MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

PART II

Contents

3 Universal sentences and how to prove and use them

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

For example, the sentence

$$\text{every natural number is either even or odd} \tag{3.1}$$

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

So this is a universal sentence.

Other examples of universal sentences are:

- Every cow has four legs.
- Every cow has nine legs[1].
- All humans are thinking beings.
- All giraffes have a long neck.
- Every giraffe has a long neck.
- Every real number is positive[2].
- Every natural number can be written as the sum of three squares of integers[3].
- Every natural number can be written as the sum of four squares of integers[4].
- Every integer is even[5].
- If a, b, c are integers, then if a divides b and c it follows that a divides $b + c$.

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

[2] This one is false.

[3] False again!

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

[5] Also false.

Universal sentences can always be rephrased is terms of "arbitrary things", as we saw in the first set of notes. For example, sentence (3.1) says

If n is an arbitrary natural number then n is either even or odd. (3.2)

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

$$\forall$$

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

Precisely, the symbol is used as follows:

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

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

  where

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

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

- So,

> If S is a set, and $P(x)$ is a statement involving the variable x, then
>
> $$(\forall x \in S)P(x)$$
>
> is a universally quantified sentence, obtained by universally quantifying the sentence $P(x)$.

3.1 How to read universal sentences

The universal sentence

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

can be read as follows:

- for every member x of S, $P(x)$ is true[6],

or as

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

or as

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

or as

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

or as

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

or as

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

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

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

$$\text{"all animals are made of cells}'' \text{ is true} \tag{3.3}$$

is just another way of saying

$$\text{all animals are made of cells}. \tag{3.4}$$

[6]See Remark 5 below.

Similarly, saying

$$P(n) \text{ is true} \tag{3.5}$$

is just another way of saying

$$P(n)\,. \tag{3.6}$$

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

3.2 Using the universal quantifier symbol to write universal statements

3.2.1 What is formal language?

Formal language is a language in which you use only formulas, and no words.

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

$$2 + 2 = 4\,. \tag{3.7}$$

And in this course you have learned how to say things such as "a is divisible by b" in formal language, by just saying

$$b|a\,. \tag{3.8}$$

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

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

in formal language?

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

(#1)	If we take any two real numbers and call them a and b, then $$(a+b)^2 = a^2 + b^2 + 2ab\,,$$

or

(#2)	If a, b are arbitrary real numbers, then $$(a+b)^2 = a^2 + b^2 + 2ab\,.$$

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

(#3)	If x, y are arbitrary real numbers, then $$(x+y)^2 = x^2 + y^2 + 2xy\,.$$

or

(#4)	If we take any two real numbers and call them x and y, then $$(x+y)^2 = x^2 + y^2 + 2xy\,.$$

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

These statements are universal sentences. And now you have learned how to ***formalize***[7] universal statements. So you can write

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

or

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

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

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

3.2.2 The road to full formalization.

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

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

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

Example 12. Suppose you wanted to say "every natural number is positive". You can write

$$(\forall n \in \mathbb{N}) n > 0\,. \tag{3.9}$$

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

Example 13. Although we do not know yet how to write something like

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

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

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

□

Example 14. Let us say "If a, b, c are integers, then if a divides b and c it follows that a divides $b + c$" in semiformal language.

We can say:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})\Big(\text{if } a|b \text{ and } a|c \text{ then } a|b+c\Big)\,, \tag{3.10}$$

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

Later, when we learn how to say "means", "there exists", "if ... then" and "and", we will be able to say (#8) and (3.10) in fully formal language.

3.3 Open and closed variables and quantified sentences

Let us recall from Part I of these notes that

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

Let me add a couple of points to that:

- Free variables are also called open variables.
- temporary constants are also called bound variables. or closed variables.

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

Example 15. Here is an example of declaring a value for a variable, and of making that declaration expire. You could write:

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

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

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

Notice that if you had written

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

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

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

Example 16. *(This is an improved version of an example in Part I of the notes).*
Consider the following paragraph:

> George Washington was the first president of the United States, and he served as president for two terms. He was succeeded by John Adams, who served only one term. When Adams ran for reelection to a second term in 1800, he was the object of malicious attacks by his opponents, and eventually lost the election to Thomas Jefferson. He then retired and never ran again for office.

In this text, the pronoun "he" appears four times. The first two times, it refers to George Washington, but the third and fourth times it refers to John Adams. So "he" is a variable. Before the beginning of this text, "he" was free: we were able to declare "he" to stand for anybody we wanted. Then the mention of George Washington had the effect of declaring "he" to stand for "George Washington". And later, you would think that the mention of John Adams had the effect of freeing "he" from begin attached to George Washington and attaching it to John Adams instead. But, with that criterion, one would expect that the mention of Thomas Jefferson would

have the effect of freeing "he" from its attachment to John Adams, and would redeclare the value of "he" to be "Thomas Jefferson". And yet, it is clear that the fourth "he"is Adams, not Jefferson. Why? I don't know. □

A CHALLENGING QUESTION FOR YOU. Try to figure out exactly why the fourth "he" in Example 16 stands for "John Adams" rather than for "Thomas Jefferson". What is he general rule? It cannot be that "the variable 'he' stands for the last man [8] mentioned immediately before" because, as we have seen, the most recently mentioned name befoe the fourth 'he' is that of Jefferson, but that 'he' clearly stands for Adams. □

3.4 A general principle: two rules for each symbol

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

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

and

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

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

The "use" rule is:

[8] I am saying "man", rather than "person", because one of the usual rules of English usage is that "he" stands for a man and "she" stands for a woman. That's why, for example, if I told you that "I just saw my friends Jim and Alice. He said that he is going to Boston this weekend, but she said she is not going", you know that "he" stands for "Jim" and not for "Alice", even though the name mentioned most recently was "Alice", not "Jim". It would have been the same if I had said "I just saw my friends Alice and Jim. He said that he is going to Boston this weekend, but she said she is not going". And if I had said "I just saw my friends Pat and Chris. He said that he is planning to go to Boston this weekend, but she said she is not going", you might be confused.

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

$$a|b\,,$$

then you can go from this to

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

And the "prove" rule is:

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

$$b = ak\,,$$

then you can go from this to

$$a|b\,.$$

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

3.4.1 Naming sentences

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

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

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

We could do this by writing

Let P be the sentence "x eats grass".

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

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

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

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

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

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

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

And then,

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

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

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

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

should be read as

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

Why do we want to do this?

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

So, for example, when I explain to you that

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

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

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

$$(\forall n \in \mathbb{Z}) n(n+1) \text{ is even}. \tag{3.11}$$

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

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

The answer is ***no***. Why? Because after the end of the sentence (3.11), n is a free variable again, so it does not have a value, so when you use "n" in the

next step, nobody knows what you are talking about, so what you wrote is meaningless, so it's not acceptable.

Suppose you want to go from (3.11) to

$$(\forall n \in \mathbb{Z}) n + n^2 \text{ is even}. \tag{3.12}$$

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

3.5 Proving and using universal sentences

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

Both are very simple, very natural rules.

Here is the "use" rule:

The rule for using universal sentences

If you have proved

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

here is what you can do with that: You can take the name of any thing whatsoever, as long as it is a member of S, and write as new step the statement that $P(x)$ is true for this particular thing. So, if that thing is called "a", you can go to $P(a)$.

This rule is called the ***specialization rule***, because it says that if a statement is true in general (that is, for all things that belong to some set S), then it is true in each special case (that is, for a particular thing that belongs to S).

And here is the "prove" rule:

The rule for proving universal sentences

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

Let x be an arbitrary member of S,

and then prove $P(x)$

If you manage to do that, then you are allowed to write

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

in the next step of your proof.

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

Example 19. Suppose you know that

(&) All cows eat grass.

and that

(&&) Suzy is a cow.

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

(&&) Suzy eats grass.

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

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

whereas (&&) says

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

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

Remark 6. Notice that in the previous example there were two occasions when I introduced a variable by declaring its value:

- I introduced the variable "$P(x)$", and I declared that it would stand for the sentence "x eats grass". You may complain that a variable is supposed to be a letter. But if you look carefully what I wrote on page 42, you will see that a variable is a "letter or string of symbols". So I can perfectly well use "$P(x)$", which is a string of four symbols, as a variable.
- I introduced the variable "C", and I declared that it would stand for the set of all cows. □

Example 20. In subsection 3.4.2 I asked the question: *how do we got from (3.11) to (3.12)?*

Here is how.

1. We know that
$$(\forall n \in \mathbb{Z})n(n+1) \text{ is even}\,. \tag{3.13}$$
.2 Let n be an arbitrary integer[9].
3. Then, by the specialization rule, from step 1,
$$n(n+1) \text{ is even}\,. \tag{3.14}$$
4. But $n(n+1) = n + n^2$.

[9]Remember that, aftet we wrote sentence (3.13), the variable n becomes free, so we can make it bound again by declaring a value for it, as we do in this step.

5. So, using rule SEE, we conclude that

$$n + n^2 \text{ is even}. \tag{3.15}$$

6. We have proved (3.15) under the assumption that n was an arbitrary integer. So, by the rule for proving universal sentences, we can conclude that:

$$(\forall n \in \mathbb{Z}) n + n^2 \text{ is even}. \tag{3.16}$$

Q.E.D.

Remark 7. Naturally, nobody would really write all that. What one wold write is:

We know that

$$(\forall n \in \mathbb{Z}) n(n+1) \text{ is even}. \tag{3.17}$$

But $n(n+1) = n + n^2$.

So

$$(\forall n \in \mathbb{Z}) n + n^2 \text{ is even}. \tag{3.18}$$

Q.E.D.

But at this point, before you start omitting steps, I want you to understand that ***those steps are there, and it is only because you know how to put them in if you had to, that you can omit them.***

The key question is this: ***when you omit one or several steps, will it be clear to the reader how to fill them in?***.

- If it is clear to you that it is going to be clear to the reader, then you don't need to include those steps.
- If you think that it is not going to be clear, then it is better to put them in.
- And if you don't know, it's better to err in the direction of too much detail than in the direction of too little detail.
- But, on the other hand, if you tell the readers too many things that are completely obvious to them, then the readers might be offended, thinking that you are insulting their intelligence.

- However, ***in this course you should not worry about the danger that I, or the graders, might be offended.*** Of course, we know how the proofs are supposed to go, but you should write as if we didn't know. So it's always O.K. to give details.

So, as you can see, the final answer to the question "how much detail should I give?" is, really, "I don't know, it depends". So writing mathematics is like any other kind of writing: you never know for sure what *has* to be said, what *can* be left unsaid, and what *has* to be left unsaid. You have to use your own judgment, and do what seems best to you. And that depends on which specific readers you are writing for. □

4 More theorems about the integers

4.1 Cancellation, multiplication by zero, and subtraction

We now study some very simple but important facts, such as the cancellation law of addition, the formula $n.0 = 0$, and the operation of subtraction of integers.

4.1.1 The cancellation law of addition

If we have an equality $a+c = b+c$, we would like to be able to "cancel" the c that appears on both sides and conclude that $a = b$. The following theorem tells us that this is possible.

Theorem 10. *If a, b, c are integers such that $a + c = b + c$, then $a = b$.*

NOTE: In semiformal language, the statement we want to prove is

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(\text{if } \ a + c = b + c \ \text{ then } \ a = b)\,. \tag{4.19}$$

Proof. We want to prove (4.19).

Let a, b, c be arbitrary integers.

Assume that $a + c = b + c$.

Then

$$c + (-c) = 0\,. \tag{4.20}$$

Therefore

$$\begin{aligned} a &= a+0 && (4.21)\\ &= a+(c+(-c)) && (4.22)\\ &= (a+c)+(-c) && (4.23)\\ &= (b+c)+(-c) && (4.24)\\ &= b+(c+(-c)) && (4.25)\\ &= b+0 && (4.26)\\ &= b\,. && (4.27) \end{aligned}$$

So $a = b$.

We have proved "$a = b$" assuming "$a + c = b + c$". So the rule for proving an "if. . .then" sentence enables us to conclude that

$$\text{if } \ a+c=b+c \ \text{ than } \ a=b\,. \tag{4.28}$$

We have proved (4.20) for arbitrary integers a, b, c. Therefore, by the rule for proving universal sentences,

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\forall c \in \mathbb{Z})(\text{if } \ a+c=b+c \ \text{ then } \ a=b)\,.$$

Q.E.D.

NOTE: The meaning of the string of equalities (4.21), (4.22), (4.23), (4.24), (4.25), (4.26), (4.27), is

$$\begin{aligned} a &= a+0\,,\\ a &= a+(c+(-c))\,,\\ a &= (a+c)+(-c)\,,\\ a &= (b+c)+(-c)\,,\\ a &= b+(c+(-c))\,,\\ a &= b+0\,,\\ \text{and} \quad a &= b\,. \end{aligned}$$

Problem 7. Provide the justification *of each of the eight steps (4.20), (4.21), (4.22), (4.23), (4.24), (4.25), (4.26), (4.27) of the proof of Theorem 10.*

Here is a justification of (4.20): According to Basic Fact BFZ5, for every integer n the integer $-n$ satisfies $n + (-n) = 0$. That is,

$$(\forall n \in \mathbb{Z})n + (-n) = 0.$$

Then, by the specialization rule, we get $c + (-c) = 0$.

And here is a justification of (4.21): The Equality Axiom says that "$x = x$ for every x", that is[10] $(\forall x)x = x$. Then, by the specialization rule we can conclude that $a + 0 = a + 0$. Basic Fact BFZ4 says that $(\forall n \in \mathbb{Z})n + 0 = n$. Then, by the specialization rule we can conclude that $a + 0 = a$. And then, using the SEE rule, we can substitute "a" for the first "a+0" in "a+0 = a+0' and get $a = a + 0$.

YOU DO THE OTHERS. □

4.1.2 Multiplication by zero

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

Theorem 11. *If n is an integer then $n.0 = 0$.*

Proof.

Let n be an arbitrary integer.

We know from BFZ4 that $0 + 0 = 0$.

Hence $n.(0+0) = n.0$. (Reason: $n.0 = n.0$ by the Equality Axiom. And $0 + 0 = 0$, so Rule SEE enables us to conclude that $n.(0 + 0) = n.0$.)

But $n.(0 + 0) = n.0 + n.0$ by the distributive law.

Hence $n.0 + n.0 = n.0$.

[10]The ***unrestricted quantifier*** $(\forall x)$ means "for all things x", that is "if x is an arbitrary thing then". You could think of "$(\forall x)$" as meaning "$(\forall x \in U)$", where U is the "universal set", that is the set whose members are all the things that exist, including cows, planets, cells, rivers, people, numbers of every kind and even sets. It turns out that, for reasons that will be explained later, it is not a good idea to allow such a set to exist, so the "universal set" interpretation of the quantifier "$(\forall x)$", while helpful, should not be made too much of.

But $0 + n.0 = n.0$ by BFZ4.

So $n.0 + n.0 = 0 + n.0$.

Using the cancellation law (i.e., Theorem 10), with $n.0$ in the role of a, 0 in the role of b, and $n.0$ in the role of c, we get $\boxed{n.0 = 0}$. **Q.E.D.**

4.1.3 Is there a cancellation law of multiplication?

Exactly as we proved that if we have an equality $a + c = b + c$ then we can "cancel" the c and conclude that $a = b$, one would expect to be able to prove a similar result for multiplication: if $ac = bc$ then $a = b$. This, however, is impossible. For example, $2 \times 0 = 3 \times 0$, because $2 \times 0 = 0$ and $3 \times 0 = 0$, but 2 is not equal to 3.

It turns out that if we only try to cancel c when c is different from zero, then this is possible: it is true that

(CL) if $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, $c \neq 0$, and $ac = bc$, then $a = b$.

But this is much harder to prove, and at this point we do not have the knowledge needed to prove it.

And this is so for a very deep reason: ***using the basic facts we have presented so far, it is impossible to prove the cancellation law (CL)***.

And when I say "it is impossible" I do not just mean "it is very hard", or "I do not know how to do it", or even "nobody has been able to do it". I mean something much stronger: I can ***prove*** that it is impossible to prove (CL) from the Basic Facts we have at his point. I will try to explain this later in the course.

4.1.4 Some very 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 12. *If m, n are integers, then*

$$-mn = (-m).n\,.$$

Proof.

Let $m.n$ be arbitrary integers.

Then

$$\begin{aligned}
-mn &= (-mn) + 0 && (4.29)\\
&= -(mn) + 0.n && (4.30)\\
&= -(mn) + (m + (-m)).n && (4.31)\\
&= -(mn) + \Big(mn + (-m)n\Big) && (4.32)\\
&= \Big((-mn) + mn\Big) + (-m)n && (4.33)\\
&= \Big(mn + (-mn)\Big) + (-m)n && (4.34)\\
&= 0 + (-m)n && (4.35)\\
&= (-m)n\,. && (4.36)
\end{aligned}$$

So $\boxed{-mn = (-m)n}$. **Q.E.D.**

Theorem 13. *If n is an integer, then*

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

Proof. Let n be an arbitrary integer. Then

$$\begin{aligned}
-(-n) &= -(-n) + 0 && (4.37)\\
&= -(-n) + (n + (-n)) && (4.38)\\
&= (-(-n)) + ((-n) + n) && (4.39)\\
&= \Big(- (-n) + (-n)\Big) + n && (4.40)\\
&= \Big((-n) + (-(-n))\Big) + n && (4.41)\\
&= 0 + n && (4.42)\\
&= n\,. && (4.43)
\end{aligned}$$

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

Problem 8. **Provide the justification** *of each of the eight steps (4.29), (4.30), (4.31), (4.32), (4.33), (4.34), (4.35), (4.36), of the proof of Theorem 12 and of each of the seven steps (4.37), (4.38), (4.39), (4.40), (4.41), (4.42), (4.43) of the proof of Theorem 13* □

Theorem 14. *If n is an integer then $-n = (-1).n$.*

Proof. Let n be an arbitrary integer. Then

$$\begin{aligned} (-1).n &= -(1.n) && (4.44)\\ &= -n\,. && (4.45) \end{aligned}$$

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

Theorem 15. *If m, n are integers, then*

$$(-m).(-n) = mn\,.$$

Proof. Let m, n be arbitrary integers. Then

$$\begin{aligned} (-m).(-n) &= m.(-(-n))) && (4.46)\\ &= m.n\,. && (4.47) \end{aligned}$$

So $\boxed{(-m).(-n) = mn\,.}$ **Q.E.D.**

Problem 9. **Provide the justification** *of*

1. *each of the two steps (4.44), (4.45) of the proof of Theorem 14,*
2. *each of the two steps (4.46), (4.47) of the proof of Theorem 15.* □

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.

4.1.5 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 21.

- ***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.
- ***Subtraction*** [11] ***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 real numbers*** are binary operations whose arguments are real numbers.
- ***Minus*** 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". (As explained in Part I of these notes (on page 21), I strongly recommend that you read "$-n$" as "minus n" rather than, say, "negative n".)
- There is a similar "minus" unary operation on the real numbers.

[11] Addition and multiplication of integers appear in the Basic Facts. Subtraction does not. We will have to ***define*** what subtraction is, and that will be done in Subsection 4.1.6.

- The ***scalar 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 $\vec{w}$. □

4.1.6 Subtraction

We would like to be able to talk about the ***difference*** of two integers m and n, i.e., the number $m - n$. The Basic Facts do not say anything about differences, but they talk about "minus" an integer, and using this we can define subtraction, i.e., the operation of computing the difference of two integers.

Definition 11. If m and n are integers, then $m - n$ (read as "m minus n") is the integer $m + (-n)$. □

And then we can prove a simple formula that you already know:

Theorem 16. *If m and n are integers, then*

$$(m - n) + n = m\,.$$

Proof. Let m, n be arbitrary integers. Then

$$\begin{aligned}
(m - n) + n &= (m + (-n)) + n && (4.48)\\
&= m + ((-n) + n) && (4.49)\\
&= m + (n + (-n)) && (4.50)\\
&= m + 0 && (4.51)\\
&= m\,. && (4.52)
\end{aligned}$$

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

Problem 10. **Provide the justification** *of each of the five steps (4.48), (4.49), (4.50), (4.51), (4.52) of the proof of Theorem 16.* □

5 Even and odd integers

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

5.1 The meaning of "even" and "odd" for integers

We will begin by giving a precise definition of what it means for an integer to be "even", and what it means to be "odd".

Definition 12. An integer n is <u>even</u> if n is divisible by 2. □

Definition 13. An integer n is <u>odd</u> if $n - 1$ is even. □

Example 22.

1. The number 0 is even, because $0 = 2 \times 0$, so 0 is divisible by 2.
2. The number 1 is odd, because $1 - 1 = 0$, so $1 - 1$ is even.
3. The number 2 is even, because $2 = 2 \times 1$, so 2 is divisible by 2.
4. The number 3 is odd, because $3 - 1 = 2$, and 2 is even. □
5. The number 0 is even, because $0 = 2 \times 0$, so $2|0$.
6. The number -1 is odd, because $(-1) - 1 = -2$, and $-2 = 2 \times (-1)$, so -2 is even and then -1 is odd. □

5.2 The parity of a sum and a product

We can now 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".

Theorem 17. *The sum of two even integers is even. That is: if a and b are integers and both a and b are even, then $a + b$ is even.*

Proof.

Let a and b be arbitrary even integers.

Then a and b are divisible by 2.

But we know (from Theorem 6 in Part I of these notes) that if x, y, z are integers such that $x|y$ and $y|z$ then $x|y+z$. Therefore $a+b$ is divisible by 2.

So $\boxed{a+b \text{ is even}}$. **Q.E.D.**

Theorem 18. *The sum of an even integer and an odd integer is an odd integer. That is: if a and b are integers, a is even, and b is odd, then $a+b$ is odd.*

Proof.
Let a, b be arbitrary integers.
Suppose a is even and b is odd.
Then Definition 13 tells us that $b-1$ is even.
So it follows from Theorem 17 that $a+(b-1)$ is even.
But $a+(b-1)=(a+b)-1$.
So $(a+b)-1$ is even.
Therefore Definition 13 tells us that $\boxed{a+b \text{ is odd}}$. **Q.E.D.**

Problem 11. ***Prove*** *that the product of two even integers is divisible by* 4. □

Next, we prove that "odd plus odd is even", that is, that the sum of two odd integers is an even integer.

Theorem 19. *The sum of two odd integers is an even integer. That is: if a and b are integers, and a and b are both odd, then $a+b$ is even. (Or, in fully formal language: $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\text{if } 2|a-1 \text{ and } 2|b-1 \text{ then } 2|a+b)$.)*

Proof.
Let a, b be arbitrary integers.
Assume that a and b are odd.
We want to prove that $a+b$ is even.
Since a is odd, $a-1$ is even.
Since b is odd, $b-1$ is even.
Since the sum of two even integers is even, $(a-1)+(b-1)$ is even.

But $(a-1)+(b-1) = (a+b)-2$.
So $(a+b)-2$ is even.
On the other hand, 2 is even.
So the sum $\Big((a+b)-2\Big)+2$ is even.
But $\Big((a+b)-2\Big)+2 = a+b$.
So $\boxed{a+b}$ is even.

Q.E.D.

Next, we prove that "even times anything is even". The precise statement of this is as follows:

Theorem 20. *The product of two integers, one of which is even, is an even natural number. That is: if a, b are integers, and a is even or*[12] *b is even, then ab is even.*

Proof. Without loss of generality[13], we may assume that a is even.
Since a is even, we can write $a = 2k$ for some integer k.
Then $ab = (2k)b = 2(kb)$.
Since kb is an integer, it follows from Definition 12 that $\boxed{ab \text{ is even}}$.

Q.E.D.

Now that we know what happens to the product of two integers when one of them is even, there remains the case when both are odd.

Theorem 21. *The product of two odd integers is odd. That is: if a and b are odd integers, then ab is odd.*

Proof. **YOU DO THIS ONE.**

Problem 12. ***Prove*** *Theorem 21.* □

We have already described how evenness and oddness behave when we add and multiply integers. Addition and multiplication are two of the three

[12] See the box on page 65 for a detailed explanation of the meaning of "or". In particular, it is important to understand that "or", im mathematics, is always ***inclusive***. So, for example, "a is even or b is even" is true when a is even, when b is even, and when both a and b are even.

[13] See the box on "Without loss of generality", on page 68.

operations on integers that occur in the basic facts. The third one is the "minus" operation, so we have to see how this operation is related to evenness and oddness.

The answer is very simple:

Theorem 22. *If n is an integer, then*

- *If n is even then $-n$ is even.*
- *If n is odd then $-n$ is odd.*

Proof. YOU DO THIS ONE.

Problem 13. ***Prove*** *Theorem 22.* □

5.3 A little bit of logic: disjunctions, conjunctions, and their truth values

We have already encountered several examples of sentences involving "or" and sentences involving "and".

Example 23.

- In the statement of Theorem 20, the sentence "If a is even or b is even then ab is even" appears. This sentence is an ***implication***, that is, of the form "If A then B", which we will learn later to write as $A \Longrightarrow B$. The sentence A is called the premise and the sentence B is called the conclusion. In our case,
  - A is the sentence "a is even or b is even".
  - B is the sentence "ab is even".

  So A is an "or" sentence, that is, a sentence of the form "P or Q". where P is "a is even" and Q is "b is even". Such a sentence is called a disjunction.

  We use the symbol "$\vee$" for "or", so the disjunction "a is even or b is even" can be written as "a is even $\vee$ b is even". And, if you want to use even more formal language, you may recall that "x is even" means "$2|x$". So we could rewrite the sentence "If a is even or b is even then ab is even" in fully formal language as follows:

$$(2|a \vee 2|b) \Longrightarrow 2|ab\,.$$

- In the statement of Theorem 17, the sentence "If a is an even integer and b is an even integer then $a + b$ is even". This sentence is also an implication, that is, of the form "If A then B", which we can write as $A \implies B$. The sentence A is the premise and the sentence B is the conclusion. In our case,
  - A is the sentence "a is an even integer and b is an even integer".
  - B is the sentence "$a + b$ is even".

  So A is an "and" sentence, that is, a sentence of the form "P and "Q". where P is "a is an even integer" and Q is "b is and even integer". Such a sentence is called a conjunction.

  We use the symbol "$\wedge$" for "and", so the conjunction "a is an even integer and b is an even integer" can be written as "a is and even integer $\wedge$ b is an even integer". And, if you want to use even more formal language, you may recall that "x is an even integer" means "$x \in \mathbb{Z} \wedge 2|x$". So we could rewrite the sentence "If a is an even integer and b is an even integer then ab is even" in fully formal language as follows:

$$\Big((a \in \mathbb{Z} \wedge 2|a) \wedge (b \in \mathbb{Z} \wedge 2|b)\Big) \implies 2|a + b\,. \qquad \square$$

The meaning of "or" in mathematics

In English, when we use the word "or", it can have two different meanings:

1. ***Inclusive*** "or", that is, "one or the other or both".

or

2. ***Exclusive*** "or", that is, "one or the other but not both".

For example, if a store announces that

> If you are a student or a senior citizen then you are entitled to a 15% discount on your purchases.

then, obviously, anyone who is both a student and a senior citizen will be entitled to a discount. So this is an example of ***inclusive*** or.
On the other hand, if a restaurant waiter asks you "would you like tea or coffee?", then it is clear that you can have one or the other but not both, so this an example of ***exclusive*** or.

In mathematics, "or" is always inclusive.

So, if I say, for example,

> if a and b are integers and a is even or b is even, then the product ab is even,

then this also applies to the case when both a and b are even.

DISJUNCTIONS AND THEIR TRUTH VALUES

The symbol "$\vee$" stands for "or". If A and B are sentences, then we write "$A \vee B$" for "A or B".
A sentence of the form $A \vee B$ is called a disjunction.
In a disjunction $A \vee B$, A is the first disjunct and B is the second disjunct
For example, if A is the statement "2 is an odd natural number", and B is the statement "2 is an even natural number", then we can read $A \vee B$ as "2 is an odd natural number or 2 is an even natural number" or, even better, as "2 is odd or even".

The truth value of a disjunction. When is a disjunction $A \vee B$ true? When is it false?
That depends on whether A and B are true or false. Precisely:
If A ***and*** B ***are false then*** $A \vee B$ ***is false. In all other cases,*** $A \vee B$ ***is true.*** So the truth value of $A \vee B$ is given in terms of the truth values of A and B by the following ***truth table***:

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

This captures the fact that "or" is inclusive: when both A and B are true, the "or" sentence $A \vee B$ is true.

CONJUNCTIONS AND THEIR TRUTH VALUES

If A and B are sentences, then we can form the sentence "A and B".
The symbol "$\wedge$" stands for "and". If A and B are sentences, then we write "$A \wedge B$" for "A and B".
A sentence of the form $A \wedge B$ is called a conjunction.
In a conjunction $A \wedge B$, A is the first conjunct and B is the second conjunct
For example, if A is the statement "6 is divisible by 2", and B is the statement "6 is divisible by 3", then we can read $A \wedge B$ as "6 is divisible by 2 and 6 is divisible by 3" or, even better, as "6 is divisible by 2 and by 3".

The truth value of a conjunction. When is a conjunction $A \wedge B$ true? When is it false?
That depends on whether A and B are true or false. Precisely:
If A ***and*** B ***are true then*** $A \wedge B$ ***is true. In all other cases,*** $A \wedge B$ ***is false.*** So the truth value of $A \wedge B$ is given in terms of the truth values of A and B by the following ***truth table***:

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

Without loss of generality

Suppose we want to prove that something happens in each of two (or three, or four) possible cases. Suppose all the cases are "the same", in the following precise sense: each of the cases becomes Case 1 if you just change the names of the objects involved. Then it suffices to do the proof for Case 1, because the statement for the other cases follows easily by just applying the result of Case 1.
When we are in this situation, we can say "assume, without loss of generality, that are in case 1". What this means is that, ***once we prove our result for Case 1, the result for the other cases follows automatically, and there is no need to write a separate proof for each case.*** Why is this so? The reason is that, once we have the result for Case 1, then the result for the other cases follows from this by just changing the names of the objects involved.
EXAMPLE: Suppose we want to prove that "if a is even or b is even then ab is even". Then we have to consider two cases: when a is even and when b is even. Suppose we prove what we want in the first case, when a is even. That is, we prove that "if a is even then ab is even". Then the result for the second case "if b is even then ab is even") follows immediately, because we can apply the first result with "b"in the role of "a" and "a" in the role of "b". (If you do not feel comfortable with this, think of it as follows: if we have proved that "if a is even then ab is even", then we could equally well state our result by saying that "if x is even then xy is even". But then the fact that "if b is even then ab is even follows by applying our first result with b in the role of x and a in the role of y.

5.4 Introduction to the proof that "every integer is even or odd and not both"

We would now like to prove that an integer cannot be both even and odd, and it has to be either even or odd.

That is, we want to prove that:

(A) If $n \in \mathbb{Z}$ then n is even or n is odd.

(B) If $n \in \mathbb{Z}$ then n is not both even and odd.

It turns out that ***we cannot prove (A) and (B) using the basic facts about the integers that we have so far.*** And when I say "we cannot prove (A) and (B)" I do not mean that "it is very hard to prove (A) and (B)", or "nobody has figured out yet how to prove (A) and (B) but maybe some day somebody will". I mean something much stronger: ***I can prove to you that statements (A) and (B) cannot be proved from the Basic Facts BFZ1, BFZ2, BFZ3, BFZ5, BFZ6 listed on Page 20 of Part I of these notes.***

You may find this hard to believe. How can I ***prove*** that something cannot be proved? I will show you how, by actually keeping my promise and proving what I said I am going to prove. But I am not ready to it right now. You will have to wait a few days.

In oder to develop a better understanding of our problem, let us temporarily agree to call an integer n "good" if it has the property we are interested in, that is, if n is even or odd and not both even and odd.

Then what we would like to do is to prove that every integer is good.

And the idea of how to do it is to follow a four-step program:

1. First, we will prove that 1 is odd and not even, so 1 is good.

2. Next, we will prove that goodness is passed on from each natural number to its successor; that is: if a natural number n is good then $n + 1$ is good.

3. From the two facts above, it will follow that every natural number is good, but we will need a new and very important new basic fact to prove that, namely, the Principle of Mathematical Induction.

4. Finally, once we know that every natural number is good, it will be easy to conclude, using Theorem 22, that every integer is good.

5.5 The proof that 1 is not even: preliminary remarks

The first step of our four-step program is to prove that 1 is good. We already know that 1 is odd. So to prove that 1 is good we need to prove that 1 is not even.

In order to do prove that 1 is not even, we will need a list of new basic facts, because the basic facts that we have so far are not sufficient.

And, in addition, our argument is going to be a ***proof by contradiction***.

So, before I give the proof, let us explain what a "proof by contradiction" is.

5.6 Proofs by contradiction

Proof by contradiction is probably the most important and most widely used of all proof strategies. So you should not only learn what proofs by contradiction are, but ***acquire the habit of always***[14] ***seriously considering the possibility of using the proof by contradiction strategy when you are trying to figure out how to do a proof.***

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

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

5.6.1 What is a contradiction?

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

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

Example 24.

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

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

- The sentence "$2 + 2 = 7$ and $2 + 2 = 4$" is ***not*** a contradiction either. It is a false statement (because it is the conjunction of two sentences one of which is false), but that does not make it a contradiction.
- The sentence "$2 + 2 = 7$ and $2 + 2 \neq 7$" ***is*** a contradiction. because it is of the form "A and no A", with the sentence "$2 + 2 = 7$" in the role of A.
- The sentence "$n = 1$ and $n \neq 1$" is a contradiction.
- The sentence "John Adams was the first U.S. president" is false, but it ***not*** a contradiction.
- The sentence "John Adams was the first U.S. president and was the second U.S. president" is false, but it ***not*** a contradiction.
- The sentence "John Adams was the first U.S. president and was not the first U.S. president" ***is*** a contradiction. □

5.6.2 What is a proof by contradiction?

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

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

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

WARNING

Having explained very precisely what a contradiction is, I have to warn you that mathematicians will often say things like "'$2 + 2 = 7$'" is a contradiction".
This is not quite true, but when a mathematician says that every mathematician will understand what is really intended.
What the person who said "'$2 + 2 = 7$' is a contradiction" really meant is something like this:

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

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

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

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

5.7 New basic facts about the integers

As I have already explained, we need some new basic facts.

Here is a first list[15] of new basic facts:

[15] This is not the full list. We will need one more basic fact, the Principle of Mathematical Induction. But that is coming later.

BASIC FACTS ABOUT THE INTEGERS II

BFZ6: 1 is a natural number, and 0 is not a natural number.
BFZ7: Every natural number is an integer.
BFZ8: The sum and the product of two natural numbers is a natural number. That is

$$m+n \in \mathbb{N} \text{ and } m.n \in \mathbb{N} \qquad \text{whenever } m \in \mathbb{N}\,,\, n \in \mathbb{N} \tag{5.53}$$

BFZ9: Every integer is either a natural number, or minus a natural number, or zero, that is[a]:

$$\text{If } n \in \mathbb{Z} \text{ then } n \in \mathbb{N} \vee -n \in \vee n = 0\,. \tag{5.54}$$

BFZ10: If n is a natural number and $n \neq 1$, then $n-1$ is a natural number as well.

[a] Here I am using the "$\vee$" symbol for "or".

5.8 The proof that 1 is not even

Using the new basic facts, I can finally prove that 1 is good. As explained before, we already know that 1 is odd, so what we need to prove is that 1 is not even.

And here, finally, is the proof.

Theorem 23. 1 *is not even.*

Proof. We are going to do a proof by contradiction . Since we want to prove that 1 is not even, we will assume that 1 is even and derive a contradiction.

- Suppose[16] 1 was even.
- Then there would exist an integer k such that $1 = 2k$.
- According to Basic fact BFZ9, either $k \in \mathbb{N}$, or $-k \in \mathbb{N}$, or $k = 0$.

[16] "Suppose" means the same as "assume", or "imagine". What we are doing here is set out to explore an imaginary world in which 1 is even, until we find out that such a world is impossible, so it is impossible for 1 to be even, so 1 cannot be even.

- The possibility that $k = 0$ is excluded, for the following reason:
  - Suppose that $k = 0$.
  - Then $1 = 2k = 2 \times 0 = 0$, so $1 = 0$.
  - But $1 \neq 0$ by Basic Fact BFZ1 (or also by BFZ6, because $1 \in \mathbb{N}$ and $0 \notin \mathbb{N}$).
  - So $1 = 0$ and $1 \neq 0$, which is a contradiction[17].
- The possibility that $-k \in \mathbb{N}$ is also excluded, for the following reason[18]:
  - Suppose that $-k \in \mathbb{N}$.
  - Since $1 = 2k$, we have $-1 = -2k = 2 \times (-k)$.
  - Since $2 \in \mathbb{N}$ and $-k \in \mathbb{N}$, we conclude that $2 \times (-k) \in \mathbb{N}$.
  - Since $2 \times (-k) = -1$, it follows that $-1 \in \mathbb{N}$.
  - But $1 \in \mathbb{N}$.
  - So $1 + (-1) \in \mathbb{N}$, that is, $0 \in \mathbb{N}$.
  - But $0 \notin \mathbb{N}$.
  - So $0 \in \mathbb{N}$ and $0 \notin \mathbb{N}$, which is a contradiction.
- Since one of the three possibilities $k \in \mathbb{N}$, $k = 0$, $-k \in \mathbb{N}$ occurs, and the first two cannot occur, it follows that $k \in \mathbb{N}$.
- Next, we are going to prove that $k \neq 1$.
  - Assume[19] that $k = 1$.
  - Then $1 = 2k = 2 \times 1 = 2 = 1 + 1$.
  - So $1 = 2$.
  - Since $1 = 0 + 1$ and $2 = 1 + 1$, we have $0 + 1 = 1 + 1$.
  - So, by the cancellation law, $0 = 1$.

[17] Notice that here, within our main proof by contradiction, we have another proof by contradiction : We want to prove that $k \neq 0$; so we assume that $k = 0$ and prove that $1 = 0$. But we know that $1 \neq 0$. So we can conclude that $1 = 0$ and $1 \neq 0$, which is a contradiction. Therefore $k \neq 0$.

[18] Another proof by contradiction ! We want to prove that $-k \notin \mathbb{N}$, so we assume that $-k \in \mathbb{N}$ and prove that $0 \in \mathbb{N}$. But we know that $0 \notin \mathbb{N}$. So we can conclude that $0 \in \mathbb{N}$ and $0 \notin \mathbb{N}$, which is a contradiction. Therefore $-k \notin \mathbb{N}$.

[19] Here we start another proof by contradiction !

  - But $0 \neq 1$.
  - So $0 = 1$ and $0 \neq 1$, which is a contradiction.

- Since the assumption that $k = 1$ had led us to a contradiction, we can conclude that $k \neq 1$.
- Then by Basic Fact BFZ10, $k - 1 \in \mathbb{N}$.
- Then $0 + 1 = 1 = 2k = 2(k - 1) + 2 = (2(k - 1) + 1) + 1$
- So $0 = 2(k - 1) + 1$
- But $2(k - 1) + 1 \in \mathbb{N}$.
- Hence $0 \in \mathbb{N}$.
- But $0 \notin \mathbb{N}$.
- Hence $0 \in \mathbb{N}$ and $0 \notin \mathbb{N}$.

We have proved a contradiction, assuming that 1 is even.
Hence $\boxed{\text{1 is not even}}$. **Q.E.D.**

5.9 How is the parity of an integer n related to that of $n + 1$?

In the previous subsection we proved that 1 is not even, so 1 is good. With this, we have successfully completed the first step of the four-step program outlined on page 69.

We now move on to the second step. We want to prove that goodness is passed on from each natural number n to its successor $n + 1$.

Recall that the parity of an integer n is the answer to the question whether n is even or odd. More precisely, if I ask you "what is the parity of n?", the answer should be "even", if n even, and "odd", if n is odd[20]. In other words, if I want to ask you "is n even or odd?" I could ask instead "what is the parity of n?"

Suppose I am given an integer n, and I know the parity of n (that is, I know, for example, that it is even). Can I tell whether its successor, $n + 1$, is even or odd? And how about the other way around? If I know the parity of $n + 1$, can I tell what the parity of n is?

[20] At this point, we do not know yet that every integer has to be even or odd, nor do we know that it cannot be both. So it is conceivable that the answer to the parity question for a particular integer n might be "it's both even and odd", or "it's neither". Soon we are going to prove that every integer has to be even or odd and cannot be both.

The answer to this is quite easy. It is given by the following *parity reversal theorem*, that says that the parity of $n+1$ is exactly the parity of n, reversed.

Theorem 24. *Let n be an integer. Then*

(1) If n is even then $n+1$ is odd.
(2) If n is odd then $n+1$ is even.
(3) If $n+1$ is even then n is odd.
(4) If $n+1$ is odd then n is even.

Proof.

Proof of statement (1):

Suppose n is even.
To prove that $n+1$ is odd, we have to show that $(n+1)-1$ is even.
But $(n+1)-1 = n$, and n is even.
Hence $\boxed{n+1 \text{ is odd}}$ by Theorem 18.

Proof of statement (2):

Suppose n is odd.
According to Definition 13, $n-1$ is even.
Also, we know that 2 is even.
So, by Theorem 17, $(n-1)+2$ is even.
But $(n-1)+2 = n+1$.
So $\boxed{n+1 \text{ is even}}$.

Proof of statement (3):

Suppose $n+1$ is even.
It is clear that -2 is even. (Reason: $-2 = 2 \times (-1)$, so $2|-2$.)
Theorem 17 then tell us that $(n+1)+(-2)$ is even.
But $(n+1)+(-2) = n-1$.
So $n-1$ is even.
Then, according to Definition 13, $\boxed{n \text{ is odd}}$.

Proof of statement (4):

Suppose $n+1$ is odd.
Then Definition 13 tells us that $(n+1)-1$ is even.

But $(n+1)-1=n$.
So $\boxed{n \text{ is even}}$.

We have thus completed the proofs of all four statements. **Q.E.D.**

It follows from Theorem 24 that the property we called "goodness" is passed on from each integer n to its successor, that is:

Theorem 25. *If an integer n is good (that is, n is even or odd and not both) then $n+1$ is good as well.*

Proof.

Let n be an arbitrary integer.

Assume n is good.

Then n is even or odd and not both even and odd.

Assume n is even.

Then n is not odd.

Since n is even Theorem 24 tells us that $n+1$ is odd.

Since n is not odd, Theorem 24 tells us that $n+1$ is not even. (Reason[21]: if $n+1$ was even, then the theorem would imply that n is odd; but n is not odd.)

So $n+1$ is odd and $n+1$ is not even.

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

Now assume that n is odd.

Then n is not even.

Since n is odd Theorem 24 tells us that $n+1$ is even.

Since n is not even, Theorem 24 tells us that $n+1$ is not odd. (Reason[22]: if $n+1$ was odd, then the theorem would imply that n is even; but n is not even.)

So $n+1$ is even and $n+1$ is not odd.

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

So we have proved that $n+1$ is good in both cases, when n is even and when n is odd.

[21] Here is another proof by contradiction !

[22] And here we have another proof by contradiction !

But one of these two cases necessarily occurs, because n is even or odd.

So $\boxed{n+1 \text{ is good.}}$ **Q.E.D.**

5.10 Why induction is needed

We now know that 1 is good.

And we also know that if an integer n is good, then $n+1$ is good.

So,

- 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".

And for this we need a new basic fact: the ***Principle of Mathematical Induction (PMI)***.

Remark 8. ***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. □

5.11 Introduction to the Principle of Mathematical Induction

Is is true that *every natural number is good?*.
We would like to prove that the answer is "yes".
How can we do that?
We already 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 we just did. But it much better not to rely on vague phrases like "and so on", and to have instead a precise 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 25. 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 26. 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[23]. Suppose you have a flier 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 flier, but you have only one copy. Then all you have to do is

(1) Give the flier to person No. 1,

and

(2) Make sure that each person passes on the flier to the person next in line after reading it[24].

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

5.12 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 9. There are other numbers (that is, people have invented other numbers), such as zero, the negative numbers -1, -2, etc., fractions such

[23]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.

[24]For example, you could include in the flier, in big letters, the statement PLEASE PASS THIS ON TO THE PERSON NEXT IN LINE TO YOU.

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 follow either that it 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 BFZ11 ABOUT THE INTEGERS)

BFZ11: 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. I will be using the symbol "$\Longrightarrow$" for "if...then". (That is, "$A \Longrightarrow B$" means "if A then b".)

THE PRINCIPLE OF MATHEMATICAL INDUCTION (BASIC FACT BFZ11 ABOUT THE INTEGERS), FORMAL LANGUAGE VERSION

BFZ11: Suppose $P(n)$ is any statement about a variable natural number n. Then

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

Remark 10. If you want to get a better understanding of what we are doing, you may have noticed that

1. Basic Facts BFZ1 to BFZ5 (that is, Part I of the list of basic facts) are facts about the integers. (The natural numbers are never even mentioned there.)

2. Basic Facts BFZ6 to BFZ10 (that is, Part II of the list of basic facts) are facts about how the integers and the natural numbers are related.

3. Basic fact BFZ11 (the PMI) is about the natural numbers only. □

5.13 Our first proof by induction: every natural number is even or odd and not both

We are now ready, finally, to prove the theorem that we had announced before, that every integer is even or odd and not both.

First we prove the result for natural numbers:

Lemma 2. *Every natural number is even or odd and no natural number is both.*

Proof. We are going to prove this result by induction.
Let $P(n)$ be the statement:

$$n \text{ is even or odd and not both}\,. \tag{5.55}$$

Then we want to prove that

$$(\forall n \in \mathbb{N})P(n)\,. \tag{5.56}$$

For this purpose, we must prove that:

(I) $P(1)$ is true.

(II) Any time the statement $P(n)$ is true for one particular n, it follows that $P(n+1)$ is true. (That is: $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.)

Proof of (I):

We want to prove that $P(1)$ is true. That is, we want to prove that 1 is even or odd and 1 is not both even and odd.

Theorem 23 tells us 1 is not even.

And we know that 1 is odd.

So 1 is odd and not even.

So 1 is even or odd and not both. That is, $\boxed{P(1)}$ is true.

Proof of (II).

We want to prove that $(\forall n \in \mathbb{N})(\text{if } P(n) \text{ then } P(n+1))$.

Let n be an arbitrary natural number.

Assume $P(n)$. (That is, assume that $P(n)$ is true.)

Then n is even or odd and not both.

So n is even or n is odd.

We consider first the case when n is even.

Assume that n is even.

Then Theorem 24 tell us that $n+1$ is odd.

In addition, n is not odd.

So Theorem 24 also implies that $n+1$ is not even. (Reason[25]: if $n+1$ was even then the theorem would imply that n is odd. But n is not odd. So n is odd and n is not odd, which is a contradiction.)

So $n+1$ is odd and not even.

[25]Notice that we have a proof by contradiction here.

Hence $\boxed{P(n+1) \text{ is true.}}$

Next we consider the case when n is odd.

Assume that n is odd.

Then Theorem 24 tell us that $n+1$ is even.

In addition, n is not even.

So Theorem 24 also implies that $n+1$ is not odd. (Reason[26]: if $n+1$ was odd then the theorem would imply that n is even. But n is not even. So n is even and n is not even, which is a contradiction.)

So $n+1$ is even and not odd.

Hence $\boxed{P(n+1) \text{ is true.}}$

We have proved that $P(n+1)$ is true in both the case when n is even and the case when n is odd.

And we know that one of these two cases necessarily occurs.

So $\boxed{\boxed{P(n+1) \text{ is true.}}}$

We have proved $P(n+1)$ assuming $P(n)$. This proves that

$$\text{if } P(n) \text{ is true then } P(n+1) \text{ is true.}$$

We have proved that if $P(n)$ is true then $P(n+1)$ is true for an arbitrary natural number n.

So $\boxed{(\forall n \in \mathbb{N})\Big(\text{if } P(n) \text{ then } P(n+1)\Big).}$

This completes the proof of Part (II).

So we have proved (I) and (II). By the PMI, our desired conclusion (5.56) follows. **Q.E.D.**

Next, we prove a small lemma:

Lemma 3. *Let n be an integer such that n is even or odd and not both. Then $-n$ is even or odd and not both.*

Proof. **YOU DO THIS ONE.**

[26] Another proof by contradiction !

Problem 14. ***Prove*** *Lemma 3.* □

And now, finally, we can prove the result for all integers.

Theorem 26. *Every integer is even or odd and no integer is both even and odd.*

Proof. We want to prove the universal sentence "every integer is even or odd and not both."

Let n be an arbitrary integer.
Then by Basic Fact BFZ9, either $n \in \mathbb{N}$ or $n = 0$ or $-n \in \mathbb{N}$.
So we have to consider three cases: $n \in \mathbb{N}$, $n = 0$, and $-n \in \mathbb{N}$.
First, we study the case when $n \in \mathbb{N}$.

Assume that $n \in \mathbb{N}$.

Then Lemma 2 tells us that $\boxed{n \text{ is even or odd and not both.}}$

Next, we look at the case when $n = 0$.

Assume that $n = 0$.

Then n is even. (Reason: $0 = 2 \times 0$. So $2|0$.)

Furthermore, n is not odd. (Reason: if 0 was odd then Theorem 24 would imply that 1 is even. But we know that 1 is not even.

So n is even and not odd.

Therefore $\boxed{n \text{ is even or odd and not both.}}$

Finally, we look at the case when $-n \in \mathbb{N}$.

Assume that $-n \in \mathbb{N}$.

Then by Lemma 2, $-n$ is even or odd and not both.

Therefore, by Lemma 3, $-(-n)$ is even or odd and not both.

But $-(-n) = n$.

So $\boxed{n \text{ is even or odd and not both.}}$

So we have proved that n is even or odd and not both in all three cases, $n \in \mathbb{N}$, $n = 0$, and $-n \in \mathbb{N}$.

Since one of these cases must necessarily occur, we can conclude that $\boxed{n \text{ is even or odd and not both.}}$

Since we have proved that n is even or odd and not both for an arbitrary integer n, it follows from the rule for proving universal statements that $\boxed{\text{every integer is even or odd and not both.}}$ **Q.E.D.**