MATHEMATICS 300 — SPRING 2019

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Part II

Contents

1 A summary of Logic **2**

1.1 Terms and sentences 2

1.1.1 Nouns and noun phrases in English 2

1.1.2 The "use-mention" distinction 3

1.1.3 Terms in mathematical language 6

1.1.4 Examples of terms and sentences 6

1.1.5 The value of a term 8

1.1.6 Terms as instructions for a computation, i.e., as programs . 9

1.1.7 Letter variables in terms 10

1.1.8 Bound (dummy, closed) variables in terms 11

1.1.9 What is a dummy (free, open) variable? 14

1.1.10 Other examples of dummy variables in terms 16

1.1.11 Bound (dummy, closed) variables in sentences 18

1.1.12 A challenging problem 23

1.1.13 A convention about naming sentences 23

1.1.14 Some problems 25

1.2 Substitution 26

1.3 Forming sentences: the grammar of formal language 28

1.4 How sentences are constucted 29

1.4.1 The seven logical connective symbols 29

1.4.2 The quantifiers 30

1.4.3 Sentence types 30

1.5 Forming sentences 30

1.5.1 When do we put parentheses? 31

1.6 The 14 logical rules 32

1.7 Some problems, with solutions 35

2 An introduction to elementary arithmetic **45**
2.1 What is arithmetic? . . . 45
2.2 Numbers . . . 45
2.2.1 Operations . . . 46
2.3 Other number systems: The integers modulo n . . . 49
2.4 Rings . . . 56
2.4.1 Commutative and non-commutative rings . . . 59
2.4.2 Examples of commutative and noncommutative rings . . . 62
2.4.3 The additive inverse . . . 62
2.4.4 Multiplication by zero . . . 64
2.4.5 Identity; rings with identity . . . 65
2.4.6 Fields . . . 67
2.4.7 Is there a cancellation law for multiplication? . . . 67
2.4.8 A few very simple proofs: $2 + 2 = 4$, etc. . . . 69
2.4.9 Divisibility; factors . . . 73
2.4.10 More easy theorems . . . 76
2.4.11 Subtraction . . . 79
2.4.12 A few elementary formulas . . . 79
2.5 Even and odd numbers . . . 81
2.5.1 The meaning of "even" and "odd" . . . 81
2.5.2 The parity of a sum and a product . . . 83
2.5.3 Odd and even numbers: what we know so far . . . 85
2.6 The natural numbers and the Principle of Mathematical Induction 86
2.6.1 New facts we need about $\mathbb{Z}$: the natural numbers . . . 86
2.6.2 What do we need to prove the missing facts? . . . 87
2.6.3 Why we need the Principle of Mathematical Induction . . . 88
2.6.4 Why induction is needed . . . 89
2.6.5 "And so on" is dangerous . . . 90
2.6.6 Why induction is valid . . . 91

3 Induction **93**
3.1 Introduction to the Principle of Mathematical Induction . . . 93
3.2 The Principle of Mathematical Induction (PMI) . . . 95
3.3 The proof by induction that every integer is of one and only one of the forms $2k$, $2k + 1$, $k \in \mathbb{Z}$ . . . 96
3.3.1 Our first proof by induction: the successor theorem . . . 97
3.3.2 A remark on the importance of parentheses . . . 99
3.3.3 Our second proof by induction: the sum theorem . . . 99
3.3.4 Our third proof by induction: proof that every integer is of one and onlty one of the forms $2k$, $2k + 1$, $k \in \mathbb{Z}$ . . . 100

4 Examples of proofs by induction **103**
4.1 Some divisibility theorems 103
4.2 An inequality 105
4.3 More inequalities, with applications to the computation of some limits 107
4.3.1 An application of Theorem 38: computing $\lim_{n\to\infty} \sqrt[n]{n}$ . . . 110
4.4 Some formulas for sums 112
4.5 Inductive definitions 114
4.5.1 The inductive definition of powers of a real number 116
4.5.2 The inductive definition of the factorial 117
4.5.3 The inductive definition of summation. 118
4.5.4 Inductive definition of product. 119
4.5.5 A simple example of a proof by induction using inductive definitions 120
4.5.6 Another simple example of a proof by induction using inductive definitions 121
4.5.7 Another simple example 122

5 Other forms of induction **127**
5.1 Induction with a different starting point (sometimes called "generalized induction") 127
5.2 Induction going forward and backward 131
5.3 Examples of proofs using induction going forward and backward . 134
5.3.1 A very simple example 134
5.3.2 Divisibility properties of products of consecutive integers . 137

1 A summary of Logic

1.1 Terms and sentences

1.1.1 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.

1.1.2 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 anumal 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[1] was "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[2]. I probably want to say that that the name of that cow over there is the 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 gropus of words (i.e.,. talk about the word or gourp of words), you ***must*** enclose the word or group of words in quotation marks.

[1]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.

[2]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.

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

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

1.1.3 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[3] the terms "four", "4", "two plus two", "$2+2$" , "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 "$\sum_{i=5}^{10}$".

1.1.4 Examples of terms and sentences

Example 1. The following expressions are terms:

- New York City;
- Mount Everest;

[3]Notice the use of the quotation marks, in keeping with the *use vs. mention* distinction explained in subsection 1.1.2. 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.)

- 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:

- $2 + 2 = 4$,
- $2 + x = 4$,
- $x + y = 0$,
- $x + y = 0$,
- $x + y > 0$,
- $(\exists y \in \mathbb{R})x + y = 0$,
- $(\exists y \in \mathbb{R})x + y < 0$,
- $(\forall y \in \mathbb{R})x + y = 0$,
- $(\forall y \in \mathbb{R})(\exists z \in \mathbb{R})y + z = x$.
- $(\forall x \in \mathbb{R})x.0 = 0$,
- $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})x + y > 0$,
- $(\forall x \in \mathbb{R})x^2 \geq 0$,
- $\sum_{x=1}^{5} x^2 = y$.
- $(\forall x \in \mathbb{R})x.0 = 0$,
- $\sum_{x=1} 5x^2 = y$.

1.1.5 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 "$\sum_{i=5}^{10} i^3 = 2,955$".

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***[4] 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 threee functions, then the expression "$((f+g) \cdot g) \circ h$" is a term whose value is a function.

- ***Sets***[5] 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 Cartesion product of $\mathbb{Z}$ and $\mathbb{R}$.

1.1.6 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 3 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 3, 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 3 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 "$\sum_{i=5}^{10} i^3$" 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:

[4] We will talk about functions later in the course.
[5] We will discuss sets in detail later later in the course.

   (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.

1.1.7 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 values to each of the 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:

$$\text{Let } \; x = 3\,, \;\; y = -1\,, \;\; z = 4\,.$$

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

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.

1.1.8 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***[6]. (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 and are very long. For example, the term

$$32 + 5\frac{1+\sqrt{5}}{2} - 23\left(\frac{1+\sqrt{5}}{2}\right)^2 + +7\left(\frac{1+\sqrt{5}}{2}\right)^3 + 19\left(\frac{1+\sqrt{5}}{2}\right)^4 \qquad (1.1)$$

can be written as

$$\left(32 + 5x - 23x^2 + 7x^3 + x^4\right)_{x=\frac{1+\sqrt{5}}{2}} \ , \qquad (1.2)$$

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".

[6]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.

Another example is the term

$$1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 + 7^3 + 8^3 + 9^3 + 10^3\,, \tag{1.3}$$

that can be written as

$$\sum_{k=1}^{10} k^3\,, \tag{1.4}$$

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 (1.2) is much shorter than the term (1.1), and the term (1.4) is much shorter than the term (1.3). And the diffrence becomes even more dramatic if consider very long terms, in which there is a computattion 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

$$\sum_{k=1}^{10{,}000} k^3\,. \tag{1.5}$$

If you wanted to write this without using the $\sum$ notation, you would have to write a sums of $10,000$ terms, which would of course be enormously long[7].

It is clear that:

- In (1.2), 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

$$(32 + 5u - 23u^2 + 7u^3 + u^4)_{u=\frac{1+\sqrt{5}}{2}}\,, \tag{1.6}$$

[7]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 inthe course we will see how to figure this out and get the answer farily fast.

this would describe exactly the same computationas (1.6), and the term would have exactly the same value and (1.2).

- Similarly, in (1.4), 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

$$\sum_{i=1}^{10} i^3\,,$$

or

$$\sum_{j=1}^{10} j^3\,,$$

or[8]

$$\sum_{x=1}^{10} x^3\,,$$

or

$$\sum_{\alpha=1}^{10} \alpha^3\,,$$

or

$$\sum_{\diamond=1}^{10} \diamond^3\,,$$

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

- 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

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

[8]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.

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

1.1.9 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

$$\sum_{j=1}^{N} j^2\,, \tag{1.7}$$

$$\sum_{x=1}^{N} x^2\,, \tag{1.8}$$

$$\sum_{q=1}^{N} q^2\,, \tag{1.9}$$

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 yuo have to do this: you give k all natural number values between 1 and N, for each such value you compute its suqare, and then you add all the results. In order to be able to do this, you have to ask "who is N?", but you don't 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.

1.1.10 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 gerenate 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

$$\text{the function } \mathbb{R} \ni x \mapsto 3(x+1)^4 + 6(x-1)^2 + e^x + e^{x^2}, \qquad (1.10)$$

  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 $3(x+1)^4 + 6(x-1)^2 + e^x + e^{x^2}$.

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

$$\text{the function } \mathbb{R} \ni u \mapsto 3(u+1)^4 + 6(u-1)^2 + e^u + e^{u^2},$$

and that would be exactly the same function. So ***the variable*** x ***in a funtion definition such as (1.10) is dummy.***

Remark 1. 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. □

1.1.11 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 2.

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 oepn 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 "$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2)$" 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

   $$(\forall m \in \mathbb{Z})(2|m \Longrightarrow 4|m^2)\,, \tag{1.11}$$
   $$(\forall q \in \mathbb{Z})(2|q \Longrightarrow 4|q^2)\,, \tag{1.12}$$
   $$(\forall u \in \mathbb{Z})(2|u \Longrightarrow 4|u^2)\,, \tag{1.13}$$

   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 persons 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 definte 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

   $$(\forall m \in \mathbb{Z})(a|m \implies b|m^2)\,, \tag{1.14}$$
   $$(\forall q \in \mathbb{Z})(a|q \implies b|q^2)\,, \tag{1.15}$$
   $$(\forall u \in \mathbb{Z})(a|u \implies b|u^2)\,, \tag{1.16}$$

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

   (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 "$(\forall n \in \mathbb{Z})(a|n \implies b|n^2)$", 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 person 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

$$p \in \mathbb{Z} \wedge p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(jk = p \implies (j = 1 \vee k = 1)\Big) \quad (1.17)$$

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

$$(\forall p \in \mathbb{Z})\left(p > 1 \wedge (\forall j \in \mathbb{N})(\forall k \in \mathbb{N})\Big(jk = p \implies (j = 1 \vee k = 1)\Big)\right) \quad (1.18)$$

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[9] (1.18). This, of course, is wrong. The students want to say "p is prime if and only if (1.17) holds", but instead they end up saying "every integer is prime", without understanding the difference. ***Please do not do that in your exam.*** □

Example 3. In each of the following sentences, the variable n is bound:

[9] 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.

- "$(\forall n \in \mathbb{Z}) n^2 - n$ 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".)

- "$\sum_{n=1}^{m} n^3 = \left(\frac{m(m+1)}{2}\right)^2$". (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

Example 4. The same letter varible can occur is 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 abotu an ***occurrence*** of a variabel being free or bound.

For example, let S be the sentence

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

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

1.1.12 A challenging problem

Example 5. The sentence

$$
\begin{aligned}
&(\exists u \in \mathbb{N})(\exists v \in \mathbb{N})(\forall k \in \mathbb{N})\Big(k < m \Longrightarrow \\
&(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(\exists q' \in \mathbb{Z})(\exists r' \in \mathbb{Z}) \\
&\Big(u = (1+kv)q + r \wedge r < v \wedge u = (1+(k+1)v)q' + r' \wedge r' < v \\
&\wedge r' > r \wedge \wedge(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})\big(ab = r' \Longrightarrow (a = 1 \wedge b = 1)\big) \qquad (1.19) \\
&\wedge (k = 1 \Longrightarrow r = 2) \wedge (k = m-1 \Longrightarrow r' = n) \wedge \\
&(\forall s \in \mathbb{N})\big((r < s \wedge s < r') \\
&\Longrightarrow (\exists c \in \mathbb{N})(\exists d \in \mathbb{N})(c > 1 \wedge d > 1 \wedge cd = s)\big)\Big)\Big)
\end{aligned}
$$

contains the 14 variables $u, v, k, m, q, r, q', r', a, b, s, c, d, n$. All these variables are bound, except for m and n. And, believe it or not, the sentence says something very simple: "n is the m-th prime number". (The first prime number is 2. The second prime number is 3. And so on: the $m+1$-th prime number is the smallest prime number larger that the m-th prome number.)

So, for example, (1.19) is true for $m = 1$, $n = 2$, for $m = 2$, $n = 3$, for $m = 3$, $n = 5$, for $m = 4$, $n = 7$, for $m = 5$, $n = 11$, for $m = 6$, $n = 13$, and so on. And it is false if $m = 1$ and $n \neq 2$, or if $m = 2$ and $n \neq 3$, or if $m = 3$ and $n \neq 5$, or if $m = 4$ and $n \neq 7$, or if $m = 5$ and $n \neq 11$, or if $m = 6$ and $n \neq 13$. □

Problem 1. ***A challenging problem. Prove*** that the sentence (1.19) says "n is the m-th prime number". I am not asking you to do this as homework, because it is very complicated. You would have to prove two implications: (1) that if (1.19) holds then n is the m-th prime number, and (2) that if n is the m-th prime number then (1.19) holds. The first part is easier, although it is quite a lot of work. The second part is harder, and requires using the Chinese Remainder Theorem. □

1.1.13 A convention about naming sentences

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 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.

Example 6.

- 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.)

1.1.14 Some problems

Problem 2. ***Prove*** each of the following propositions:

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

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. $(\forall n \in \mathbb{N})\Big(n^3 < 2^n + 257 \Longrightarrow (n+1)^3 < 2^{n+1} + 257\Big)$.

1.2 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.

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

Example 7. One of the rules of logic is Rule $\forall_{use}$, which says that 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 sentcen $P(x)$ and any term t, with no restictions. Then we would be able to take the sentence

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R}) y \neq x$$

which is of the form $(\forall x \in \mathbb{R})P(x)$, with $P(x)$ being the sentence "$(\exists y \in \mathbb{R})x \neq y$", and substitute for x the term "y", obtaining the sentence

$$(\exists y \in \mathbb{R})y \neq y\,,$$

which is definitely false.

Example 8. Here is another example, showing what can go wrong with substitutions if you allow substitutions of terms that are not free.

Suppose we did allow substitutions of terms that are not free.

Then you could have a proof in which at some point you declare y to be 5, by writing

$$\text{Let} \qquad y = 5\,.$$

Suppose that you then prove that

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

which is clearly true.

Then you would be able to use Rule $\forall_{use}$ and conclude that

$$(\exists y \in \mathbb{R})y \neq 5\,. \tag{1.20}$$

If we let $P(x)$ be the sentence "$(\exists y \in \mathbb{R})y \neq x$", then (1.20) is $P(5)$. Since we have "$y = 5$", Rule SEE (substitution of equals for equals) would allow use to go to $P(y)$, i.e.,

$$(\exists y \in \mathbb{R})y \neq y\,. \tag{1.21}$$

But ***(1.21) is manifestly false!***

In order to avoid the problems that have been exhibited in the teo previous examples, 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 "$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})y \neq x$" 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 "$(\exists y \in \mathbb{R})y \neq y$".

1.3 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 moos" is not a grammatically correct English sentence, because the subject is the noun "cows", which is plural, and the verb is "moos", which is singular[10]

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

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 anpother part that deals with the formation of atomicn 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.
- 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.

[10]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 "moos", "swims", "walks") and the plural is without the "s" (as in "moo", "swim", "walk"), so "cows moo" and "ducks swim" are grammatically correct, but "cows moos" and "ducks swims" are not. Go figure!

Example 9. 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.

Example 10. Suppose we had written

is of the form $A \Longrightarrow B$, we enclosed

we first form the sentence "if n is even then $n+1$ is odd", that is,

and 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.

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

you could use "x" to stand for any number you want,

1.4 How sentences are constucted

1.4.1 The seven logical connective symbols

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.

1.4.2 The quantifiers

- A quantifier is an expression

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

  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,

1.4.3 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 "$(\exists x \in S)P(x)$").

1.5 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 11. 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.

1.5.1 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 12. Suppose you want to say

> It is not true that p is prime if and only if $p > 1$ and for every natural number k if $k|p$ then $k = 1$ or $k = p$.

You start with the atomic sentences "p is prime", "$p > 1$", "$k|p$", "$k = 1$" and "$k = p$". You conbine "$k = 1$" and "$k = p$" by forming "$k = 1 \vee k = p$". Then you want to combine "$k = 1 \vee k = p$" with "$k|p$" and form the implication "if $k|p$ then $k = 1 \vee k = p$. But, since "$k = 1 \vee k = p$" us a disjunction, we

have to enclose it in parentheses first. So we get "$k|p \Longrightarrow (k = 1 \vee k = p)$". Now we want to universally quantify this by writing "$(\forall k \in \mathbb{N})$" to its left. But, since "$k|p \Longrightarrow (k = 1 \vee k = p)$" is an implication, we have to enclose it in parentheses first. So we get "$(\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)$". Now we form the conjunction of this with "$p > 1$". Since "$(\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)$ is not an "$\wedge$" or "$\vee$" or "$\Longrightarrow$" or "$\Longleftrightarrow$" sentence, we do not need to enclose it in partheses. So we write

$$p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big). \tag{1.22}$$

Next, we want to combine this with "p is prime" using a biconditional. Since (1.22) is a "$\wedge$" sentence, we have to enclose it in parentheses first. So we get

$$p \text{ is prime} \Longleftrightarrow \Big(p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\Big). \tag{1.23}$$

(The sentence "p is prime" does nto need to be enclosed in parnetheses, because it is not an "$\wedge$" or "$\vee$" or "$\Longrightarrow$" or "$\Longleftrightarrow$" sentence.) Finally, we want to negate that by writing "$\sim$" in front. But, since (1.23) is a biconditional, we have to enclose it in parentheses first. So we get, finally,

$$\sim \Big(p \text{ is prime} \Longleftrightarrow \Big(p > 1 \wedge (\forall k \in \mathbb{N})\Big(k|p \Longrightarrow (k = 1 \vee k = p)\Big)\Big)\Big). \tag{1.24}$$

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

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 $P(t)$.

1.7 Some problems, with solutions

Problem 3. For the sentence

$$(\forall n \in \mathbb{Z})(\exists m \in \mathbb{Z})m > n\,, \tag{1.25}$$

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 (1.25) says: "for every integer n there exists an integer m such that $m > n$".
ii. The variables occurring in (1.25) 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 (1.25):*

> 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 4. For the sentence

$$(\exists m \in \mathbb{Z})m > n\,, \tag{1.26}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.26) says: "there exists an integer m such that $m > n$".
ii. The variables occurring in (1.26) 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 5. For the sentence

$$(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})m > n\,, \tag{1.27}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.27) says: "there exists an integer m such that m is larger than every integer".
ii. The variables occurring in (1.27) 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 (1.27) 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 6. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \Longrightarrow 4|n^2), \tag{1.28}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.28) says: "the square of every even integer is divisible by 4".

ii. The only variable occurring in (1.28) 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 (1.28):*

We want to prove the universal sentence (1.28), 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 7. For the sentence

$$(\forall n \in \mathbb{Z})2|n \Longrightarrow 4|n^2\,, \tag{1.29}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.29) says: "if every integer is even then n^2 is divisible by 4".
ii. The only variable occurring in (1.25ax) is n. This variable occurs in (1.29) 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 8. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \wedge 4|n^2), \tag{1.30}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.30) says: "for every integer n, n is even and n^2 is divisible by 4".
ii. The only variable occurring in (1.28) 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 (1.30) 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 9. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \vee 4|n^2), \tag{1.31}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.31) says: "for every integer n, n is even or n^2 is divisible by 4".
ii. The only variable occurring in (1.28) 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 (1.31) 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 10. For the sentence

$$(\forall n \in \mathbb{Z})(2|n \iff 4|n^2), \tag{1.32}$$

perform exactly the same tasks i., ii., iii., and iv. (a. and b.) as in Problem 3.

Solution.

i. Sentence (1.28) 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 (1.28) 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 (1.32):

We want to prove the universal sentence (1.32). 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 6.

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 $\implies_{prove}$, that $4|n^2 \implies 2|n$.

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

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

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

Q.E.D.

Problem 11. Let A, B, C be propositions. ***Prove***, using the rules of logic, that

$$\big(A \Longrightarrow (B \Longrightarrow C)\big) \Longleftrightarrow \Big((A \wedge B) \Longrightarrow C\Big)\,. \tag{1.33}$$

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

$$\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \Longrightarrow \big((A \wedge B) \Longrightarrow C\big)\,, \tag{1.34}$$

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

$$\big((A \wedge B) \Longrightarrow C\big) \Longrightarrow \Big(A \Longrightarrow (B \Longrightarrow C)\Big), \tag{1.35}$$

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 (1.34) and (1.35), we can conclude from Rule $\Longleftrightarrow_{prove}$ that

$$\Big(A \Longrightarrow (B \Longrightarrow C)\Big) \Longleftrightarrow \big((A \wedge B) \Longrightarrow C\big), \tag{1.36}$$

Q.E.D.

Problem 12. Let $P(x)$, $Q(x)$, be one-variable predicates, and let S be a set.

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

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longleftrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \tag{1.37}$$

   (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 (1.37) is true.)

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

$$(\forall x \in S)(P(x) \vee Q(x)) \Longleftrightarrow \Big((\forall x \in S)P(x) \vee (\forall x \in S)Q(x)\Big) \tag{1.38}$$

   cannot be proved using the rules of logic. (HINT: Find an example of a pair of predicates $P(x)$, $Q(x)$ for which (1.38) is false.)

Solution. First, we prove (1.37).

Sentence (1.37) is a biconditional, of the form $P \Longleftrightarrow Q$. So, in order to prove it, we will use Rule $\Longleftrightarrow_{prove}$, and prove both $P \Longrightarrow Q$ and $Q \Longrightarrow P$.

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

Assume

$$(\forall x \in S)(P(x) \wedge Q(x))\,. \tag{1.39}$$

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 (1.39)]

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 (1.39)]

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

$$(\forall x \in S)P(x) \wedge (\forall x \in S)P(x)\,, \tag{1.40}$$

by Rule $\wedge_{prove}$.

Since we have proved 1.40) assuming (1.39), we can go to

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)\,, \tag{1.41}$$

completing the proof of (1.41).

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

$$(\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\,. \tag{1.42}$$

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

Let u be an arbitrary member of S.

It follows from (1.42) 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

$$(\forall x \in S)(P(x) \wedge Q(x))\,. \tag{1.43}$$

Since we have proved (1.43) assuming (1.42), it follows from Rule $\Longrightarrow_{prove}$ that

$$\Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big) \Longrightarrow (\forall x \in S)(P(x) \wedge Q(x))\,. \tag{1.44}$$

completing the proof of (1.44).

Since we have proved (1.41) and (1.44), it follws by Rule $\Longleftrightarrow_{prove}$ that

$$(\forall x \in S)(P(x) \wedge Q(x)) \Longleftrightarrow \Big((\forall x \in S)P(x) \wedge (\forall x \in S)Q(x)\Big)\,, \tag{1.45}$$

Q.E.D.

We now prove that (1.38) cannot be proved. We do this by exhibitng examples of a set S and predicates $P(x)$, $Q(x)$ for which (1.38) 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.

2 An introduction to elementary arithmetic

2.1 What is arithmetic?

According to the Oxford English Dictionary (OED), the Oxford Learner's Dictionafry (OPD), and *Dictionary.com* (Dc), arithmetic is

- the branch of mathematics dealing with the properties and manipulation of numbers (OED),
- the type of mathematics that deals with the adding, multiplying, etc. of numbers (OLD),
- the theory of numbers; the study of the divisibility of whole numbers, the remainders after division, etc. (Dc).

So, as you can see, arithmetic is concerned with the properties of the basic operations on numbers: addition, subtraction, multiplication and division. And, as the definition in *Dictionary.com* indicates, ***the most interesting of these operations is division***.

2.2 Numbers

And, as we have discussed before, there are many kinds of "numbers". These numbers are organized into ***number systems***. The most important examples of number systems are:

1. the integers,
2. the rational numbers,
3. the real numbers,

4. the complex numbers[11].

In mathematical language, for each of these number systems the set of numbers has a name:

- the set of all integers is called $\mathbb{Z}$; so "$x \in \mathbb{Z}$" is a way to say that x is an integer[12];
- the set of all rational numbers is called $\mathbb{Q}$; so "$x \in \mathbb{Q}$" is a way to say that x is a rational number;
- the set of all real numbers is called $\mathbb{R}$; so "$x \in \mathbb{R}$" is a way to say that x is a real number;
- the set of all complex numbers is called $\mathbb{C}$; so "$x \in \mathbb{C}$" is a way to say that x is a complex number.

2.2.1 Operations

Unary and binary operations

An operation is a way of combining one or several objects of one or several kinds, called the inputs, or arguments, of the operation and producing a new object, called the result, or output, which may be of the same kind as the arguments.
An operation with one argument is called a unary operation.
An operation with two arguments is called a binary operation.

Example 13.

- ***Addition of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer $m + n$, called the ***sum*** of m and n.
- ***Multiplication of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer mn, called the ***product*** of m and n.

[11] If you are not familiar with the complex numbers, do not worry; we are not going to need them in this course, but in any case I will explain what they are later.

[12] It is customary to use letters such as m, n, p, q, rather than x, for integers, but it is perfectly legitimate to use x.

- ***Subtraction of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer $m-n$, called the ***difference*** of m and n.
- ***Addition, multiplication, and subtraction of rational numbers*** are binary operations whose arguments and outputs are rational numbers.
- ***Addition, multiplication, and subtraction of real numbers*** are binary operations whose arguments and outputs are real numbers.
- ***Addition, multiplication, and subtraction of complex numbers*** are binary operations whose arguments and outputs are complex numbers.
- ***Minus*** (or "***negative of***") is a unary operation on the integers: it takes an integer n as input and results in an integer $-n$, called "minus n", or "the negative of n", or "the additive inverse of n".
- Thera are similar "minus" unary operations on the rational numbers, the real numbers, and the complex numbers..
- The ***scalar product*** (a.k.a ***dot product***) of vectors in two or three dimensions is a binary operation that takes as inputs two vectors $\vec{v}, \vec{w}$ and produces as output a real number $\vec{v}\cdot\vec{w}$, called the ***scalar product***, or ***dot product***, of $\vec{v}$ and $\vec{w}$.
- The ***vector product*** of vectors in three dimensions is a binary operation that takes as inputs two three-dimensional vectors $\vec{v}, \vec{w}$ and produces as output a vector $\vec{v}\times\vec{w}$, called the ***vector product*** of $\vec{v}$ and $\vec{w}$. □

So in all the four number systems that we have seen so far—$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$—there are two important binary operations, addition and multiplication.

But these operations behave differently, and for that reason $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are very different. For example:

- In $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, the following "division theorem" is true[13]:

$$(\forall x)(\forall y)(y \neq 0 \Longrightarrow (\exists z)x = yz)\,. \tag{2.46}$$

[13]As explained in the box on page 48, if we are working in a number system $\mathfrak{N}$, the quantifiers "$(\forall x)$", "$(\forall y)$", "$(\exists z)$" mean "$(\forall x \in \mathfrak{N})$", "$(\forall y \in \mathfrak{N})$", "$(\exists z \in \mathfrak{N})$".

In other words, given any x and any y, as long as $y \neq 0$, it is possible to ***divide*** x ***by*** y ***exactly***, that is, find a "quotient" z such that $yz = x$.

- In $\mathbb{Z}$, the "division theorem" (2.46) is not true, but there is a different theorem, the division theorem for integers[14]:

$$(\forall x)(\forall y)\Big(y \neq 0 \Longrightarrow (\exists z)(x = yz + r \wedge 0 \leq r < |y|)\Big)\,. \tag{2.47}$$

In other words, given any x and any y, as long as $y \neq 0$, it is possible to ***divide*** x ***by*** y ***with a remainder*** that is, find a "quotient" z and a "small remainder" r such that $x = yz + r$; the remainder r is 'small" in the precise sense that $0 \leq r < |y|$..

- For example:
  - In $\mathbb{Q}$, if we take $x = 23$, $y = 6$, and we want to divide x by y, we can find z such that $x = yz$. (The value of z is $\frac{23}{6}$, of course.)
  - But in $\mathbb{Z}$ the situation is very different: if we take $x = 23$, $y = 6$, and we want to divide x by y, we can find z, r such that $x = yz + r$ and $0 \leq r < 6$. (The values of z and r are: $z = 3$, $r = 5$.)

AN IMPORTANT CONVENTION ABOUT QUANTIFIERS

When we are studying a particular number system $\mathfrak{N}$, then we just write "$(\forall x)$" and "$(\exists x)$" instead of "$(\forall x \in \mathfrak{N})$" and "$(\exists x \in \mathfrak{N})$". In other words: when the range of a variable in a quantifier is not specified it is understood that the range is $\mathfrak{N}$. So, for example, if we are studying $\mathbb{R}$, the real number system, and we want to say "for every real number x there exists an integer n that is larger than x", we can write "$(\forall x)(\exists n \in \mathbb{Z})n > x$". It is understood that "$(\forall x)$" means "$(\forall x \in \mathbb{R})$". But we have to write "$(\exists n \in \mathbb{Z})$", because if we wrote "$(\exists n)$" this would be interepreted as "$(\exists n \in \mathbb{R})$".

[14] In this case, the conventions of the box on page 48 tell us, since we have announced that we are working in $\mathbb{Z}$, that the quantifiers "$(\forall x)$", "$(\forall y)$", "$(\exists z)$", "$(\exists r)$" mean mean "$(\forall x \in \mathbb{Z})$", "$(\forall y \in \mathbb{Z})$", "$(\exists z \in \mathbb{Z})$", "$(\exists r \in \mathbb{Z})$".

2.3 Other number systems: The integers modulo n

In order to understand how $\mathbb{Z}$ is different from other number systems, mathematicians have come to the conclusion that it is very convenient and very interesting to study lots of other number systems, in addition to $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. So let me start by presenting a whole infinite class of new number systems: the integers modulo n.

For each natural number n such that $n \geq 2$, we define the set $\mathbb{Z}_n$ of ***integers modulo*** n.

- The members of $\mathbb{Z}_n$ are the numbers $0, 1, 2, \ldots, n-1$, so $\mathbb{Z}_n$ has n members[15].
- The operations of ***addition*** and ***multiplication*** in $\mathbb{Z}_n$ are performed as follows: to add or multiply two members a, b of $\mathbb{Z}_n$, we add them or multiply them as ordinary integers. and then "reduce the result modulo n", by subtracting a multiple of n so as to produce a result that belongs to $\mathbb{Z}_n$.

Example 14. The set $\mathbb{Z}_7$ of integers modulo 7 has seven members: 0, 1, 2, 3, 4, 5, and 6. That is,

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

To add or multiply two members of $\mathbb{Z}_7$ in $\mathbb{Z}_7$ we add them or multiply them as integers, but if the result is 7 or larger than 7 then we subtract 7, and then subtract 7 again if necessary, until we end up with a result in $\mathbb{Z}_7$. So,

[15]This is why we take $n \geq 2$. We could also study $\mathbb{Z}_1$, the integers modulo 1, but this set would have only one member, namely, 0, and this would not be interesting.

for example, the following are true in $\mathbb{Z}_7$:

$$\begin{aligned} 2+3 &= 5\,, \\ 3+4 &= 0\,, \\ 2+6 &= 1\,, \\ 4+5 &= 2\,, \\ 5+6 &= 4\,, \\ 2\times 3 &= 6\,, \\ 3\times 4 &= 5\,, \\ 2\times 6 &= 5\,, \\ 4\times 5 &= 6\,, \\ 5\times 6 &= 2\,. \end{aligned}$$

(For example, we get the equality $5 \times 6 = 2$ as follows: in $\mathbb{Z}$, 5 times 6 is equal to 30, but then we have to reduce modulo 7, for which purpose we have to subtract 7 four times, i.e., subtract 28, thus ending up with 2 as the final result.)

Example 15. The set $\mathbb{Z}_{12}$ of integers modulo 12 has twelve members: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11. That is,

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\,.$$

To add or multiply two members of $\mathbb{Z}_{12}$ in $\mathbb{Z}_{12}$ we add them or multiply them as integers, but if the result is 12 or larger than 12 then we subtract 12, and then subtract 12 again if necessary, until we end up with a result belonging to $\mathbb{Z}_{12}$. So, for example, the following are true in $\mathbb{Z}_{12}$:

$$\begin{aligned} 2+3 &= 5\,, \\ 3+4 &= 7\,, \\ 4+9 &= 1\,, \\ 9+7 &= 4\,, \\ 2\times 3 &= 6\,, \\ 3\times 4 &= 0\,, \\ 4\times 9 &= 0\,, \\ 9\times 7 &= 3\,. \end{aligned}$$

(For example, we get the equality $9 \times 7 = 3$ as follows: in $\mathbb{Z}$, 9 times 7 is equal to 63, and then we have to reduce modulo 12, for which purpose we have to subtract 12 five times, i.e., subtract 60, thus ending up with 3 as the final result.)

Example 16. The set $\mathbb{Z}_{103}$ of integers modulo 103 has 103 members, namely, all the integers n such that $0 \leq n < 103$. I do not write down the full list for obvious reasons. But it is possible to write down a formal definition using the langauge of sets, as follows

$$\mathbb{Z}_{103} = \{n \in \mathbb{Z} : 0 \leq n < 103\}\,. \tag{2.48}$$

(The rigth-hand side of (2.48) means "the set of all integers n such that $0 \leq n < 103$".)

To add or multiply two members of $\mathbb{Z}_{103}$ in $\mathbb{Z}_{103}$ we add them or multiply them as integers, but if the result is 103 or larger than 103 then we subtract 103, and then subtract 103 again if necessary, until we end up with a result belonging to $\mathbb{Z}_{103}$. So, for example, the following are true in $\mathbb{Z}_{103}$:

$$\begin{aligned} 56 + 87 &= 40\,, \\ 56 \times 87 &= 31\,. \end{aligned}$$

How do we find that $56 \times 87 = 41$? You compute the product 56×87 in $\mathbb{Z}$, and get

$$56 \times 87 = 4872 \qquad \text{in} \quad \mathbb{Z}\,.$$

Then, using the method for dividing integers that you learned in high school, you get

$$4872 = 47 \times 103 + 31 \qquad \text{in} \quad \mathbb{Z}\,.$$

so in $\mathbb{Z}_{103}$ $56 \times 87 = 31$.

Problem 13. In a number system $\mathfrak{N}$ in which there is a multiplicative identity[16] 1, a multiplicative inverse of a number $a \in \mathfrak{N}$ is a member b of $\mathfrak{N}$ such that $ab = 1$.

Find

1. a multiplicative inverse of 4 in $\mathbb{Z}_7$,

[16]The defition of "multiplicative identity" is given in Definition 7, on page 65.

2. a multiplicative inverse of 23 in $\mathbb{Z}_{41}$,

3. a multiplicative inverse of 48 in $\mathbb{Z}_{103}$.

Solution:

1. To find a multiplicative inverse of 4 in $\mathbb{Z}_7$ we just use trial and error: we try multiplying 4 in $\mathbb{Z}_7$ by all the members of $\mathbb{Z}_7$ until we find one for which the product is 1. Clearly, $0 \times 4 = 0$, $1 \times 4 = 4$, and $2 \times 4 = 1$. So 2 ***is a multiplicative inverse of*** 4 ***in*** $\mathbb{Z}_7$.

2. To find a multiplicative inverse of 23 in $\mathbb{Z}_{41}$, trial and error would take too long, so we try something smarter: we are looking for a member n of $\mathbb{Z}_{41}$ such that $23n = 1$ in $\mathbb{Z}_{41}$. This means that, in $\mathbb{Z}$, $23n - 1$ is divisible by 41, i.e., $23n - 1 = 41q$ for some integer q. So we try to find integers n, q such that $23n + 41(-q) = 1$. In other words, we have to solve the Diophantine equation[17]

$$23u + 41v = 1\,,$$

and then take $n = u$, $q = -v$.

And we know how to do that: we solve the equation

$$23u + 41v = c$$

for some positve integer value of c, and then we do it for msaller and smaller value sof c until we get to $c - 1$.

An obvious first choice of u, v is $u - 2$, $v = -1$. We have

$$23 \times 2 + 41 \times (-1) = 5\,, \tag{2.49}$$

so we have solved $23u + 41v = c$ for $c = 5$. which is not the same as $c = 1$, but is close.

Now we multiply both sides by 4 and get

$$23 \times 16 + 41 \times (-4) = 40\,, \tag{2.50}$$

[17] A Diophantine equaton is an equation for which we are only interested in integer solutions.

But $40 = 41 - 1$, so

$$23 \times 16 + 41 \times (-4) = 41 - 1\,,$$

and then

$$23 \times 16 + 41 \times (-5) = -1\,,$$

Then

$$23 \times (-16) + 41 \times 5 = 1\,,$$

Now, $-16 = 25 - 41$, so

$$23 \times (25 - 41) + 41 \times 5 = 1\,,$$

and then

$$23 \times 25 - 23 \times 41 + 41 \times 5 = 1\,,$$

$$23 \times 25 - 18 \times 41 = 1\,,$$

so, finally,

$$23 \times 25 = 1 + 18 \times 41\,.$$

This means that in $\mathbb{Z}_{41}$ $23 \times 25 = 1$, and we have shown that the multiplicative inverse[18] of 23 is 25. So, finally, our answer is $\boxed{25}$.

Verification: In $\mathbb{Z}_{41}$:

$$\begin{aligned} 23 \times 25 &= 23 \times 5 \times 5 \\ &= 115 \times 5 \\ &= (82 + 33) \times 5 \\ &= (41 \times 2 + 33) \times 5 \\ &= 33 \times 5 \\ &= 165 \\ &= 164 + 1 \\ &= 41 \times 4 + 1 \\ &= 1\,. \end{aligned}$$

[18]Strictly speaking, we have shown that 25 is ***a*** multplicative inverse of 23 in $\mathbb{Z}_{41}$ $23 \times 25 = 1$. There could be other multipicative inverses. It turns out that ***there are no other inverses***.

3. To find a multiplicative inverse of 48 in $\mathbb{Z}_{103}$ we use a similar method as for the previous question. First. we observe that 48×2 equals 96, which in 103 is equal to -7. So $48 \times 2 = -7$. Next, $7 \times 15 = 105$, so $7 \times 15 = 2$ in $\mathbb{Z}_{103}$, and then $(-7) \times 15 = -2$. Then

$$\begin{aligned} (48 \times 2) \times 15 &= (-7) \times 15 \\ &= -2\,, \end{aligned}$$

but

$$\begin{aligned} (48 \times 2) \times 15 &= 48 \times (2 \times 15) \\ &= 48 \times 30\,, \end{aligned}$$

so $48 \times 30 = -2$, and then $48 \times (-30) = 2$. Since $-30 = 73$ in $\mathbb{Z}_{103}$, we get

$$48 \times 73 = 2\,.$$

Now, $104 = 2 \times 52$, so $2 \times 52 = 1$ in $\mathbb{Z}_{103}$. Hence

$$\begin{aligned} (48 \times 73) \times 52 &= 2 \times 52 \\ &= 1\,, \end{aligned}$$

while, on the other hand, $(48 \times 73) \times 52 = 48 \times (73 \times 52)$. So $48 \times (73 \times 52) = 1$. So the desired multiplicative inverse of 48 in $\mathbb{Z}_{103}$ is 73×52.

Finally,

$$\begin{aligned} 73 \times 52 &= -30 \times 52 \\ &= -3 \times 10 \times 52 \\ &= -3 \times 520 \\ &= -3 \times 5 \\ &= -15 \\ &= 88\,. \end{aligned}$$

So our final answer is that $\boxed{88}$ is a multiplicative inverse of 48 in $\mathbb{Z}_{103}$.

Verification: In $\mathbb{Z}_{103}$

$$\begin{aligned} 48 \times 88 &= 48 \times 2 \times 2 \times 2 \times 11 \\ &= 96 \times 2 \times 2 \times 11 \\ &= 192 \times 2 \times 11 \\ &= (103 + 89) \times 2 \times 11 \\ &= 89 \times 2 \times 11 \\ &= 178 \times 11 \\ &= (103 + 75) \times 11 \\ &= 75 \times 11 \\ &= 825 \\ &= 824 + 1 \\ &= (103 \times 8) + 1 \\ &= 1\,. \end{aligned}$$

Problem 14. ***Prove*** that 6 does not have a multiplicative inverse in $\mathbb{Z}_{12}$.

Solution:

Suppose[19] 6 had a multiplicative inverse in $\mathbb{Z}_{12}$. Pick one such inverse [20] and call it x, so

$$6x = 1 \text{ in } \mathbb{Z}_{12}\,.$$

Multiply both sides by 2. Then, in $\mathbb{Z}_{12}$,

$$2 \times (6x) = 2 \times 1 = 2\,,$$

while on the other hand

$$2 \times (6x) = (2 \times 6) \times x = 12x = 0.x = 0\,,$$

because in $\mathbb{Z}_{12}$ $12 = 0$.

So $2 = 0$. But in $\mathbb{Z}_{12}$ 2 is not 0. So we got a contradiction. **Q.E.D.**

Problem 15. ***Prove*** that 21 does not have a multiplicative inverse in $\mathbb{Z}_{60}$.

[19] Obviously, we are doing a proof by contradiction.

[20] Since $(\exists x \in \mathbb{Z}_{12})6x = 1$, where "$6x$" stands for the product of 6 and x in $\mathbb{Z}_{12}$, Rule $\exists_{use}$ allows us to pick a witness and call it x.

Solution:

Suppose 21 had a multiplicative inverse in $\mathbb{Z}_{60}$. Pick one such inverse and call it x, so

$$21x = 1 \text{ in } \mathbb{Z}_{60}\,.$$

Multiply both sides by 20. Then, in $\mathbb{Z}_{60}$,

$$20 \times (21x) = 20 \times 1 = 20\,,$$

while on the other hand

$$20 \times (21x) = 20 \times (3 \times 7x) = (20 \times 3) \times 7x = 60 \times 7x = 0 \times 7x = 0\,,$$

because in $\mathbb{Z}_{60}$ 60.

So $20 = 0$. But in $\mathbb{Z}_{60}$ 20 is not 0. So we got a contradiction. **Q.E.D.**

Problem 16. ***Prove*** that if $n \in \mathbb{N}$, $n > 1$, and n is not prime, then it is not true that every nonzero member of $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$.

Solution: **YOU DO THIS ONE.**

Hint: Read carefully the solutions of problems 14 and 15 and use the same method, Write $n = pq$, with $p, q \in \mathbb{Z}$ and $1 < p < n$, so $1 < q < n$, and then $p \in \mathbb{Z}_n$ and $q \in \mathbb{Z}_n$. Prove by contradiction that p (or q if you prefer) does not have a multiplicative inverse in $\mathbb{Z}_n$. □

2.4 Rings

All the number systems that we have discussed so far (that is, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the integers modulo n for every $n \in \mathbb{N}$ such that $n > 1$) have an operation of addition and an operation of multiplication. And these operations have certain properties that are similar for all these number systems.

Definition 1. A ring is a set $\mathfrak{R}$—whose members are called[21]

[21] What I mean by this is: Once it is clear that we are working on a specific ring $\mathfrak{R}$—say $\mathbb{Z}$, or $\mathbb{Q}$, or $\mathbb{E}$, or $\mathbb{Z}_5$, or $\mathbb{Z}_{239}$— then we can talk about "numbers", meaning "members of $\mathfrak{R}$". But if we have not made it clear which ring we are talking about, then statements like "let x be a number" are meaningless. You can see this by asking the question you should always ask: ***how do I say this in formal langiuage?"*** In formal language, there is no way to say "x is a number". You can say "x is an integer", or "x is a rational number", or 'x is a real number", or "x is an integer modulo 57", by saying "$x \in \mathbb{Z}$", or "$x \in \mathbb{Q}$", or "$x \in \mathbb{R}$", or "$x \in \mathbb{Z}_{57}$", But you cannot say "x is a number". On the other hand, if for example you declare at the beginning of a text that "from now on, until further notice, 'number' means 'integer' ", then you can talk about "numbers", with the understanding that this means "integers". And when you write "$(\exists x)P(x)$", this means "$(\exists x \in \mathbb{Z})P(x)$".

"numbers"—equipped with

1. a binary operation called ***addition***, that for every $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ produces a new object $x + y$ called "x plus y", or ***the sum of*** x ***and*** y;

2. a binary operation called ***multiplication***, that for every $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ produces a new object $x.y$ (or xy, or $x \times y$) called "x times y", or ***the product of*** x ***and*** y;

in such a way that the following "ring axioms" are satisfied.

THE RING AXIOMS

RA1: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(x + y \in \mathfrak{R} \wedge .x.y \in \mathfrak{R})$.
RA2: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})x + y = y + x$.
RA3: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x + (y + z) = (x + y) + z$.
RA4: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x(yz) = (xy)z$.
RA5: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x(y+z) = xy+xz \wedge (x+y)z = xz+yz$.
RA6: $(\exists x \in \mathfrak{R})(\forall y \in \mathfrak{R})x + y = y$.
RA7: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\exists z \in \mathfrak{R})z + y = x$.

Let us read and try to understand the ring axioms:

- Axiom RA1 is a ***closure axiom***: it says that $\mathfrak{R}$ is closed under addition and multiplication, meaning, simply, that the sum onad the product of two members of $\mathfrak{R}$ is in $\mathfrak{R}$.

- Axiom RA2 is the ***commutative law of addition***: the sum of two numbers is the same if you add them in the opposite order: $x+y = y+x$ for every $x, y \in \mathfrak{R}$.

- Axiom RA3 is the ***associative law of addition***: if x, y, z are three members of $\mathfrak{R}$ then $x + (y + z) = (x + y) + z$.

- Axiom RA4 is the ***associative law of multiplication***: if x, y, z are three members of $\mathfrak{R}$ then $x(yz) = (xy)z$.

- Axiom RA5 is the ***distributive law of multiplication with respect to addition***: if x, y, z are three members of $\mathfrak{R}$ then $x(y+z) = xy+xz$, and also $(x+y)z = xz+yz$.

- Axiom RA6 is the ***zero axiom***. This requires some explanation:

  - **Definition 2**. An ***additive identity*** of a ring $\mathfrak{R}$ is a member a of $\mathfrak{R}$ such that $a + x = x$ for every $x \in \mathfrak{R}$. □

  - It can be proved that ***an addtive identity, if it exists, is unique***. That is, we have

    Theorem 1. *If a and b are additive identities in $\mathfrak{R}$, then $a = b$.*

    Proof. Let a, b be additive identities. Then $a + x = x$ for every $x \in \mathfrak{R}$, so in particular $a + b = b$. Also, $b + x = x$ for every $x \in \mathfrak{R}$, so in particular $b + a = a$. But $a + b = b + a$ by the commutative law, so $a = b$. **Q.E.D.**

  - Axiom RA6 says that ***an additive identity exists***. Since we have proved that the additive identity, when it exists, is unique, we can take this unique additive identity and give it a name: zero.

    So we have

    Definition 3. In a ring $\mathfrak{R}$, the unique additive identity of $\mathfrak{R}$ is called zero, and is denoted by the symbol "0".

    It follows that

    $$(\forall x \in \mathfrak{R})0 + x = x\,, \tag{2.51}$$

    and, since $x + 0 = 0 + x$ for every x, it is also true that

    $$(\forall x \in \mathfrak{R})x + 0 = x\,, \tag{2.52}$$

- Axiom RA7 is the ***subtraction axiom***. This also requires explanation:

  - First, we define the notion of "difference" of two members of $\mathfrak{R}$:

    Definition 4. If $\mathfrak{R}$ is a ring and a, b are members of $\mathfrak{R}$, then a member c of $\mathfrak{R}$ is said to be ***a difference of*** b ***minus*** a if $c + a = b$. If a difference of b minus a exists and is unique, then we call it ***the*** difference of b minus a, and write "$b - a$" to denote it.

– Axiom RA7 says that for every pair a, b of member of $\mathfrak{R}$ there exists a difference of b minus a. And then we can prove

Theorem 2. *If $\mathfrak{R}$ is a ring then for every pair a, b of members of $\mathfrak{R}$ the difference of b minus a (which exists by Axiom RA7) is unique.*

Proof. Let c_1, c_2 be two differences of b minus a. Then c_1 and c_2 satisfy

$$\begin{aligned} c_1 + a &= b\,, \\ c_2 + a &= b\,. \end{aligned}$$

Let d be a member of $\mathfrak{R}$ such that $d + a = 0$. (Such d exists, by Axiom RA7, applied with $y = a$, $x = 0$.) Then

$$\begin{aligned} c_1 &= c_1 + 0 && (2.53)\\ &= c_1 + (d + a) && (2.54)\\ &= c_1 + (a + d) && (2.55)\\ &= (c_1 + a) + d && (2.56)\\ &= b + d && (2.57)\\ &= (c_2 + a) + d && (2.58)\\ &= c_2 + (a + d) && (2.59)\\ &= c_2 + 0 && (2.60)\\ &= c_2\,. && (2.61) \end{aligned}$$

So $c_1 = c2$.

– In view of Theorem 2, the difference b minus a exists and is unique for all a, b in $\mathfrak{R}$. So we can give ita name and call it $b - a$.

Problem 17. Prvide a justification for each of the nine steps (2.53), (2.54), (2.55), (2.56), (2.57), (2.58), (2.59), (2.60), (2.61) of theproof of Theorem 2. □

2.4.1 Commutative and non-commutative rings

You may have noticed that we did not include in our list of axioms the commutative law of multiplication:

THE COMMUTATIVE LAW OF MULTIPLICATION

RA8: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})xy = yx$.

We did so on purpose, because there are interesting rings for which the commutative law of multiplication does not hold.

Example 17. I will give you examples of ***noncommutative rings***, i.e., rings for which the commutative law of multiplication is not valid.

We use $M_{2\times 2}(\mathbb{R})$ to denote the set of all 2 by 2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with real entries (that is, such that a, b, c, d are real numbers).

We also use $M_{2\times 2}(\mathbb{Q})$ to denote the set of all 2 by 2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with rational ntries (that is, such that a, b, c, d are rational numbers).

And we also use $M_{2\times 2}(\mathbb{Z})$ to denote the set of all 2 by 2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with integer entries (that is, such that a, b, c, d are integers).

Actually, we could consider more generally, for any ring $\mathfrak{R}$, the set $M_{2\times 2}(\mathfrak{R})$ of all 2 by 2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with entries in $\mathfrak{R}$ (that is, such that a, b, c, d belong to $\mathfrak{R}$).

Addition and multiplication in $M_{2\times 2}(\mathfrak{R})$ are the usual operations of addition and multiplication of matrices:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \tag{2.62}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}. \tag{2.63}$$

The zero of $M_{2\times 2}(\mathfrak{R})$ is the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

It is easy (but very boring) to verify that ***if $\mathfrak{R}$ is any ring, then the set $M_{2\times 2}(\mathfrak{R})$, with the operations of addition and multiplication defined by formulas (2.62) and (2.63) is a ring***.

Problem 18. ***Prove*** that *if* $\mathfrak{R}$ *is a ring then* $M_{2\times 2}(\mathfrak{R})$ is a ring. You have to prove that

1. If A, B, C are 2×2 matrices, then

$$\begin{aligned} A + B &= B + A\,, \\ A + (B + C) &= (A + B) + C\,, \\ A(BC) &= (AB)C\,, \\ A(B + C) &= AB + AC\,, \\ (A + B)C &= AC + BC\,. \end{aligned}$$

2. There exists a "zero matrix", i.e. a matrix Z such that $Z + A = A$ for every A in $M_{2\times 2}(\mathfrak{R})$. Actually, this is very easy: all you have to do is take M to be the matrix. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

3. For every A, B there exists a matrix C such that $C + A = b$. This is also very easy: all you have to do is take C to be the matrix $B - A$.□

Problem 19. ***Prove*** that in $M_{2\times 2}(\mathfrak{R})$ the commutative law of multiplication is not valid. (HINT: Compute the products $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.)

Now that we know that there exist rings for which the commutative law of multiplication does not hold, we give names to those rings for which the law does hold and to those rings for which the law does not hold::

Definition 5.

- A commutative ring is a ring for which Axiom RA8 (that is, the commutative law of multiplication) is true.
- A noncommutative ring is a ring for which Axiom RA8 (that is, the commutative law of multiplication) is not true. □

2.4.2 Examples of commutative and noncommutative rings

The following are examples of commutative rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, as well as $\mathbb{Z}_n$ (the integers modulo n) for every natural number n such that $n > 1$.

The rings $M_{2\times 2}(\mathfrak{R})$ that we studied before, in Example 17, are examples of noncommutative rings.

2.4.3 The additive inverse

Definition 6. If $\mathfrak{R}$ is a ring and $a \in \mathfrak{R}$, then the additive inverse of a is $0 - a$. □

We write "$-a$" for "$0 - a$". If you remember that $b - a$ is defined to be the unique member z of $\mathfrak{R}$ such that $z + a = b$, then in particular: $-a$ ***is the unique member*** z ***of*** $\mathfrak{R}$ ***such that*** $z + a = 0$**.**

It is then clear from Definition 6 that

$$(\forall x \in \mathfrak{R})(-x) + x = 0\,. \tag{2.64}$$

Using additive inverses, we can prove a very useful little theoren, called the ***cancellation law for addition***, because it tells us that when we have an equality $a + b = a + c$ we can "cancel" the a term and end up with $b = c$.

Theorem 3. *Let $\mathfrak{R}$ be a ring, and let a, b, c be members of $\mathfrak{R}$. Then, if $a + c = b + c$, it follows that $b = c$.*

Proof.

$$\begin{aligned} b &= 0 + b && (2.65)\\ &= ((-a) + a) + b && (2.66)\\ &= (-a) + (a + b) && (2.67)\\ &= (-a) + (a + c) && (2.68)\\ &= ((-a) + a) + c && (2.69)\\ &= 0 + c && (2.70)\\ &= c && (2.71) \end{aligned}$$

So $b = c$. QED

Problem 20. Write down the justifications of each of the seven steps (2.65), (2.66), (2.67), (2.68), (2.69), (2.70), (2.71) of the proof of Theorem 3.

THE THREE NOTATIONS FOR MULTIPLICATION: $x.y$, xy, $x \times y$

Usually, we write "$x.y$" to denote the product of x and y (and we read this as "x times y".

But sometimes we write "'xy" rather than "$x.y$". (This is called juxtaposition: we write the name of one number and then the name of the other number, with nothing in between.)

The juxtaposition notation "xy" is more convenient when the numbers you are multiplying are being referred to by letter names, such as x, or y, or a, or b, or m, or n.

But when we are using ***numerals***[a], it would be disastrous if we used juxtaposition. For example, suppose we wanted to talk about "two times three", and we wrote "23". Then everybody would read this as "twenty-three"! So we do not want that. And it would not be any better if we wrote "2.3"? No! If we did this, then everybody would read "2.3" as "two point three", i.e., as the number which is equal to $\frac{23}{10}$, or $2 + \frac{3}{10}$. So, in order to avoid having these problems, we allow an alternative notation for the product of x times y, namely, "$x \times y$'.

And we use this notation for multiplication of numerals. So, for example, "two times three" is written as "2×3".

[a] A numeral is an expression that is the name of a natural number. For example, "1", "2", "35", "307", "$2,530,983$" are numerals. "Numeral" is not the same as "number". A numeral is not a number; it is a string of symbols that serves as the name of a number. And a numeral can stand for different numbers, depending on which number system you are working in. For example, in $\mathbb{Z}$ the numeral "85" stands for the number eighty-five. But in $\mathbb{Z}_{80}$ "85" is also another name for the number 5.

HOW TO READ THE "-" (MINUS) SIGN

I strongly recommend that you read "$-x$" as "minus x", rather that as "negative x".
Here is why: when you say "negative x", you are giving the strong impression that $-x$ is a negative number.
However, $-x$ ***need not be negative.*** For example, if $x = -5$, then $-x$ is 5, which is positive.
When you say "minus x", the danger that you will mistakenly think that $-x$ is negative is much smaller.

2.4.4 Multiplication by zero

As an application of the cancellation law, we prove that "anything multiplied by zero is zero".

Theorem 4. *Let $\mathfrak{R}$ be a ring. Then $x.0 = 0$ and $0.x = 0$ for every $x \in \mathfrak{R}$.*

Proof. We will prove that $(\forall x \in \mathfrak{R})x.0 = 0.$ and leave the proof of the other equality, i.e., $(\forall x \in \mathfrak{R})0.x = 0$, to the reader.

1. Let $x \in \mathfrak{R}$ be arbitrary.
2. $(\forall u)u = u.$ [Equality axiom]
3. $x.0 = x.0$ [Rule $\forall_{use}$]
4. $(\forall u \in \mathfrak{R})u + 0 = u).$ [Axiom RA8]
5. $0 + 0 = 0$ [Rule $\forall_{use}$]
6. $x.(0 + 0) = x.0$ [Rule SEE]
7. $x.(0 + 0) = x.0 + x.0$ [From Axiom RA7]
8. $x.0 + x.0 = x.0$ [Rule SEE]
9. $x.0 + 0 = x.0$ [Rule $\forall_{use}$, from Step 4]
10. $x.0 + x.0 = x.0 + 0$ [Rule SEE]
11. $x.0 = 0$ [From Theorem 3, and Step 10]

Q.E.D.

2.4.5 Identity; rings with identity

The basic axioms for rings never mention 1, and it is easy to give examples of rings that do not have a "one" (see Example 18 on page 66 below). But first let us be precise:

Definition 7. In a ring $\mathfrak{R}$, a multiplicative identity, or identity, is a member u of $\mathfrak{R}$ such that $ux = x$ and $xu = x$ for every $x \in \mathfrak{R}$. □

And it is easy to prove that an identity, when it exists, is unique:

Theorem 5. *Let $\mathfrak{R}$ be a ring. Then, if an identity in $\mathfrak{R}$ exists, then there is only one identity in $\mathfrak{R}$.*

Proof. Suppose u, v are identities. Then $uv = u$, because v is an identity, so $(\forall x \in \mathfrak{R})xv = x$. And $uv = v$, because u is an identity, so $(\forall x \in \mathfrak{R})ux = x$. So $u = v$. **Q.E.D.**

Definition 8.

- A ring with identity is a ring $\mathfrak{R}$ equipped with a special member called 1 ("one") for which the following axioms hold:

THE MULTIPLICATIVE IDENTITY AXIOMS
RA9: $1 \in \mathfrak{R}$,
RA10: $(\forall x \in \mathfrak{R})(x.1 = x \wedge 1.x = x)$,
RA11: $1 \neq 0$.

- A commutative ring with identity is a commutative ring $\mathfrak{R}$ which is also a ring with identity. □

So on a commutative ring with identity all 13 axioms RA1 through RA13 hold.

And, clearly, Axiom RA10 says that 1 is an identity of $\mathfrak{R}$. So we could equally well have defined "ring with identity" by saying the following:

- A ring with identity is a ring that has an identity and is such that this identity is not equal to zero.
- If $\mathfrak{R}$ is a ring with identity, then we know from Theorem 5 that this identity is unique.
- The unique identity of a ring with identity is called 1.

Example 18.

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the $\mathbb{Z}_n$ for every n, are commutative rings with identity.
- The rings $M_{2\times 2}(\mathfrak{R})$ introduced earlier in Example 17 are rings with identity but are noncommutative. The multiplicative identity of $M_{2\times 2}(\mathfrak{R})$ is the 2×2 identity matrix $\mathbb{I}_2$, given by

$$\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

- Let $\mathfrak{E}$ denote the set of all even integers. That is,

$$\mathfrak{E} = \{n \in \mathbb{Z} : 2|n\}.$$

  Then $\mathfrak{E}$ is a commutative ring without identity.

2.4.6 Fields

Definition 9. A field is a commutative ring with identity $\mathfrak{R}$ for which the following Multiplicative Inverse Axiom holds:

THE MULTIPLICATIVE INVERSE AXIOM

RA12: For every $x \in \mathfrak{R}$ such that $x \neq 0$ there exists a $y \in \mathfrak{R}$ such that $xy = 1$. (In formal langauge:
$(\forall x \in \mathfrak{R})(x \neq 0 \Longrightarrow (\exists y \in \mathfrak{R})xy = 1).)$

So in a field all twelve axioms RA1 to RA12 hold.

Example 19.

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.
- $\mathbb{Z}$ is not a field.
- We will prove later that
  - If $n \in \mathbb{N}$ and n is prime, then $\mathbb{Z}_n$ is a field.
  - If $n \in \mathbb{N}$, $n > 1$, and n is not prime, then $\mathbb{Z}_n$ is not a field.

2.4.7 Is there a cancellation law for multiplication?

In Theorem 3, on page 62, we proved the "cancellation law for addition": *in a ring $\mathfrak{R}$, if we have an equality $a+b = a+c$ then we can "cancel" the a and conclude that $b = c$,*

Is there a similar result for multiplication? Is it true that if $ab = ac$ then we can cancel a and conclude that $b = c$?

This is clearly impossible. For example, in the integers (or in any ring), $0.b = 0$ and $0.c = 0$ for every b, c, so if there was a cancellation law for multiplication, it would follow that $b = c$, for all b and all c.

It turns out that if we only try to cancel a when a is different from zero, then this is possible in some rings but not in all of them.

One example of a class of rings for which the cancellation law for multiplication is valid is that of ***fields***.

Theorem 6. *Let $\mathfrak{R}$ be a field. Then the following cancellation law for multiplication holds:*

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})(\forall c \in \mathfrak{R})\Big((a \neq 0 \wedge ab = ac) \Longrightarrow b = c\Big)\,. \tag{2.72}$$

Proof. Since $a \neq 0$, it follows from Axiom RA15 that there exists $u \in \mathfrak{R}$ such that $ua = 1$. Then

$$\begin{aligned} b &= 1.b && (2.73)\\ &= (u.a).b && (2.74)\\ &= u.(a.b) && (2.75)\\ &= u.(a.c) && (2.76)\\ &= (u.a).c && (2.77)\\ &= 1.c && (2.78)\\ &= c\,. && (2.79) \end{aligned}$$

So $b = c$. **Q.E.D.**

Problem 21. Write down the justifications of each of the seven steps (2.73), (2.74), (2.75), (2.76), (2.77), (2.78), (2.79), of the proof of Theorem 6.

Another example of a ring in which there is a cancellation law for multiplication is $\mathbb{Z}$:

Theorem 7. *The following cancellation law for multiplication holds in $\mathbb{Z}$:*

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big((a \neq 0 \wedge ab = ac) \Longrightarrow b = c\Big)\,. \tag{2.80}$$

Proof. Let a, b, c be arbitrary integers such that $a \neq 0$ and $ab = ac$.

Then a and b are rational numbers[22]. Since the set $\mathbb{Q}$ of rational numbers is a field, the cancellation law for multipicaton holds in $\mathbb{Q}$ (Theorem 6). Since $ab = ac$ and $a \neq 0$, it follows that $b = c$. **Q.E.D.**.

Example 20.

- The cancellation law

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})(\forall c \in \mathfrak{R})\Big((a \neq 0 \wedge ab = ac) \Longrightarrow b = c\Big) \qquad (2.81)$$

  holds if $\mathfrak{R} = \mathbb{Z}_7$.

  You can prove this directly by computing all 49 products ab, for all $a, b \in \mathbb{Z}_7$, and verifying that it never happens that $ab = ac$, $a \neq 0$, and $b \neq c$. But you can save a lot of time by using the fact, that will be proved later, that ***if*** n ***is prime then*** $\mathbb{Z}_n$ ***is a field.*** Once you know this, it follows that $\mathbb{Z}_7$ is a field, because 7 is prime, and then the cancellation law (2.81) holds for $\mathfrak{R} = \mathbb{Z}_7$, because of Theorem 6.

- The cancellation law (2.81) holds if $\mathfrak{R} = \mathbb{Z}_{103}$.

  You can prove this directly by computing all $10,609$ products ab, for all $a, b \in \mathbb{Z}_{103}$. But it is easier to observe that 103 is prime.

- The cancellation law (2.81) does not hold if $\mathfrak{R} = \mathbb{Z}_{12}$.

  Proof: Let $a = 3$, $b = 5$, $c = 9$. Then, in $\mathbb{Z}_{12}$, $ab = 3$, $ac = 3$, and $a \neq 0$. But $b \neq c$. □

2.4.8 A few very simple proofs: $2 + 2 = 4$, etc.

From now on, until further notice, we work on a commutative ring with identity, called $\mathfrak{R}$*. So, for example:*

- *When we write "*$(\forall x)$*" or "*$(\exists x)$*", this means "*$(\forall x \in \mathfrak{R})$*" or "*$(\exists x \in \mathfrak{R})$*" (See the box on page 48.)*

[22] Or real numbers, if you prefer.

- *The word "number" means "member of $\mathfrak{R}$".*

Why are we working on a general commutative ring with identity? The main reason is that, once we prove something in such a general situation, then the result is automatically valid in all the commutative rings with identity that we know, that is, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the $\mathbb{Z}_n$. (And if we learn about a new commutative ring with identity $\mathfrak{A}$, then the result will be known to be valid in $\mathfrak{A}$ as well.)

If you want to, you can think that we are working, say, just on $\mathbb{Z}$. But then if you want to use the same theorem for another ring, such as $\mathbb{R}$, you would have to do one of two things:

- *Prove the theorem again on $\mathbb{R}$,*
- *Quote the theorem proved for $\mathbb{Z}$, and point out that "the proof only uses the axioms for a commutative ring with identity, so the result is valid on $\mathbb{R}$ as well".*

In my view, it is much better to prove the theorems directly, once and for all, in the most general possible setting.

Definition 10. $2 = 1 + 1$. □

Definition 11. $3 = 2 + 1$. □

Definition 12. $4 = 3 + 1$. □

And, now that we know what 1, 2, 3, and 4 are, we are ready to prove a theorem.

Theorem 8. $2 + 2 = 4$.

Proof. First, we observe that

$$2 + 2 = 2 + 2\,, \tag{2.82}$$

by the Equality Axiom.

On the other hand,

$$2 = 1 + 1$$

by Definition 10.

Hence Rule SEE enables us to conclude that

$$2 + 2 = 2 + (1 + 1)\,. \tag{2.83}$$

On the other hand,

$$2 + (1 + 1) = (2 + 1) + 1\,, \tag{2.84}$$

by the associative law of addition.

Hence

$$2 + 2 = (2 + 1) + 1\,. \tag{2.85}$$

But

$$2 + 1 = 3\,, \tag{2.86}$$

by Definition 11.

Hence

$$2 + 2 = 3 + 1\,. \tag{2.87}$$

Finally, Definition 11 tells us that

$$3 + 1 = 4\,. \tag{2.88}$$

Hence

$$\boxed{2+2=4}\,. \tag{2.89}$$

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.

Theorem 9. $2 \times 2 = 4$.

Proof. The Equality Axiom implies that

$$2 \times 2 = 2 \times 2\,. \tag{2.90}$$

And Definition (10) tells us that $2 = 1 + 1$. So, using Rule SEE, we get

$$2 \times 2 = 2 \times (1 + 1)\,. \tag{2.91}$$

By the distributive law of addition,

$$2 \times (1 + 1) = 2 \times 1 + 2 \times 1\,. \tag{2.92}$$

Hence

$$2 \times 2 = 2 \times 1 + 2 \times 1\,. \tag{2.93}$$

By Axiom RA10, $2 \times 1 = 2$. Hence

$$2 \times 2 = 2 + 2\,. \tag{2.94}$$

Finally, Theorem 8 tells us that $2 + 2 = 4$. it follows that

$$\boxed{2 \times 2 = 4}\,. \tag{2.95}$$

Q.E.D.

So far, we have introduced and given names to four integers, namely, 1, 2, 3, and 4. We can then go on and introduce a few more.

Definition 13. $5 = 4 + 1$. □

Definition 14. $6 = 5 + 1$. □

Definition 15. $7 = 6 + 1$. □

Definition 16. $8 = 7 + 1$. □

Definition 17. $9 = 8 + 1$. □

And we can prove things about these numbers, such as, for example:

Theorem 10. $3 + 3 = 6$.

Proof. YOU DO THIS ONE.

Theorem 11. $3 \times 2 = 6$.

Proof. YOU DO THIS ONE.

Theorem 12. $4 + 3 = 7$.

Proof. YOU DO THIS ONE.

Problem 22. Prove Theorems 10, 11, and 12. In each proof, you are allowed to use the facts known so far, that is, the axioms for a commutative ring with identity, the definitions given so far, and the theorems proved so far. So, for example: in your proof of Theorem 10 you are allowed to use the axioms, Definitions 10, 11, 12, 13, 14, 15, 16, 17, and Theorems 8 and 9; in your proof of Theorem 11 you are allowed to use the axioms, definitions 10, 11, 12, 13, 14, 15, 16, 17, and Theorems 8, 9, and 10; and in your proof of Theorem 12 you are allowed to use the axioms, definitions 10, 11, 12, 13, 14, 15, 16, 17, and Theorems 8, 9, 10; and 11. □

2.4.9 Divisibility; factors

In this section we are particularly interested in the integers and their divisibility properties. But we will state the general definitions for a general commutative ring $\mathfrak{R}$ with identity.

If $a \in \mathfrak{R}$ and $b \in \mathfrak{R}$, you would like to "divide a by b", and obtain a "quotient" q, i.e., a $q \in \mathfrak{R}$ that multiplied by b gives you back a.

For example, if $\mathfrak{R}$ was a field, then this would always be possible (if $b \neq 0$), because b has a multiplicative inverse c, and then $a = 1.a = (b.c).a = b.(c.a)$, so we can take $q = c.a$, and we get $a = b.q$.

But on a general commutative ring with identity, such as $\mathbb{Z}$, it is not always possible to divide a by b.. For example, in $\mathbb{Z}$, if $a = 4$ and $b = 3$, then an integer q such that $3q = 4$ does not exist[23] 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.

[23]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 in*** $\mathbb{Z}$***.r***.

.

"DIVIDES", "IS DIVISIBLE BY", "FACTOR", "MULTIPLE"

Definition 18. Let $\mathfrak{R}$ be a commutative ring with identity, and let $a \in \mathfrak{R}$, $b \in \mathfrak{R}$.

1. We say that b is a <u>factor</u> of a if there exists a $k \in \mathfrak{R}$ 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 <u>divides</u> a if b is a factor of 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 2. 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 s divisible by m,
- $m|n$. □

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 statementsd.

Let us prove some theorems about divisibility. We work in a commutative ring $\mathfrak{R}$ with identity.

Theorem 13. *If a, b, c are members of $\mathfrak{R}$ such that a divides b and a divides c, then a divides $b + c$.*

Proof. Since $a|b$, Definition 18 tells us that we may pick $j \in \mathfrak{R}$ such that

$$b = aj\,. \tag{2.96}$$

Since $a|c$, Definition 18 tells us that we may pick $k \in \mathfrak{R}$ such that

$$c = ak\,. \tag{2.97}$$

Then

$$b + c = aj + ak\,. \tag{2.98}$$

The distributive law (Axiom RA7) tells us that

$$aj + ak = a(j + k)\,. \tag{2.99}$$

Therefore

$$b + c = a(j + k)\,. \tag{2.100}$$

Since $j \in \mathfrak{R}$ and $k \in \mathfrak{R}$, it follows that $j + k \in \mathfrak{R}$.

Hence Equation (2.100) implies that the exists an $\ell \in \mathfrak{R}$ such that $b+c = a\ell$. (It suffices to take $\ell = j + k$.)

So $\boxed{a \text{ divides } b + c}$. **Q.E.D.**

Theorem 14. *If a, b, c are members of $\mathfrak{R}$ such that a divides b and b divides c, then a divides c.*

Proof. **YOU DO THIS ONE.**

Problem 23. Prove Theorem 14

Corollary 1. *If a, b, c are members of $\mathfrak{R}$ such that a divides b, then a divides bc.*

Proof.

It follows from the definition of "divides" (Definition 18) that b divides bc.

So a divides b and b divides bc.

Therefore Theorem 14 tells us that $\boxed{a \text{ divides } bc}$.

Q.E.D.

2.4.10 More easy theorems

Here are some very easy but important theorems. Proving these things is the boring part of doing mathematics, and when you are an experienced mathematician you would not waste any time doing these proofs, but that's because it's easy to figure out how to do them. A beginner should know how to do these proofs, and then, once you know how to do them, you will not need to do them any more.

Theorem 15. *If $u \in \mathfrak{R}$, then*

$$-(-u) = u\,.$$

Proof.

$$\begin{aligned} -(-u) &= (-(-u)) + 0 && (2.101)\\ &= (-(-u)) + ((-u) + u) && (2.102)\\ &= \Big((-(-u)) + (-u)\Big) + u && (2.103)\\ &= 0 + u && (2.104)\\ &= u\,. && (2.105) \end{aligned}$$

Theorem 16. *If $u \in \mathfrak{R}$, and $v \in \mathfrak{R}$, then*

$$-uv = (-u).v \text{ and } uv = u(-v)\,.$$

Proof.

Let $u \in \mathfrak{R}$, $v \in \mathfrak{R}$ be arbitrary.

We will prove that $uv = (-u)v$. And we leave the other equality, $-uv = u(-v)$, to the reader.

Then

$$\begin{aligned} -uv &= (-uv) + 0 && (2.106)\\ &= -(uv) + 0.v && (2.107)\\ &= -(uv) + (u + (-u)).v && (2.108)\\ &= -(uv) + \Big(uv + (-u)v\Big) && (2.109)\\ &= \Big((-uv) + uv\Big) + (-u)v && (2.110)\\ &= \Big(uv + (-uv)\Big) + (-u)v && (2.111)\\ &= 0 + (-u)v && (2.112)\\ &= (-u)v + 0 && (2.113)\\ &= (-u)v\,. && (2.114) \end{aligned}$$

So $\boxed{-uv = (-u)v}$. **Q.E.D.**

Problem 24. **Provide the justification** of each of the nine steps (2.106), (2.107), (2.108), (2.109), (2.110), (2.111), (2.112), (2.113), (2.114), of the proof of Theorem 16.

Theorem 17. *If* $u \in \mathfrak{R}$ *then* $-u = (-1).u$.

Proof. Let $u \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned} (-1).u &= -(1.u) && (2.115)\\ &= -u\,. && (2.116) \end{aligned}$$

So $\boxed{(-1).u = -u.}$ **Q.E.D.**

Theorem 18. *If* $u \in \mathfrak{R}$ *and* $v \in \mathfrak{R}$*, then*

$$(-u).(-v) = uv\,.$$

Proof. Let $u \in \mathfrak{R}$, $v \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned} (-u).(-v) &= -\Big(u.(-v)\Big) && (2.117)\\ &= u.(=(-v)) && (2.118)\\ &= u.v\,. && (2.119) \end{aligned}$$

So $\boxed{(-u).(-v) = uv\,.}$ **Q.E.D.**

Problem 25. **Provide the justification** of

1. each of the two steps (2.115), (2.116) of the proof of Theorem 17,
2. each of the three steps (2.117), (2.118) , (2.119), of the proof of Theorem 18. □

Now I would like to talk about the operation of ***subtraction*** of integers. But before I do that let us say a few words about operations in general.

2.4.11 Subtraction

We would like to be able to talk about the ***difference*** of two members x and y of a ring $\mathfrak{R}$, i.e., about the number $y - x$. The ring axioms do not say anything about differences. But Axiom RA7 tells us that for every $x, y \in \mathfrak{R}$ there exists a member z of $\mathfrak{R}$ such that $z + y = x$, and we have proved (in Theorem 2, on page 59, that this number is unique and given it the name $x - y$ ("x minus y").

The operation that sends any two members x, y of $\mathfrak{R}$ to $x - y$ is called ***subtraction***.

And, naturally, the formula

$$(x - y) + y = x$$

holds for every $x, y \in \mathfrak{R}$.

Also, we have defined "$-x$" to stand for "$0 - x$".

Using this, it is very easy to prove a simple formula that you already know:

Theorem 19. *If $u \in \mathfrak{R}$ and $v \in \mathfrak{R}$, then $u - v = u + (-v)$.*

Proof. Let $u \in \mathfrak{R}$, $b \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned} u - v &= (u - v) + 0 && (2.120)\\ &= (u - v) + ((-v) + v) && (2.121)\\ &= (u - v) + (v + (-v)) && (2.122)\\ &= ((u - v) + v) + (-v) && (2.123)\\ &= u + (-v)\,. && (2.124) \end{aligned}$$

So $\boxed{(u - v) = u + (-v)}$, as desired. **Q.E.D.**

Problem 26. **Provide the justification** of each of the five steps (2.120), (2.121), (2.122), (2.123), (2.124) of the proof of Theorem 19. □

2.4.12 A few elementary formulas

You are certainly familiar with the formulas $(a + b)^2 = a^2 + 2ab + b^2$, and $(a - b)(a + b) = a^2 - b^2$. What do those formulas become for general rings?

First we need to define "square".

Definition 19. Let $\mathfrak{R}$ be a ring, and let $a \in \mathfrak{R}$. The square of a is the member a^2 of $\mathfrak{R}$ given by

$$a^2 = a.a\,. \tag{2.125}$$

Theorem 20. *Let $\mathfrak{R}$ be a ring, and let $a, b \in \mathfrak{R}$. Then*

$$(a+b)^2 = a^2 + ab + ba + b^2\,. \tag{2.126}$$

If $\mathfrak{R}$ is a commutative ring with identity, then Formula (2.126) becomes

$$(a+b)^2 = a^2 + 2ab + b^2\,. \tag{2.127}$$

Remark 3. What is the precise meaning of the sum in the right-hand side of Formula (2.126)? Addition is a ***binary*** operation: it makes sense to talk about the sum $x+y$ of ***two*** numbers. But, what is the meaning of $x+y+z$? The answer is: "$x+y+z$" means $(x+y)+z$, or $x+(y+z)$, whichever one you prefer. It does not matter which of the two you use, because $(x+y)+z$ and $x+(y+z)$ are equal, thanks to the associative law of addition.

Similarly, "$x+y+z+w$" means $(x+y)+(z+w)$, or $\big(x+(y+z)\big)+w$, or $\big((x+y)+z\big)+w$, or $x+\big((y+z)+w\big)$, or or $x+\big(y+(z+w)\big)$ whichever one you prefer. And it does not matter which of the two you use, because $(x+y)+(z+w)$, $\big(x+(y+z)\big)+w$, $\big((x+y)+z\big)+w$, $x+\big((y+z)+w\big)$, and $x+\big(y+(z+w)\big)$ are all equal, thanks to the associative law of addition.

Proof of Theorem 20.
We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= (aa+ab)+(ba+bb)\\ &= a^2+ab+ba+b^2\,.\end{aligned}$$

This proves Formula 2.126.

If $\mathfrak{R}$ is commutative, then $ab=ba$, so we can rewrite Formula 2.126 as

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

If in addition $\mathfrak{R}$ has a identity, then $ab+ab = 1.ab+1.ab = (1+1)ab = 2ab$, so we get Formula 2.127. **Q.E.D.**

Problem 27. Do what we did in Theorem 20 for the formula for $(a+b)(a-b)$. That is, write the statement of the theorem analogous to Theorem 20, and prove it. □

Problem 28. Do what we did in Theorem 20 for the formula for $(a+b)^3$. That is, write the definition of "cube", and then write the statement of the theorem analogous to Theorem 20, and prove it. □

2.5 Even and odd numbers

2.5.1 The meaning of "even" and "odd"

One of the most common properties of integers that mathematicians study is their ***parity***, that is, whether they are "even" or "odd".

Even though "even" and "odd" are concepts normally used for integers and only for integers (for example, nobody talks about real numbers being "even" or "odd", and this is so for a good reason, as we shall see) we will begin by giving a precise definition of the meaning of "even" and "odd" for a general ring. This will make it possible to compare the facts about "even" and "odd" for integers with those for other fields, and will help us see why what heppens for $\mathbb{Z}$ is significantly different from what happens in other rings such as $\mathbb{Q}$ or $\mathbb{R}$ or the $\mathbb{Z}_n$, and will help us understand why the case of $\mathbb{Z}$ the most interesting one.

For simplicity, I will limit myself to commutative rings with identity, although one could talk about "even" and "odd" for more general rings.

Definition 20. Let $\mathfrak{R}$ be a commutative ring with identity. Then

- A member x of $\mathfrak{R}$ is <u>even</u> if x is divisible by 2, that is, if we can write

  $$x = 2k$$

  for some $k \in \mathfrak{R}$. .
- A member x of $\mathfrak{R}$ is <u>odd</u> if x is not even. □

Example 21.

1. The number 0 is even, because $0 = 2 \times 0$ (since $x.0 = 0$ for every $x \in \mathfrak{R}$), so 0 is divisible by 2.

2. In the ring $\mathbb{R}$, the number 1 is even, because $1 = 2 \times \frac{1}{2}$, so $(\exists x \in \mathbb{R})1 = 2x$.

3. Actually, ***in*** $\mathbb{R}$ ***every number is even***, because given any $x \in \mathbb{R}$ we can write $x = 2 \times \frac{x}{2}$, so $(\exists u \in \mathbb{R})x = 2u$.

4. In any field $\mathfrak{F}$, every member x of $\mathfrak{F}$ is even, for the same reason as before, ***provided that*** $\frac{x}{2}$ ***exists***. When does $\frac{x}{2}$ exist? Well, $\frac{x}{2}$ is the result of multiplying x by the multiplicative inverse of 2, and the multiplicative inverse of 2 exists if $2 \neq 0$. (The multiplicative inverse axiom says that $\frac{1}{u}$ exists if $u \neq 0$.) A ring $\mathfrak{R}$ is said to be a ***ring of characteristic two*** if, in $\mathfrak{R}$, 2 is equal to 0, i.e., if $1+1 = 0$. So, ***in a field*** $\mathfrak{F}$***, if*** $\mathfrak{F}$ ***is not of characteristic two, then every member of*** $\mathfrak{F}$ ***is even***.

5. The ring $\mathbb{Z}_2$ has two members, 0 and 1. We know that 0 is even. As for 1, it is not even. because $0 + 0 = 0$ and $1 + 1 = 0$, so it is not possible to write 1 as $k + k$ for some $k \in \mathbb{Z}_2$. So ***in*** $\mathbb{Z}_2$ 0 ***is even and*** 1 ***is odd***.

6. If $n \neq 2$, then the ring $\mathbb{Z}_n$ is not of characteristic 2. So, ***if*** $n \in \mathbb{N}$***,*** $n > 2$***, and*** $\mathbb{Z}_n$ ***is a field, then every member of*** $\mathbb{Z}_n$ ***is even***. (We will see later that $\mathbb{Z}_n$ is a field if and only if n is prime.)

7. In $\mathbb{Z}_6$, 0, 2 and 4 are even, and 1, 3 and 5 are odd.

8. In $\mathbb{Z}$, 1 is odd, but we cannot prove that yet, if all we know is that $\mathbb{Z}$ is a commutative ring with identity. The reason is that $\mathbb{R}$ is also a commutative ring with identity, and in $\mathbb{R}$ 1 is even. If we could prove that 1 is odd using only the axioms for a commutative ring with identity, then it would follow that 1 is odd in every commutative ring with identity. But 1 is even in $\mathbb{R}$, and $\mathbb{R}$ is a commutative ring with identity.

The morale of these examples is: knowing that $\mathbb{Z}$ is a commutative ring with identity is not enough to prove things we know are true in $\mathbb{Z}$, such as the following:

- 1 is odd,
- an integer n is even if and only if $n + 1$ is odd.

- the sum of two odd numbers is even,
- the product of two odd numbers is odd.

It follows that, ***in order to understand $\mathbb{Z}$ better we need more tools, going beyond the fact that $\mathbb{Z}$ is a commutative ring with identity.***

2.5.2 The parity of a sum and a product

We would now like to prove the rules that I am sure you know: "even plus even is even", "odd plus even is odd", "odd plus odd is even", "even times anything is even", "odd times odd is odd". As you will see, we will be able to prove ssome of them, but not all of them. And then we will discusws why this is so.

Theorem 21. *In a commutative ring with identity $\mathfrak{R}$, the sum and difference of two even members of $\mathfrak{R}$ is even. That is:*

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})\Big((2|a \wedge 2|b) \Longrightarrow (2|a+b \wedge 2|a-b)\Big)\,. \tag{2.128}$$

Proof. Since a and b are even, we can write

$$a = 2j \qquad \text{and} \qquad b = 2k\,,$$

with $j, k \in \mathfrak{R}$. Then

$$a+b = 2(j+k) \qquad \text{and} \qquad a-b = 2(j-k)\,,$$

and $j+k \in \mathfrak{R}$. $j-k \in \mathfrak{R}$. So So $\boxed{a+b \text{ and } a-b \text{ are even}}$. **Q.E.D.**

Theorem 22. *In a commutative ring with identity $\mathfrak{R}$, the sum of an even member of $\mathfrak{R}$ and an odd member of $\mathfrak{R}$ is odd. That is:*

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})\Big((2|a \wedge \sim 2|b) \Longrightarrow \sim 2|a+b\Big)\,. \tag{2.129}$$

Proof. We do a proof by contradiction.

> Suppose $a+b$ was even.
> Since a is even, it would follow from Theorem 21 that $(a+b)-a$ is even.

But $(a+b)-a=b$, so b is even.
But b is odd. So b is not even.
So $\boxed{b \text{ is even and } b \text{ is not even}}$.
Hence we have proved a contradiction.

Therefore $\boxed{a+b \text{ is odd}}$. **Q.E.D.** **Q.E.D.**

Problem 29. ***Prove*** that the product of two even integers is divisible by 4.□

Next, we prove that "even times anything is even". That is, that the product of an even number times a number is even.

Theorem 23. *In a commutative ring with identity $\mathfrak{R}$, the product of two members of $\mathfrak{R}$, one of which is even, is even. That is*

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})(2|a \Longrightarrow 2|ab)\,. \tag{2.130}$$

Proof. Since a is even, we can write $a=2k$, $k \in \mathfrak{R}$.
But then $ab=(2k)b=2(kb)$, and $kb \in \mathfrak{R}$. So $\boxed{ab \text{ is even}}$. **Q.E.D.**

Another thing that is very simple to do is relate the parity of a to that of $-a$:

Theorem 24. *In a commutative ring with identity $\mathfrak{R}$, if $a \in \mathfrak{R}$ then $-a$ is even if and only if a is even. That is*

$$(\forall a \in \mathfrak{R})(2|a \Longleftrightarrow 2|-a)\,. \tag{2.131}$$

Proof. YOU DO THIS ONE.

Problem 30. ***Prove*** Theorem 24. □

So far, we have proved that

- "even±even=even",
- "even±odd=odd",
- "−even=even",
- "even×anything=even".

But some of the things you know are missing. For example, you know that

(M1) "odd±odd=even",

(M2) "odd×odd=odd".

It turns out that ***(M1) and (M2) cannot be proved from the commutative ring axioms alone.*** The reason for this is that ***there are commutative rings with identity in which (M1) and (M2) are false.*** (We will construct an example of that in later in these notes.)

2.5.3 Odd and even numbers: what we know so far

Let us make a brief stop to examine the situation so far. We have proved some facts bout "even" and "odd" numbers in a commutative ring $\mathfrak{R}$ with identity, and here are several "missing facts", things that we all know are true but have not yet been able to prove.

Proven facts:

(PF1) Every number[24] is even or odd and not both. (This is a trivial consequence of the fact that we have defined "odd" to mean "not even".)

(PF2) 0 is even.

(PF3) If $n \in \mathfrak{R}$ and n is even then $-n$ is even.

(PF4) The sum of two even numbers is even.

(PF5) The sum of an odd number and an even number is odd.

(PF6) The product of an even number and any number is even.

Missing facts:

(MF1) 1 is odd.

(MF2) The sum of two odd integers is even.

(MF3) The product of two odd integers is odd.

(MF4) If n is an integer then n is odd if and only if $(\exists k \in \mathbb{Z})n = 2k + 1$.

[24]Remember that we have fixed a ring $\mathfrak{R}$. so "number" means "member of $\mathfrak{R}$".

(MF5) For every integer n, one and only one of the follwoing two sentences is true:

$$(\exists k \in \mathbb{Z}) n = 2k\,, \tag{2.132}$$

$$(\exists k \in \mathbb{Z}) n = 2k + 1\,. \tag{2.133}$$

We have proved the "proven facts" (PF1), (PF2), (PF3), (PF4), (PF5), (PF6), using only the axioms for a commutative ring with identity, which means that these facts are true in any commutative ring with identity, nt just in $\mathbb{Z}$.

And now we would like to be able to prove the five "missing facts" (MF1), (MF2), (MF3), (MF4), (MF5) But ***we cannot do that from the axioms of a commutative ring with identity***, because there are commutative ring with identity in which these four facts are not true. (For example: in $\mathbb{R}$ every number is even. So, in particular, it's not true that 1 is odd, and it's not true that if n is even then $n + 1$ is odd.)

It follows from this that ***at this point we need a new axiom***, something that will be valid for $\mathbb{Z}$ but not for other rings such as $\mathbb{Q}$ or $\mathbb{R}$. And ***that new thing we need is induction***.

2.6 The natural numbers and the Principle of Mathematical Induction

The ring axioms never mention the natural numbers. So, if all we know about $\mathbb{Z}$ is that it is a commutative ring with identity, then we know nothing about the natural numbers. But the Principle of Mathematical Induction (PMI) is about the natural numbers. So, in order to be able to state the PMI, we need to introduce the natural numbers first.

2.6.1 New facts we need about $\mathbb{Z}$: the natural numbers

Let us list some basic facts about thr set $\mathbb{N}$ that you know very well:

BASIC FACTS ABOUT THE NATURAL NUMBERS

BFN1: $(\forall n \in \mathbb{N})n \in \mathbb{Z}$. (That is: Every natural number is an integer.)

BFN2: $1 \in \mathbb{N} \wedge 0 \notin \mathbb{N}$. (That is: 1 is a natural number, and 0 is not a natural number.)

BFN3: $(\forall n \in \mathbb{N})n + 1 \in \mathbb{N}$. (That is: If n is a natural number then $n + 1$ is a natural number.)

BFN4: $(\forall n \in \mathbb{Z})(n \in \mathbb{N} \vee -n \in \mathbb{N} \vee n = 0)$. (That is: Every integer is either a natural number, or minus a natural number, or zero.)

2.6.2 What do we need to prove the missing facts?

It turns out that the key missing fact is (MF5): ***For every integer*** n ***one and only one of equations (2.132), (2.133), holds.***

We now show that if (MF5) is true then the other four "missing facts" follow.

Theorem 25. *If (MF5) is true, then*

(MF1) 1 *is odd.*

(MF2) The sum of two odd integers is even.

(MF3) The product of two odd integers is odd.

(MF4) If n *is an integer then* n *is odd if and only if* $(\exists k \in \mathbb{Z})n = 2k + 1$.

Proof. Let us assume that (MF5) is true. That is, let us assume that

(MF5) *For every integer* n*, one and only one of the follwoing two sentences is true:*

$$(\exists k \in \mathbb{Z})n = 2k\,, \tag{2.134}$$

$$(\exists k \in \mathbb{Z})n = 2k + 1\,. \tag{2.135}$$

Let us prove (MF4). Let n be an arbitrary integer. We want to prove that

$$\sim 2|n \Longleftrightarrow (\exists k \in \mathbb{Z})n = 2k + 1\,. \tag{2.136}$$

Since we are assuming that (MF5) is true, one of Formulas (2.134, (2.135 is true. Clearly, (2.134 holds if and only if $2|n$. So (2.135 holds if and only if $\sim 2|n$, i.e., if and only if n is odd. This proves (MF4).

Now let us prove (MF1), i.e., that 1 is odd. Since (MF4) holds, 1 is odd if and only if $(\exists k \in \mathbb{Z})1 = 2k+1$. But "$(\exists k \in \mathbb{Z})1 = 2k+1$" is true, because $k = 0$ is a witness. So 1 is odd, and we have proved (MF1).

Now let us prove (MF2) and (MF3). Let m, n be odd integers. We want to prove that $m+n$ and $m.n$ are odd.

Using (MF4), since m and n are odd, we can write

$$m = 2j+1\,, \qquad n = 2k+1 \qquad j \in \mathbb{Z},\ k \in \mathbb{Z}\,. \tag{2.137}$$

Then $m + n = (2j + 1) + (2k + 1) = 2j + 2k + 2 = 2(j + k + 1)$, so $m+n = 2(j+k+1)$. Since $j+k+1 \in \mathbb{Z}$, it follows that $\boxed{m+n \text{ is even}}$.

Also, $m.n = (2j+1)(2k+1) = 2j \times 2k + 2j + 2k + 1 = 2(2jk+j+k)+1$. So $m.n = 2(2jk + j + k) + 1$. Since $2jk + j + k \in \mathbb{Z}$, it follows from (MF4) that $\boxed{m.n \text{ is odd}}$. **Q.E.D.**

2.6.3 Why we need the Principle of Mathematical Induction

At this point, we now know that in order to prove the missing facts all we need is to prove (MF5), because then the other four missing facts (MF1), (MF2), (MF3), (MF4) follow.

Let us call an integer n "good" if the following is true

$(G(n))$ One and only one of the following two facts is true:
$(\exists k \in \mathbb{Z})n = 2k$, $(\exists k \in \mathbb{Z})n = 2k+1$.

Then it is clear that (MF5) is exactly the assertion that "every integer is good", that is, $(\forall n \in \mathbb{Z})G(n)$. (I am writing "$G(n)$" for "$n$ is good".)

The key fact about "goodness" is that ***goodness is passed on from each integer n to its successor***, that is:

Theorem 26. *If an integer n is good (that is, if one and only one of the formulas "$(\exists k \in \mathbb{Z})n = 2k$", "$(\exists k \in \mathbb{Z})n = 2k+1$" is true) then $n+1$ is good as well.*

Proof. Let n be an arbitrary integer.

Assume $\boxed{\boxed{n \text{ is good}}}$.

Then we may pick an integer k such that $n = 2k \vee n = 2k + 1$.

Assume $\boxed{n = 2k}$.

Then $n + 1 = 2k + 1$.

Furthermore, $n + 1$ cannot be written as $2j$ for some $j \in \mathbb{Z}$. (Reason: if $n + 1 = 2j$, $j \in \mathbb{Z}$, it could follow that $n = 2j - 1$, so $n = 2(j - 1) + 1$, so $n = 2\kappa + 1$, where $\kappa = j - 1$, and then $n = 2k$ and $n = 2\kappa + 1$, with $k\kappa \in \mathbb{Z}$, contradicting the fact that n is good.

Hence $\boxed{n + 1 \text{ is good}}$.

Assume $\boxed{n = 2k + 1}$.

Then $n+1 = 2k+2$, so $n+1 = 2(k+1)$, and then $n+1 = 2\kappa$, where $\kappa = k + 1$.

Furthermore, $n + 1$ cannot be equal to $2j + 1$ for some $j \in \mathbb{Z}$. (Reason: if $n+1$ was equal to $2j+1$ for a $j \in \mathbb{Z}$, it would follow that $n = (2j+1)-1$, so $n = 2j$, and then $n = 2k+1 \wedge n = 2j$, $j, k \in \mathbb{Z}$, contradicting the fact that n is good.

Hence $\boxed{n + 1 \text{ is good}}$.

So we have proved that $n+1$ is good both in the case when $n = 2k$ and in the case when $n = 2k + 1$. Since one of the cases occurs, $\boxed{\boxed{n + 1 \text{ is good.}}}$

Since we have shown that $n + 1$ is good assuming that n is good, we have proved that $\boxed{\boxed{n \text{ is good} \implies n + 1 \text{ is good.}}}$

Since this has been shown for an arbitrary integer n, we have proved that $\boxed{\boxed{\boxed{(\forall n \in \mathbb{Z})(n \text{ is good} \implies n + 1 \text{ is good.})}}}$ **Q.E.D.**

2.6.4 Why induction is needed

So, if we prove that 1 is good, we will know two things:

(1) 1 is good.

(2) If an integer n is good, then $n + 1$ is good.

So, if we look at the natural numbers, then goodness is a property that

(i) is true of the first[25] natural number,

(ii) is passed on from each natural number to its successor[26].

From this it should follow that all natural numbers are good. Now can we prove that?

We could argue as follows:

- 1 is good.
- Since 1 is good, 2 must be good, because $2 = 1 + 1$.
- Since 2 is good, 3 must be good, because $3 = 2 + 1$.
- Since 3 is good, 4 must be good, because $4 = 3 + 1$.
- Since 4 is good, 5 must be good, because $5 = 4 + 1$.
  ... .
- ***And so on.***

So it would follow that all the natural numbers are good. And, once we know that, it will be easy to show that all the integers are good. (We will do that later.)

In order to actually prove rigorously that every natural number is good, we need to make precise the vague words "and so on".

2.6.5 "And so on" is dangerous

Arguing as in the previous section, by saying "this is true for $n = 1$, for $n = 2$, for $n - 3$, for $n = 4$, and so on, so it's true for all natural numbers n" is a completely invalid way of arguing that a universal proposition about natural numbers is true. Anyone who argues that way is likely to make a lot of mistakes, because there is absolutely no reason for a proposition about natural numbers n to be true for all n, just because it is true for $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$, and many more values of n.

An obvious example is the statement "$n < 10,000,001$". This is clearly true for $n = 1$, $n = 2$, $n = 3$, "and so on". You can actually check that it is

[25] "The first natural number" is 1, of course

[26] The "successor" of n is $n + 1$.

true for the first ten million values of n. So you may want to conclude that, with ten million examples, that is enough to imply that "$n < 10,000,001$" is true for every $n \in \mathbb{N}$. But it is very clear that for $n = 10,000,001$ the statement is false, so it is not true for all $n \in \mathbb{N}$.

A remarkable example of a similar phenomenon occurs with the expression $n^2 + n + 41$. It can be verified that $n^2 + n + 4$ is a prime number for $n = 1$, $n = 2$, and so on, up to $n = 39$.

For example:

- For $n = 1$, $n^2 + n + 41 = 43$, which is prime.
- For $n = 2$, $n^2 + n + 41 = 47$, which is prime.
- For $n = 3$, $n^2 + n + 41 = 53$, which is prime.
- For $n = 4$, $n^2 + n + 41 = 61$, which is prime.
- For $n = 5$, $n^2 + n + 41 = 71$, which is prime.
- For $n = 6$, $n^2 + n + 41 = 83$, which is prime.
- For $n = 7$, $n^2 + n + 41 = 97$, which is prime.
- For $n = 8$, $n^2 + n + 41 = 97$, which is prime.
- For $n = 9$, $n^2 + n + 41 = 131$, which is prime.
- For $n = 10$, $n^2 + n + 41 = 151$, which is prime.
- For $n = 11$, $n^2 + n + 41 = 173$, which is prime.
- For $n = 12$, $n^2 + n + 41 = 197$, which is prime.
- .....

So you may be tempted to conclude that $n^2 + n + 41$ is prime for every natural number n. But this is wrong. In fact, it is easy to see that for $n = 40$ $n^2 + n + 41$ is not prime.

2.6.6 Why induction is valid

To justify concluding that every natural number n is good we need more than the observation that 1, 2, 3, 4, 5, "and so on", are good. What we need is to know that every natural number n passes on the property of being good to its successor. If we know that then we can be sure that all the natural numbers are good, because if we count 1, 2, 3, 4, 5, ..., then at each step the corresponding number will be good, and the counting process will eventually reach every natural number[27], so all the natural numbers must be good.

[27] Why? Because that's what the natural numbers are: they are the numbers that can be reached by counting

The mathematical statement that makes this precise is the ***Principle of Mathematical Induction (PMI)***.

The Principle of Mathematical Induction is probably one of the two most important proof techniques that you will learn in this course. (The other one is proof by contradiction.) You cannot prove almost anything serious in arithmetic without using Induction.

3 Induction

3.1 Introduction to the Principle of Mathematical Induction

Remember from the previous section that we are calling an integer n "good" if n is even or odd and not both even and odd.

We want to know if it is true that ***every natural number is good***. (Actually, we want to know that every integer good. But once we know that every natural number is good, it takes only a small extra step to prove that every integer good.)

We would like to prove that the answer is "yes, every natural number is good".

How can we do that?

Suppose we prove that 1 is good. Then we will 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.)

Armed with this information, how can we prove that every natural number is good?

We could use the "and so on" argument, as in the previous section. But it 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 22. 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 23. 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[28]. Suppose you have a flyer with an announcement that you want all the people in the queue to read. (For 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[29].

The PMI says the obvious thing: if you do (1) and (2) then everybody will eventually get your flyer. □

[28]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 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.

[29]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.

3.2 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***.

Remark 4. 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.

Let us add the PMI to our list of basic facts about the integers:

THE PRINCIPLE OF MATHEMATICAL INDUCTION (BASIC FACT BFN5 ABOUT THE NATURAL NUMBERS)

BFN5: Suppose $P(n)$ is any statement about a variable natural number n. 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 (BASIC FACT BFN5 ABOUT THE NATURAL NUMBERS, FORMAL LANGUAGE VERSION

BFZ6: Suppose $P(n)$ is any statement about a variable natural number n. Then

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\Big) \Longrightarrow (\forall n \in \mathbb{N})P(n)\,. \tag{3.138}$$

3.3 The proof by induction that every integer is of one and only one of the forms $2k$, $2k+1$, $k \in \mathbb{Z}$

We are now ready, finally, to prove the theorem that we had announced before, that for every integer n one and only one of the conditions $(\exists k \in \mathbb{Z})n = 2k$, $(\exists k \in \mathbb{Z})n = 2k+1$, holds.

We will prove this by induction. But in the proof we are going to need two results, also proved by induction. So we prove those two results first.

3.3.1 Our first proof by induction: the successor theorem

The ***successor theorem*** is very simple, and the proof is just a couple of lines. But it is a very imprtant fact.

Theorem 27. *If n is a natural number and $n \neq 1$ then $n-1$ is a natural number. (That is, $(\forall n \in \mathbb{N})(n \neq 1 \Longrightarrow n-1 \in \mathbb{N})$.)*

Proof.

Let $P(n)$ be the predicate "$n \neq 1 \Longrightarrow n-1 \in \mathbb{N}$)".
Basis step. Proof of $P(1)$.
$P(1)$ says "$1 \neq 1 \Longrightarrow 1-1 \in \mathbb{N}$)".
And this implication is true because the premise "$1 \neq 1$" is false,
So $\boxed{P(1)}$.

Inductive step. We prove that $(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)$.

Let $n \in \mathbb{N}$ be arbitrary. We want to prove $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.
$P(n+1)$ says "$n+1 \neq 1 \Longrightarrow n \in \mathbb{N}$)".
And the implication "$n+1 \neq 1 \Longrightarrow n \in \mathbb{N}$)" is true because the conclusion "$n \in \mathbb{N}$ is true, since we are assuming that $n \in \mathbb{N}$.
So $\boxed{P(n+1)}$.

So $P(n) \Longrightarrow P(n+1)$. [Rule $\Longrightarrow_{prove}$]

Hence $\boxed{(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)}$ [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, $(\forall n \in \mathbb{N}) * n \neq 1 \Longrightarrow n \in \mathbb{N})$. **Q.E.D.**

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.**

3.3.2 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.

3.3.3 Our second proof by induction: the sum theorem

Theorem 28. *The sum of two natural numbers ia a natural number. (That is:* $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m+n \in \mathbb{N}$.*)*

Proof. We want to prove that $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m+n \in \mathbb{N}$.

Let m be an arnitrary natural number.

We want to prove that

$$(\forall n \in \mathbb{N})m+n \in \mathbb{N}\,. \qquad (3.139)$$

We prove (3.139) by induction.

Let $P(n)$ be the sentence "$m+n \in \mathbb{N}$".

We will prove $P(1)$ and $(\forall n \in \mathbb{N})P(n)$.

Basis step. We want to prove $P(1)$. But $P(1)$ says "$m+1 \in \mathbb{N}$". And this is true because of Basic Fact BFN3, which tells us that if $k \in \mathbb{N}$ then $k+1 \in \mathbb{N}$, together with the fact that $m \in \mathbb{N}$. 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. We want to prove $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.
Then $m + n \in \mathbb{N}$.
By Basic fact BFN3, $(m + n) + 1 \in \mathbb{N}$.
But $(m + n) + 1 = m + (n + 1)$, by the asociative law of addition.
So $m + (n + 1) \in \mathbb{N}$.
That is, $P(n + 1)$.

So we have proved $P(n) \Longrightarrow P(n+1)$.

Hence $\boxed{(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$.

It follows from the PMI that $(\forall n \in \mathbb{N})P(n)$, i.e., that (3.139) holds.

Since we have proved (3.139) for arbitrary $m \in \mathbb{N}$, we can conclude that $\boxed{(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m + n \in \mathbb{N}}$. **Q.E.D.**

Problem 31. Using exactly the same method as in the proof of Theorem 28, ***prove*** that the product of two natural numbers is a natural number. (That is, prove that $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})m.n \in \mathbb{N}$.) □

3.3.4 Our third proof by induction: proof that every integer is of one and onlty one of the forms $2k$, $2k + 1$, $k \in \mathbb{Z}$

We now show how we can prove Missing Fact (MF5), the key missing fact in our study of even and odd integers.

Theorem 29. *For every integer n, one and only one of the sentences*

$$(\exists k \in \mathbb{Z})n = 2k\,, \tag{3.140}$$
$$(\exists k \in \mathbb{Z})n = 2k + 1\,. \tag{3.141}$$

holds.

As in previous sections, let us call an integer "good" if one and only one of (3.140), (3.141), holds. And let us write "$G(n)$" for "n is good".

We want to prove that $(\forall n \in \mathbb{Z})G(n)$.

First, we are going to prove by induction that $(\forall n \in \mathbb{N})G(n)$.

Basis step. We have to prove $G(1)$, i.e., that 1 is good.

It is clear that 1 can be written in the form $2k + 1$, with $k \in \mathbb{Z}$. (Just take $k = 0$.) So to prove that 1 is good we have to prove that itis not possible to find an integer k such that $1 = 2k$.

> Suppose it was possible to write $1 = 2k$, $k \in \mathbb{Z}$.
>
> Then either $k \in \mathbb{N}$ or $-k \in \mathbb{N}$ or $k = 0$, by Basic fact BFN4.
>
> The possibility that $k = 0$ is excluded because if $k = 0$ then $1 = 2k = 2 \times .0 = 0$, so $1 = 0$. But one of the axioms for a commutative ring with identity says that $1 \neq 0$, so we got a contradiction
>
> The possibility that $-k \in \mathbb{N}$ is excluded because if $-k \in \mathbb{N}$ then $-2k \in \mathbb{N}$ (because $-2k = -k + (-k)$ and the sum of two natural numbers is a natural number), and then $1 - 2k \in \mathbb{N}$ (because $1 \in \mathbb{N}$, and the sum of two natural numbers is a natural number); but $1 = 2k$, so $1 - 2k = 0$; so $0 \in \mathbb{N}$, but Basic Facts BFN2 says that $0 \notin \mathbb{N}$; so we got a contradiction
>
> Hence $k \in \mathbb{N}$. And either $k = 1$ or $k \neq 1$. If $k = 1$ then $1 = 2$, because $1 = 2k$. But then $0 = 1 - 1 = 2 - 1 = 1$, so $1 = 0$. But one of the axioms for a commutative rign with identity says that $1 \neq 0$, so we got a contradiction, and this excludes the possibility that $k = 1$.
>
> So $k \in \mathbb{N}$ and $k \neq 1$. Since $k \in \mathbb{N}$ and $k \neq 1$, the successor theorem tells us that $k - 1 \in \mathbb{N}$. But then $0 = 1 - 1 = 2k - 1 = k + (k - 1)$, and $k + (k - 1) \in \mathbb{N}$, because $k \in \mathbb{N}$, $k - 1 \in \mathbb{N}$, and the sum of two natural numbers is a natural number. So $0 \in \mathbb{N}$, but Basic Facts BFZ2 says that $0 \notin \mathbb{N}$, so we got a contradiction.
>
> So we have proved that if is impossible to write $1 - 2k$, $k \in \mathbb{Z}$.

Hence $\boxed{\text{1 is good}}$.

Inductive step. We have to prove that $(\forall n \in \mathbb{N})\big(G(n) \Longrightarrow G(n+1)\big)$. But we have alrady proved this, in Theorem 26, on page 88, which says precisely that goodness is passed on from an integer n to its successor $n + 1$.

Since we have proved ($G(1)$ and $(\forall n \in \mathbb{N})\big(G(n) \Longrightarrow G(n+1)\big)$, it follows from the PMI that

$$(\forall n \in \mathbb{N})G(n)\,, \tag{3.142}$$

i.e., every natural number is good.

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 inetegr toits successor.

So we have proved that every onteger is good. **Q.E.D.**

4 Examples of proofs by induction

4.1 Some divisibility theorems

Theorem 30. *If n is natural number, then $8^n - 5^n$ is divisible by 3.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N})3|8^n - 5^n\,. \tag{4.143}$$

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

$$8^n - 5^n = 3k\,,\ \ k \in \mathbb{Z}\,.. \tag{4.144}$$

Then

$$8 \times (8^n - 5^n) = 3 \times 8k\,. \tag{4.145}$$

So

$$8^{n+1} - 8 \times 5^n = 3 \times 8k\,, \tag{4.146}$$

and then

$$8^{n+1} = 8 \times 5^n + 3 \times 8k\,, \tag{4.147}$$

But $8 = 5 + 3$, so

$$8 \times 5^n = 5 \times 5^n + 3 \times 5^n = 5^{n+1} + 3 \times 5^n\,, \tag{4.148}$$

so

$$8^{n+1} = 5^{n+1} + 3 \times 5^n + 3 \times 8k\,, \tag{4.149}$$

and then

$$8^{n+1} = 5^{n+1} + 3(5^n + 8k)\,, \tag{4.150}$$

so that

$$8^{n+1} - 5^{n+1} = 3(5^n + 8k)\,, \tag{4.151}$$

Let $j = 5^n + 8k$. Then $j \in \mathbb{Z}$ and

$$8^{n+1} - 5^{n+1} = 3j\,. \tag{4.152}$$

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 30

Theorem 31. *If n is natural number, then $11^n - 4^n$ is divisible by 7.*

Theorem 32. *If n is natural number, then $22^n - 10^n$ is divisible by 12.*

Theorem 33. *If n is natural number, then $31^n - 18^n$ is divisible by 13.*

Problem 32. ***Prove*** Theorem 31. □

Problem 33. ***Prove*** Theorem 32. □

Problem 34. ***Prove*** Theorem 33. □

Problem 35. *If, after reading the proof of Theorem 30 and solving Problems 32, 33, 34, you get the feeling that these are all the same thing,* ***try to prove*** *the following general theorem:*

Theorem 34. *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 41 on page 122. But you shoud try to prove it by yourself before you look at the proof.) □

4.2 An inequality

Here is another example of a proof by induction.

Theorem 35. *If n is a natural number, then $2^n < n! + 3$.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N}) 2^n < n! + 3\,. \tag{4.153}$$

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

$$2^n < n! + 3\,. \tag{4.154}$$

Therefore, multiplying both sides of (4.154) by 2, we get

$$2^{n+1} < 2n! + 6\,. \tag{4.155}$$

On the other hand, $n + 1 = n - 1 + 2$, so

$$(n+1)! = (n+1)n! = (n-1)n! + 2n!\,. \tag{4.156}$$

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

$$2n! + 3 < (n+1)!\,. \tag{4.157}$$

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 36.

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 $3^n < n! + 123$?

4.3 More inequalities, with applications to the computation of some limits

Let us use induction to prove an inequality:

Theorem 36. *If x is a positive real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{4.158}$$

Proof. We want to prove that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{4.159}$$

Let x be an arbitrary real number.

We want to prove that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{4.160}$$

We prove this by induction.

Let $P(n)$ be the predicate "$x > 0 \implies (1+x)^n \geq 1 + nx$".

Base step. We have to prove $P(1)$.

But $P(1)$ says "$x > 0 \implies 1 + x \geq 1 + x$", 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

$$(\forall n \in \mathbb{N})(P(n) \implies P(n+1))\,. \tag{4.161}$$

Let n be an arbitrary natural number. We want to prove that $P(n) \implies P(n+1)$.

Assume $P(n)$.

Then

$$x > 0 \implies (1+x)^n \geq 1 + nx\,. \tag{4.162}$$

We want to prove

$$x > 0 \implies (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{4.163}$$

Assume $x > 0$.

Then it follows from (4.162) (by Rule $\implies_{use}$) that

$$(1+x)^n \geq 1 + nx\,. \tag{4.164}$$

Multiplying both sides of (4.164) by $1 + x$ (which is possible because $1 + x > 0$), we get

$$(1+x)^{n+1} \geq (1+x)(1+nx)\,. \tag{4.165}$$

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

$$(1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{4.166}$$

Since we proved (4.166) under the assumption that $x > 0$, it follows that

$$x > 0 \Longrightarrow (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{4.167}$$

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 (4.161) holds.

This compleetes the inductive step.

. Since we have also proved$P(1)$, we can use the PMI to conclude that (4.160) holds, i.e., that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{4.168}$$

Since we have proved for an arbitrary real number x, we can conclude that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,, \tag{4.169}$$

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

Problem 37. In the proof of Theorem 36, we translated the statement to be proved into formal language as Formula (4.159) and then followed the rules of logic, plus the PMI, to prove it.

Suppose instead that we had translated the statement of Theorem 36 in a different way, as

$$(\forall n \in \mathbb{N})(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{4.170}$$

1. ***Prove that this translation is equivalent to Formula (4.159)***, 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 $U \iff V$ is true.)

2. ***Write a different proof*** of Theorem 36, using the translation (4.170) instead of (4.159).

Problem 38. By looking carefully at the proof of Theorem 36, ***prove*** the following stronger result:

Theorem 37. *If $x \in \mathbb{R}$ and $x \geq -1$, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{4.171}$$

With a little bit more work, it is possible to prove a result stronger than Theorem 36::

Theorem 38. *If x is a nonnegative real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2\,. \tag{4.172}$$

Proof.

YOU DO THIS ONE.

HINT. Just repeat the proof of Theorem 36 up to the point when you multiply by $1+x$, and at that point keep the x^2 term. □

Problem 39. ***Prove*** Theorem 38. □

4.3.1 An application of Theorem 38: 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

$$\lim_{n\to\infty} \sqrt[n]{n} = 1\,. \tag{4.173}$$

Define

$$\alpha_n = \sqrt[n]{n} - 1\,.$$

To prove (4.173), we have to prove that

$$\lim_{n\to\infty} \alpha_n = 0\,. \tag{4.174}$$

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

$$(1+\alpha_n)^n = n\,. \tag{4.175}$$

Using the inequality of Theorem 38, we get

$$(1+\alpha_n)^n \geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2\,. \tag{4.176}$$

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

$$0 \le \alpha_n \le \sqrt{\frac{2}{n-1}}\,.$$

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 (4.173 is proved.

4.4 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 4.5.3 on page 118.)

Theorem 39. *If n is an arbitrary natural number, then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,. \tag{4.177}$$

(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

$$\begin{aligned}\sum_{k=1}^{n+1} k &= (\sum_{k=1}^{n} k) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\Big[\frac{n}{2} + 1\Big] \\ &= (n+1) \times \frac{n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}\,.\end{aligned}$$

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 40. *If n is a natural number, then*

$$\sum_{k=1}^{n} k^3 = \Big[\frac{n(n+1)}{2}\Big]^2\,, \tag{4.178}$$

that is:

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \Big[\frac{n(n+1)}{2}\Big]^2\,.$$

Proof. **YOU DO THIS ONE.**

Problem 40.

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 40. □

Problem 41.

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

$$\sum_{k=1}^{n} k^2 = \frac{n + 3n^2 + 2n^3}{6}\,. \tag{4.179}$$

3. ***Prove*** that Formula (4.179) holds for every natural number n. □

4.5 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

$$2{\times}3{\times}5{\times}7{\times}11{\times}13{\times}17{\times}19{\times}23{\times}29{\times}31{\times}37{\times}41{\times}43{\times}47{\times}53{\times}59{\times}61{\times}67{\times}71 \,,$$

we could write

$$2 \times 3 \times \cdots \times 71 \,. \tag{4.180}$$

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 (4.180), 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

$$3 \times 5 \times 7 \times \cdots \times 71 \,. \tag{4.181}$$

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 coudn'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 cannot we use other patterns that aren't "true" as well as true ones?

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***.

4.5.1 The inductive definition of powers of a real number

The way to define "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 21. ***(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:

$$a^5 = a.a.a.a.a.$$

4.5.2 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 22. The factorial of a natural number n is the number $n!$ given by

$$1! = 1\,, \tag{4.182}$$

$$(n+1)! = n! \times (n+1) \quad \text{for } n \in \mathbb{N}\,. \tag{4.183}$$

In addition, we define

$$0! = 1\,,$$

so $n!$ is defined for every nonnegative integer n. □

Example 24. Let us compute 7! using the inductive definition. Using (4.183) we get $7! = 7\times 6!$. Then using (4.183) 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 $7! = 7\times 6\times 5\times 4!$, and then $4! = 4\times 3!$, so $7! = 7\times 6\times 5\times 4\times 3!$. 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, (4.182) 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. □

4.5.3 The inductive definition of summation.

Definition 23. 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 sum (or summation) 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:

$$\begin{aligned}\sum_{j=1}^{1} a_j &= a_1\,,\\ \sum_{j=1}^{n+1} a_j &= \Big(\sum_{j=1}^{n} a_j\Big) + a_{n+1} \quad \text{for} \quad n\in\mathbb{N}\,.\end{aligned}$$

And we also define $\sum_{j=1}^{0} a_j = 0$.

Example 25. Let us compute $\sum_{j=1}^{5} j^2$. We have

$$\begin{aligned}
\sum_{j=1}^{5} j^2 &= \Big(\sum_{j=1}^{4} j^2\Big) + 5^2 \\
&= \bigg(\Big(\sum_{j=1}^{3} j^2\Big) + 4^2\bigg) + 5^2 \\
&= \Big(\sum_{j=1}^{3} j^2\Big) + 4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{2} j^2\Big) + 3^+4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{1} j^2\Big) + 2^2 + 3^+4^2 + 5^2 \\
&= 1^2 + 2^2 + 3^+4^2 + 5^2 \\
&= 1 + 4 + 9 + 16 + 25 \\
&= 55\,.
\end{aligned}$$

4.5.4 Inductive definition of product.

Definition 24. 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:

$$\begin{aligned}
\prod_{j=1}^{1} a_j &= a_1\,, \\
\prod_{j=1}^{n+1} a_j &= \Big(\prod_{j=1}^{n} a_j\Big) \times a_{n+1} \quad \text{for} \quad n \in \mathbb{N}\,.
\end{aligned}$$

And we also define $\prod_{j=1}^{0} a_j = 1$.

Example 26. If you compare the inductive definition of a product with the inductive definition of the factorial, you can easily see that

$$n! = \prod_{j=1}^{n} j \qquad \text{for every } \; n \in \mathbb{N}\,.$$

4.5.5 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

$$(\forall n \in \mathbb{N})P(n) \tag{4.184}$$

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

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{4.185}$$

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 $P(n) \implies P(n+1)$ for arbitrary n, it follows that (4.185) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (4.184 holds, that is, that $(\forall n \in \mathbb{N}) n < 2^n$. **Q.E.D.**

4.5.6 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

$$(\forall n \in \mathbb{N})(n \geq 4 \implies P(n)) \,. \tag{4.186}$$

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

$$(\forall n \in \mathbb{N})\Big(n \geq 4 \implies (P(n) \implies P(n+1))\Big) \,. \tag{4.187}$$

Let n be an arbitrary natural number such that $n \geq 4$..
We want to prove that $P(n) \implies P(n+1)$.

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 $P(n) \implies P(n + 1)$.

Since we have proved $P(n) \implies P(n + 1)$ for arbitrary n, it follows that (4.187) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (4.186) holds, that is, that $(\forall n \in \mathbb{N})\Big(n \geq 4 \implies (2^n < n!)\Big)$.
Q.E.D.

4.5.7 Another simple example

Let us prove

Theorem 41. *If a, b are arbitrary integers, then for every nonnegative integer[30] n the integer $a^n - b^n$ is divisible by $a - b$.*

Example 27. 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.)

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.

[30] Recall that the ***nonnegative integers*** are the natural numbers as well as zero.

Let a, b be arbitrary integers.

We will prove that

$$(\forall n \in \mathbb{N}) a - b | a^n - b^n \,, \tag{4.188}$$

and also that "$a - b | a^n - b^n$" is true for $n = 0$.

First we prove (4.188) by induction.

Let $P(n)$ be the statement[31] "$a - b$ 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

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1)) \,. \tag{4.189}$$

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

$$a^n - b^n = (a - b)k \,. \tag{4.190}$$

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 $a^{n+1} - b^{n+1} = (a - b)\big(ak + b^n\big)$.

[31] 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.

Clearly, $ak + b^n$ is an integer[32].

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 $P(n) \Longrightarrow P(n+1)$.

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary n, it follows that (4.189) holds.

So we have completed the basis step and the inductive step, and then the PMI tells us that (4.188 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 42.

1. ***Provide a detailed proof*** of the step that we skipped in the proof of Theorem 41, 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.)

[32]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!***.

2. ***Provide an alternative proof*** of Theorem 41, 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 43. One of the consequences of Theorem 41 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[33] 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.) □

[33]That is, the sum with alternating signs: first figure minus second figureplus third figure minus fourth figure, etc, etc.

5 Other forms of induction

5.1 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 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 42. *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 42. 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

$$P(s_*) \tag{5.191}$$

and

$$(\forall n \in \mathbb{Z}_{\geq s_*})\big(P(n) \implies P(n+1)\big)\,. \tag{5.192}$$

Then

$$(\forall n \in \mathbb{Z}_{\geq s_*})P(n)\,. \tag{5.193}$$

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 42. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$, and let

$$\mathbb{Z}_{\geq s_*} = \{n \in \mathbb{Z} : n \geq s_*\}\,. \tag{5.194}$$

Then

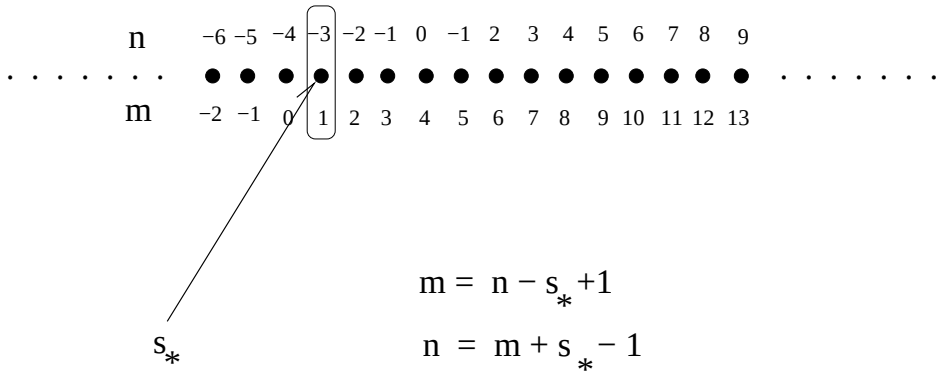
$$\Big(P(s_*) \wedge (\forall n \in \mathbb{Z}_{s_*})\big(P(n) \implies P(n+1)\big)\Big) \implies (\forall n \in \mathbb{Z}_{s_*})P(n)\,. \tag{5.195}$$

Proof of Theorem 42.

Assume that $P(n)$ is a 1-variable predicate and s_* is an arbitrary integer. We want to prove that if (5.191) and (5.192) hold, then (5.193) holds.

So we assume that (5.191) and (5.192) hold, and we try to prove that (5.193) 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

$$m = n + 1 - s_* \,. \tag{5.196}$$

(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:

$$n = m + s_* - 1 \,. \tag{5.197}$$

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 $Q(m) \Longrightarrow Q(m+1)$ is true for every $m \in \mathbb{N}$, because "$Q(m) \Longrightarrow Q(m+1)$" is equivalent to "$P(m + s_* - 1) \Longrightarrow P(m + s_*)$", 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 5. Theorem 42 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 42, if we take s_* to be 1, is exactly the PMI. □

Example 28. Let us prove the following:

Theorem 43. *If n is an integer such that $n \geq 4$, then $2^n < n!$.*

Proof. We want to prove that

$$(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow 2^n < n!)\,. \tag{5.198}$$

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 $P(4)$.

$P(4)$ aays "$2^4 < 4!$".

And $2^4 = 16$, $4! = 24$, so $2^4 < 4!$.

Therefore $\boxed{P(4) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(b) \Longrightarrow P(n+1))\Big)$.

Let $n \in \mathbb{Z}$ be arbitrary.

We want to prove $n \geq 4 \Longrightarrow (P(b) \Longrightarrow P(n+1))$.

Assume $n \geq 4$. We want to prove $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.

The inductive hypothesis $P(n)$ tells us that $2^n < n!$.

Then

$$2^{n+1} < 2n! \,. \tag{5.199}$$

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 $\boxed{P(n) \Longrightarrow P(n+1)}$ (by Rule $\Longrightarrow_{prove}$).

So $\boxed{n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))}$ (by Rule $\Longrightarrow_{prove}$).

Hence $\boxed{(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)}$ (by Rule $\forall_{use}0$.

This completes the inductive step.

Since we have proved $\boxed{P(4) \wedge (\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)}$, 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.**

5.2 Induction going forward and backward

The PMI says that, if a property is true of 1, and is passed on to the right, so each 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 if yo start at any integer s_*.

It is clear that if in addition each integer n also passes on the property to its predecessor $n-1$ (that is, if $P(n) \Longrightarrow P(n_1)$ for every $n \in \mathbb{Z}$), then $P(n)$ will be true for every integer n.

INDUCTION GOING FORWARD AND BACKWARD

Theorem 44. *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 $P(n)$ is true for one particular integer n, it follows that $P(n-1)$ 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 44. Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that

$$P(s_*) \tag{5.200}$$

and

$$(\forall n \in \mathbb{Z})\Big(P(n) \Longrightarrow \big(P(n+1) \wedge P(n-1)\big)\Big)\,. \tag{5.201}$$

Then

$$(\forall n \in \mathbb{Z})P(n)\,. \tag{5.202}$$

And we can say the same thing in even more formal language:

INDUCTION GOING FORWARD AND BACKWARD (VERY FORMAL LANGUAGE VERSION)

Theorem 44. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$. Then

$$\left(P(s_*) \wedge (\forall n \in \mathbb{Z})\Big(P(n) \Longrightarrow \big(P(n+1) \wedge P(n-1)\big)\Big)\right) \Longrightarrow (\forall n \in \mathbb{Z})P(n)\,. \tag{5.203}$$

It will be useful to reformulate the forward and backward induction condition in a slightly different way.

Suppose we prove that

$$(\forall n \in \mathbb{Z})\big(P(n) \Longleftrightarrow P(n+1)\big)\,. \tag{5.204}$$

Then given any integer n, if we assume that $P(n)$ is true, we can apply (5.204) to this particular integer, and conclude that $P(n) \iff P(n+1)$. so $P(n) \implies P(n+1)$.

And we can apply (5.204) to the integer $n-1$, and conclude that $P(n-1) \iff P(n)$. so $P(n) \implies P(n-1)$.

In other words, if (5.204) holds, then the condition (5.201) is satisfied. So, if we know that $P(s_*)$ for some starting integer s_*, we can conclude that $P(n)$ holds for every integer n.

This gives us the following slightly different version of the principle on induction going forward and backward:

INDUCTION GOING FORWARD AND BACKWARD
A SLIGHTLY DIFFERENT VERSION

Theorem 45.. *Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that*

$$P(s_*) \tag{5.205}$$

and

$$(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)\,. \tag{5.206}$$

Then

$$(\forall n \in \mathbb{Z})P(n)\,. \tag{5.207}$$

5.3 Examples of proofs using induction going forward and backward

5.3.1 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 divisblie 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 46. *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:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\,, \tag{5.208}$$

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 $n \in \mathbb{Z}$,

$$5|(n+1)^5 - (n+1) \Longleftrightarrow 5|n^5 - n\,. \tag{5.209}$$

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 $(\forall n \in \mathbb{Z})\big(P(n) \Longleftrightarrow P(n+1)\big)$. But Formula (5.209) says precisely that $P(n) \Longleftrightarrow P(n+1)$ for all $n \in \mathbb{Z}$,

This completes the inductive step. **Q.E.D.**

Problem 44. ***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:

$$\begin{aligned}(a+b)^7 &= a^7 + 7a^6b + 21a^5b^2 + 35a^5b^3 + 35a^3b^4 + 21a^2b^5 + 5ab^6 + b^7\\ (a+b)^{[}11] &= a^{11} + 11a^{10}b + 55a^9b^2 + 165a^8b^3 + 330a^7b^4 + 462a67b^5\\ &\quad +462a^5b^6 + 330s^4b^7 + 165a^3b^8 + 55a^2b^9 + 11ab^{10} + b^{11}\,.\end{aligned}$$

Remark 6. If you have done problem 44 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.) □

5.3.2 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

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \,\Big|\, n(n+1)(n+2)\cdots(n+k-1) \tag{5.210}$$

   or, using a notation without the mysterious and incomprehensible symbol "$\cdots$":

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \,\Big|\, \prod_{j=1}^{k}(n+j-1) \tag{5.211}$$

5. And we will indeed prove (5.211) 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 (5.211) 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 47. *If n is an integer, then $n(n+1)$ is even, i.e., divisible by 2. That is,*

$$(\forall n \in \mathbb{N})2|n(n+1)\,. \tag{5.212}$$

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 48. *If n is an integer, then $n(n+1)(n+2)$ is divisible by 6. That is,*

$$(\forall n \in \mathbb{Z}) 6 | n(n+1)(n+2) \,. \tag{5.213}$$

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

$$(\forall n \in \mathbb{Z}) \big(P(n) \iff P(n+1) \big) \,. \tag{5.214}$$

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

$$\begin{aligned}(n+1)(n+2)(n+3) &= (n+3)(n+1)(n+2)\\ &= n(n+1)(n+2)+3(n+1)(n+2)\\ &= n(n+1)(n+2)+3\times 2k\\ &= n(n+1)(n+2)+6k\,.\end{aligned}$$

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 $6|(n+1)(n+2)(n+3) \iff 6|n(n+1)(n+2)$, i.e., that $P(n) \iff P(n+1)$.

Since we have shown that $P(n) \iff P(n+1)$ for an arbitrary integer n, it follows that $(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)$, and this completes the inductive step.

It the follows from Theorem 45 that $P(n)$ is true for all integers n. That is, (5.213) holds. **Q.E.D.**

In the proof of Theorem 48 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 49. *If n is an integer, then $n(n+1)(n+2)(n+3)$ is divisible by 24. That is,*

$$(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)\,. \tag{5.215}$$

Proof. **YOU DO THIS ONE.** In the proof of Theorem 48 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 $(\forall n \in \mathbb{Z})6|n(n+1)(n+2)$.

Problem 45. ***Prove*** Theorem 49. □

Theorem 50. *If n is a natural number, then $n(n+1)(n+2)(n+3)(n+4)$ is divisible by* 120*. That is,*

$$(\forall n \in \mathbb{Z})120|n(n+1)(n+2)(n+3)(n+4)\,. \tag{5.216}$$

Proof. **YOU DO THIS ONE.** In the proof of Theorem 49 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 46. ***Prove*** Theorem 50.

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 nmakes it natural to make the following

Conjacture. For every natural number k the product of k consecurive 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 51. *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 ate 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 $j = 3$.)

Thet what we want to prove is the following statement:

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\, k! \Big| \prod_{j=1}^{k} (n+j-1)\,. \tag{5.217}$$

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

$$\forall n \in \mathbb{Z})\, k! \Big| \prod_{j=1}^{k} (n+j-1)\,. \tag{5.218}$$

In the proof, we are going to be working a lot with products such as $\prod_{j=1}^{k}(n+j-1)$. So it is better to give them a simpler name, to make it easier to work with them.

Let us use $a(n,k)$ to denote the product of k consecutive integers starting with n. 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, of course, the following formula holds for all $k \in \mathbb{N}$, $n \in \mathbb{Z}$:

$$a(n,k) = \prod_{j=1}^{k} (n+j-1) \tag{5.219}$$

or, if you prefer "..." notation,

$$a(n,k) = n \times (n+1) \times (n+2) \cdots \times (n+k-2) \times (n+k-1)\,. \tag{5.220}$$

Using this notation, the predicate $P(k)$ says:

$$\forall n \in \mathbb{Z})\, k! \Big| a(n,k)\,. \tag{5.221}$$

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

$$(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)\,. \tag{5.222}$$

Let $k \in \mathbb{N}$ be arbitrary. We want to prove that

$$P(k) \Longrightarrow P(k+1)\,. \tag{5.223}$$

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

$$(\forall n \in \mathbb{Z})\,(k+1)!\Big|a(n,k+1)\,. \tag{5.224}$$

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,
* ee 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 (5.224) is true,
* and, since (5.224) is a universal sentence about "all integers n", we are goin to do the proof by induction going forward and backward.

We let $Q(n)$ be the predicate

$$(k+1)!\Big|a(n,k+1)\,. \tag{5.225}$$

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

$$(\forall n\in\mathbb{Z})\big(Q(n)\iff Q(n+1)\big)\,. \tag{5.226}$$

Let $n\in\mathbb{Z}$ be arbitrary. We want to prove

$$Q(n)\iff Q(n+1)\,. \tag{5.227}$$

$Q(n)$ 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

$$a(n+1,k+1)-a(n,k+1)\quad\text{is divisible by }(k+1)!\,. \tag{5.228}$$

Before we do that,let me explain why this is a significant fact.
Suppose we have proved (5.228).
Assume $Q(n)$ 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 $a(n,k+1)+(a(n+1,k+1)-a(n,k+1))$ is divisible by $(k+1)!$. But this sum is $a(n+1,k+1)$, So $a(n+1,k+1))$ is divisible by $(k+1)!$. That says that $Q(n+1)$ holds.
Conversely, assume $Q(n+1)$ holds. Then $a(n+1,k+1)$ 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 difference $a(n+1,k+1)-\big(a(n+1,k+1)-a(n,k+1)\big)$ is divisible by $(k+1)!$. But this difference is $a(n,k+1)$, So $a(n,k+1))$ is divisible by $(k+1)!$. That says that $Q(n)$ holds.
Summarizing, we have shown that, if (5.228) is true, then $Q(n)\implies Q(n+1)$ and $Q(n+1)\implies Q(n)$, so $Q(n)\iff Q(n+1)$, which is exactly what we are trying to prove to complete the n-induction.

In other words: *all we need to do is prove (5.228) and that will complete our proof.*

We now prove (5.228).

The number $a(n, k+1)$ is the product of $k+1$ consecutive integers starting with n and ending with $n+k$. And this is clearly the product of n times k consecutive integers starting with $n+1$. That is,

$$a(n, k+1) = n \times a(n+1, k)\,. \tag{5.229}$$

Similarly, the number $a(n, k+1)$ is the product of $k+1$ consecutive integers starting with $n+1$ and ending with $n+k+1$. And this is clearly the product of k consecutive integers starting with $n+1$, mutliplied by $n+k+1$. That is,

$$a(n+1, k+1) = a(n+1, k) \times (n+1+k)\,. \tag{5.230}$$

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 formula

$$a(n+1, k+1) - a(n, k+1) = (k+1) \times a(n+1, k)\,. \tag{5.231}$$

(see the example in the box below to understand this formula).

THE FORMULA
$a(n+1,k+1) - a(n,k+1) = (k+1) \times a(n+1,k)$:
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 key point:*** 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 cah use $P(k)$. Add $P(k)$ says that

$$\forall n \in \mathbb{Z})\, k! \Big| a(n,k)\,. \tag{5.232}$$

So we can use (5.232).
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 (5.228) and, as explained before, it follows that $\boxed{Q(n) \iff Q(n+1)}$.

Since we have proved that $Q(n) \iff Q(n+1)$ for arbitrary $n \in \mathbb{Z}$, this shows that $\boxed{(\forall n \in \mathbb{Z})\big(Q(n) \iff Q(n+1)\big)}$.

This completes the inductive step of the n-induction.

We have proved that $Q(0)$ and $(\forall n \in \mathbb{Z})\big(Q(n) \iff Q(n+1)\big)$. By the PMI Going Forward and Backward, is follows that

$$(\forall n \in \mathbb{Z})Q(n)\,. \tag{5.233}$$

–] Since $Q(n)$ is the predicate "$(k+1)!\Big|a(n,k+1)$", we have proved

$$(\forall n \in \mathbb{Z})(k+1)!\Big|a(n,k+1)\,, \tag{5.234}$$

that is, we have proved $P(k+1)$.

Since we have proved $P(k+1)$ assuming $P(k)$, it follows that

$$P(k) \Longrightarrow P(k+1)\,. \tag{5.235}$$

Since we have proved (5.235) for an arbitrary natural numebr k, it follows that

$$(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)\,. \tag{5.236}$$

So we have proved $P(1)$ and $(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)$. It follows from the PMI that

$$(\forall k \in \mathbb{N})P(k)\,. \tag{5.237}$$

But $P(k)$ is the predicate "$(\forall n \in \mathbb{Z})\,k!\Big|a(n,k)$".

So we have proved

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\,k!\Big|a(n,k)\,, \tag{5.238}$$

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