $\frac{n!}{(k-1)!(n-(k-1))!}$ and $\frac{n!}{k!(n-k)!}$ and the answer turns out to be $\frac{(n+1)!}{k!(n-k)!}$. ***This is <u>not</u> a proof by induction.***

The proof of Theorem 50 should be very easy, by induction. Theorem 49 easily implies that if all the binomial coefficients $\begin{pmatrix} n \\ k \end{pmatrix}$ are integers for a given n, then all the

binomial coefficients $\begin{pmatrix} n+1 \\ k \end{pmatrix}$ are integers as well. And this is basically the inductive step.

But ***you should write the proof carefully and correctly.*** In particular, pay attention to the fact that what you want to prove is a statement with ***two quantifiers***, but in a proof by induction of $(\forall n \in \mathbb{N} \cup \{0\})P(n)$, the sentence $P(n)$ has to have n as an open variable, and no other open variables. So you cannot take $P(n)$ to be a closed formula such as

$$(\forall n \in \mathbb{N} \cup \{0\})(\forall j \in \mathbb{N} \cup \{0\})\left(k \leq n \Longrightarrow \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}\right),$$

and you cannot take $P(n)$ to be "$k \leq n \Longrightarrow \begin{pmatrix} n \\ k \end{pmatrix} \in \mathbb{Z}$" either, because this formula has two open variables.

Also, you should pay attention in your inductive step to the fact that Formula (13.300) cannot be applied if $k = 0$, so you will have to consider the case when $k = 0$ separately. □

13.4.2 A second proof of the integrality of the binomial coefficients

We want to prove that the binomial coefficients $\begin{pmatrix} n \\ k \end{pmatrix}$ are integers, for $n, k \in \mathbb{N} \cup \{0\}$ and $k \leq n$.

First we write

$$\begin{aligned} n! &= 1 \times 2 \times \cdots \times (n-k) \times (n+1-k) \times \cdots \times n \\ &= \big(1 \times 2 \times \cdots \times (n-k)\big) \times \big((n+1-k) \times \cdots \times n\big) \\ &= (n-k)! \times \big((n+1-k) \times \cdots \times n\big) \,. \end{aligned}$$

We then observe that $(n+1-k) \times \cdots \times n$ is the product of k consecutive integers starting at $n+1-k$, which is the number that in the proof of Theorem 48 we called $a_{n+1-k,k}$.

In other words,

$$n! = (n-k)! \times a_{n+1-k,k} \,. \tag{13.301}$$

Finally, we use Theorem 48 to conclude that $a_{n+1-k,k}$ is divisible by $k!$. Hence we can write

$$a_{n+1-k,k} = k! \times m \,,$$

where m is an integer.

It then follows that

$$\begin{aligned} n! &= (n-k)! \times k! \times m \\ &= \big((n-k)! \times k!\big) \times m \,. \end{aligned}$$

so $n!$ is divisible by $(n-k)! \times k!$, and this completes the proof of Theorem 50. **Q.E.D.**

13.5 Strong induction (a.k.a. "complete induction")

Suppose we are trying to prove a proposition that is of the form $(\forall n \in \mathbb{N})P(n)$. It may happen that we cannot prove the implication $P(n) \implies P(n+1)$, because property P is not inherited by $n+1$ from n for every n, but the property is inherited by $n+1$ from some previous natural number, such as $n-1$, or $n-2$. Then ***it still follows that*** $(\forall n \in \mathbb{N})P(n)$.

Example 60. Let $P(n)$ be the predicate[83] "$n = 1 \vee n$ is a product of prime numbers".

We would like to prove that

$$(\forall n \in \mathbb{N})P(n)\,, \tag{13.302}$$

that is, that

$$(\forall n \in \mathbb{N})\big(n = 1 \vee n \text{ is a product of prime numbers}\,,$$

or, equivalently,

$$(\forall n \in \mathbb{N})\Big(n \geq 2 \implies \big(n \text{ is a product of prime numbers}\big)\Big)\,.$$

(That is, "if n is a natural number and $n \geq 2$ then n is a product of prime numbers.)

[83] The precise meaning of "is a product of prime numbers" was defined in section 2.3.3, Definition 4, on page 12. In particular, we insist on the fact that ***a single prime number is a product of primes according to our definition.***

To prove this, we would like to use induction. The basis step is easy: $P(1)$ is true, because $P(1)$ says "$1 = 1 \vee 1$ is a product of prime numbers", and this is obviously true because $1 = 1$.

But when we get to the inductive step, and we try to prove that implication $P(n) \implies P(n+1)$ for every n, we get into trouble.

Look, for example, at $n = 47$ and $n = 60$. We want to prove that $P(47) \implies P(48)$ and $P(60) \implies P(61)$. But, although $P(48)$ and $P(61)$ are true (because $48 = 2 \times 2 \times 2 \times 3$, and 61 is prime, so both 48 and 61 are products of primes), the reasons that $P(48)$ and $P(61)$ are true have nothing to do with the facts that $P(47)$ and $P(60)$ are true.

Indeed:

- $P(48)$ is true because
  - $48 = 8 \times 6$,
  - 8 and 6, are both products of primes, ***because all the natural numbers that are*** ≤ 47 ***are products of primes***,
  - so 48 is a product of primes.
- And $P(61)$ is true because
  - 61 is prime. $\square$

So, as Example 60 shows, it is not going to be possible to prove the implication $P(n) \Longrightarrow P(n+1)$ for every n.

On the other hand, if we associate to the predicate $P(n)$ another predicate, $Q(n)$, defined by

$$Q(n) \text{ means } \text{“}P(1) \wedge P(2) \wedge \cdots \wedge P(n)\text{”} ,$$

that is,

$$Q(n) \text{ means } \text{“}(\forall k \in \mathbb{N})\big(k \leq n \Longrightarrow P(k)\big)\text{”}.$$

then it is clear that

$\big(*\big)$ ***if we prove that*** $(\forall n \in \mathbb{N})Q(n)$***, then it follows that*** $(\forall n \in \mathbb{N})P(n)$***.***

(Why? Suppose that $(\forall n \in \mathbb{N})Q(n)$. Let $n \in \mathbb{N}$ be arbitrary. Then $Q(n)$ is true, by Rule $\forall_{use}$. Therefore the proposition $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ is true, so in particular $P(n)$ is true. Hence $(\forall n \in \mathbb{N})P(n)$.)

Furthermore,

$\big(**\big)$ ***To prove that*** $(\forall n \in \mathbb{N})Q(n)$ ***by induction, in the inductive step, when we want to prove that the implication*** $Q(n) \Longrightarrow Q(n+1)$ ***is true, it suffices to prove that the weaker implication*** $Q(n) \Longrightarrow P(n+1)$ ***is true.***

(Why? Let us assume that $Q(n)$. We want to prove that $Q(n+1)$. That is, we need to prove the conjunction

"$P(1) \wedge P(2) \wedge \cdots \wedge P(n) \wedge P(n+1)$". But we already know that "$P(1) \wedge P(2) \wedge \cdots \wedge P(n)$" is true, because that is what $Q(n)$ is. So all we need in order to prove $Q(n+1)$ is to prove $P(n+1)$.)

Strong Induction (a.k.a. "complete induction")

Let $P(n)$ be a one-variable predicate.
Let $Q(n)$ be the predicate

$$P(1) \wedge P(2) \wedge \cdots \wedge P(n)\,,$$

so that $Q(n)$ means

$$(\forall k \in \mathbb{N})\big(k \leq n \Longrightarrow P(k)\big)\,.$$

Then, if

$$P(1)$$

and

$$(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow P(n+1)\big)\,,$$

it follows that $(\forall n \in \mathbb{N})P(n)$.

Example 61. Let us prove

Theorem 51. *If n is a natural number and $n \geq 2$ then n is a product of prime numbers.*

Proof. Let $P(n)$ be the predicate "if $n \geq 2$ then n is a

product of prime numbers".

Let $Q(n)$ be the predicate "$P(k)$ is true for all natural numbers k such that $k \leq n$".

We prove $(\forall n \in \mathbb{N})P(n)$ using strong induction.

For this purpose, we prove the two propositions $P(1)$ and $(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow P(n+1)\big)$.

Basis step. We have to prove $P(1)$. But $P(1)$ says "if $1 \geq 2$ then 1 is a product of prime numbers", and this is an implication with a false premise. So $P(1)$ is true.

Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow P(n+1)\big)\,. \tag{13.303}$$

Let $n \in \mathbb{N}$ be arbitrary. We want to prove that $Q(n) \Longrightarrow P(n+1)$.

Assume $Q(n)$. We want to prove $P(n+1)$.

So we want to prove that $n+1$ is a product of prime numbers.

But $n+1$ is either prime, or not prime.

If $n+1$ is prime, then it is a product of primes, and $P(n+1)$ holds.

If $n+1$ is not prime, then, since $n+1 \neq 1$, it follows that $n+1$ is the product $j \times k$ of two natural numbers that are both > 1.

Clearly, then, $j \leq n$ and $k \leq n$. (If j was

> $> n$, then j would be $\geq n+1$ and, since $k>1$, it would follow that $jk > n+1$. But this is not possible, because $jk = n+1$. So $j \leq n$. A similar argument proves that $k \leq n$.)
>
> Since $Q(n)$ holds, both j and k are products of primes.
>
> And then $n+1$, the product of j and k, is also a product of primes.
>
> So $P(n+1)$ holds.
>
> We have proved that $P(n+1)$ holds in both cases, when $n+1$ is prime and when $n+1$ is not prime.
>
> Hence we have proved $P(n+1)$, assuming $Q(n)$.
>
> So we have proved that $Q(n) \Longrightarrow P(n+1)$, assuming that n is an arbitrary natural number.

Hence we have proved $(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow P(n+1)\big)$, completing the inductive step.

Since we have proved both $P(1)$ and $(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow P(n+1)\big)$, it follows from the strong principle of mathemtical induction that $(\forall n \in \mathbb{N})P(n)$, that is,

$$(\forall n \in \mathbb{N})\big(n \geq 2 \Longrightarrow n \text{ , is a product of primes .}$$

This completes our proof. **Q.E.D.**

13.5.1 Stronger and weaker statements

Remark 13. Why did I say that the implication $Q(n) \implies P(n+1)$ is "weaker" than the implication $P(n) \implies P(n+1)$?

Intuitively, a proposition A is weaker than a proposition B if it gives less information. This means that knowing that B is true tells us that A is true, so if we know that B is true then we know that A is true. (So if we know B then we know B and A, but if we know A we only know A; we don't know B.)

More formally, we have

Definition 21. A proposition A is weaker than a proposition B if the proposition $B \implies A$ is true. And in that case we also say that B is stronger than A. □

Example 62. Let A be the proposition "you got a passing grade", let B be the proposition "you got an 'A' grade". Which one gives you more information? Obviously, B does. So A should be weaker than B, and B should be stronger than A.

And, indeed, the proposition $B \implies A$ is clearly true. So A is weaker than B according to our definition. □

Returning now to $P(n)$ and $Q(n)$, it is clear that

$$\Big(P(n) \Longrightarrow P(n+1)\Big) \Longrightarrow \Big(Q(n) \Longrightarrow P(n+1)\Big). \tag{13.304}$$

(Proof: Assume that $P(n) \Longrightarrow P(n+1)$. We want to prove that $Q(n) \Longrightarrow P(n+1)$. Assume $Q(n)$. We want to prove $P(n+1)$. Clearly, $Q(n) \Longrightarrow P(n)$. Since we are assuming $Q(n)$, it follows from the Modus Ponens rule—i.e., Rule $\Longrightarrow_{use}$—that $P(n)$ is true. Since we are assuming that $P(n) \Longrightarrow P(n+1)$, it follows again from the Modus Ponens rule that $P(n+1)$. So we have proved $Q(n) \Longrightarrow P(n+1)$, assuming $P(n) \Longrightarrow P(n+1)$. Hence (13.304) holds.)

So we see that "$Q(n) \Longrightarrow P(n+1)$" is weaker than "$P(n) \Longrightarrow P(n+1)$" in the very precise sense of Definition 21. □

Problem 75. For each of the following pairs A, B of propositions, indicate which one is stronger and which one is weaker. (You may assume that n and f are arbitrary objects that have been given to you, that is, they are fixed objects but you do not know who they are.)

1. A is "n is a natural number" and B is "n is an integer".
2. A is "if n is a natural number then $n > 0$" and B is "if n is an integer then $n > 0$".

3. A is "f is a continuous function on an interval $[a, b]$" and B is "f is a differentiable function on an interval $[a, b]$".

4. A is "every continuous function on an interval $[a, b]$ has a maximum and a minimum on $[a, b]$", and B is "every differentiable function on an interval $[a, b]$ has a maximum and a minimum on $[a, b]$". □

Problem 76. ***Prove, using the 14 rules of logic***, that

1. *If A, B, C are propositions, then if A is weaker than B then $A \implies C$ is stronger than $B \implies C$.* (See also Example 63 below.)

2. *If A, B, C are propositions, then if B is stronger than C it follows that $A \implies B$ is stronger than $A \implies C$.*

3. *If A, B, C, D are propositions, then if B is stronger than A and C is stronger than D it follows that $A \implies C$ is stronger than $B \implies D$.*

4. *If A, B, C are propositions, then if A is weaker than B then $A \wedge C$ is weaker than $B \wedge C$.*

5. *If $X(n)$ and $Y(n)$ are predicates with the open variable n* (so that for each fixed n $X(n)$ and $Y(n)$

are propositions) then if $X(n)$ is weaker that $Y(n)$ for each n in some set S, *it follows that the proposition "$(\forall n \in S)X(n)$" is weaker than "$(\forall n \in S)Y(n)$" and the proposition "$(\exists n \in S)X(n)$" is weaker than "$(\exists n \in S)Y(n)$".* □

Example 63. Why is strong induction called "strong induction"?

The reason is this:

- Clearly, for each $n \in \mathbb{N}$ the proposition $Q(n)$ is stronger than $P(n)$.
- Hence for each $n \in \mathbb{N}$ the implication "$Q(n) \implies P(n+1)$" is weaker than "$P(n) \implies P(n+1)$" (because of the first result of Problem 76).
- So "$(\forall n \in \mathbb{N})\big(Q(n) \implies P(n+1)\big)$" is weaker than "$(\forall n \in \mathbb{N})\big(P(n) \implies P(n+1)\big)$" (because of the third result of Problem 76).
- Hence "$P(1) \wedge (\forall n \in \mathbb{N})\big(Q(n) \implies P(n+1)\big)$" is weaker than "$P(1) \wedge (\forall n \in \mathbb{N})\big(P(n) \implies P(n+1)\big)$" (because of the second result of Problem 76).
- And then the implication

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})\big(Q(n) \implies P(n+1)\big)\Big) \implies (\forall n \in \mathbb{N})P(n) \tag{13.305}$$

is stronger than the implication

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})\big(P(n) \Longrightarrow P(n+1)\big)\Big) \Longrightarrow (\forall n \in \mathbb{N})P(n)\,. \tag{13.306}$$

But (13.306) is the ordinary Principle of Mathematical Induction, and (13.305) is the strong Principle of Mathematical Induction.

So the strong PMI is indeed stronger than the ordinary PMI. □

14 The main theorems of elementary integer arithmetic I: the division theorem

We now study the phenomena that make the natural numbers and the integers different in crucial ways from the real numbers. The root of this difference is that the division operation on $\mathbb{N}$ and $\mathbb{Z}$ is very different from division on $\mathbb{R}$.

14.1 What is the division theorem about?

The first important fact about the integers is the ***division theorem***. It deals with an issue that you know very well, namely, what happens if you have an integer a and an integer b and you want to "divide" a by b:

1. First of all: dividing by zero is never a good idea, so we have to work with integers a and b such that $b \neq 0$.

2. Dividing a by b should amount, roughly, to finding a number q, called the "quotient of a by b", such that

$$a = bq\,. \tag{14.307}$$

3. If we were dealing with real numbers rather than integers, then it is always possible[84] to find q. The

[84] Assuming, of course, that $b \neq 0$.

real number q that satisfies (14.307) is denoted by the expression $\frac{a}{b}$, that we read as "a over b", or "a divided by b".

4. The situation is different when we are dealing with integers rather than real numbers. In this case, it is not always possible to find an integer q for which (14.307) is satisfied *exactly*. But we can come close: we can find an integer q for which (14.307) is satisfied *approximately*.

5. Precisely, let us rewrite (14.307) as follows:

$$a = bq + r \qquad \text{and} \quad r = 0\,. \tag{14.308}$$

Then what happens is this: we cannot satisfy (14.308), but we can satisfy

$$a = bq + r \qquad \text{and} \quad r \text{ is small}\,. \tag{14.309}$$

6. And the precise meaning of "small", if $b > 0$, is "$0 \leq r < b$". So what you will be satisfying (if $b > 0$) is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < b\,. \tag{14.310}$$

7. The number q is called the ***quotient of the division of*** a ***by*** b, and the number r is called the ***remainder of the division of*** a ***by*** b.

8. The reason that r is called the "remainder" is very straightforward: suppose you have, say, 27 dollar bills, and you want to divide them equally among 5 people. Then the best you can do is give 5 dollars to each of the five people, and when you do that 2 dollars will "remain".

9. Notice that, if instead of 27 dollar bills you were dealing with, say, 27 gallons of water, then you would be able to divide the water equally, by giving 5.4 gallons to each of the five people. But with dollar bills you cannot do that. That's because ***dollar bills are countable***, whereas ***water is uncountable***. In other words,

   - You can talk about the ***amount*** of water in a tank, and ***amounts of water are measured in terms of real numbers***.
   - And you cannot talk about the ***number*** of water in a tank.
   - You can talk about the ***number*** of dollar bills in your wallet, and ***numbers of dollar bills are measured in terms of natural numbers***. (And if you want to consider negative amounts as well, e.g. to talk about debts, you would use ***integers***.)

- And you cannot [85] talk about the ***amount*** of dollar bills in your wallet.
- If you have a units of a countable quantity such as dollar bills or coins, and b persons among whom you want to divide your a units equally, then the best you can do is give q units to each of the b persons, where q is the quotient of the division of a by b, and when you do that there will be a remainder of r undistributed dollar bills, where r is the remainder of the division of a by b.
- What happens if b is negative? Well, in this case you certainly cannot have $0 \leq r < b$, because if $b < 0$ this is impossible. But you can ask for a remainder r such that $0 \leq r < |b|$, where $|b|$ is the ***absolute value*** of b, that is, the number defined by

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0 \end{cases} . \tag{14.311}$$

- So the final condition is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < |b| . \tag{14.312}$$

[85] I really mean "you shouldn't, because it's wrong". Strictly speaking, you can say anything you want, in this free counrty of ours. But there are rules of grammar, and according to those rules it is wrong to say things like "a large amount of people were at the rally", or "she has a large amount of dollar bills". But it's O.K. to ta;lk about "a large amount of money". "People", like "dollar bills", or "coins", is countable. "Water", like "money", is uncountable.

The division theorem says precisely that given integers a, b, there exist integers q, r such that (14.312) holds, provided, of course, that b is not equal to zero. And in addition it makes the very important and very useful assertion that q and r are ***unique***, that is, there is only one possible choice of q and r.

14.1.1 An example: even and odd integers

Example 64 Let us apply the division theorem to the case when $b = 2$. Suppose a is an integer.

What does the division theorem tell us about a?

The theorem makes two assertions, namely,

1. that the quotient and remainder exist (that's the ***existence part***),
2. that the quotient and remainder are unique (that's the ***uniqueness part***).

So let us look at each of these two parts, and see what it tells us about a.

The existence part of the theorem tells us that we can find integers q and r such that

$$a = 2q + r \text{ and } 0 \leq r < 2\,.$$

Since $0 \leq r < 2$ and r is an integer, it follows that $r = 0$ or $r = 1$.

If $r = 0$ then $a = 2q$, so a is divisible by 2, that is, a is even.

If $r = 1$ then $a = 2q+1$, so $a-1 = 2q$, and then $a-1$ is divisible by 2, that is, $a-1$ is even, and, according to our definition of "odd", this implies that a is odd.

So we have shown that: either $r = 0$, in which case a is even, or $r = 1$, in which case a is odd. So ***the existence part of the division theorem tells us that*** a ***must be even or odd.***

The uniqueness part of the theorem tells us that we cannot find integers q, r such that

$$a = 2q + r \text{ and } 0 \leq r < 2\,,$$

and also find different integers q', r' such that

$$a = 2q' + r' \text{ and } 0 \leq r' < 2\,.$$

In particular, it is not possible to find integers q, q' such that

$$a = 2q \text{ and } a = 2q' + 1\,.$$

In other words, a cannot be both even and odd. So ***the uniqueness part of the division theorem tells us that*** a ***cannot be both even and odd.***

Summarizing: ***the division theorem, for*** $b = 2$***, tells us that an integer*** a ***has to be even or odd and cannot be both even and odd.*** And this

is exactly Theorem 26, that we had to work so hard to prove!

In other words: ***The division theorem (that is, Theorem 52 below) is a generalization of the theorem that says that every integer is even or odd and not both.*** □

Now that we understand what the division theorem says for $b = 2$, let us look at what it says for other values of b.

- Theorem 52 says that, when you try to divide an integer a by 2, then one and only one of two things will happen:
  1. you will be able to divide a by 2 exactly, with a remainder equal to zero, and conclude that a is even,
  2. you will not be able to divide a by 2 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a - 1$ is divisible by 2, so a is odd.
- The division theorem, applied with $b = 2$, says exactly that that every integer is even or odd and not both.
- The division theorem, applied with $b = 3$, says that, when you try to divide an integer a by 3, then one and only one of three things will happen:

1. you will be able to divide a by 3 exactly, with a remainder equal to zero, and conclude that a is divisible by 3,
2. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a = 3q + 1$ for some integer q, so $a - 1$ is divisible by 3.
3. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 2, and conclude that $a = 3q + 2$ for some integer q, so $a - 2$ is divisible by 3.

- The division theorem, applied with $b = 4$, says that, when you try to divide an integer a by 4, then one and only one of four things will happen: $4|a$, $4|a-1$, $4|a-2$, $4|a-3$.
- The division theorem, applied with $b = 5$, says that, when you try to divide an integer a by 5, then one and only one of five things will happen: $5|a$, $5|a-1$, $5|a-2$, $5|a-3$, $5|a-4$.
- $\cdots$
- The division theorem, applied with $b = 29$, says that, when you try to divide an integer a by 29, then one

and only one of 29 things will happen: $29|a-j$ for $j \in \mathbb{Z}$, $0 \leq j < 29$.

- $\cdots$
- The division theorem, applied with $b = 372,508$, says that, when you try to divide an integer a by $372,508$, then one and only one of $372,508$ things will happen: $372,508|a-j$ for $j \in \mathbb{Z}$, $0 \leq j < 372,508$.

14.2 Precise statement of the division theorem

And here is, finally, the division theorem:

The division theorem for integers

Theorem 52. *If a, b are integers, and $b \neq 0$, then there exist unique integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b|.$$

14.2.1 The quotient and the remainder

Definition 22. If a, b are integers, and $b \neq 0$, then the unique integers q, r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|$$

called, respectively, the quotient and the remainder of the division of a by b.

We use $\mathrm{QUO}(a, b)$ and $\mathrm{REM}(a, b)$ to denote the quotient and the remainder of the division of a by b. □

It follows from Definition 22 that, if $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and $b \neq 0$, then

1. $a = b \times \mathrm{QUO}(a, b) + \mathrm{REM}(a, b)$,
2. $\mathrm{QUO}(a, b) \in \mathbb{Z}$,
3. $\mathrm{REM}(a, b) \in \mathbb{Z}$ and $0 \leq \mathrm{REM}(a, b) < |b|$,
4. if q, r are integers such that $a = bq+r$ and $0 \leq r < |b|$, then $q = \mathrm{QUO}(a, b)$ and $r = \mathrm{REM}(a, b)$.

14.2.2 Some problems

Problem 77. ***Prove*** the following theorem.

Theorem 53. *If n is an integer, then there exist unique integers q, r such that*

$$n^2 = 4q + r \qquad \text{and} \qquad r = 0 \vee r = 1\,.$$

(HINT: First write $n = 4k + s$, with $0 \leq s < 4$, and then prove that $\mathrm{REM}(n^2, 4)$ must be 0 or 1.) □

Problem 78. ***Prove*** the following theorem.

Theorem 54. *If m, n are integers, then there exist unique integers q, r such that*

$$m^2 + n^2 = 4q + r \qquad \text{and} \qquad r = 0 \vee r = 1 \vee r = 2\,.$$

(HINT: Use Theorem 53.) □

Problem 79. ***Prove*** that if $n = 3,409,583$, then there do not exist integers p, q such that $p^2 + q^2 = n$. □

14.3 Proof of the division theorem

The proof of the division theorem will be split up into two parts.

1. We will first prove the existence part. That is, we will prove

   Theorem 52.I. *If a, b are integers and $b \neq 0$ then there exist integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.*

2. Then, after we have proved the existence result — i.e.., Theorem 52.I—- we will prove the uniqueness result. That is, we will prove

   Theorem 52.II. *If a, b are integers and $b \neq 0$, and q, r, q', r' are integers such that*

   $$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|\,,$$

   and

   $$a = bq' + r' \qquad \text{and} \qquad 0 \leq r' < |b|\,,$$

   then $q = q'$ and $r = r'$.

14.3.1 Proof of the existence part of the division theorem, using induction going forward and backward

We want to prove that

$$(\forall a\in\mathbb{Z})(\forall b\in\mathbb{Z})\Big(b\neq 0 \Longrightarrow (\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\Big)\,. \quad (14.313)$$

This is logically equivalent[86] to

$$(\forall b\in\mathbb{Z})(\forall a\in\mathbb{Z})\Big(b\neq 0 \Longrightarrow (\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\Big)\,. \quad (14.314)$$

and to

$$(\forall b\in\mathbb{Z})\Big(b\neq 0 \Longrightarrow (\forall a\in\mathbb{Z})(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\Big)\,. \quad (14.315)$$

So we are going to prove (14.315).

Let b be an arbitrary integer. We want to prove

$$b\neq 0 \Longrightarrow (\forall a\in\mathbb{Z})(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\,. \quad (14.316)$$

Assume that $b\neq 0$. We want to prove

$$(\forall a\in\mathbb{Z})(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\,. \quad (14.317)$$

Proposition (14.317) is a universal sentence whose universal quantifier is "$(\forall a\in\mathbb{Z})$". So we have the option of using induction forward and backward, and we are going to do it that way.

We let $P(a)$ be the statement

$$(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<|b|)\,. \quad (14.318)$$

We are going to prove $(\forall a\in\mathbb{Z})P(a)$ by induction going forward and backward.

Basis step. We have to prove $P(0)$.

Clearly, $P(0)$ says that

$$(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(0=bq+r\wedge 0\leq r<|b|)\,, \quad (14.319)$$

[86]Two propositions A, B are logically equivalent if the proposition $A\iff B$ can be proved by pure logic, that is, using only the rules of logic. It is an easy exercise to see that, if $P(x,y)$ is a 2-variables predicate (that is, a sentence with the open variables x,y) and S is a set, then $(\forall x\in S)(\forall y\in S)P(x,y)$ is logically equivalent to $(\forall y\in S)(\forall x\in S)P(x,y)$.

which is an existential sentence.

To prove 14.319, we can use Rule $\exists_{prove}$, and for that purpose we have to produce witnesses, i.e., integers q, r such that

$$0 = bq + r \text{ and } 0 \leq r < |b| \,. \tag{14.320}$$

And this is very easy: just take $q = 0$, $r = 0$.

Then, with this choice of q, r, it is clear that (14.320) holds. (Notice that here we are using the fact that $b \neq 0$, to conclude that $r < |b|$.)

Hence (14.319) is true, and we have proved $\boxed{P(0)}$, and completed the basis step.

Inductive step. We have to prove that

$$(\forall a \in \mathbb{Z})\big(P(a) \iff P(a+1)\big) \,. \tag{14.321}$$

Let a be an arbitrary integer.

We want to prove "$P(a) \iff P(a+1)$".

For this purpose, we are going use Rule $\iff_{prove}$, and this requires that we prove the pair of implications "$P(a) \implies P(a+1)$" and "$P(a+1) \iff P(a)$".

Proof of "$P(a) \implies P(a+1)$".

Assume $P(a)$.

Then

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|) \,. \tag{14.322}$$

So we may pick integers q, r such that

$$a = bq + r \wedge 0 \leq r < |b| \,. \tag{14.323}$$

We want to prove that $P(a+1)$ is true, i.e., that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a + 1 = bq + r \wedge 0 \leq r < |b|) \,, \tag{14.324}$$

and for that purpose we need witnesses q', r' for (14.324).

The most obvious choice would be to take $q' = q$, $r' = r + 1$.

Then $a + 1 = bq' + r'$. But we cannot prove that $r' < |b|$, because from "$r < |b|$" all we can conclude is that $r' \leq |b|$, and that's not what we need.

On the other hand, if we knew that $r + 1 < |b|$, then the conclusion "$r' < |b|$" would follow.

Therefore, so we have found the desired witnesses q', r', and proved (14.324), under the assumption that $r + 1 < |b|$.

We now have to take care of the possibility that $r + 1 \geq |b|$.

In that case, since $r < |b|$, it follows that $r + 1 = |b|$. (REASON: r and $|b|$ are integers, so if $r < |b|$ then $r + 1 \leq |b|$. So if $r + 1 \geq |b|$ it follows that $r + 1 = |b|$.)

Then

$$\begin{aligned} a + 1 &= bq + r + 1 \\ &= bq + |b| \,. \end{aligned}$$

Define an integer μ as follows:

$$\mu = \begin{cases} 1 & \text{if} \quad b > 0 \\ -1 & \text{if} \quad b < 0 \,. \end{cases}$$

Then $|b| = \mu b$.

Therefore

$$\begin{aligned} a + 1 &= bq + |b| \\ &= bq + \mu b \\ &= b(q + \mu) \\ &= b(q + \mu) + 0 \,. \end{aligned}$$

Hence, if we choose our witnesses q', r' by letting $q' = q + \mu$ and $r' = 0$, it follows that $a + 1 = bq' + r'$ and $0 \leq r' < |b|$. So we have also proved (14.324).

So we have proved (14.324) in both cases, when $r + 1 < |b|$ and when $r + 1 \geq |b|$.

Hence we have proved (14.324), i.e., we have proved $P(a+1)$.

Since we have proved $P(a+1)$ assuming $P(a)$, it follows from Rule $\Longrightarrow_{prove}$ that we have proved $\boxed{P(a) \Longrightarrow P(a+1)}$.

Proof of "$P(a + 1) \Longrightarrow P(a)$".

Assume $P(a + 1)$.

Then

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a + 1 = bq + r \wedge 0 \leq r < |b|) \,, \qquad (14.325)$$

So we may pick integers q, r such that

$$a + 1 = bq + r \wedge 0 \leq r < |b| \,. \tag{14.326}$$

We want to prove that $P(a)$ holds, i.e., that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|) \,, \tag{14.327}$$

and for that purpose we need witnesses q', r' for (14.327).

The most obvious choice is to take $q' = q$, $r' = r - 1$.

Then $a = bq' + r'$ (because $a + 1 = bq + r$, $q' = q$, and $r' = r - 1$). And $r' < |b|$ (because $r < |b|$ and $r' < r$.) But we cannot prove that $r' \geq 0$, because r could be 0, in which case r' would be -1.

On the other hand, if we knew that $r > 0$, then the conclusion "$0 \leq r' < |b|$" follows.

So we have found the desired witnesses q', r', and proved (14.327), under the assumption that $r > 0$.

We now have to take care of the possibility that $\boxed{r = 0}$.

In that case, we have

$$\begin{aligned} a + 1 &= bq + r \\ &= bq \,. \end{aligned}$$

So

$$\begin{aligned} a &= bq - 1 \\ &= bq - |b| + |b| - 1 \\ &= bq - \mu b + |b| - 1 \\ &= b(q - \mu) + |b| - 1 \,, \end{aligned}$$

where μ is the number defined earlier.

Hence, if we choose our witnesses q', r' by letting $q' = q - \mu$ and $r' = |b| - 1$, it follows that $a = bq' + r'$ and $0 \leq r' < |b|$. So we have also proved (14.327).

So we have proved (14.327) in both cases, when $r > 0$ and when $r = 0$.

Hence we have proved (14.327), i.e., we have proved $P(a)$.

Since we have proved $P(a)$ assuming $P(a+1)$, it follows from Rule $\Longrightarrow_{prove}$ that we have proved $\boxed{P(a+1) \Longrightarrow P(a)}$.

Since we have proved the implications $P(a) \implies P(a+1)$ and $P(a+1) \implies P(a)$, it follows from Rule $\iff_{prove}$ that we have proved $\boxed{P(a) \iff P(a+1)}$.

Since we have proved $P(a+1) \iff P(a)$ for an arbitrary integer a, it follows from Rule $\forall_{prove}$ that

$$(\forall a \in \mathbb{Z})\big(P(a) \iff P(a+1)\big)\,. \tag{14.328}$$

Then the principle of mathematical induction going forward and backward implies that $(\forall a \in \mathbb{Z})P(a)$, that is,

$$(\forall a \in \mathbb{Z})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,. \tag{14.329}$$

Proposition (14.329) was proved under the assumption that $b \neq 0$. Hence

$$b \neq 0 \implies \Big((\forall a \in \mathbb{Z})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\Big)\,. \tag{14.330}$$

Proposition (14.330) was proved for an arbitrary integer b. Hence

$$(\forall b \in \mathbb{Z})\left(b \neq 0 \implies \Big((\forall a \in \mathbb{Z})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\Big)\right). \tag{14.331}$$

And this completes the existence proof. **Q.E.D.**

14.3.2 Proof of the uniqueness part of the division theorem

We now prove, finally,

Theorem 52.II. *If a and b are integers and $b \neq 0$, then the integers q, r such that $a = bq + r$ and $0 \leq r < |b|$ are unique.*

Proof.

Let $a \in \mathbb{Z}$ be arbitrary. Let $b \in \mathbb{Z}$ be arbitrary.

Assume that $b \neq 0$. We want to prove that

(*) If q, q', r, r' are integers such that

$$\begin{aligned} a &= bq + r\,, && (14.332)\\ 0 &\leq r < b\,, && (14.333)\\ a &= bq' + r'\,, && (14.334)\\ 0 &\leq r' < b\,, && (14.335) \end{aligned}$$

then $q = q'$ and $r = r'$.

Let q, q', r, r' be integers such that (14.332), (14.333), (14.334), and (14.335) hold.

We will prove that $q = q'$ and $r = r'$.

Without loss of generality, we may assume that $r \geq r'$. (Reason: if r was $< r'$, just change the names of r, r' and call them r' and r.)

Then

$$0 \leq r - r' < b\,. \qquad (14.336)$$

(Reason: 0 is $\leq r - r'$ because $r \geq r'$. And $r - r' < b$ because $r - r' \leq r$, since $r' \geq 0$, and $r < b$.)

On the other hand, $a = bq + r$ and $a = bq' + r'$, so

$$bq + r = bq' + r'\,.$$

Therefore

$$b(q' - q) = r - r'\,. \qquad (14.337)$$

Then

$$|b| \cdot |q' - q| = |r - r'|\,, \qquad (14.338)$$

because $|xy| = |x| \cdot |y|$ for arbitrary real numbers x, y.

Since q and q' are integers, the number $|q - q'|$ is a nonnegative integer.

We now prove[87] that $q = q'$.

Assume that $q \neq q'$.

Then the nonnegative integer $|q - q'|$ is not zero, so it is a natural number.

And then $|q - q'| \geq 1$.

Therefore (14.338) implies that $|r - r'| \geq |b|$.

[87] by contradiction , naturally.

But $r - r' \geq 0$, because $r \geq r'$.
Hence $|r - r'| = r - r'$.
It follows that $r - r' \geq |b|$.
So it's not true that $r - r' < |b|$.
But (14.336) tells us that $r - r' < |b|$.
So $r - r' < |b|$ and $\sim r - r' < |b|$, which is a contradiction.

This proves that $\boxed{q = q'}$.

And then (14.338) implies that $\boxed{r = r'}$.

So we have proved (**), for arbitrary integers a, b such that $b \neq 0$.

This completes the proof of the uniqueness part. So our proof is complete.**Q**.**E**.**D**.

14.3.3 Another proof of the existence part of the division theorem, using well ordering

Let a, b be arbitrary integers such that $b \neq 0$.

We want to prove

(E) *There exist integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b| . \tag{14.339}$$

Let S be the set of all integers r such that $r \geq 0$ and $s = a - bq$ for some integer q. In other words,

$$S = \{s \in \mathbb{Z} : (\exists q \in \mathbb{Z}) s = a - bq\{ . \tag{14.340}$$

We prove that

(I) S has a smallest member,

(II) if r is the smallest member of S, then $0 \leq r < |b|$ and $r = a - bq$ for some $q \in \mathbb{Z}$.

Proof of (I). The well ordering principle tells us that S has a smallest member, provided we prove that

1. S is a set of integers,
2. S is bounded below,
3. S is nonempty.

The fact that S is a set of integers is obvious from the definition of S, i.e., formula (14.340).

It also follows from formula (14.340) that S is bounded below, since every member of S is ≥ 0.

Finally, S is nonempty for the following reason: take $q = -b|a|$, and let $s = a - bq$, then

$$s = a - bq = a - b(-b|a|) = a + b^2|a| \geq a + |a| \geq 0\,;$$

then $s \in S$ (because $s \in \mathbb{Z}$, $s \geq 0$, $s = a - bq$, and $q \in \mathbb{Z}$).

Since we have proved that the three conditions needed to be able to apply the WOP hold, we can apply the WOP and conclude that S has a smallest member.

Proof of (II). Let r be the smallest member of S. Then r is nonnegative, because all the members of S are nonnegative. And, since $r \in S$, we may pick $q \in \mathbb{Z}$ such that $r = a - bq$. Then $a = bq + r$ and $r \geq 0$.

Only one thing is missing, namely, proving that $r < |b|$. We prove this by contradiction.

Assume that $r \geq |b|$.

Let

$$m = \begin{cases} 1 & \text{if} \quad b > 0 \\ -1 & \text{if} \quad b < 0 \end{cases} .$$

Then $m \in \mathbb{Z}$ and $mb = |b|$.

Let $q' = q + m$, and let $r' = r - |b|$. Then $r' \in \mathbb{Z}$, and the assumption that $r \geq |b|$ implies that $r' \geq 0$.

Furthermore, if we let $q' = q + m$, then $q' \in \mathbb{Z}$, and

$$r' = r - |b| = r - mb = a - bq - mb = a - b(q+m) = a - bq' .$$

Since $r' \geq 0$, $r' = a - bq'$, and $q' \in \mathbb{Z}$, it follows that $r' \in S$.

But $r' = r - |b|$, and $b \neq 0$, so $r' < r$. Hence r is not the smallest member of S, because $r' \in S$ and $r' < r$.

So the assumption that $r \geq |b$ has led us to a contradction. Hence $r < |b|$.

So we have proved that S has a smallest member r, that $0 \leq r < |b|$, and that $a = bq + r$ for some integer q. This completes the proof of the existence of q and r.