MATHEMATICS 300 — SPRING 2004

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

(Updated April 9, 2004)

Contents

1 Information on the course

1.1 Course schedule

Our class meets on **Tuesdays and Thursdays, 5th period (2:50pm to 4:10pm)**, in Beck Hall 011.

1.2 About the instructor

My *name* is **H.J. Sussmann.** My *office* is **Hill 538**.

My *Rutgers phone extension* is 5-5407.
My *e-mail address* is **sussmann@math.rutgers.edu**.

1.3 Web page

I have set up a *Web page* for our Math 300 section:

http://www.math.rutgers.edu/˜sussmann/math300page.html

All the instructor's notes will be available there.

1.4 Office hours

My office hours will be:

- **Tuesday and Thursday, 4th period** (1:10 pm to 2:30 pm) in my office, **Hill 538**;
- any other time, by appointment, in my office, Hill 538.

1.5 Homework, midterms, final exam.

Homework and quizzes will count for about one third of your grade. There will be *two midterms*, which will count—together—for another third of your grade. The *final exam* will count for the remaining third.

Midterm dates: Thursday, March 4 and **Tuesday, April 20**.

Final exam date: Friday, May 7 12:00-3:00 pm.

1.6 The textbook and the instructor's notes

We will be using:

- the book *Chapter Zero, Fundamental Notions of Abstract Mathematics*, by **Carol Schumacher**,
- the notes written by the instructor.

You should read and study carefully all the instructor's notes.
The material of these notes is an integral part of the course, as much as that of the book. *Furthermore, the notes contain all kinds of important information. For example, in this set of notes there are lots of things you need to know in order to do your homework.*

1.7 Readings for the first 7 days (January 20, 22, 27, 29, and February 3, 5)

- the book's Chapter 0, "Introduction, an Essay,"
- the book's Chapter 1 (**all of it!**),
- the instructor's notes, Part 1 (omitting §4.4, on quaternions).

2 Homework

2.1 Homework assignments for the first four weeks of classes (i.e., until February 12)

Before you start writing your homework, read carefully the rest of this handout, in particular §3 on "writing mathematics and submitting homework," and §6 on mathematical writing. Pay attention to §3.3, on "answering questions in this course."

2.1.1 Homework assignment no. 1, due on Thursday January 29.

Items 8, 11, 16, 21 of the "thought experiment list". NOTE: *the list consists of the 16 items in Section 1.1 of the book (page 8) plus the following seven items added in class:*

17. $\exists x, \exists y, x^2 - y^2 = 28$.

18. $\exists x, \exists y, x^2 - y^2 = 29$.

19. $\exists x, \exists y, x^2 - y^2 = 30$.

20. Every prime number gretaer than 2 is odd.

21. $\exists x, (x > 3$ and x is prime and $x + 2$ is prime and $x + 4$ is prime$)$.

22. Every year must have a Friday the 13th.

23. The statement of 22 remains true even if we change the order of the months (without changing the number of days of each month.

NOTE: *In Items 17, 18, 19, 21, the range of the variables x, y, is $\mathbb{Z}$, the set of all integers.*

2.1.2 Homework assignment no. 2, due on Thursday February 5.

A. Exercises 1.6.4, 1.7.1, 1.7.3, 1.7.7, 1.7.8, 1.8.3, 1.8.5, 1.8.9, 1.8.10, 1.8.11, in pages 20, 21, 22, 23, 24, 25, 26, 27 of the book.

B. Items 9 and 10 of the "thought experiment list."

C. The definitions of "even" and "odd" are as follows:

DEFINITION OF "EVEN": Let n be an integer. We say that n is *even* if there exists an integer k such that $n = 2k$.

DEFINITION OF "ODD": Let n be an integer. We say that n is *odd* if there exists an integer k such that $n = 2k + 1$.

(Using more symbols and fewer words, we could also say

$$\forall n \in \mathbb{Z}, (n \text{ is } \mathbf{even} \iff \exists k \in \mathbb{Z}, n = 2k),$$

$$\forall n \in \mathbb{Z}, (n \text{ is } \mathbf{odd} \iff \exists k \in \mathbb{Z}, n = 2k + 1). \;)$$

C.1. Rewrite the definitions of "even integer" and "odd integer" using only words, with no letter symbols whatsoever.

C.2. Write a definition of "even integer" without mentioning the concept of divisibility or the number 2.

D The definitions of "even" and "odd" also make sense in other number systems such as $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, etc. It suffices to replace the word "integer" throughout by "member of $\mathbb{Z}_2$" (or of $\mathbb{Z}_3$, or of $\mathbb{Z}_4$, etc.), or, equivalently, by "integer modulo 2" (or "integer modulo 3," or "integer modulo 4," etc.), and to carry out all the operations such as addition in $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, etc.

For example, 32 is a member of $\mathbb{Z}_{37}$, and 32 is odd in $\mathbb{Z}_{37}$. (*Proof*: in $\mathbb{Z}_{37}$ we have $2 \times 34 + 1 = 68 + 1 = 69 = 32$, so there exists an integer k modulo 37 (namely, $k = 34$), such that $32 = 2 \times k + 1$ in $\mathbb{Z}_{37}$, and this says that 32 is odd in $\mathbb{Z}_{37}$.) In addition, 32 is also even in $\mathbb{Z}_{37}$, because $32 = 2 \times 16$ in $\mathbb{Z}_{37}$. So the statement that "a number cannot be both even and odd" need not be true in every nymber system. It is true in $\mathbb{Z}$, but not in $\mathbb{Z}_{37}$.

For what values of the positive integer m is it true that "in $\mathbb{Z}_m$, a number cannot be both even and odd"?

2.1.3 Homework assignment no. 3, due on Thursday February 12.

A. The definition of "divisible" is as follows:

- Let n, m be integers. We say that n is *divisble* by m if there exists an integer k such that $n = k.m$.

1. Write the above definition in a more formal way, similarly to what we did in page 4 with the definitions of "even" and "odd."
2. Write the above definition in plain English, using only words, with no letter symbols or any other mathematical symbols.
3. Prove: if n, m, k are integers, n is divisible by k, and m is divisible by k, then $n + m$ is divisible by k.
4. Prove: if n, m, k are integers, n is divisible by k, and n is divisible by m, then n is divisible by $m + k$.

B. For integers, write definitions of "less than" and "less than or equal to" in which you only use the predicates "is a natural number" and "=", the operation "+" , and the quantifiers. (Do not use vague words. For example, last year some students wrote things such as "$x < y$ if x is to the left of y." "To the left of" is vague, and in any case it is not allowed here, so you cannot use it.)

C. Your even 4-digit pin number k is determined as follows: write your last name, count the number of letters, let a be the result, let b (11 to 41) be the day of your birth plus 10, let c (21 to 32) be the month of your birth plus 20, let $d = a \times b \times c$, let $e = d + 5,312$. If e has more than 4 digits, keep only the first four, and call the result f (for example, if $e = 13,043$ then $f = 1,304$). If f is even, then $k = f$. If f is odd, then $k = f + 1$.

   Express your number k as the sum of two primes. *Justify your answer.* In particular, make sure that you prove that the two numbers you found are prime. For example, if you want to answer that 2026=2013+13 (which would be wrong because 2013 is not prime) do not leave it like that. You have to prove that the two numbers you found are prime.

D. Exercises 2.2.3, 2.2.4, 2.3.2, 2.3.3, 2.3.8, in pages 42-43-44 of the book.

2.1.4 Supplementary problems for the first four weeks of classes (January 20 to February 12), due on February 17.

Here are some supplementary problems. Don't worry if some of these problems seem too hard. They are meant to be challenging. Just do as much as you can. Hand in the solutions **not later than February 17**.

One of the main purposes of this set of questions is to get you to experience what it is like to think about problems that could be quite hard (even if they seem easy!), so that you will appreciate what it means to find a **truly good solution**. For you to see this, you have to think about the problems first, and if you cannot solve them **after you have tried to** and then you see the solution, you will understand much better what a **real proof** is.

A. Prove that every year must have a Friday the 13th. (This is Item 22 of the "thought experiment" list.)

B. (This is Item 23 of the "thought experiment" list.) In the planet of the Klingons, they have a calendar exactly like the one we use here on Earth (there are 12 months, January has 31 days, February has 28 or

29, March has 31, April has 30, etc.), except for one thing: the order of the months is different. We do not know what it is, but we know for sure that it is different from ours. (For example, it may be that June is the first month, September is the second one, etc.) Is it still necessarily true that every year must have a Friday the 13th? *Prove that it is true*, no matter what the order of the months is, *or prove that it need not be true* (that is, that there is a way to reorder the months so that not every year has a Friday the 13th).

C. (*Optional. This could be quite hard! Do not worry if you cannot do it, but at least try to* **think** *about it.*) Express the number $4,582,623$ as the sum of the squares of two natural numbers.

D. (*Optional. Hard.*) Suppose two integers a and b are sums of two squares of integers. Prove that the product ab must also be the sum of two squares of integers. (NOTE: here is an example of the kind of situation we are talking about. The number 13 is the sum of two squares, because $13 = 4+9$. The number 8 is the sum of two squares, because $8 = 4+4$. So, if our statement is true, it ought to be the case that the number 13×8 is the sum of two squares. And, indeed, it *is* true, because $13 \times 8 = 104$ and $104 = 100 + 4 = 10^2 + 2^2$.)

E. (*Optional. Hard.*) Suppose two integers a and b are sums of three squares of integers. Prove that the product ab must also be the sum of three squares of integers.

F. Here are five sentences about giraffes, cows, sheep, Olivia, Dolly, and the binary relation "taller than."

(1) Cows are taller than sheep. (That is, "every cow is taller than every sheep," or, if you prefer, "for every x and every y, if x is a cow and y is a sheep, then x is taller than y.")

(2) Giraffes are taller than cows.

(3) If something is taller than something else which is in turn taller than a third thing, then the first one is taller than the third one. (That is "for every x, every y and every z, if x is taller than y and y is taller than z, then x is taller than z.")

(4) Olivia is a giraffe.

(5) Dolly is a sheep.

Using sentences (1), (2), (3), (4), (5), *and* **no other fact** *about giraffes, cows, sheep, Olivia, Dolly, and the binary relation "taller than,"* prove that Olivia is taller than Dolly.

3 Writing mathematics & submitting homework

3.1 Write clearly in complete sentences

You should write so that you can be easily understood by a properly trained English-speaking individual. In particular, this means that you must

- Use *complete English sentences*, that make clearly identifiable *statements* with a *clear meaning* that can can be understood by anyone reading what you wrote. For example:
  - If you tell me that "she is very smart," but you haven't told me who "she" is, then I don't know what you are talking about, so you haven't made a statement with a clear meaning.
  - If you write "$x > 0$," but you haven't told me who "x" is, then I don't know what you are talking about, so you haven't made a statement.
  - If I ask you to state Pythagoras' theorem and your answer only says "$a^2 + b^2 = c^2$," then nobody will know what you are talking about, because you have not said what "a," "b," and "c" are supposed to be.[1]
- Avoid exaggerated or incorrect use of cryptic mathematical notation.
- Explain what you are doing.

[1] Here is a correct statement of Pyhtagoras' theorem: *Let c be the lenght of the hypothenuse of a right triangle, and let a, b be the lengths of the other two sides. Then $a^2 + b^2 = c^2$.*

- Make sure that letter "variables" are only used if either: (i) it has been said before what these letters stand for, or (ii) they are "closed variables" (or "dummy variables," or "bound variables") in the sense that will be discussed in detail in class, and is also explained in §6.

- Provide proper connectives between equations as well as between ideas.

- Make sure that all the rules of English grammar (including those of spelling and punctuation) are strictly obeyed.

- Try to say things correctly, following all the rules, but *in your own words.* Please *no rote learning.* If you have to memorize a definition or a statement, then that is not a good sign, because it indicates lack of understanding.

- Please proofread carefully what you hand in. Ideally, you should read and reread and revise almost any formal communication. **Neatness and clarity count**, as you well know if you've tried to read any complicated document.

- *Do not assume that the people reading your paper can read your mind. Do assume that they are intelligent, but also assume that they are busy, and cannot and will not spend an excessive amount of time puzzling out your meaning. Communication is difficult, and written technical communication is close to an art.*

Effective written exposition will be worth at least 50% of your grade. Conversely, bad or unclear exposition may be penalized as much as 50% of the grade or even more.

- The best reference known to me on effective writing is *The Elements of Style* by Strunk and White, a very thin paperback published by Macmillan. It isn't expensive, and it is easy to read. I recommend it.

3.2 Your written work

You should pay attention to presentation, especially for the homework:

- A nicely typed homework (e.g., using a word processor) is preferable to handwritten work. Handwritten work is acceptable too, but in that case:
  - If you have to cross out lots of words, then you should rewrite the whole thing anew, **cleanly and neatly**. If you are not willing to spend some of your time doing this; if what you hand in shows that you were in a hurry and that you did not make the effort to write things neatly and properly, then there is no reason for the instructor or the grader to spend any of our time reading what you wrote, and we will not do it.
  - You should use a pen. Never use a pencil.
  - Use any color other than red (for example, black, blue, or green), but DO NOT USE RED. (Reason: The use of red is reserved for the instructor's and grader's comments.)
- Make sure that **your name appears in every sheet of paper you hand in**, and that if you are handing in more than one sheet then the sheets are **stapled** and the pages are **numbered**.
- If you tear off the sheets from a spiral notebook, please make sure before you hand them in that there are none of those ugly hanging shreds of paper at the margins. Use scissors, or a cutter, if necessary.

If you hand in a homework assignment that has at least one of the following flaws:

- **it is written carelessly or in a hurry,**
- **it has lots of words crossed out,**
- **it has unreadable handwriting,**
- **it has pages that are unstapled or unnumbered or fail to show your name,**
- **it has shreds of paper at the margins,**
- **it is written using pencil rather than a pen,**
- **it is written in red,**

then the assignment will be marked "unacceptable" and returned unread.

3.3 Answering questions in this course

In this course, whenever you are given a problem where you are asked to do something, your answer should be either:

(a) doing what you were asked to do,

or

(b) showing—that is *proving*—that it cannot be done.

(See, for example, Problems 2, 3, 4, 5, 8, 10, 12 below, where the correct answer is "what you asked me to do cannot be done.")

Notice that, when the answer is that "it cannot be done," it is not enough for you to *say* that it cannot be done. *You have to tell me why.* In other words, you have to *prove* that it cannot be done.

This remark is very important, and will apply throughout the semester, not just during the first week. And it applies to all your work, to the homework, the quizzes, the midterm exams, and the final exam. So please read it and reread it until you are sure you got the point. ♢

3.4 Some examples of problems with correct answers

Here are some examples of problems with correct solutions:

PROBLEM 1: Express the number 26 as a sum of two odd natural numbers.

ANSWER: $26 = 3 + 23$. ♢

REMARK: *There are lots of other solutions, of course! For example, here are two solutions different from the one given above:* $26 = 7 + 19$, $26 = 13 + 13$.

PROBLEM 2: How many solutions does Problem 1 have?

ANSWER: This question cannot be answered in a unique way, because we have not told you exactly what is meant by a "solution of Problem 1," and, depending on how you define what is meant by a "solution," the answers to our question may be different.

Here are two equally legitimate ways to define "solution of Problem 1":

First way: A *solution of Problem 1* is an ordered pair (n, m) of odd natural numbers such that $n + m = 26$. (What this means is that a solution consists of specifying a first odd natural number n and a second odd natural number m such that $n + m = 26$. So "$n = 3$ and $m = 23$" is a solution, and "$n = 23$ and $m = 3$" is a *different* solution.)

According to this definition of "solution of Problem 1," there are exactly **13 solutions**, namely, the ordered pairs $(1, 25)$, $(3, 23)$, $(5, 21)$, $(7, 19)$, $(9, 17)$, $(11, 15)$, $(13, 13)$, $(15, 11)$, $(17, 9)$, $(19, 7)$, $(21, 5)$, $(23, 3)$, $(25, 1)$.

Second way: A *solution of Problem 1* is an unordered pair $\{n, m\}$ of odd natural numbers such that $n + m = 26$.

According to this definition of "solution of Problem 1," there are exactly **7 solutions**, namely, the unordered pairs $\{1, 25\}$, $\{3, 23\}$, $\{5, 21\}$, $\{7, 19\}$, $\{9, 17\}$, $\{11, 15\}$, $\{13, 13\}$). (What this means is that a solution consists of specifying two odd natural numbers whose sum is 26, without singling out one of them as the "first" one. So in this case "$n = 3$ and $m = 23$" is a solution, and "$n = 23$ and $m = 3$" is *the same* solution.) ♢

PROBLEM 3: Express the number 27 as the sum of two odd natural numbers.

SOLUTION: This is impossible. REASON: the sum of two odd numbers is always even. Since 27 is odd, it cannot be the sum of two odd numbers. $\diamondsuit$

PROBLEM 4: Prove that $2 + 2 = 5$.

SOLUTION: This cannot be done. REASON: The statement "$2 + 2 = 5$" is false, and false statements cannot be proved.

PROBLEM 5: Prove that for every positive integer x there is another positive integer y such that $0 < y < x$.

SOLUTION: This cannot be done. REASON: The statement that we are being asked to prove is false, and a false statement cannot be proved.

The reason that the statement is false is as follows: 1 is a positive integer, and there is no positive integer y such that $0 < y < 1$, because 1 is the smallest positive integer. So if we take x to be 1 then the conclusion is not true. So it is not true that "for *every* positive integer x there is another positive integer y such that $0 < y < x$." $\diamondsuit$

PROBLEM 6: Express the number 12 as the difference of the squares of two natural numbers.

SOLUTION: $12 = 16 - 4$, so $12 = 4^2 - 2^2$. $\diamondsuit$

PROBLEM 7: Express the number 20 as the sum of the squares of two natural numbers.

SOLUTION: $20 = 4 + 16 = 2^2 + 4^2$. $\diamondsuit$

PROBLEM 8: Express the number 4 as the sum of the squares of two positive integers.

SOLUTION: This cannot be done. REASON: here are all the ways to express 4 as a sum of two positive integers:

$$4 = 1 + 3\,, \qquad 4 = 2 + 2\,.$$

In neither of these two equalities are the two terms on the right-hand side squares.

PROBLEM 9: Express the number 4 as the sum of the squares of two integers.

SOLUTION: $4 = 0 + 4 = 0^2 + 2^2$. $\diamondsuit$

PROBLEM 10: Express the number 12 as the sum of the squares of two integers.

SOLUTION: This cannot be done. REASON: here are all the ways to express 12 as a sum of two nonnegative integers:

$$12 = 0+12,\ 12 = 1+11,\ 12 = 2+10,\ 12 = 3+9,\ 12 = 4+8,\ 12 = 5+7,\ 12 = 6+6.$$

In none of these expressions are the two terms on the right-hand side squares of natural numbers. $\diamondsuit$

PROBLEM 11: Express the number 12 as the sum of the squares of three natural numbers.

SOLUTION: $12 = 4 + 4 + 4$, so $12 = 2^2 + 2^2 + 2^2$. $\diamondsuit$

PROBLEM 12: Express the number 15 as the sum of the squares of three integers.

SOLUTION: This cannot be done. REASON: If we are going to write 15 as the sum of three squares, then we should be able to write it as the sum of two nonnegative integers, one of which is a square, while the other is the sum of two squares.

So let us look at all the ways to write 15 as a sum of two nonnegative integers, see in which cases one of these numbers is square, and then see if the other number is the sum of two squares.

Here are all the ways to express 15 as a sum of two nonnegative integers:

$$\begin{array}{llll} 15 = 0 + 15, & 15 = 1 + 14, & 15 = 2 + 13, & 15 = 3 + 12, \\ 15 = 4 + 11, & 15 = 5 + 10, & 15 = 6 + 9, & 15 = 7 + 8\,. \end{array}$$

There are four expressions in the above list where one of the numbers is a square:

$$15 = 0 + 15, \quad 15 = 1 + 14, \quad 15 = 4 + 11, \quad 15 = 6 + 9\,.$$

In each case, we must ask whether the other number is a sum of two squares.

For "15=0+15," we have to see if 15 is the sum of two squares. The answer is "no," because we already have the list of all (eight) ways of writing 15 as a sum of two nonnegative integers, and in no case are both those numbers suqares.

For "15=1+14," we have to see if 14 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 14 are 0, 1, 4, and 9. So if are going to write 14 as a sum of two squares, the only possibilities are $14 = 0 + 14$, $14 = 1 + 13$, $14 = 4 + 10$, $14 = 9 + 6$. But in all these cases the other number—that is, 14, 13, 10, or 6—is not a square.)

For "15=4+11," we have to see if 11 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 11 are 0, 1, 4, and 9. So if are going to write 11 as a sum of two squares, the only possibilities are $11 = 0 + 11$, $11 = 1 + 10$, $11 = 4 + 7$, $14 = 9 + 5$. But in all these cases the other number (that is, 11, 10, 7, or 5) is not a square.)

Finally, for "15=6+9," we have to see if 6 is the sum of two squares. The answer is "no." (Reason: the only squares not greater than 6 are 0, 1, and 4. So if are going to write 6 as a sum of two squares, the only possibilities are $6 = 0 + 6$, $6 = 1 + 5$, $6 = 4 + 2$. But in all these cases the other number (that is, 6, 5, or 2) is not a square.) $\diamondsuit$

PROBLEM 13: Express the number 15 as the sum of the squares of four natural numbers.

SOLUTION: $15 = 1 + 1 + 4 + 9 = 1^2 + 1^2 + 2^2 + 3^2$. $\diamondsuit$

PROBLEM 14: Express the number 674 as the sum of the squares of four natural numbers.

SOLUTION: $674 = 144 + 400 + 121 + 9 = 12^2 + 20^2 + 11^2 + 3^2$. $\diamondsuit$

REMARK: You may be thinking *how on Earth did the author of these notes figure out how to solve problem 14?* That's a good question. It turns out that there is a technique for doing this, but it's not easy to explain. Maybe we will talk about it later in the course. But keep in mind that the question "how did I find a solution to problem 14?" is quite different from the question "is $674 = 12^2 + 20^2 + 11^2 + 3^2$ a correct solution?" This second question is easy to answer: you just compute $12^2 + 20^2 + 11^2 + 3^2$ and verify that what you get is 674. $\diamondsuit$

REMARK: You may have noticed that I gave you examples of natural numbers that could be expressed as the sum of two squares, and of natural numbers that could not. Then I gave you examples of natural numbers that could be expressed as the sum of three squares, and of natural numbers that could not. But for *four* squares what I have done is different: I gave you examples of natural numbers that could be expressed as the sum of four squares, but I did not give you examples of natural numbers that could not. Is there a reason for this? The answer is **yes**. The mathematician Lagrange (1736-1813) proved that **every natural number can be expressed as the sum of the squares of four natural numbers.** This is a hard theorem, and I will try to say a few words about it later in the course. $\diamondsuit$

4 A first look at the world of mathematical objects: number systems

"The time has come," the Walrus said,
"To talk of many things:
Of shoes—and ships—and sealing wax—
Of cabbages–and kings
And why the sea is boiling hot—
And whether pigs have wings."

BOX NO. 1: SUMMARY OF CHAPTER 4.

There are many different types of mathematical objects. Among them, there are **numbers** of various kinds, and also lots of other things that are not numbers.
Numbers belong to **number systems**. The most important number systems are:

- $\mathbb{N}$, the set of *natural numbers*,
- $\mathbb{Z}$, the set of *integers*,
- $\mathbb{Q}$, the set of *rational numbers*,
- $\mathbb{R}$, the set of *real numbers*,
- $\mathbb{C}$, the set of *complex numbers*,
- $\mathbb{K}$, the set of *quaternions*,
- $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, and, more generally, $\mathbb{Z}_n$—the set of *integers modulo* n—for every natural number n such that $n \geq 2$.

In addition to numbers, there are all kinds of other mathematical objects, such as *sets*, *lists*, *operations*, *functions*, *relations*, *arrays* of various kinds and, in particular, *matrices*, *linear spaces* (such as $\mathbb{R}^2$, $\mathbb{R}^3$, $\mathbb{R}^4$, etc.), *geometrical figures* such as *curves* of different kinds (for example, lines, parabolas, ellipses, hyperbolas, cycloids, exponential curves), *surfaces* (such as planes, spheres, cylinders, cones, ellipsoids, paraboloids, hyperboloids), and other figures (e.g., triangles, squares, rectangles, discs, balls), and many, many more things.
We will talk about those other things later. For the moment, we just concentrate on **number systems**.

Our first task is to take a look at the rich and varied collection of things that populate the mathematical world. Some of them should be familiar to you, others may be less so or not at all. Do not worry if you find in our list things that you have never heard of before: we will be coming back to the list later, and discussing all the items in much greater detail.

Mathematicians like to give names to things so that they can talk about complicated objects without repeating their long descriptions every time.

So let us start by agreeing to use ***WMO*** as our name for the world of mathematical objects.

4.1 Numbers: $\mathbb{Z}_+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

The best known inhabitants of ***WMO*** are **numbers** and **number systems**. There are several different kinds of numbers, and they can be organized into *number systems*. A number can belong to different number systems, in the same way as, say, a person can belong to different associations. (For example, somebody could be a member, say, of the American Association of University Professors, the Rutgers Alumni Association, and the Sierra Club. Similarly, the number 3 belongs to lots of different number systems, such as, for example, $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, ..., $\mathbb{Z}_{397}$, ...)

It is convenient to give the number systems **names**, and to introduce mathematical symbols to represent them. Here are some examples:

1. The set $\mathbb{N}$ of **natural numbers**. (Natural numbers are also called **positive integers**, or—sometimes—**whole numbers**.) The members of this set are the integers $1, 2, 3 \ldots$. So, for example,

   1 is a member of $\mathbb{N}$ (or "1 belongs to $\mathbb{N}$"),

   2 is a member of $\mathbb{N}$ (or "2 belongs to $\mathbb{N}$"),

   ......

   385 is a member of $\mathbb{N}$ (or "385 belongs to $\mathbb{N}$"),

   ......

   $10,891,032$ is a member of $\mathbb{N}$ (or "$10,891,032$ belongs to $\mathbb{N}$"),

   ......

   0 is not a member of $\mathbb{N}$ (or "0 does not belong to $\mathbb{N}$"),

   -1 is not a member of $\mathbb{N}$ (or "-1 does not belong to $\mathbb{N}$"),

   3.5 is not a member of $\mathbb{N}$ (or "3.5 does not belong to $\mathbb{N}$"),

   and so on.

2. The set $\mathbb{Z}$ of all **integers**. The members of $\mathbb{Z}$ are the natural numbers as well as 0 and the negatives of natural numbers, i.e., the numbers -1, -2, -3, etc.

3. The set $\mathbb{Z}_+$ of all **nonnegative integers**. The members of this set are exactly the same as the members of $\mathbb{N}$, except only for the fact that 0, which is not a member of $\mathbb{N}$, counts as a member of $\mathbb{Z}_+$.

BOX NO. 2: THE SYMBOL "$\in$" ("BELONGS TO").

We use the symbol $\in$ (read "belongs to," or "is a member of," or "belonging to," or "in") to indicate *membership in a set*:

If A is a set and x is an object, then "$x \in A$" means "x belongs to A," or "x is a member of A."

The symbol $\notin$ (read "does not belong to," or "is not a member of," or "not belonging to," or "not in") indicates non-membership:

If A is a set and x is an object, then "$x \notin A$" means "x does not belong to A," or "x is not a member of A."

For example the following statements are true:

$$
\begin{array}{rrrr}
1 \in \mathbb{N}\,, & 2 \in \mathbb{N}\,, & 385 \in \mathbb{N}\,, & 10,891,032 \in \mathbb{N}\,, \\
0 \notin \mathbb{N}\,, & -1 \notin \mathbb{N}\,, & 3.5 \notin \mathbb{N}\,, & \pi \notin \mathbb{N}\,, \\
\frac{8}{5} \notin \mathbb{N}\,, & \frac{10}{5} \in \mathbb{N}\,, & \frac{382,403,313}{9} \in \mathbb{N}\,, & \pi + 7 \notin \mathbb{N}\,, \\
3+7 \in \mathbb{N}\,, & 8-1 \in \mathbb{N}\,, & 1-8 \notin \mathbb{N}\,, & \pi - (2-\pi) \notin \mathbb{N}\,, \\
1 \in \mathbb{Z}\,, & 2 \in \mathbb{Z}\,, & 385 \in \mathbb{Z}\,, & 10,891,032 \in \mathbb{Z}\,, \\
0 \in \mathbb{Z}\,, & -1 \in \mathbb{Z}\,, & 3.5 \notin \mathbb{Z}\,, & \pi \notin \mathbb{Z}\,, \\
\frac{8}{5} \notin \mathbb{Z}\,, & \frac{10}{5} \in \mathbb{Z}\,, & \frac{382,403,313}{9} \in \mathbb{Z}\,, & \pi + 7 \notin \mathbb{Z}\,, \\
3+7 \in \mathbb{Z}\,, & 8-1 \in \mathbb{Z}\,, & 1-8 \in \mathbb{Z}\,, & \pi^2 - (2-\pi)^2 - 4\pi \in \mathbb{Z}\,, \\
0 \in \mathbb{Z}_+\,, & 1 \in \mathbb{Z}_+\,, & 4 \in \mathbb{Z}_+\,, & -3 \notin \mathbb{Z}_+\,.
\end{array}
$$

4. The set $\mathbb{R}$ of all **real numbers**. Every natural number is a member of $\mathbb{R}$. Every integer is a member of $\mathbb{R}$. In addition, there are many other real numbers besides the integers.

   For example the following statements are true:

$$\begin{array}{rrrr}
1 \in \mathbb{R}\,, & 2 \in \mathbb{R}\,, & 385 \in \mathbb{R}\,, & 10,891,032 \in \mathbb{R}\,, \\
0 \in \mathbb{R}\,, & -1 \in \mathbb{R}\,, & 3.5 \in \mathbb{R}\,, & \pi \in \mathbb{R}\,, \\
\frac{8}{5} \in \mathbb{R}\,, & \frac{10}{5} \in \mathbb{R}\,, & \frac{382,403,313}{9} \in \mathbb{R}\,, & \pi + 7 \in \mathbb{R}\,, \\
3 + 7 \in \mathbb{R}\,, & 8 - 1 \in \mathbb{R}\,, & 1 - 8 \in \mathbb{R}\,, & \pi - (2 - \pi) \in \mathbb{R}\,.
\end{array}$$

A real number (and, in particular, an integer) is "positive" if it is > 0. A number is "nonnegative" if it is ≥ 0.

In particular, 0 **is not positive**, but 0 **is nonnegative.** 0 **is a nonnegative integer, but** 0 **is not a positive integer.**

5. The set $\mathbb{Q}$ of all **rational numbers**. (Rational numbers are often called "fractions"). By definition, a *rational number* is a real number that can be expressed as the quotient (or "ratio[2]) of two integers. So, for example, $\frac{8}{3} \in \mathbb{Q}$, $6 \in \mathbb{Q}$, $\frac{9}{3} \in \mathbb{Q}$, $-6 \in \mathbb{Q}$, $-\frac{9}{3} \in \mathbb{Q}$.

Remark 1. Do not confuse the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ with the letters N, Z, R. They are different! (This is very convenient. If we agreed to use N as the name for the set of natural numbers, then the meaning of the letter N would be fixed for ever, and we would not be able to use N for other things.) $\diamondsuit$

Another way of saying that "$\mathbb{N}$ is the set consisting of 1, 2, 3, 4, and so on," is to write

$$\mathbb{N} = \{\, 1, 2, 3, 4, \ldots \,\}\,. \tag{4.1.1}$$

Similarly,

$$\mathbb{Z} = \{\, 0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots \,\}\,.$$

4.2 The complex numbers

For a long time, people used the word "number" to mean "real number." But then the "complex numbers" were invented, and mathematicians decided, after long discussions on whether this was a good thing to do, that these "complex numbers" were objects worth admitting as *bona fide* numbers as well. So we can add a sixth example to our list of number systems:

[2] "Ratio" is an old word for "quotient."

6. The set $\mathbb{C}$ of all *complex numbers*. Here are some examples of these "numbers":

$$3\,,\qquad i\,,\qquad 3+i\,,\qquad 4-i\,,\qquad 35-67i\,,\qquad \frac{8}{5}\,,\qquad \frac{8}{5}-\pi i\,.$$

Complex numbers can be **added** and **multiplied**. To add two complex numbers, you just add separately the "i-parts" and the "non-i-parts." So, for example,

$$3+i+(4-2i)=7-i\,,\ \ 3+(8+5i)=11+5i\,,\ \ \frac{8}{5}+i+\Big(\frac{12}{5}+83i\Big)=4+84i\,.$$

To multiply two complex numbers, you just multiply as you would real numbers, except that every time you run into $i.i$ you put -1 instead. For example:

$$\begin{aligned}(23+7i).(4+2i) &= 23.4+7.4.i+23.2.i+7.2.i.i\\ &= 92+28i+46i+14.i.i\\ &= 92-14+28i+46i\\ &= 78+72i\,.\end{aligned}$$

Remark 2. The invention, or discovery, of the complex numbers was a long process, driven by the effort to prove the "fundamental theorem of algebra." This theorem ought to say that an n-th order equation has n solutions, so for example the equation $x^2+1=0$ should have two solutions, the equation $x^7+3x^5+4x^2+5=0$ should have seven solutions, and so on. But the only way for $x^2+1=0$ to have two solutions is to stipulate that there is a number x such that $x^2=-1$, that is, that a "square root of -1" exists. This, however, leads to all kinds of difficulties, if you think that this square root—let us call it i—is an ordinary real number. For example, every real number is either positive or negative or zero. Now, i of course cannot be zero, so i is either positive or negative. Since the product of two positive numbers is positive, if i was positive then i^2 would have to be positive. Since the product of two negative numbers is positive, if i was negative then i^2 would have to be positive. So in either case, whether i is positive or negative, the number i^2 would have to be positive. But $i^2=-1$, so -1 would have to be positive, and this is not possible. The way out of this was to think of i as not being an ordinary number, really, but only a symbol to be manipulated according to certain rules. So, for example, following what **Descartes** wrote in 1637, one can "imagine" that the equation $x^2 + 1 = 0$ has two roots (i and $-i$) but these imagined roots are not "real" numbers. Earlier, in 1572, **Bombelli** had given precise rules for the manipulation of these imaginary numbers. **Argand** in 1814 had the idea of representing complex numbers as points in a two-dimensional plane. The term "complex number" was actually introduced by **Gauss** in 1831. The term "conjugate" had been introduced by **Cauchy** in 1821. $\diamondsuit$

BOX NO. 3: THE SYMBOL "$\subseteq$" ("IS A SUBSET OF").

We use the symbol $\subseteq$ (read "is a subset of," or "is contained in") to indicate *set inclusion*, and the symbol $\not\subseteq$ (read "is not a subset of") to indicate that the inclusion does not hold.
If A and B are sets, the expression "$A \subseteq B$ (read "A is a subset of B") means that *every member of A belongs to B*.
For example: if A is the set of all U.S. Senators, and B is the set of all citizens of the U.S., then "$A \subseteq B$" and "$B \not\subseteq A$" are true statements.
The following statements about $\mathbb{Z}_{>0}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, are true:

$$
\begin{array}{cccc}
\mathbb{Z}_+ \subseteq \mathbb{Z}_+\,, & \mathbb{Z}_+ \not\subseteq \mathbb{N}\,, & \mathbb{N} \subseteq \mathbb{Z}_+\,, & \mathbb{N} \subseteq \mathbb{N}\,, \\
\mathbb{N} \subseteq \mathbb{Z}\,, & \mathbb{Z} \not\subseteq \mathbb{N}\,, & \mathbb{Z} \subseteq \mathbb{Z}\,, & \mathbb{Z}_+ \subseteq \mathbb{Z}\,, \\
\mathbb{Z} \subseteq \mathbb{Q}, & \mathbb{Q} \not\subseteq \mathbb{Z}\,, & \mathbb{Z} \subseteq \mathbb{R}\,, & \mathbb{N} \subseteq \mathbb{Q}, \\
\mathbb{Q} \not\subseteq \mathbb{N}\,, & \mathbb{Q} \not\subseteq \mathbb{Z}\,, & \mathbb{R} \not\subseteq \mathbb{Q}, & \mathbb{Q} \subseteq \mathbb{R}\,.
\end{array}
$$

BOX NO. 4: NOT ALL REAL NUMBERS ARE RATIONAL.

In Box No. 3 we asserted that $\mathbb{R} \not\subseteq \mathbb{Q}$. How do we know that?
For "$\mathbb{R} \subseteq \mathbb{Q}$" to be true, it would have to be the case that every real number is rational. Yet, this is *not* the case, because there are real numbers that are not rational. A famous example is $\sqrt{2}$. We will prove later that

$$\boxed{\text{The number } \sqrt{2} \text{ is not rational.}}$$

Actually, many other real numbers are not rational, although in lots of interesting cases this is very hard to prove. For example, the numbers π and e are not rational.

4.3 The integers modulo n

Here are some more examples of important "number systems" of a rather different kind. These systems will be very important to us later.

7.a. The set $\mathbb{Z}_{12}$ (read this as "z-twelve") of all *integers modulo* 12. The members of $\mathbb{Z}_{12}$ are the following 12 integers:

$$0\,,\ 1\,,\ 2\,,\ 3\,,\ 4\,,\ 5\,,\ 6\,,\ 7\,,\ 8\,,\ 9\,,\ 10\,,\ 11\,.$$

Addition and multiplication are carried out in the usual way, except that any time you get 12 or something larger, you must "reduce modulo 12," that is, subtract 12 and keep subtracting 12 until you get a member of $\mathbb{Z}_{12}$. For example, the following equalities are true in $\mathbb{Z}_{12}$:

$$\begin{array}{ccccc} 3+5=8\,, & 6+9=3\,, & 8+9=5\,, & 7+1=8\,, & 11+11=10\,, \\ 4.2=8\,, & 6.9=6\,, & 8.7=8\,, & 7.11=5\,, & 7.7=1\,. \end{array}$$

Remark 3. The numbers modulo 12 are very natural objects, and you are very much used to working with them. For example, suppose you start at 10 o'clock and work 8 hours. What time is it when you finish? The answer is "$10+8$ modulo 12," that is, 6 o'clock. If a movie theatre starts its show at 8 o'clock and shows a 2-hour movie 8 times, without intermission, what time is it at the end of the show? The answer is "$10+2.8$ modulo 12," that is, 2 o'clock.

Naturally, if you wanted to keep track of "am" vs. "pm" then you would want to use so-called "military time," that is, work in $\mathbb{Z}_{24}$, the numbers modulo 24. (In $\mathbb{Z}_{24}$, $16+13=5$, and $8.5=16$, and so on.)$\diamondsuit$

7.b. The set $\mathbb{Z}_7$ of all *integers modulo* 7.

The members of $\mathbb{Z}_7$ are the following 7 numbers:

$$0\,,\ 1\,,\ 2\,,\ 3\,,\ 4\,,\ 5\,,\ 6\,.$$

Addition and multiplication are carried out in the usual way, except that any time you get 7 or something larger, you must "reduce modulo 7," that is, subtract 7 and keep subtracting 7 until you get a member of $\mathbb{Z}_7$. For example, the following equalities are true in $\mathbb{Z}_7$:

$$\begin{array}{rrrrr} 3+2=5\,, & 6+5=11\,, & 4+3=0\,, & 2+6=1\,, & 4+2=6\,, \\ 4.2=1\,, & 6.5=2\,, & 3.4=5\,, & 3.3=2\,, & 3.5=1\ \ . \end{array}$$

Remark 4. Like the members of $\mathbb{Z}_{12}$, the numbers modulo 7 are also very natural objects that you are very much used to working with. For example, let us think of the days of the week as numbered, starting with Sunday as Day No. 0. In other words, think of

Sunday	as day No.	0
Monday	as day No.	1
Tuesday	as day No.	2
Wednesday	as day No.	3
Thursday	as day No.	4
Friday	as day No.	5
Saturday	as day No.	6

Suppose today is Thursday. What day of the week is it going to be 5 days from today? The answer is ***Tuesday***, of course. Why? Because

Thursday is Day 4, so 5 days from today is Day $4+5$, that is, Day 2, modulo 7.

Suppose today, January 5, is a Wednesday. Whay day of the week is February 11 going to be? ANSWER: today is Day 3; to go from January 5 to February 11 you must add 36 days (that is, 31 days to go to February 5, and 6 more to go to February 11), so you'll end up in Day 3+36=39, which is equal to 4 modulo 7. So February 11 is going to be a Day 4, that is, ***a Thursday***.

Suppose today, January 5, is a Wednesday. Whay day of the week is July 5 going to be, assuming that we are NOT in a leap year? ANSWER: today is Day 3; to go from January 5 to July 5 we must add 31 days (to get to February 5), then 28 days (to get to March 5, using the fact that we are not in a leap year), then 31 days (to get to April 5), then 30 days (to get to May 5), then 31 days (to get to June 5), and, finally, 30 days (to get to July 5). So we end up in Day $3+31+28+30+31+30$ which, modulo 7, is the same as $3+3+0+2+3+2$, that is, 13, that is, 6 (modulo 7). So ***July 5 is going to be a Saturday***. ♢

7.c. Naturally, one could consider integers modulo any other number, not just 12 or 24. For example, $\mathbb{Z}_3$ is the set of **integers modulo** 3. So $\mathbb{Z}_3$ has exactly three members, namely,

$$0\,,\qquad 1\,,\qquad \text{and}\qquad 2\,.$$

Arithmetic modulo 3 is very simple. The addition table is as follows:

$$\begin{aligned}
0+0 &= 0\,,\\
0+1 &= 1+0=1\,,\\
0+2 &= 2+0=2\,,\\
1+1 &= 2\,,\\
1+2 &= 2+1=0\,,\\
2+2 &= 1\,,
\end{aligned}$$

and the multiplication table is

$$\begin{aligned}
0.0 &= 0.1=1.0=0.2=2.0=0\,,\\
1.1 &= 2.2=1\,,\\
1.2 &= 2.1=2\,.
\end{aligned}$$

Remark 5. To say that an equality holds in $\mathbb{Z}_n$, we can say just that, or we can say that the equality holds (or is true) "modulo n."

For example, we can say that

$$5+8=2 \qquad \text{in} \quad \mathbb{Z}_{11}\,,$$

or that

$$5+8=2 \qquad \text{modulo} \quad 11\,.$$

Also, if it is clear from the context that we are working in $\mathbb{Z}_n$, then there is no need to say "in $\mathbb{Z}_n$" or "modulo n." (Example: after we said in Page 24 that "the following equalities are true in $\mathbb{Z}_{12}$," we then just went ahead and wrote things like $8.7 = 8$, without explaining again that this was meant to be "in $\mathbb{Z}_{12}$," or "modulo 12." There was no need, because we had already stated clearly that we were working in $\mathbb{Z}_{12}$. ♢

Remark 6. If you look at the way we defined the integers modulo n, you may think that the integers that are larger than n do not belong to $\mathbb{Z}_n$. (For example, the integer 8 does not belong to $\mathbb{Z}_7$, because $\mathbb{Z}_7$ consists of the integers 0, 1, 2, 3, 4, 5, and 6, and nothing else.) We can, however, assign a value to a symbolic expression such as 8 in $\mathbb{Z}_7$, by letting

$$8=1+1+1+1+1+1+1+1\,,$$

where the sum is understood to be in $\mathbb{Z}_7$. Then, in $\mathbb{Z}_7$, the expression "8" denotes the number 1, and we can write

$$8=1 \qquad \text{in} \qquad \mathbb{Z}_7\,.$$

Notice that

$$8\neq 1 \qquad \text{in} \qquad \mathbb{Z}\,.$$

So the symbol 8, when we are working in $\mathbb{Z}_7$, is the name of a thing which is not the integer 8. (If it was the same, then "$8 \neq 1$" would also be true in $\mathbb{Z}_7$.)

One can also talk about *negatives* of integers modulo n. What do we mean by "the negative" of an integer modulo n? We just mean "the integer modulo n that added in $\mathbb{Z}_n$ to our given integer modulo n yields 0."

For example, what is the negative of 3 in $\mathbb{Z}_7$? Well, in $\mathbb{Z}_7$ the sum of 3 and 4 is 0. Therefore **the negative of 3 in $\mathbb{Z}_7$ is 4**. We can also write this using the symbol "−":

$$-3 = 4 \qquad \text{in} \qquad \mathbb{Z}_7\,,$$

or

$$-3 = 4 \qquad \text{modulo} \quad 7\,.$$

$\diamondsuit$

An important application of arithmetic modulo 3 is that it enables us to find a simple criterion to check if a given integer is divisible by 3. The key fact here is that $10 = 1$ modulo 3. This means that if we are working modulo 3 then a big number such as $4,687$ is just the same (in $\mathbb{Z}_3$) as $4 + 6 + 8 + 7$, i.e. as 25, which is equal to 1 in $\mathbb{Z}_3$. So $4,687$ is not divisible by 3.

BOX NO. 5 : When is a natural number divisible by 3?

Take some natural number like 16,547. Is it divisible by 3? Naturally, you can do the division and see what happens. But can you tell quickly and directly?
When we say that a number is "divisible by 3" what we mean is that if you start subtracting 3s from it until you cannot do that any more (that is, until you get to 0, 1 or 2), then you end up with 0. In other words, ***our number is equal to* 0 *modulo* 3.**
So in our example we need to find out whether 16,547 is equal to 0, 1 or 2 modulo 3. Now:

$$16,547 = 1 \times 10,000 + 6 \times 1,000 + 5 \times 100 + 4 \times 10 + 7 \times 1\,.$$

Also, 10 is just equal to 1 modulo 3. So $100 = 10 \times 10 = 1 \times 1 = 1$ modulo 3. And $1,000 = 10 \times 10 \times 10 = 1 \times 1 \times 1 = 1$ modulo 3. And so on. Therefore, the following is true modulo 3:

$$16,547 = 1 + 6 + 5 + 4 + 7 = 23 = 2\,.$$

So 16,547 ***is not divisible by* 3.**
The point of the above argument is that

$$\begin{aligned} 10,000 &= 1 \quad \text{modulo } 3\,, \\ 6,000 &= 6 \quad \text{modulo } 3\,, \\ 500 &= 5 \quad \text{modulo } 3\,, \\ 40 &= 4 \quad \text{modulo } 3\,, \\ 7 &= 7 \quad \text{modulo } 3\,, \end{aligned}$$

so

$$16,547 = 1 + 6 + 5 + 4 + 7 = 23 = 2 \qquad \text{modulo } 3.$$

The general criterion is this: **to find out if an integer is divisble by 3, just add the digits in its decimal expression. If the sum of the digits is divisible by 3, then the given number is divisible by 3. Otherwise it is not.**

QUESTION 1. Which of the following three natural numbers are divisible by 3?

$$999,111,999,111$$
$$543,043,664,987$$
$$6,915,571,375,016,461,671,444,102,534$$

BOX NO. 6 : When is a natural number divisible by 11?

The situation here is very similar to what we found when we looked at divisibility by 3, but with an important twist. Now 10 is not equal to 1 modulo 11, but to -1. So if we look at a natural number like $16,547$, the 7 should count as a 7 modulo 11, the 4 as a -4, the 5 as 5, the 6 as a -6, and the 1 as a 1.
(Reason: $16,547 = 1\times 10,000+6\times 1,000+5\times 100+4\times 10+7$. Modulo 11, we have $10 = -1$, $100 = 10^2 = 1$, $1,000 = -1$, $10,000 = 1$. So, $16,547 = 1 - 6 + 5 - 4 + 7$ modulo 11.) Therefore $16,547 = 3$ modulo 11, and then $16,547$ ***is not divisible by* 11.**

The general criterion is this: ***to find out if an integer is divisble by* 11*, just add the digits in its decimal expression with alternating signs (plus, minus, plus, minus, and so on). If the alternating sum of the digits is divisible by* 11*, then the given number is divisible by* 11*. Otherwise it is not.***

QUESTION 2. Which of the three natural numbers of the previous question are divisible by 11?

QUESTION 3. Formulate and justify a criterion for testing if a number is divisible by 9.

QUESTION 4. Is the following true or false? If you take a natural number, reverse the order of its decimal figures, and subtract the smaller of the numbers you got from the larger, then what you get is divisible by 3. (Here are two examples: (1) start with 925, then get

529 by reversing the order of the figures, then subtract, and you get $925 - 529$, which is equal to $\boxed{396}$; (2) start with 386, then get 683 by reversing the order of the figures, then subtract, and you get $683 - 386$, which is equal to $\boxed{297}$. In both cases, we got numbers that are divisible by 3. The question for you is: is this going to to happen no matter which natural number we take?)

QUESTION 5. Is the following true or false? If you take a natural number, reverse the order of its decimal figures, and subtract the smaller of the numbers you got from the larger, then what you get is divisible by 11. (Here are two examples: (1) start with 925, then get 529 by reversing the order of the figures, then subtract, and you get $925 - 529$, which is equal to $\boxed{396}$; (2) start with 386, then get 683 by reversing the order of the figures, then subtract, and you get $683 - 386$, which is equal to $\boxed{297}$. In both cases, we got numbers that are divisible by 11. The question for you is: is this going to to happen no matter which natural number we take?)

QUESTION 6. Is the following true or false? If you take a natural number, reverse the order of its decimal figures, and add the two numbers, then what you get is divisible by 3. (Here are two examples: (1) start with 321, then get 123 by reversing the order of the figures, then add, and you get $321 + 123$, which is equal to $\boxed{444}$; (2) start with 801, then get 108 by reversing the order of the figures, then add, and you get $801 + 108$, which is equal to $\boxed{909}$. In both cases, we got numbers that are divisible by 3. The question for you is: is this going to to happen no matter which natural number we take?)

7.d. Even simpler is $\mathbb{Z}_2$, the set of **integers modulo** 2. Clearly, $\mathbb{Z}_2$ has exactly two members, namely,

$$0 \qquad\qquad \text{and} \qquad\qquad 1\,.$$

Arithmetic modulo 2 is so ridiculously simple that we can fit the complete addition and multiplication tables together in one line:

$$0+0=0\,,\ 0+1=1+0=1\,,\ 1+1=0\,,\ 0.0=0.1=1.0=0\,,\ 1.1=1\,.$$

QUESTION 7. Does the equation $x^2 + 1 = 0$ have a solution in $\mathbb{Z}_7$?

ANSWER. Let us write down explicitly the squares of all members of $\mathbb{Z}_7$:

$$0^2 = 0\,,\ \ 1^2 = 1\,,\ \ 2^2 = 4\,,\ \ 3^2 = 2\,,\ \ 4^2 = 2\,,\ \ 5^2 = 4\,,\ \ 6^2 = 1\,.$$

The only way for $x^2 + 1$ to be equal to zero would be for x^2 to be equal to 6. But in the above list we see clearly that there is no member of $\mathbb{Z}_7$ whose square is 6. So the answer is **NO**.

QUESTION 8. Does the equation $x^2 + 1 = 0$ have a solution in $\mathbb{Z}_{17}$?

ANSWER. In $\mathbb{Z}_{17}$, $4.4 = 16$, so $4.4 + 1 = 16 + 1 = 0$. So the answer is **YES**.

QUESTION 9. Does the equation $x^2 + 1 = 0$ have a solution in $\mathbb{Z}_{101}$?

ANSWER. In $\mathbb{Z}_{101}$, $10^2 + 1 = 101 = 0$, so the answer is **YES**.

QUESTION 10. Does the equation $x^2 + 1 = 0$ have a solution in $\mathbb{Z}_{103}$?

COMMENT. This is not easy. It turns out that the answer is “no.” Of course, you could verify this by listing the squares of all 103 members of $\mathbb{Z}_{103}$ and checking that you never get 102 (which is -1 in $\mathbb{Z}_{103}$). But this would be a lot of work. There ought to be a smarter way. Maybe we can **prove** that the answer is “no” without having to do lengthy boring computations? Try to think about it. We will come back to this problem later.

QUESTION 11. In $\mathbb{Z}_{24}$, are there two nonzero numbers whose product is equal to zero?

ANSWER. In $\mathbb{Z}_{24}$, $8.3 = 0$. So the answer is **YES**.

QUESTION 12. In $\mathbb{Z}_4$, does the equation $a^2 + b^2 = 3$ have a solution?

ANSWER. Here are the values of $a^2 + b^2$ for all possible choices of $a, b \in \mathbb{Z}_4$,

$$\begin{array}{rcl} 0^2 + 0^2 & = & 0\,, \\ 0^2 + 1^2 = 1^2 + 0^2 & = & 1\,, \\ 0^2 + 2^2 = 2^2 + 0^2 & = & 0\,, \\ 1^2 + 1^2 & = & 2\,, \\ 1^2 + 2^2 = 2^2 + 1^2 & = & 1\,, \\ 2^2 + 2^2 = & = & 0\,. \end{array}$$

We see that the right-hand side is never equal to 3. So the answer is **NO**.

QUESTION 13. In $\mathbb{Z}_{17}$, are there two nonzero numbers whose product is equal to zero?

ANSWER. If you multiply two numbers in $\mathbb{Z}_{17}$, the only way the product can be equal to zero in $\mathbb{Z}_{17}$ is if, when you reduce modulo 17, you get zero. That is, the product of these two numbers must be divisible by 17. But 17 is a prime number, so there is no way to multiply two nonzero numbers smaller than 17 and get a product which is divisible by 17. So the answer is **NO**.

Remark 7. Clearly, the class of number systems presented in this subsection consists of *infinitely many* "number systems," namely, the systems

$$\mathbb{Z}_2, \quad \mathbb{Z}_3, \quad \mathbb{Z}_4, \quad \mathbb{Z}_5, \ldots, \quad \mathbb{Z}_{397}, \ldots, \quad \text{and so on}. \qquad \diamondsuit$$

4.4 The quaternions

In 1843 **W. R. Hamilton** (1805-1865) invented the **quaternions**, which we include as the eighth item in our list.

8. The set $\mathbb{K}$ of all **quaternions**. Quaternions are like complex numbers, but with four components rather than two. So for example $3+4i-7j+25k$ and $-1+2i+9j+k$ are quaternions. To multiply quaternions, you just multiply as you would ordinary real or complex numbers, except that when you run into products such as $i.j$ or $k.i$ you rewrite them using the following "multiplication table":

$$\begin{array}{ll} i.j = k\,, & j.i = -k\,, \\ j.k = i\,, & k.j = -i\,, \\ k.i = j\,, & i.k = -j\,, \\ i.i = j.j = k.k = -1\,. & \end{array}$$

For example, suppose that we want to multiply

$$(3+4i-7j+25k).(-1+2i+9j+k)\,.$$

BOX NO. 7: Hamilton discovers the quaternions.

Hamilton was knighted in 1835 and that year his second son, Archibald Henry, was born. But the next few years did not bring him much happiness. After the discovery of algebraic couples, he tried to extend the theory to triplets, and this became an obsession that plagued him for many years. The following autumn he went to Bristol for a meeting of the British Association, and Helen took the children with her to Bayly Farm for ten months. His cousin Arthur died, and not long after Helen returned from her mother's she went away again to England this time leaving the children behind after the birth of a daughter, Helen Eliza Amelia. At this point, William became depressed and started to have problems with alcohol so his sister came back to live at Dunsink.
Helen returned in 1842 when Hamilton was so preoccupied with the triplets that even his children were aware of it. Every morning they would inquire:

Well, Papa can you multiply triplets?

but he had to admit that he could still only add and subtract them.
On 16 October 1843 (a Monday) Hamilton was walking in along the Royal Canal with his wife to preside at a Council meeting of the Royal Irish Academy. Although his wife talked to him now and again Hamilton hardly heard, for the discovery of the quaternions, the first noncommutative algebra to be studied, was taking shape in his mind:

> *And here there dawned on me the notion that we must admit, in some sense, a fourth dimension of space for the purpose of calculating with triples ... An electric circuit seemed to close, and a spark flashed forth.*

He could not resist the impulse to carve the formulae for the quaternions

$$i = j = k = ijk = -1$$

in the stone of Brougham Bridge as he and his wife passed it. Hamilton felt this discovery would revolutionise mathematical physics and he spent the rest of his life working on quaternions. He wrote:-

> *I still must assert that this discovery appears to me to be as important for the middle of the nineteenth century as the discovery of fluxions [the calculus] was for the close of the seventeenth.*

Here is the calculation in full:

$$
\begin{aligned}
&(3+4i-7j+25k).(-1+2i+9j+k)\\
&\quad = 3.(-1)+3.2.i+3.9.j+3.k+4.(-1).i+4.2.i.i+4.9.i.j+4.i.k\\
&\qquad +(-7).(-1).j+(-7).2.j.i+(-7).9.j.j+(-7).j.k+25.(-1).k\\
&\qquad +25.2.k.i+25.9.k.j+25.k.k\\
&\quad = -3+6i+27j+3k-4i+8i.i+36i.j+4i.k+7j\\
&\qquad -14j.i-63j.j-7j.k-25k+50k.i+225k.j+25k.k\\
&\quad = -3+6i+27j+3k-4i-8+36k-4j+7j\\
&\qquad +14k+63-7i-25k+50j-225i-25\\
&\quad = (-3-8+63-25)+(6-4-7-225)i+(27-4+7+50)j\\
&\qquad +(3+36+14-25)k\\
&\quad = \;\; 27-230i+80j+28k\,.
\end{aligned}
$$

5 Reading formulas precisely

It is important that you acquire from the very beginning the habit of reading mathematical formulas aloud precisely and correctly. For example, the correct way to read the formula

$$3 \in \mathbb{N} \tag{5.0.2}$$

aloud is

3 belongs to $\mathbb{N}$

or

3 is a member of $\mathbb{N}$

or

3 is in $\mathbb{N}$

or

3 is a natural number.

But you **cannot** read (5.0.2) as, for example, "3 is contained in $\mathbb{N}$." "Is contained" means something else!

Here is another example: Formula (4.1.1) is read as

$\mathbb{N}$ is the set consisting of 1, 2, 3, 4, etc.

It would be **wrong** (**very** wrong!) to read it as "$\mathbb{N}$ is 1, 2, 3, 4, etc." Do you see why this is bad? The best way to understand it is to think of more familiar examples.

For example, you cannot say that "the U.S. Supreme Court is Chief Justice Rehnquist and Justice Scalia and Justice Thomas and Justice O'Connor and Justice Souter and Justice Kennedy and Justice Ginsburg and Justice Breyer and Justice Stevens." Why not? Because the U.S. Supreme Court is **one single thing, not nine things!** What you *can* say is:

> The U.S. Supreme Court is a court whose members are Chief Justice Rehnquist and Justices Scalia, Thomas, O'Connor, Souter, Kennedy, Ginsburg, Breyer, and Stevens.

Similarly, the set $\mathbb{N}$ of natural numbers is **one single object, not many objects**, so you can say "$\mathbb{N}$ is the set consisting of 1, 2, 3, 4, etc." but you cannot say "$\mathbb{N}$ is 1, 2, 3, 4, etc."

Also, you cannot say "$\mathbb{N}$ is the natural numbers," or "$\mathbb{N}$ is natural numbers." (Actually, "$\mathbb{N}$ is the natural numbers" is bad, but "$\mathbb{N}$ is natural numbers" is even worse. Why?) What you should say is "$\mathbb{N}$ is the set of natural numbers," or "$\mathbb{N}$ is the set of all natural numbers."[3]

Similarly, you cannot say "$\mathbb{Z}$ is the integers." (And "$\mathbb{Z}$ is integers" would be even worse!!!) The correct ways to say it are

- $\mathbb{Z}$ is the set of all integers,

[3] Recommended reading: the short story "Pigs is pigs," by Ellis Parker Butler. You can find it in the Web sites `http://www.ellisparkerbutler.info/epb/pigsispigs.asp` `http://www.ellisparkerbutler.info/epb/biblio.asp?id=2149&print=YES` . It's funny, and one of the things that make it funny is precisely the misuse of the verb "is" in "Pigs is pigs."

- $\mathbb{Z}$ is the set whose members are all the integers,
- $\mathbb{Z}$ is the set whose members are the integers,
- $\mathbb{Z}$ is the set consisting of all the integers.

FOOD FOR THOUGHT. Can you say "$\mathbb{Z}$ is a set of integers"? (Hint: The answer depends very much on what you are trying to say or what question you are trying to answer. To answer this question, you should give examples of (a) a question for which "$\mathbb{Z}$ is a set of integers" would be a correct answer, and (b) a question for which "$\mathbb{Z}$ is a set of integers" would not be a correct answer.)

6 Some remarks on mathematical writing

When we talk about mathematical objects, we often use *letters* (or other special symbols such as $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, 0, 1, 2, etc.). The way letters are used in mathematical discourse may often appear mysterious to the students. The first thing you need to do is to realize that it is not mysterious at all. It is, in fact, quite simple!

Letters are only used in mathematics in order to shorten certain statements that would otherwise be too long.

6.1 Some examples

Example 1. Suppose you want to define the word "cousin." You could say:

> A person is said to be a *cousin* of another person if one of the first person's parents is a sibling of one of the second person's parents. (6.1.1)

This is O.K., but having to talk about the "first person" and the "second person" and having to repeat the word "person" so many times makes it awkward. So what we can do is give names to those persons, for example x and y, and say the following:

> Let x and y be persons. Then x is said to be a *cousin* of y if one of x's parents is a sibling of one of y's parents. (6.1.2)

Example 2. Suppose you want to say

> If you take two real numbers, add them, and square the sum, then you get the same result as if you had squared each number separately, added the squares, and added to the result twice the product of the two numbers. (6.1.3)

This is awfully complicated, awkward, and ugly. You can make it much shorter by saying

> Let x, y be two real numbers. Then $(x+y)^2 = x^2+y^2+2xy$. (6.1.4)

or

> For all real numbers x, y, $(x+y)^2 = x^2+y^2+2xy$. (6.1.5)

We can say (6.1.5) even more concisely, by writing

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, \Big((x+y)^2 = x^2+y^2+2xy\Big). \tag{6.1.6}$$

Here the symbol $\forall$ is the **universal quantifier**. Statement (6.1.6) is read as follows:

> For all real numbers x and for all real numbers y, the square of x plus y is equal to the sum of the square of x, the square of y, and twice the product of x and y. (6.1.7)

Actually **you can even read (6.1.6) without any letter variables at all.** How? Well, that's precisely what (6.1.3) does! $\diamondsuit$

Example 3. Suppose you want to say

> If you take the number $\frac{\sqrt{5}-1}{2}$, and add it to its square, you get 1. (6.1.8)

You could say this as follows:

$$\left(\frac{\sqrt{5}-1}{2}\right)^2 + \frac{\sqrt{5}-1}{2} = 1\,. \tag{6.1.9}$$

Or you could give a name to the number, say a, and write

> Let $a = \frac{\sqrt{5}-1}{2}$. Then $a^2 + a = 1$. (6.1.10)

Example 4. Suppose you want to say

> It is possible to find a real number whose cube, added to its square, is equal to the number itself. (6.1.11)

Again, this looks horribly complicated and ugly, and you can make it much shorter by saying

> There exists a real number x such that $x^2 + x^3 = x$. (6.1.12)

or

> There is a real number x such that $x^2 + x^3 = x$. (6.1.13)

or

> $x^2 + x^3 = x$ for some real number x. (6.1.14)

We can say this thing even more concisely, by writing

$$\exists x \in \mathbb{R}, (x^2 + x^3 = x) \,. \tag{6.1.15}$$

Here the symbol $\exists$ is the **existential quantifier**. Statement (6.1.15) is read as follows:

There exists a real number x such that $x^2 + x^3 = x$. (6.1.16)

There exists a real number x such that the sum of the square of x and the cube of x cube equals x. (6.1.17)

or even, if you don't want to use any letter variables at all

There exists a real number such that the sum of the square of the number plus the cube of the number equals the number itself. (6.1.18)

or, if you prefer, you can read it as statement (6.1.11) above. $\diamondsuit$

6.2 A very important remark on reading existential statements

An **existential statement** is a statement that asserts that there exists an object of a certain kind. For example:

Somebody killed Polonius (6.2.1)

is an existential statement, because it says that there is a person who killed Polonius. Using the symbolism of existential quantifiers, we could rewrite (6.2.1) as

$\exists x, x$ killed Polonius. (6.2.2)

The correct way to read the three-character expression "$\exists x$," (including the comma) is "there exists an x such that". For example:

- you should read (6.2.2) as "there exists x such that x killed Polonius," or "there exists x who killed Polonius."
- a statement of the form "$\exists x \in \mathbb{R}$, something about x" is read as

  There exists a real number x such that something about x. (6.2.3)

  or

  There exists an x belonging to $\mathbb{R}$ such that something about x. (6.2.4)

It is **wrong** (**very** wrong!) to read (6.2.2) as "there exists x and x killed Polonius."

Similarly, you should **never** read "$\exists x \in \mathbb{R}$, something about x" as

There exists a real number x and something about x. (6.2.5)

QUANTIFIERS

The symbols $\exists$ and $\forall$ are the **quantifiers**.

" $\exists$ " is the **existential quantifier**.

" $\forall$ " is the **universal quantifier**.

IMPORTANT! The 3-symbol string "$\exists x$," is read "there exists x such that," or "there exists an x such that," or "there is and x such that." **Do not forget the "such that."** Students sometimes read "$\exists x$," as "there exists x and," This is wrong and could be very confusing. (Think about this, and ask the intructor if you don't see why "there exists x and" is bad.)

A statement of the form "$\forall x$,blahblahblah-about-x" is a **universal statement**. We read it "For all x blahblahbla-about-x."

EXAMPLE: What kind of statement is "$\forall x, \exists y, y < x$"?
ANSWER: It is a universal statement, because it says that "for all , x something is true." The "something" that is true about x is an *existential statement*, namely, that "there exists a y such that $y < x$."
Let us be more precise. Let us give a name to our statement, say S. So from now until the end of this box the letter S stands for[a] the statement "$\forall x, \exists y, y < x$." Then what we just said is that S *is a universal statement* and, in fact, S is of the form "$\forall x, T$," where T *is an existential statement*, namely, "$\exists y, y < x$." So T is of the form "$\exists y, W$," where W is the statement "$y < x$."

QUESTION: Suppose we are talking about integers. What does "$\forall x, \exists y, y < x$" say in plain English? Is it true?
ANSWER: it says "for every integer there is a smaller integer." This is true, because given any integer x we can let $y = x - 1$, and then $y < x$.

QUESTION: Suppose we are talking about natural numbers. What does "$\forall x, \exists y, y < x$" say in plain English? Is it true?
ANSWER: it says "for every natural number there is a smaller natural number." This is false, because if we take x to be 0 then there is no natural number y such that $y < x$.

[a]Pay attention to what we have just done! Does it look familiar? If it does not, read §6.4 and then come back to this box. You will see that what we have done is this: we introduced a new letter, namely, S, and declared it to be a constant, by declaring its value to be the statement "$\forall x, \exists y, y < x$." This is exactly the same kind of thing we did in Example 3 when we introduced the letter a and declared it to be a constant with value $\frac{\sqrt{5}-1}{2}$. In Example 3 the letter a is used as a *numerical constant*, that is, a constant whose value is a number. Here we are using the letter S as a *statement constant*, that is, a constant whose value is a statement. In both cases, the letters are thing-symbols (that is, they stand for a thing, which is a number in one case and a statement in the other case) and are constants (that is, they stand for a fixed thing).

A statement of the form "$\exists x$,blahblahblah-about-x" is an **existential statement**. We read it "There exists x such that blahblahblah-about-x."

If you read (6.2.2) as "there exists x and x killed Polonius," or "$\exists x \in \mathbb{R}$, something about x" as in (6.2.5) then you are completely changing the meaning of the statement, and you are not conveying what it actually means.

EXAMPLE: Suppose you want to explain what it means for two people to be "siblings or half-siblings" using an existential quantifier. You could say:

> Let x and y be persons. We say that x *and* y *are siblings or half-siblings* if $x \neq y$ and $\exists z, z$ is a parent of x and a parent of y. (6.2.6)

How would you read this in plain English? You would certainly **not** say "there exists a z and z is a parent of x and a parent of y."!

What you would say (somewhat awkwardly, I know!) is "there exists a z who is parent of x and a parent of y," or (even more awkwardly, but still correctly) "there exists a z such that z is a parent of x and a parent of y."

It is important that you acquire as soon as possible the habit of using "such that" correctly. Please start right now! $\diamondsuit$

RECOMMENDED QUESTION FOR YOU TO THINK ABOUT: If I were to say "There exists a real number such that $x^2 + x^3 = x$," this would **not** be acceptable. Why? What is missing?

ANOTHER RECOMMENDED QUESTION FOR YOU TO THINK ABOUT: Is (6.1.15) true? Why?

6.3 More examples

Example 5. Suppose you want to say

> For each integer between 2 and 25, take that integer, square it, add 5, and compute the multiplicative inverse of the result (that is, 1 over the result). Having done this for all the integers between 2 and 25 (including 2 and 25 themselves), add all the resulting numbers. Then the number you get is smaller than 20. (6.3.1)

Once again, this is awful, so you can shorten the whole thing and just say

$$\text{Let } N = \textstyle\sum_{k=2}^{25} \frac{1}{k^2+5}\,. \text{ Then } N < 20. \tag{6.3.2}$$

Or, if you prefer, you could just say:

$$\textstyle\sum_{k=2}^{25} \frac{1}{k^2+5} < 20\,. \tag{6.3.3}$$

RECOMMENDED QUESTIONS FOR YOU TO THINK ABOUT: Is it true or false that $\sum_{k=2}^{25} \frac{1}{k^2+5} < 20$? How about $\sum_{k=2}^{25} \frac{1}{k^2} < 20$? And $\sum_{k=2}^{25} 1 < 20$? And what would you say if I ask you whether it's true that $\sum_{n=2}^{25} \frac{1}{k^2+5} < 20$?

Example 6. Suppose you want to say

> If you take the function that to each real number assigns its cube, and integrate it from 0 to 4, then the result is 64. (6.3.4)

Again, this can be made much shorter by saying

$$\text{Let } N = \textstyle\int_0^4 x^3\,dx\,. \text{ Then } N = 64. \tag{6.3.5}$$

Or you could just say:

$$\textstyle\int_0^4 x^3\,dx = 64\,. \tag{6.3.6}$$

RECOMMENDED QUESTIONS FOR YOU TO THINK ABOUT: Is it true or false that $\int_0^4 x^3\,dx = 64$? Is it true or false that $\int_0^4 y^3\,dx = 64$?

Example 7. Suppose you want to say:

> The set of all real numbers whose square is larger than the cube of the number has at least two different members. (6.3.7)

We can make this shorter by saying

> Let S be the set of all real numbers x such that $x^2 > x^3$. Then S has at least two members. (6.3.8)

or

> Let $S = \{x \in \mathbb{R} : x^2 > x^3\}$. Then S has at least two members. (6.3.9)

Or you could just say:

> Let $S = \{x \in \mathbb{R} : x^2 > x^3\}$. Then $\exists x \exists y, (x \in S, y \in S,$ and $x \neq y)$. (6.3.10)

Example 8. Suppose you want to say that

> I am older than 20 and less than 70, and my brother is younger than I am, but his age is larger than half my age. (6.3.11)

Here too we can be more concise, and say

> Let x be my age and let y be my brother's age. Then $20 < x < 70$ and $\frac{x}{2} < y < x$. (6.3.12)

6.4 Constants and variables

In all the examples we have discussed so far, we have used **special symbols** (most commonly letters, such as x, y, a, k, N, n, S) as labels, so that we can avoid writing clumsy phrases such as "the number that we have been talking about." Sometimes we use other special symbols, such as Greek letters (α, β, ε, etc.), letters modified in a particular way (for example $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{C}$), numerals $(0, 1, 2, \ldots)$

These special symbols stand for *objects*, or *things* of various kinds (numbers, human beings, sets, functions, wolfes, stars), so we are going to call them *individual symbols*, or *thing-symbols*. (There are other kinds of mathematical symbols that do not stand for things. For example: the universal quantifier $\forall$, the existential quantifier $\exists$, the symbol $+$ for the addition operation. We will talk about many of these symbols later.)

All the thing-symbols we have used are either

$\boxed{\textbf{constants} \quad \text{or} \quad \textbf{variables} \quad \text{(also called } \textbf{dummy variables}\text{).}}$

A *constant* is a symbol that stands for a thing that stays fixed throughout an explanation or argument.

For instance, in Example 3, the letter a stands for the number $\frac{\sqrt{5}-1}{2}$. We made this clear by **introducing** the letter a by means of the **declaration**

$$\text{Let } a = \tfrac{\sqrt{5}-1}{2}.$$

That is, we **declared** the value of a to be $\frac{\sqrt{5}-1}{2}$, so from that moment on we know that a stands for "$\frac{\sqrt{5}-1}{2}$."

Variables (also called "dummy variables") are letters used as an *internal label* within a statement, but which do not have a value outside this statement.

This may look complicated, but it is in fact quite simple. Actually, it is something you are probably used to if you write computer programs in a language like Pascal. You often introduce a variable to keep track of some number with which you perform several operations. For example, you may want to keep track of a list of 20 numbers, called list[1], list[2], . . ., up to list[20]. Suppose you want to add the 20 numbers, and end up with a number called "sum" as the result. You could write the following program:

```
begin
    sum := 0;
    For i := 1 to 20 do sum := sum + list[i];
end.
```

In this program, the letter i is just a label used to keep track of the variable index that keeps changing all the time. You could have written instead

```
begin
    sum := 0;
    For k := 1 to 20 do sum := sum + list[k];
end.
```

and you would have achieved the same thing. *Within the program*, the letter i (or k in our second version) has a value that keeps changing all the time. *Outside the program*, it does not make sense to ask "what is the value of i?"

Notice that what we are doing with this program is computing the sum

$$\text{Sum} = \sum_{i=1}^{20} \text{list}[i]\,,$$

which is exactly the same as saying

$$\text{Sum} = \sum_{k=1}^{20} \text{list}[k]\,,$$

or

$$\text{Sum} = \sum_{\alpha=1}^{20} \text{list}[\alpha]\,,$$

or

$$\text{Sum} = \sum_{\clubsuit=1}^{20} \text{list}[\clubsuit]\,.$$

The distinctive feature of a dummy variable is that you could have used any other symbol instead, and you would be saying exactly the same thing. For example, if you write

$$\text{For all real numbers } x,\ y,\ (x+y)^2 = x^2 + y^2 + 2xy\,, \tag{6.4.1}$$

or

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, ((x+y)^2 = x^2 + y^2 + 2xy)\,, \tag{6.4.2}$$

then that has exactly the same meaning as if you had written

$$\text{For all real numbers } a,\ b,\ (a+b)^2 = a^2 + b^2 + 2ab\,, \tag{6.4.3}$$

or

$$\forall a \in \mathbb{R}, \forall b \in \mathbb{R}, ((a+b)^2 = a^2 + b^2 + 2ab)\,, \tag{6.4.4}$$

or

$$\text{For all real numbers } \alpha,\ \beta,\ (\alpha+\beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta\,, \tag{6.4.5}$$

or

$$\forall\alpha \in \mathbb{R}, \forall\beta \in \mathbb{R}, \left((\alpha+\beta)^2 = \alpha^2+\beta^2+2\alpha\beta\right), \tag{6.4.6}$$

or

$$\text{For all real numbers } m,\ n,\ (m+n)^2 = m^2+n^2+2mn\,, \tag{6.4.7}$$

or

$$\forall m \in \mathbb{R}, \forall n \in \mathbb{R}, \left((m+n)^2 = m^2+n^2+2mn\right), \tag{6.4.8}$$

or

$$\text{For all real numbers } \diamond,\ \#,\ (\diamond+\#)^2 = \diamond^2+\#^2+2\diamond\#\,. \tag{6.4.9}$$

or

$$\forall\diamond \in \mathbb{R}, \forall\# \in \mathbb{R}, \left((\diamond+\#)^2 = \diamond^2+\#^2+2\diamond\#\right). \tag{6.4.10}$$

Similarly, instead of $\exists x \in \mathbb{R}, \Big(x^2+x^3=x\Big)$,

you could have said $\exists z \in \mathbb{R}, \Big(z^2+z^3=z\Big)$,

or $\exists a \in \mathbb{R}, \Big(a^2+a^3=a\Big)$,

or $\exists \omega \in \mathbb{R}, \Big(\omega^2+\omega^3=\omega\Big)$,

or $\exists \aleph \in \mathbb{R}, \Big(\aleph^2+\aleph^3=\aleph\Big)$,

or $\exists \diamond \in \mathbb{R}, \Big(\diamond^2+\diamond^3=\diamond\Big)$.

Just one more example:

Instead of $\displaystyle\sum_{k=2}^{25}\frac{1}{k^2+5} < 20\,,$ you could have said $\displaystyle\sum_{n=2}^{25}\frac{1}{n^2+5} < 20\,,$

or $\displaystyle\sum_{\rho=2}^{25}\frac{1}{\rho^2+5} < 20\,,$ or $\displaystyle\sum_{GNU=2}^{25}\frac{1}{GNU^2+5} < 20\,.$

The "dummy variables" in the above examples (that is, i, k, α, $\clubsuit$, x, y, a, b, β, m, n, $\diamond$, $\#$, z, ω, $\aleph$, ρ, GNU) are really just **internal tags**, using to keep track of numbers **within a particular statement**. Outside this text, they variables do not have any meaning. For example, after you have written

$$\sum_{k=2}^{25}\frac{1}{k^2+5} < 20\,,$$

it would not make sense for me to ask you "what is the value of k?" The letter k is just a tag to specify a *range of values*, as part of a set of instructions on how to compute a sum. Any other letter could be used instead, so in fact "k isn't really there." You can persuade yourself of this in another way, by remembering that

$$\sum_{k=2}^{25} \frac{1}{k^2+5} < 20$$

is just another way of saying

- For each integer between 2 and 25, take that integer, square it, add 5, and compute the multiplicative inverse of the result. Having done this for all the integers between 2 and 25 (including 2 and 25 themselves), add all the resulting numbers. Then the number you get is smaller than 20.

As you can see, there is no value of k there!

Similarly, when we say $\int_0^4 x^3\,dx = 64$, this is just a way of saying "if you take the function that to each real number assigns its cube, and integrate it from 0 to 4, you get 64." Once again, there is no value of x there! You could equally well have said $\int_0^4 y^3\,dy = 64$, or $\int_0^4 u^3\,du = 64$, or $\int_0^4 \aleph^3\,d\aleph = 64$.

And when we say $\exists x \in \mathbb{R}, x^2 = 2$, this is just a way of saying "there is a real number whose square is 2" (or, even better, "2 has a square root"). This statement does not talk about x.

This way of speaking and writing, using dummy variables, is very useful, especially when what we are trying to say is quite long. But **you have to be careful** when writing this way, and have to make sure that you are using the letters correctly.

In a statement, a thing-symbol can only be used if either its value has been declared before or it is a dummy variable.

6.5 Examples of things you should NOT write

Suppose you write

$$x^2 + x = 90$$

just like that, without any words before or after explaining what x is, or making it a dummy variable. Then what you wrote is **not a statement**[4]. We have no way to tell if what you wrote is true or false, because we have no idea what you are talking about.

If you write something like this in your homework, then I will

(a) Give you a grade of **x**. (Then you will come and ask me "what is this x?" And I will tell you "well, if you explain to me what your x is, then I will tell you what my x is." Then you will probably answer "x is a number." And then I will reply: "O.K., the x I have written in your homework is a grade.")

or

(b) Give a special assignment to you: "read page x of the book and tell me what it says next week."

[4]It's more or less the same situation as if somebody walked into our classroom and said "she has arrived." If we already know who "she" is supposed to be then this makes sense. But if we don't then our reaction would probably be to ask "who are you talking about?" The word "she" is a *pronoun*. It stands for somebody, and a sentence using "she" is meaningless if we do not know which person "she" stands for. Similarly, the letter x in "$x^2 + x = 90$" functions like a pronoun. The sentence "$x^2 + x = 90$" is meaningless if you do not know who—or what— x stands for.

For comparison, here are some perfectly meaningful statements you could have written:

1. Let $x = 9$. Then $x^2 + x = 90$.

2. Let $x = 6$. Then $x^2 + x = 90$.

3. Let x be the number of planets of the solar system. Then $x^2 + x = 90$.

4. $x^2 + x = 90$ for every real number x.

5. $x^2 + x = 90$ for some real number x.

6. $\forall x \in \mathbb{R}, (x^2 + x = 90)$.

7. $\exists x \in \mathbb{R}, (x^2 + x = 90)$.

8. The equation $x^2 + x = 90$ has a solution $x \in \mathbb{R}$. (Or "the equation $x^2 + x = 90$ has a real solution.")

Some of these are true, while the others are false. (Precisely: 1,3,5,7,8 are true; 2,4,6 are false. Moreover: 6 is just another way of saying the same thing as 4, and 7 and 8 are just alternative ways of stating 5.)

Notice that in 1, 2 and 3 the letter x is a constant: its value is declared before the letter is used to make a statement. In 4, 5, 6, 7 and 8 the letter x is a dummy variable.

Again for comparison, let us now write some things that do **not** have a completely precise meaning:

A. The equation $x^2 = 2$ has a solution.

B. The equation $x^2 + 1 = 0$ has a solution.

C. The equation $3x = 5$ has a solution.

Why are these things not good enough? Because they do not specify the **range** of values within which the solution x is to be sought. For example, A is true if we look for solutions $x \in \mathbb{R}$, but false if we look for solutions $x \in \mathbb{Q}$. B is true if we look for solutions $x \in \mathbf{C}$ (the set of complex numbers) but false if we look for solutions $x \in \mathbb{R}$. C is true if we look for solutions $x \in \mathbb{Q}$ (or $x \in \mathbb{R}$) but false if we look for solutions $x \in \mathbb{Z}$.

On the other hand, the following are perfectly meaningful statements:

A1. The equation $x^2 = 2$ has a solution $x \in \mathbb{R}$. (That is: $\exists x \in \mathbb{R}, (x^2 = 2)$.)
A2. The equation $x^2 = 2$ has a solution $x \in \mathbb{Q}$. (That is: $\exists x \in \mathbb{Q}, (x^2 = 2)$.)
B1. The equation $x^2+1 = 0$ has a solution $x \in \mathbb{Z}$. (That is: $\exists x \in \mathbb{Z}, (x^2 + 1 = 0)$.)
B2. The equation $x^2+1 = 0$ has a solution $x \in \mathbb{R}$. (That is: $\exists x \in \mathbb{R}, (x^2 + 1 = 0)$.)
B3. The equation $x^2+1 = 0$ has a solution $x \in \mathbf{C}$. (That is: $\exists x \in \mathbf{C}, (x^2 + 1 = 0)$.)
C1. The equation $3x = 5$ has a solution $x \in \mathbb{Z}$. (That is: $\exists x \in \mathbb{Z}, (3x = 5)$.)
C2. The equation $3x = 5$ has a solution $x \in \mathbb{Q}$. (That is: $\exists x \in \mathbb{Q}, (3x = 5)$.)
C3. The equation $3x = 5$ has a solution $x \in \mathbb{R}$. (That is: $\exists x \in \mathbb{R}, (3x = 5)$.)
C4. The equation $3x = 5$ has a solution $x \in \mathbf{C}$. (That is: $\exists x \in \mathbf{C}, (3x = 5)$.)

(Actually, A1, B3, C2, C3 and C4 are true, whereas A2, B1, B2 and C1 are false. Of course, in each case you could say the same thing in lots of different ways. For example, instead of C2 you could say "the equation $3x = 5$ has a rational solution," or "the equation $3x = 5$ can be solved in the set of rational numbers," or "there is a rational number that satisfies the equation $3x = 5$," or "$3x = 5$ is solvable in the set of rational numbers.")

6.6 Words are important

It's the **words** that glue the formulas together and give a structure and a meaning to mathematical writing. If you just write a bunch of formulas then you probably do not know what you are saying, and if you don't know then you should not expect that the instructor or the grader will know.

Look, for example, at Statements 1, 2, 4 and 5 above. In all cases, the "formula" $x^2 + x = 90$ is the same, but the statements are quite different and have totally different meanings. That's because the words are different!

6.7 Avoid ambiguous sentences

A sentence whose meaning is imprecise because it can be interpreted in more than one way is said to be *ambiguous*. For example, the sentences

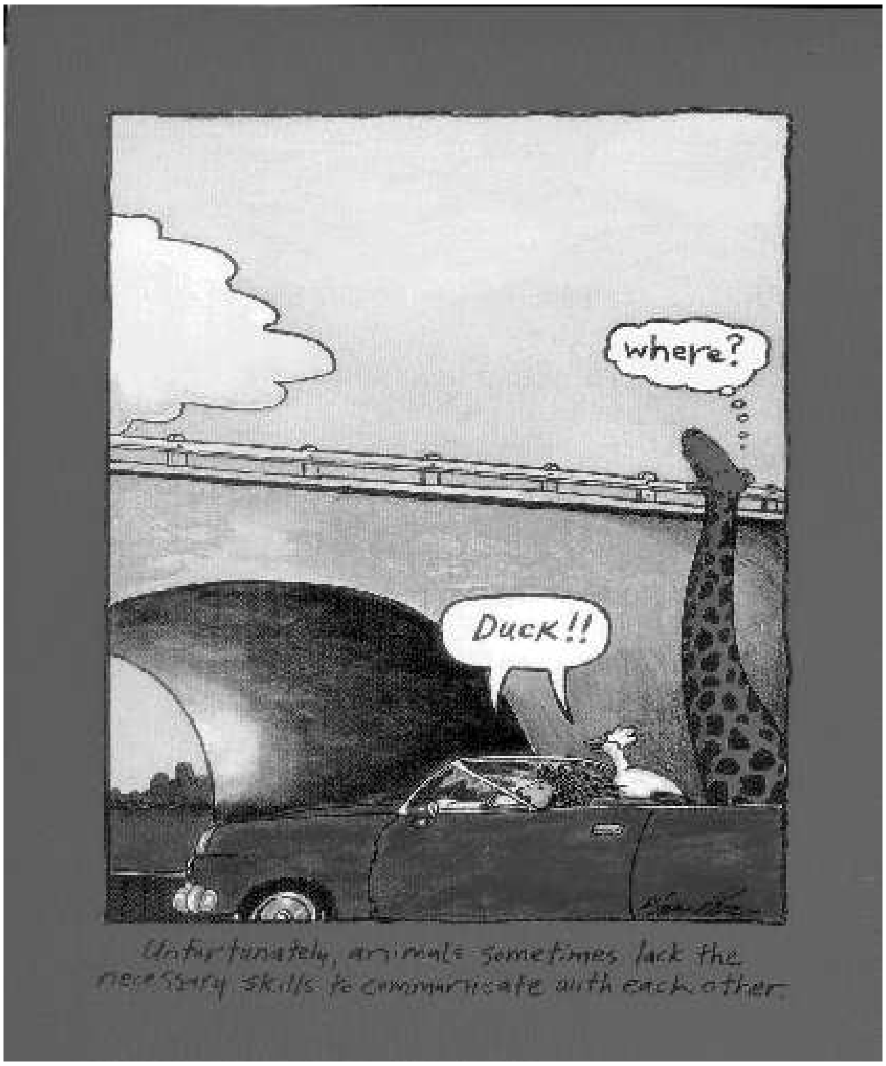
Flying planes can be dangerous
College students are turning to vegetables
I shot an elephant in my pajamas[5]
Mary had a little lamb[6]
George W. Bush and Hillary R. Clinton are married

are ambiguous. Why? Think of other examples of ambiguous sentences.

Similarly, A, B, C above are ambiguous. Another example of ambiguous sentence is a sentence where a letter does not have a declared value and is not a dummy variable either. For example, if I tell you to "read chapter x," then that's ambiguous—unless I have told you before what "x" stands for, or given you clues so you can find out, or perhaps I have said "read Chapter x for all x" (that is "read all the chapters") or "read Chapter x for some x" (that is "read one chapter")— because you don't know what x is supposed to be.

[5] "Last night I shot an elephant in my pajamas. How the elephant got into my pajamas I have no idea." (Groucho Marx)

[6] Mary had a little lamb,
Its fleece was white as snow,
Everywhere that Mary went,
The lamb was sure to go.
But also:
Mary had a little lamb,
A loaf of bread, a pot of jam,
An ice cream soda topped with fizz,
And oh! - How sick our Mary is!



7 More announcements

7.1 Reading for February 10, 12, 17 and 19

- this handout,
- the book's Chapter 2 (**all of it!**).

7.2 GOOD NEWS ABOUT THE SUPPLEMENTARY PROBLEMS!!!!

You can hand in the supplementary problems any time during the week of February 16 to 20. (For example, you can hand them in class on Thursday February 19, or bring them over to the Hill Center and put them in my mailbox on February 20.)

7.3 Homework assignment due on February 19

NOTE: this is a very short homework assignment, because you have the supplementary problems due the same week.

A. Problems 1 and 2 on page 62 of this handout.

B. Prove that the equation $x^2 + 1 = 0$ has a solution in $\mathbb{Z}_{29}$ (i.e., that the statement "$\exists x, x^2 + 1 = 0$" is true in $\mathbb{Z}_{29}$).

C. Prove that the equation $x^2 + 1 = 0$ has a solution in $\mathbb{Z}_{31}$ (i.e., that the statement "$\exists x, x^2 + 1 = 0$" is true in $\mathbb{Z}_{31}$).

8 $\mathbb{Z}_{11}$ and ISBN numbers

As explained earlier, $\mathbb{Z}_{11}$ is a set consisting of 11 members, namely, the integers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ and 10.

The members of $\mathbb{Z}_{10}$ are called ***digits***. The members of $\mathbb{Z}_2$ are called ***bits***. By analogy with these two widely used names, we are going to call the members of $\mathbb{Z}_{11}$ ***elvits***. So an ***elvit*** is one of the numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. Notice that ***there are eleven elvits***.

8.1 ISBN numbers

ISBN numbers are used to catalog and identify books. Each book has an ISBN number.

An ISBN number is a sequence

$$(m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10})$$

of ten elvits. When we work with ISBN numbers, the name of the elvit "10" is "X", so

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

The first nine of these ten elvits are required to belong to the set $\Big\{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \Big\}$, so m_{10} is the only elvit in an ISBN number that is permitted to have the value X.

Furthermore, m_{10} is a **redundant symbol**, included for error-correcting purposes. It is always given by the formula

$$m_{10} = \sum_{j=1}^{9} j m_j \,, \tag{8.1.1}$$

that is,

$$m_{10} = m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 \,.$$

Why do we use $\mathbb{Z}_{11}$ rather than $\mathbb{Z}_{10}$? And why do we use Equation (8.1.1)? I will explain this eventually. But before we do that, let us verify the formula for some books.

EXAMPLE 1. Our textbook has the ISBN number 0-201-43724-4. Let us verify (8.1.1), making sure we remember that we are working in $\mathbb{Z}_{11}$, so all the operations are performed modulo 11.

$$\begin{aligned} & m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 \\ & \quad = \quad 0 + 2 \times 2 + 3 \times 0 + 4 \times 1 + 5 \times 4 + 6 \times 3 + 7 \times 7 + 8 \times 2 + 9 \times 4 \\ & \quad = \quad 0 + 4 + 0 + 4 + 20 + 18 + 49 + 16 + 36 \\ & \quad = \quad 4 + 4 + 9 + 7 + 5 + 5 + 3 \\ & \quad = \quad 37 \\ & \quad = \quad 4 \,. \end{aligned}$$

So it works!

EXAMPLE 2. The book "An Introduction to Analysis," by William R. Wade, has the ISBN number 0-13-093089-X. Let us verify (8.1.1).

$$\begin{aligned} & m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 \\ & \quad = \quad 0 + 2 \times 1 + 3 \times 3 + 4 \times 0 + 5 \times 9 + 6 \times 3 + 7 \times 0 + 8 \times 8 + 9 \times 9 \end{aligned}$$

$$\begin{aligned}
&= 0+2+9+0+45+18+0+64+81 \\
&= 11+1+7+9+4 \\
&= 1+7+9+4 \\
&= 21 \\
&= 10 \\
&= X\,.
\end{aligned}$$

Once again, it works!

I suggest you look at a few books that you can find at home or in the library, look at heir ISBN numbers, and check that in all cases Formula (8.1.1) is true.

Now that you are convinced that ISBN numbers do indeed obey Formula (8.1.1), the three questions that you are probably asking yourself are:

1. *Why do we use $\mathbb{Z}_{11}$?,*
2. *Why do we include m_{10}, which contains absolutely no new information, since it is completely determined by the first* 9 *elvits?,*
3. *Why do we use Formula (8.1.1)?*

You will get the answers to these questions a little bit further in this handout. But it would be a good idea if you started thinking about them right now. Here is a hint:

The crucial distinction is that $\mathbb{Z}_{11}$ is a field, but $\mathbb{Z}_{10}$ is not. (The definition of "field" is given in the textbook, pages 180, 181.)

8.2 Why is $\mathbb{Z}_{10}$ not a field?

The number system $\mathbb{Z}_{10}$ is not a field because in it is not true that "every number which is not equal to zero has a multiplicative inverse." Or, in symbols, if you prefer, the statement

$$\forall x, (x \neq 0 \Rightarrow \exists y, x \cdot y = 1)$$

is not true in $\mathbb{Z}_{10}$.

How do we know that this is not true? Let us find a counterexample. I will show that $x = 2$ is a counterexample. I have to show that

$$2 \neq 0 \Rightarrow \exists y, 2 \cdot y = 1$$

isn't true. Notice that "$2 \neq 0$" *is* true, fortunately for us. (Why "fortunately for us"? Because if "$2 \neq 0$" wasn't true, then the implication that we are trying to prove, which says that "$2 \neq 0 \Rightarrow \exists y, 2 \cdot y = 1$," would be true!)

Since "$2 \neq 0$" is true, what we need is to prove that "$\exists y, 2 \cdot y = 1$" isn't true. Let us do it *by contradiction.* Suppose that there exists such a y. Pick one and call it $\bar{y}$. Then $2 \cdot \bar{y} = 1$ in $\mathbb{Z}_{10}$. This means that in $\mathbb{Z}$ the number $2 \cdot \bar{y}$ is equal to a multiple of 10 plus 1. But a multiple of 10 plus 1 must be odd, and $\bar{y}$ is even. So we have reached a contradiction, y doesn't exist, and we are done. **END OF PROOF**

8.3 Why is $\mathbb{Z}_{11}$ a field?

Let us show that, at least, it is true that "every nonzero member of $\mathbb{Z}_{11}$ has a multiplicative inverse." Here is the proof:

$$\begin{aligned} 1 \times 1 &= 1 \\ 2 \times 6 &= 1 \\ 3 \times 4 &= 1 \\ 4 \times 3 &= 1 \\ 5 \times 9 &= 1 \\ 6 \times 2 &= 1 \\ 7 \times 8 &= 1 \\ 8 \times 7 &= 1 \\ 9 \times 5 &= 1 \\ 10 \times 10 &= 1\,. \end{aligned}$$

Now, to prove that $\mathbb{Z}_{11}$ is a field we also have to prove all the other field axioms, such as, for example, the commutative law of addition (i.e., $\forall x, \forall y, x + y = y + x$), and many other things, listed in the book. I leave that up to you, if you feel like doing it. But the main part is the existence of multiplicative inverses, because this is what makes $\mathbb{Z}_{11}$ from, say $\mathbb{Z}_{10}$ or $\mathbb{Z}_{12}$.

8.4 Why do we use elvits for ISBN numbers?

In principle, we would like an ISBN number to consist of nine digits. (This would allow us to have a total of 10^9—i.e. one billion—ISBN numbers, which presumably is more than the number of books ever published or to be published up to, say, the year 2100. For example, as this is being written, the U.S. Library of Congress has 14 million books, and a total of 88 million items including manuscripts, maps, music, art prints, photographs, motion pictures, videotapes, newspapers, pamphlets, recordings and other materials.)

Now, as you well know, ISBN numbers are transmitted, copied, rewritten, etc. Each of these operations can introduce ***transmission errors***. So it is customary to introduce some ***redundancy*** into a signal to use it to ***check for errors***. (For example, when you change your password for a computer system you use, you are asked to type in the new password and then to type it in again. In principle, if you type it in correctly the first time, there is no need to type it in again, because this would convey no new information. However, if you made a mistake the first time you typed it in, you will almost certainly type in a different string of symbols the second time, because it is extremely unlikely that you will make exactly the same mistake the second time. And then the computer will know that you made a mistake somewhere, and ask you start all over again.)

For ISBN numbers, we introduce redundancy by adding an extra symbol that carries no new information but will enable us to detect the most frequent types of errors. A simple example of how this could be done, if we were using $\mathbb{Z}_{10}$, would be to take m_{10} to be the sum of the other 9 digits, i.e., to take

$$m_{10} = m_1 + m_2 + m_3 + m_4 + m_5 + m_6 + m_7 + m_8 + m_9\,. \tag{8.4.2}$$

This would detect errors consisting of getting one digit wrong. (Indeed, if you make a mistake in one of your first nine digits, that will change the sum, so the tramsitted m_{10} will no longer satisfy (8.4.2). For example, if the correct m_5 is 2, and you send a 7 instead, then the sum m_{10} will be increased by 5 in $\mathbb{Z}_{10}$.)

Naturally, ***this method will not detect more complicated errors such as, for example, if you send two wrong symbols.*** (For example, if the correct string is 0636274165, and you send is 0686774165 instead, getting two digits wrong, then (8.4.2) will still hold, because the errors in m_3 and m_5 are both 5, so their sum in $\mathbb{Z}_{10}$ is 0.) But two mistakes are a lot less likely than one mistake, so this imperfect method will enable us to detect most errors, even though some errors will still go undetected.

Another limitation of the method is that it will detect errors but ***it will not tell you how to correct them,*** because you will not know which digit is wrong. (For example, if you receive the string 0636774165, then you know for sure that it has to be wrong, because $0+6+3+6+7+7+4+1+6=0$—in $\mathbb{Z}_{10}$—whereas $m_{10}=5$, so (8.4.2) is not true. But you do not know which digit was wrong.) Again, this is a limitation of the method that we are willing to accept, because once we know that there is a mistake we can ask the sender to send us the number again.

The real problem is that there is another very common type of error that this method will not detect, namely, ***transposition errors***, in which two symbols get exchanged. (For example, if the correct 9-digit string is 0636274165, and you send instead 0616274365, so that m_3 and m_7 are interchanged, the sum of (8.4.2) will be the same.)

If we want to detect transposition errors as well as the simpler ones consisting of getting one symbol wrong, then we need a formula

$$m_{10} = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5 + a_6m_6 + a_7m_7 + a_8m_8 + a_9m_9\,, \tag{8.4.3}$$

where the coefficients $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ are all different. But then, if we insist on working in $\mathbb{Z}_{10}$, and we use (8.4.3) taking the coefficients a_j to be all different, we run into another difficulty: at least one of the a_j will have to be even (why?), and then $5a_j = 0$ in $\mathbb{Z}_{10}$, which means that if we make an error of 5 in the j-th digit, then we will not detect this error. In other words: ***if we work in $\mathbb{Z}_{10}$ there is no way to add an extra "error-detecting" digit m_{10} given by a formula (8.4.3) so that we will detect both (a) errors in the transmission of a single digit, and (b) transposition errors.***

On the other hand, let me prove to you that ***in $\mathbb{Z}_{11}$ it is possible to add an extra "error-detecting" digit m_{10} given by a formula (8.4.3) so that we will detect both (a) errors in the transmission of a single digit, and (b) transposition errors.*** Indeed, we can use the formula that is actually used in real life, namely,

$$m_{10} = m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9\,. \tag{8.4.4}$$

Notice that this corresponds to taking $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, $a_5 = 5$, $a_6 = 6$, $a_7 = 7$, $a_8 = 8$, $a_9 = 9$. These are 9 different elvits, and this is exactly as it should be, since we have already seen that in order to detect transposition errors you do need that a_j to be all different.

I will now prove to you rigorously (with your help) that ***if the m_j are elvits chosen so that (8.4.4) holds, then every error consisting of one wrong elvit or two transposed elvits will be detected.***

Here is the first half of the proof. Consider the first type of error, namely, one wrong elvit. Let j be the place where this error is made, so j is one of the numbers $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ and the correct elvit m_j is replaced by the wrong elvit $\tilde{m}_j$, but all the other elvits m_i (for $i \neq j$) are correct. Let us deal separately with the cases when $j < 10$ and $j = 10$. If $j < 10$, then the right-hand side $m_{10}^{computed}$ of (8.4.4) computed from the transmitted elvits will be $m_{10} + j(\tilde{m}_j - m_j)$, but the received 10-th elvit will be the correct m_{10}.

> Since $j \neq 0$ and $\tilde{m}_j - m_j \neq 0$, the product $j(\tilde{m}_j - m_j)$ is also different from 0

so $m_{10}^{computed}$ will not be equal to m_{10}. This means that the received ten-elvit string will not satisfy (8.4.4), so the error will be detected.

Now let us look at the remaining case, when the wrong elvit is the tenth one. In that case, the transmitted m_j (for $j = 1, 2, 3, 4, 5, 6, 7, 8, 9$) will be correct, but the transmitted value $\tilde{m}_{10}$ will be different from the true value m_{10}. The computed tenth elvit will be m_{10}, but the one received will be $\tilde{m}_{10}$, which is different. So once again the error will be detected.

This completes the first half of the proof, having to do with detecting errors in the transmission of a single elvit. Now we have to do the second part, namely, prove that the formula used in real life also detects transposition errors. And here I have a real treat for you! *I am leaving this part of the proof for you to do as a homework problem!* (No need to thank me.)

PROBLEM 1 (ON $\mathbb{Z}_{11}$): Prove that Formula (8.4.4) for ISBN numbers detects transposition errors. That is, prove the following: if a sequence $\mathbf{m} = (m_1, m_2, \cdots, m_{10})$ of ten elvits satisfies (8.4.4) then any sequence of $\tilde{\mathbf{m}}$ obtained from $\mathbf{m}$ by exchanging two different elvits (that is, any $\tilde{m} = (\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{10})$ such that, for some i, j for which $i \neq j$ and $m_i \neq m_j$, we have $\tilde{m}_k = m_k$ if $j \neq k \neq i$, $\tilde{m}_i = m_j$ and $\tilde{m}_j = m_i$) will fail to satisfy (8.4.4). (WARNING: you will have to be careful and consider separately two types of interchanges, namely, those that do not involve m_{10} and those that do. Alternatively, there is a cute trick that will enable you to deal with both cases in one swoop. See if you can figure it out.)

PROBLEM 2 (ON $\mathbb{Z}_{11}$): Suppose we wanted to increase the number of ISBN numbers by using 11 elvits instead of 10. That is, we would define an ISBN number to be a sequence $(m_1, m_2, \cdots, m_{10}, m_{11})$ of *eleven* elvits, and we would use the error-detecting formula

$$m_{11} = m_1+2m_2+3m_3+4m_4+5m_5+6m_6+7m_7+8m_8+9m_9+Xm_{10}\,. \quad (8.4.5)$$

(Recall that X is the name of 10 in $\mathbb{Z}_{11}$.) Would this still work to detect both types of errors?

8.5 A remark on fields

The crucial step in the proof of the first half of our theorem or the error-detecting properties of $\mathbb{Z}_{11}$-based ISBN numbers was the assertion that

$$\boxed{\text{In } \mathbb{Z}_{11}, \text{ if } a \neq 0 \text{ and } b \neq 0 \text{ then } ab \neq 0.}$$

How do we know that this is true? Well, we have to ***prove it***. One possible proof would go as follows: just compute all possible products ab in $\mathbb{Z}_{11}$ of two nonzero members of $\mathbb{Z}_{11}$ and in each case check that the result is not zdero. This is not too hard to do: there are only 100 such products (why?), so you can do it in a few minutes. And you can reduce the work if you allow yourself to use the commutative law of multiplication ($\forall a, \forall b(ab = ba)$), because this would reduce the number of products to 55 (why 55?).

If you do not want to work hard, there is an alternative, called thinking. The idea is to use a fact that we have already proved, namely, that $\mathbb{Z}_{11}$ ***is a field***. Recall that this means that, in $\mathbb{Z}_{11}$,

$$\forall a, (a \neq 0 \Rightarrow \exists b, ab = 1)\,, \quad (8.5.6)$$

(or, in words, "if you take a member of $\mathbb{Z}_{11}$ which is not equal to zero then there exists a member of $\mathbb{Z}_{11}$ that multiplied by the first member yields one" or, if you prefer, "every nonzero member of $\mathbb{Z}_{11}$ has a multiplicative inverse").

Now let me prove:

THEOREM: *In a field, the statement "*$\forall a, \forall b, (\text{if } a \neq 0 \text{ and } b \neq 0 \text{ then } ab \neq 0)$*" is true.*

PROOF: Let a, b be arbitrary nonzero members of the field. We want to prove that $ab \neq 0$. Suppose that $ab = 0$. (So we are doing a proof by contradiction!) Since $b \neq 0$, the field axiom (8.5.6) tells us that there exists a c such that $bc = 1$. Pick one such c and call it γ. Then $b\gamma = 1$. So

$$a = a \cdot 1 = a(b\gamma) = (ab)\gamma = 0 \cdot \gamma = 0\,.$$

So $a = 0$, contradicting the fact that $a \neq 0$. **THE END**

Obviously, you must have lost of questions at this point. For example, *how do we know that* $0 \cdot \gamma = 0$*?* It turns out that this can be proved, as a consequence of the field axioms. But I am not in a position to prove this for you now, because I have not yet given you the complete list of the field axioms. (Be patient, this will be done soon!)

REMARK: If you are curious, and want to see right now the proof of "$0.\gamma = 0$", here it goes. I will show that $\forall x, 0.x = 0$. *Proof:* Let x be arbitrary. We have $0 + 0 = 0$, using the axiom that says that $\forall y, y + 0 = y$, with $y = 0$. So $(0 + 0).x = 0.x$. But $(0 + 0).x = 0.x + 0.x$, by the distributive law. Hence $0.x + 0.x = 0.x$. Now, the additive inverse axiom says that $\forall y, \exists z, y + z = 0$. Apply this with $0.x$ in the role of y. Then $\exists z, 0.x + z = 0$. Pick one such z and call it ζ. Then $0.x + \zeta = 0$. So

$$\begin{aligned} 0.x &= 0.x + 0 \\ &= 0.x + (0.x + \zeta) \\ &= (0.x + 0.x) + \zeta \\ &= 0.x + \zeta \\ &= 0\,. \end{aligned}$$

So $0.x = 0$, and we are done. $\diamondsuit$

9 Propositional Calculus

In a propositional calculus, the **symbols** are:

1. the *propositional variables* (usually letters such as P, Q, R, S, etc., or maybe A, B, C, D, etc.),
2. the *logical connectives* $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\sim$,
3. the *parentheses* (and) .

REMARK: In the above list, we have cheated a little bit, by being somewhat vague about the list of propositional variables. (The word "etc." is a strong symptom of vagueness!!!) Exactly what are the propositional variables? Just A, B, C, D? Or just P, Q, R, S? That is, do we have only four propositional variables? Suppose that for a particular proof or definition we need formulas with 6 variables. Can we make new variables as we go along?

It would be much better if we had a completely prespecified list of variables, for example, "P, Q, R and nothing else." The trouble with this is that you may want in some cases to use 4, 5, 6, ..., 457, or any number of variables, so we really need an *infinite* collection of propositional variables. We can achieve that with finitely many symbols, as follows: we pick just one letter (for example, the P) and a "marker" symbol (for example, the vertical bar $|$), and then let the propositional variables be P, $P|$, $P||$, $P|||$, $P||||$, $P||||$, and so on. Now we have a propositional calculus with *exactly* 9 *symbols*, namely,

$$\boxed{\boxed{P \qquad | \qquad \vee \qquad \wedge \qquad \Rightarrow \qquad \Leftrightarrow \qquad \sim \qquad (\qquad)}}\ .$$

In this calculus, instead of writing something like "$(A \wedge B) \Rightarrow (C \vee D)$", we would write "$(P \wedge P|) \Rightarrow (P|| \vee P|||)$". Thus, the formulas we end up writing get a little bit longer, but we have achieved something that in this course we are always striving for, namely, **complete precision**.

Using the basic symbols of our propositional calculus, we want to write **propositional forms** (a.k.a. **sentence forms**, or **statement forms**). that is, expressions such as "$(A \wedge B) \Rightarrow A$", where we can plug in a statement for each of the variables and get a "compound statement." (For example, if we plug in "I am rich" for A and "I am smart" for B, we get the statement "if I am rich and I am smart then I am rich," which is incredibly stupid but undoubtedly true.)

Not every string of symbols will be "acceptable" to us. For example, "AB" should not be acceptable, since we would not know how to plug in statements for A and B and get something meaningful. (If you think you can plug in "I am rich" and "I am smart" for A and B, think again! What you get if you do that is "I am rich I am smart," which is certainly not a correct English sentence.)

We are going to call those strings that we would like to accept as being really "forms of compound statements" **well formed**.

REMARK: Every time you use some basic symbols to create a language, there is going to be a distinction between strings that are acceptable and strings that are not. For example, in English the string "the cow is white" (consisting of 16 symbols; we *are* counting the blank space as a separate symbol) is acceptable, but the string "eo wt hics htiwe" is not. (And what do you think about "the white is cow", or "the is cow white"? I leave these ones up to you, but you should draw from these examples the conclusion that in English the notion of an "acceptable string" is not 100% precise.)

In the so-called "formal languages" there is a precise, totally unambiguous notion of acceptability of a string. The acceptable strings are called "well formed."

For example, suppose we use the symbols

0	1	2	3	4	5	6	7	8	9

(called "digits") to name nonnegative integers. Then the strings "0", "1", "3", "70", "63", "20954", "137828", are acceptable, but "01" is not. The precise rule is as follows: a string of digits is **well formed** if it is either the "0" string or a string whose leftmost symbol is not 0.

The well-formed formulas are also called **propositional forms.** The **rules** determining which strings are well-formed formulas (i. e. propositional forms) are:

RULE 1: One-letter strings consisting of a propositional variable are well-formed formulas.

RULE 2: If $\mathcal{A}$ is a well-formed formula consisting of a single propositional variable then $\sim \mathcal{A}$ is a well-formed formula.

RULE 3: If $\mathcal{A}$ is a well-formed formula consisting of more than a single symbol then $\sim (\mathcal{A})$ is a well-formed formula.

RULE 4: If $\mathcal{A}$ and $\mathcal{B}$ are well-formed formulas each one of which consists of a single propositional variable then $\mathcal{A} \wedge \mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \Rightarrow \mathcal{B}$ and $\mathcal{A} \Leftrightarrow \mathcal{B}$ and are well-formed formulas.

RULE 5: If $\mathcal{A}$ and $\mathcal{B}$ are well-formed formulas such that $\mathcal{A}$ consists of a single propositional variable but $\mathcal{B}$ does not, then $\mathcal{A} \wedge (\mathcal{B})$, $\mathcal{A} \vee (\mathcal{B})$, $\mathcal{A} \Rightarrow (\mathcal{B})$ and $\mathcal{A} \Leftrightarrow (\mathcal{B})$ and are well-formed formulas.

RULE 6: If $\mathcal{A}$ and $\mathcal{B}$ are well-formed formulas such that $\mathcal{B}$ consists of a single propositional variable but $\mathcal{A}$ does not, then $(\mathcal{A}) \wedge \mathcal{B}$, $(\mathcal{A}) \vee \mathcal{B}$, $(\mathcal{A}) \Rightarrow \mathcal{B}$ and $(\mathcal{A}) \Leftrightarrow \mathcal{B}$ and are well-formed formulas.

RULE 7: If $\mathcal{A}$ and $\mathcal{B}$ are well-formed formulas neither of which consists of a single propositional variable, then $(\mathcal{A}) \wedge (\mathcal{B})$, $(\mathcal{A}) \vee (\mathcal{B})$, $(\mathcal{A}) \Rightarrow (\mathcal{B})$ and $(\mathcal{A}) \Leftrightarrow (\mathcal{B})$ and are well-formed formulas.

RULE 8: Only those strings obtained by applying Rules 1, 2, 3, 4, 5, 6, 7 and 8 once or repeatedly are well-formed formulas.

EXAMPLE: the string

$$((P \vee Q) \wedge (\sim Q)) \Rightarrow (P \vee Q)$$

is well formed, because one can arrive at it by applying the rules as follows:

STEP 1: P and Q are well formed, by Rule 1.

STEP 2: Applying Rule 2 with Q in the role of $\mathcal{A}$, we see that $\sim Q$ is well formed.

STEP 3: Applying Rule 4 with P in the role of $\mathcal{A}$ and Q in the role of $\mathcal{B}$, we see that $P \vee Q$ is well formed.

STEP 4: Applying Rule 7 with $P \vee Q$ in the role of $\mathcal{A}$ and $\sim Q$ in the role of $\mathcal{B}$, we see that $(P \vee Q) \wedge (\sim Q)$ is well formed.

STEP 5: Applying Rule 7 with $(P \vee Q) \wedge (\sim Q)$ in the role of $\mathcal{A}$ and $P \vee Q$ in the role of $\mathcal{B}$, we we see that $((P \vee Q) \wedge (\sim Q)) \Rightarrow (P \vee Q)$ is well formed.

EXAMPLE: I claim that the string $((P \wedge Q) \Rightarrow Q$ is ***not*** well formed. Let us try to understand *why*. First of all, you can try to produce $((P \wedge Q) \Rightarrow Q$ using the rules, and no matter how hard you try you will not be able to. But, just because you have not been able to do something it does not follow that it cannot be done. So, how do we know that $((P \wedge Q) \Rightarrow Q$ **cannot** be obtained using the rules? We need an *argument*. We need *reasoning*. We need a **proof.**

Here is a proof. First, we prove a small theorem.

THEOREM 1. *In every well-formed formula the number of left parentheses is equal to the number of right parentheses.*

PROOF. Call a string "balanced" if it has the same number of left and right parentheses. Any string obtained using Rules 1, 2 or 4 is balanced, because it has zero left parentheses and zero right parentheses. Any application of Rule 3 or 5 or 6 will add an extra left parenthesis and an extra right parenthesis, so when you apply any of these rules to a balanced string you get a balanced string. In any application of Rule 7, the number of left parentheses in the result is that of $\mathcal{A}$, plus that of $\mathcal{B}$, plus two, and the same is true for the number of right parentheses. So when you apply Rule 7 to two balanced strings you get a balanced string. So the application of Rules 1 through 7 can never create unbalanced strings. END OF PROOF.

Remark. Theorem 1 gives an example of a **necessary condition** for a string to be well formed. (We say that A is a *necessary condition* for B if A happens whenever B does, that is, if B implies A. For example: "he took the final exam" is a necessary condition for "he passed the course," because if he passed the course then he must have taken the final exam. But is of course not a "sufficient condition." Just taking the final exam is not enough to pass the course.) The theorem says that if a string is well formed then it has to have the same number of left and right parentheses. This condition is not sufficient: there are many strings—such as, for example, the string "$P)($"—that have the same number of left and right parentheses but are not well formed. How can we tell if a string is well formed? Even more precisely, can one give a **computer algorithm** to check? The answer is "yes," but this is a hard thing to do, and if you are interested you should look it up in a mathematical logic book. $\diamondsuit$

PROBLEM 3. Is $((P \vee Q) \wedge \sim Q) \Longrightarrow (P \vee Q)$ well formed? Justify your answer.

PROBLEM 4. Is $((P \vee Q) \wedge (\sim Q))(\Longrightarrow (P \vee Q))$ well formed? Justify your answer.

10 Some new information about the course

10.1 Homework assignment due on Thursday, February 26

Problems 2.3.15, 2.4.4, 2.4.11, 2.5.5 and 2.5.6 from the book, and also problems 1, 4, 6 on pages 53, 54, 55.

10.2 Homework assignment due on Thursday, March 4

Nothing.

11 Leap years: a clarification

On Tuesday, February 17, we talked about leap years, and some of us were not sure whether 2000 had been a leap year or not. The precise rule is as follows: every year divisible by 4 is a leap year, except for those years that are divisible by 100 but not by 400, but with the extra qualification that if the year number is divisible by 4000 then it is not. (For example: 1996, 2004, 2008, 1844, were, are, or will be, leap years; 1700, 1800, 1900, were not, 2000 was, 2400 will be, 4000 will not be.)

PROBLEM. Introduce letters as propositional variables, assign them appropriate statements as values, and then express the above rule for leap years as a formula of the propoitional calculus.

12 The rules for proofs

A **proof** is a sequence of **steps**, each of which must be **justified**. The justification of a step consists of showing that it is permitted by the rules, given the previous steps.

12.1 When is a step valid?

Here are the conditions telling us when a step in a proof is valid.

(V.a) it is always permitted to bring in an *axiom* (or "postulate") as a new step,

(V.b) it is always permitted to bring in one of the hypotheses as a new step (if you are proving a theorem in which there are hypotheses and a conclusion), (V.c) it is always permitted to bring in as a new step something that follows from previous steps by applying a valid *rule of inference*.

(V.d) it is always permitted to start a proof within a proof by introducing any sentence you want as an assumption (for example, "Assume pigs can fly"), or by bringing in a **new** letter as an arbitrary constant ("let a be arbitrary") or by introducing a new object characterized by a property and giving it a name ("pick a such that $a^2 = 3$", or "let $a = 5$"). However, whatever is proved after this is done is only valid in the "proof within a proof", and one can only get out of it by applying Rule 3 or Rule 11 or Rule 12. For example, if you assume that "pigs can fly", as you are certainly permitted to do, then you can prove things under this assumption. For example, you may be able to prove that "pigs have wings." However, you cannot just claim that you have proved that pigs have wings. ***You have only proved that pigs have wings under the assumption that pigs can fly.*** That is, you proved that pigs have wings in an imaginary world in which pigs can fly. Does that enable us to say something about the real world? Yes, it does, but what we can say is very little. Rule $\Longrightarrow_{in}$ will enable to conclude, for the "real world", that "if pigs can fly then pigs have wings." You still cannot conclude that pigs have wings, since you do not know that pigs can fly. (If you knew that, you could use Rule $\Longrightarrow_{out}$ to infer that pigs have wings.)

12.2 The thirteen basic rules of inference.

Here are the basic rules of inference. You will see that there are exactly thirteen of them. We could get away with fewer rules (actually, it is easy to bring the number down to seven), but these thirteen rules are very easy to remember, so I really like them this way.

RULE 1. (*The tautology rule.*) You are allowed to bring in any statement which is an instance of a tautology.

RULE 2. (Rule $\Longrightarrow_{out}$, also called *Modus Ponens.*) If you have P and $P \Longrightarrow Q$ then you can go to Q.

RULE 3. (Rule $\Longrightarrow_{in}$.) If you have started a proof within a proof by assuming P, and have proved Q, then you can get out of the proof within a proof and go back to the main proof with $P \Longrightarrow Q$.

RULE 4. (Rule $\wedge_{out}$.) (a) If you have $P \wedge Q$ then you can go to P; (b) if you have $P \wedge Q$ then you can go to Q.

RULE 5. (Rule $\wedge_{in}$.) If you have P and Q then you can go to $P \wedge Q$.

RULE 6. (Rule $\vee_{out}$, a.k.a, "proof by cases".) If you have $P \vee Q$ and $P \Longrightarrow R$ and $Q \Longrightarrow R$ then you can go to R.

RULE 7. (Rule $\vee_{in}$.) If you have $(\sim P) \Longrightarrow Q$ then you can go to $P \vee Q$.

RULE 8. (Rule $\Longleftrightarrow_{out}$.) If you have $P \Longleftrightarrow Q$ then (a) if you have P then you can go to Q; (b) if you have Q then you can go to P.

RULE 9. (Rule $\Longleftrightarrow_{in}$.) If you prove $P \Longrightarrow Q$ and $Q \Longrightarrow P$ then you can go to $P \Longleftrightarrow Q$.

RULE 10. (Rule $\forall_{out}$, a.k.a. the "specialization rule.") Suppose $p(x)$ is a formula where there is no quantifier involving x, t is a constant term, and $p(x \to t)$ is what you get from $p(x)$ by substituting t for x in **all** the occurrences of x in $p(x)$. Then, if you have $\forall x, p(x)$, you can go to $p(x \to t)$.

REMARK: a ***term*** is an expression such as x, or a, or $x + a$, or $(x + a) + 3$, or $(3x + (a + b)) \cdot (u + 25 - \pi)$, or $A \cup B$, which stands for a thing (object, entity) which may or may not involve letter variables. A ***constant term*** is one that does not contain any variables. For example, if the letters a, b have been declared to be constants before (e.g. by saying "let a, b be arbitrary integers", or "let $a = 3$"), then $a + b$ is a constant term. Rule $\forall_{out}$ says that, for example, if you have $\forall x, (x \in \mathbb{Z} \Longrightarrow x \cdot x \geq 0)$, and you have a constant term such as -3, or $3 - 7$, or $-3 + a$ (if a has been declared to be a constant) then you can apply the statement $\forall x, (x \in \mathbb{Z} \Longrightarrow x \cdot x \geq 0)$ to the special case $x = -3$ (or $x = 3 - 7$, or $x = -3 + a$) and conclude that $-3 \in \mathbb{Z} \Longrightarrow (-3) \cdot (-3) \geq 0$, $3 - 7 \in \mathbb{Z} \Longrightarrow (3 - 7) \cdot (3 - 7) \geq 0$, and $-3 + a \in \mathbb{Z} \Longrightarrow (-3 + a) \cdot (-3 + a) \geq 0$.

RULE 11. (Rule $\forall_{in}$.) Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(x \to a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. ***Suppose the letter a has not appeared before***. Then you can start a proof within a proof by saying "Let a be arbitrary." If in this proof within a proof you get to $p(x \to a)$, then you can go to $\forall x, p(x)$ in your main proof.

REMARK: Naturally, instead of "a" you could use "b," or "z," or "α," or "β," or "$\aleph$," or "$\diamond$," or any symbol you want. What is important is that what you do should apply to a *completely arbitrary* object in our universe of discourse. Otherwise, you will not be proving that $p(x)$ is true for *all* x. For example —if our universe of discourse is $\mathbf{R}$— it would not be O.K. to prove that $\forall x, \exists y, y^2 = x$ (i.e., that every real number has a real square root) by saying "Let 9 be arbitrary. Then $\exists y, y^2 = 9$ is true, so we have proved that $\forall x, \exists y, y^2 = x$." What is wrong here? What is wrong is that 9 is not an *arbitrary* real number. 9 is 9, and just because something is true for the number 9 it doesn't mean that it is true for **all** real numbers.

RULE 12. (Rule $\exists_{out}$.) Suppose $p(x)$ is a formula where there is no quantifier involving x, a is a letter, and $p(x \to a)$ is what you get from $p(x)$ by substituting a for x in **all** the occurrences of x in $p(x)$. ***Suppose that the letter*** a ***has NOT appeared before. Suppose you have proved*** $\exists x, p(x)$. Then you can start a proof within a proof by introducing a new object, calling it a, and stipulating that $p(x \to a)$. This effectively declares a to be a constant, locally, within the "proof within a proof." If you ever get to something that does *not* contain a, then you can use it outside your proof within a proof, in the main proof.

REMARK: **It is important that the new object be given a name that has not been used before.** For example, suppose $p(x)$ stands for "x killed Polonius," and our universe of discourse is the set of all people. Suppose you are told that $\exists x, p(x)$, i.e. that somebody killed Polonius. Then you can introduce a name for this individual. You can call him/her a or, if you prefer, "the killer," in which case you would be able to say that $p(x \to a)$, i.e., that a killed Polonius. But you cannot say "let's call this person Hamlet," or "let's call him Laertes," because Hamlet and Laertes are names of characters that have already appeared in the play. If you call the killer "Hamlet" or "Laertes" then you would be *prejudging*, and declaring that $p(x \to \text{Hamlet})$, i.e. that Hamlet killed Polonius, or that $p(x \to \text{Laertes})$, i.e. that Laertes killed Polonius. One of these happens to be true, and the other one is false, but in either case you cannot just conclude that it is true by merely choosing a name for the killer.)

RULE 13. (Rule $\exists_{in}$, a.k.a. the witness rule.) Suppose $p(x)$ is a formula where there is no quantifier involving x, t is a constant term, and $p(x \to t)$ is what you get from $p(x)$ by substituting t for x in **all** the occurrences of x in $p(x)$. Then from $p(x \to t)$ you can go to $\exists x, p(x)$.

REMARK: Here is an example. Suppose we are working in $\mathbb{Z}$, and you want to prove that $\exists x, x^2 + 3\cdot x = 10$. You would first show that $2^2 + 3\cdot 2 = 10$. Now, if $p(x)$ is the formula "$x^2 + 3\cdot x = 10$", then $p(x \to 2)$ is the formula "$2^2 + 3\cdot 2 = 10$". So we have proved $p(x \to 2)$, and Rule $\exists_{in}$ allows us to go to $\exists x, x^2 + 3\cdot x = 10$.

AN EXAMPLE. Here is an example that combines several of our rules. Suppose you want to prove that the sum of two odd integers is even, working in $\mathbb{Z}$. That is, you want to prove that

$$\forall x, \forall y, \Bigg(\Big((\exists k, x = 2k+1) \wedge (\exists k, y = 2k+1)\Big) \Longrightarrow (\exists k, x+y = 2k)\Bigg).$$

Here is how you could do it.

1.	Let a be arbitrary.	[V.d]
2.	Let b be arbitrary.	[V.d]
3.	Assume $(\exists k, a = 2k+1) \wedge (\exists k, b = 2k+1)$.	[V.d]
4.	$\exists k, a = 2k+1$.	[Rule $\wedge_{out}$]
5.	$\exists k, b = 2k+1$.	[Rule $\wedge_{out}$]
6.	Pick a k such that $a = 2k+1$ and call it k_1.	[Rule $\exists_{out}$]
7.	Pick a k such that $b = 2k+1$ and call it k_2.	[Rule $\exists_{out}$]
8.	$a = 2k_1 + 1$.	[From 6]
9.	$b = 2k_2 + 1$.	[From 7]
10.	$a + b = (2k_1+1) + (2k_2+1) = 2(k_1+k_2+1)$.	
11.	$\exists k, a+b = 2k$.	[Rule $\exists_{in}$]
12.	$\exists k, a+b = 2k$.	[Rule $\exists_{in}$]
13.	$\exists k, a+b = 2k$.	[Rule $\exists_{in}$]
14.	$\Big((\exists k, a = 2k+1) \wedge (\exists k, b = 2k+1)\Big) \Longrightarrow \exists k, a+b = 2k$.	[R. $\Longrightarrow_{in}$]
15.	$\forall y, \Big((\exists k, a = 2k+1) \wedge (\exists k, y = 2k+1)\Big) \Longrightarrow \exists k, a+y = 2k$.	[R. $\forall_{in}$]
16.	$\forall x, \forall y, \Big((\exists k, x = 2k+1) \wedge (\exists k, y = 2k+1)\Big) \Longrightarrow \exists k, x+y = 2k$.	[R. $\forall_{in}$]

12.3 Getting rid of some rules

The 13 rules we have given are not really needed. You could get away with a lot fewer. For example, suppose you wanted to avoid using Rule 5 (that is, Rule $\wedge_{out}$). Let me show you how you can always avoid using Rule 5. Suppose you find yourself in a situation where you have statements P and Q and you would like to go to $P \wedge Q$. If you could apply Rule 5 then of course you can do that. But suppose you want to do it without using Rule 5. Here is what you could do:

1. P
2. Q
3. $P \Longrightarrow (Q \Longrightarrow (P \wedge Q))$
4. $Q \Longrightarrow (P \wedge Q)$
5. $P \wedge Q$.

(In Step 3 we brought in a tautology. In Steps 4 and 5 we used Modus Ponens, i.e., Rule $\Longrightarrow_{out}$.)

PROBLEM: Show that the following seven rules would suffice: Rules 1, 2, 3, 10, 11, 12 and 13.

12.4 "Let a be arbitrary" vs. "pick a such that something about a"

Students are often confused by the following:

(1) you can always start a proof within a proof with "Let a be arbitrary." And you can always assume anything you want, for example that "pigs can fly", or that "Hector Sussmann is the greatest teacher in the whole universe", or that "$3 + 5 = 23$", or that "a belongs to the empty set."

REMARK: Actually, in the proof that "if A is a set then $\emptyset \subseteq A$" there is one step where we have an arbitrary a and assume $a \in \emptyset$. Remember that? The proof is, briefly, as follows:

> We want to prove that $\emptyset \subseteq A$, i.e., that $\forall x, (x \in \emptyset \Longrightarrow x \in A)$. We let a be arbitrary. Assume $a \in \emptyset$. On the other hand, we have $\forall x, (\sim x \in \emptyset)$, so by Rule $\forall_{out}$ we get $\sim a \in \emptyset$. So by Rule $\wedge_{in}$ we get $a \in \emptyset \wedge (\sim a \in \emptyset)$. But $a \in \emptyset \wedge (\sim a \in \emptyset)$ is a contradiction. So $\Big(a \in \emptyset \wedge (\sim a \in \emptyset)\Big) \Longrightarrow a \in A$ is a tautology, and we can bring it in. Then $a \in A$ by Rule $\Longrightarrow_{out}$ (Modus Ponens). So we have proved $a \in A$ under the assumptions that a is arbitrary and $a \in \emptyset$. Then we can conclude $a \in \emptyset \Longrightarrow x \in A$ under the assumption that a is arbitrary by Rule $\Longrightarrow_{in}$. So we get $\forall x, (x \in \emptyset \Longrightarrow x \in A)$, as desired.

(2) On the other hand, if you want to introduce an a such that something is true (for example, a real number a such that $a^2 = 2$) then you are required to have proved before that such an a exists (in our example, that $\exists x, x^2 = 2$). This is why you cannot, if you are working in $\mathbb{R}$, introduce an a such that $a^2 = -1$. It happens that $\exists x, x^2 = -1$ is false, so you will never be able to prove it, and unless you prove it you cannot introduce an a such that $a^2 = -1$.

How come? Why can't you circumvent the restriction of (2) and use the following subterfuge to introduce non-existent things using just (1)? Here is how it seems that this could be done. Say you are working in $\mathbb{R}$ and you want to introduce an a such that $a^2 = -1$ (even tough you know that such an a does not exist or, at least, *you don't know that it exists*).

You could do this:

Let a be arbitrary.

Assume that $a^2 = -1$.

This is perfectly legitimate. Of course there is no a such that $a^2 = -1$, but I have told you that you can assume anything you want. It does not have to be true, and you don't need to know that it is true.

So it seems that we have been able to introduce this forbidden a,after all! Indeed, we have. But the catch is, there is practically nothing we can do with such an a.

Here is an example of the kind of thing we *can* do. You will see that there is no way we can prove something false, and there is no way we could get into trouble.

EXAMPLE: Once you have a real number a such that $a^2 = -1$, it seems that you can prove that "$-1 > 0$". How do you prove this? You would use the following facts from arithmetic:

1. $\forall x, (x \neq 0 \Longrightarrow x > 0 \vee -x > 0)$,
2. $\forall x, \forall y, ((x > 0 \wedge y > 0) \Longrightarrow x \cdot y > 0)$,
3. $\forall x, x \cdot 0 = 0$,
4. $1 \neq 0$,

5. $(-1) + 1 = 0$,

6. $\forall x, x + 0 = x$,

7. $\forall x, (-x) \cdot (-x) = x \cdot x$.

You can then prove that $a \neq 0$. (Proof by contradiction: suppose $a = 0$. Then $a.a = a.0 = 0$. But $a.a = -1$. So $-1 = 0$. So $0 = (-1)+1 = 0+1 = 1$. That is, $0 = 1$, which is not true since $1 \neq 0$.)

Since $a \neq 0$, we can conclude that $a > 0$ or $-a > 0$. If $a > 0$ then $a.a > 0$, so $-1 > 0$. If $-a > 0$ then $a.a = (-a) \cdot (-a) > 0$, so $-1 > 0$. (*Notice that we have done a proof by cases.*)

So we have "proved" that $-1 > 0$, which is clearly false.

Now I claim that this "proof" of ours is not a valid proof. We cheated!

Let us see how and where we cheated. To see this, let us write things carefully, following our rules.

Let a be arbitrary.

Assume that $a^2 = -1$.

$\vdots$

Here goes the lengthy argument I gave before.

$\vdots$

$-1 > 0$.

You see? We have indeed proved that $-1 > 0$ ***under the assumption that*** $a^2 = -1$, which is like having proved that pigs have wings under the assumption that pigs can fly. ***From this, if we do things correctly, we will never be able to prove that*** -1 ***really is*** > 0***, any more than we will be able to prove that pigs really have wings.***

But, you may say, we can get out of working under the assumption that $a^2 = -1$ by using Rule $\Longrightarrow_{in}$. We sure can, but let us see what we get if we add that step.

Let a be arbitrary.

Assume that $a^2 = -1$.

$\vdots$

Here goes the lengthy argument I gave before.

$\vdots$

$-1 > 0$.

$a^2 = -1 \Longrightarrow -1 > 0$.

And we can even get out from working under the assumption that a is arbitrary, by applying Rule $\forall_{in}$

Let a be arbitrary.

Assume that $a^2 = -1$.

$\vdots$

Here goes the lengthy argument I gave before.

$\vdots$

$-1 > 0$.

$\forall x, (x^2 = -1 \Longrightarrow -1 > 0)$.

Good! Now we got something ***under no assumptions whatsoever***. But look at what we got. Our conclusion—that is, $\forall x, (x^2 = -1 \Longrightarrow -1 > 0)$—says that "if you give me any x such that $x^2 = -1$ then it follows that $-1 = 0$." This is perfectly true, vacuously, because *you cannot give me such an x, because there isn't one.* So that is as far as you can go, and you will ***never*** be able to prove that $-1 > 0$.

13 Answers to the supplementary problems

13.1 Solution to Problem A

This is **true**. Here is a proof.

Count the days of the year as the members of $\mathbb{Z}_7$ (that is, $0, 1, 2, 3, 4, 5, 6$) starting with January 1 as Day Zero. (For example, if January 1st is a Tuesday, then Tuesday is Day 0, Wednesday is Day 1, etc.) Let us look at what day of the week each 13th is, doing the calculation separately for non-leap years and for leap years.

For a non-leap year, Jan. 13 is a Day 5, Feb. 13 a Day 1, March 13 also a Day 1, April 13 a Day 4, May 13 a Day 6, June 13 a Day 2, July 13 a Day 4, August 13 a Day 0, September 13 a Day 3, October 13 a Day 5, November 13 a Day 1, December 13 a Day 3. So the 13ths fall on days $5, 1, 1, 4, 6, 2, 4, 0, 3, 5, 1, 3$. Notice that all seven members of $\mathbb{Z}_7$ occur. So at least one of these has to be a Friday.

For a leap year, Jan. 13 is a Day 5, Feb. 13 is a Day 1, March 13 is a Day 2, April 13 a Day 5, May 13 a Day 0, June 13 a Day 3, July 13 a Day 5, August 13 a Day 1, September 13 a Day 4, October 13 a Day 6, November 13 a Day 2, December 13 a Day 4. So the 13ths fall on days $5, 1, 2, 5, 0, 3, 5, 1, 4, 6, 2, 4$. Again, all seven members of $\mathbb{Z}_7$ occur. So at least one of these has to be a Friday.

Notice that we have in fact proved the following stronger statement: *Every year must have a Friday the 13th occuring not later than November, and if the year is not a leap year there has to be a Friday the 13th not later than October.*

13.2 Solution to Problem B

It is **not true** that every year must have a Friday the 13th even if you reorder the months.

Here is a proof. Let us reorder the months as follows: January, April, June, May, September, November, August, October, February, March, July, December.

Assume that we are dealing with a non-leap year. Let us do the calculation as in Problem A. Jan. 13 is a Day 5, April 13 is a Day 1, June 13 a Day 3, May 13 a Day 5, September 13 a Day 1, November 13 a Day 3, August 13 a Day 5, October 13 a Day 2, February 13 is a Day 5, March 13 is a Day 5, July 13 a Day 1, December 13 a Day 4. Se we get $5, 1, 3, 5, 1, 3, 5, 2, 5, 5, 1, 4$. Day 0 is missing!! So all we need to do is take a year which is not a leap year and such that January 1 is a Friday, and that year will *not* have a Friday the 13th.

13.3 Solution to Problem C

This number *cannot* be expressed as the sum of two squares. PROOF: Modulo 4, our huge number is equal to 3. And in $\mathbb{Z}_4$ it is not possible to express 3 as the sum of two squares, as we showed on Page 25 of the first set of notes.

An alternative argument, if you do not want to use $\mathbb{Z}_4$. Let h denote our huge number. Then $h = 4k+3$ for some integer k. (Of course, you can easily compute k, but we don't need to know what k is.) Suppose there are integers a, b such that $h = a^2 + b^2$. Write $a = 4\alpha + r$, $b = 4\beta + s$, where α, β, r, s are integers and $0 \leq r < 4$, $0 \leq s < 4$. Then

$$\begin{aligned} h &= a^2 + b^2 \\ &= (4\alpha + r)^2 + (4\beta + s)^2 \\ &= 16\alpha^2 + 8\alpha r + r^2 + 16\beta^2 + 8\beta s + s^2 \\ &= 4(4\alpha^2 + 2\alpha r + 4\beta^2 + 2\beta s) + r^2 + s^2 \\ &= 4\kappa + r^2 + s^2 , \end{aligned}$$

where $\kappa = 4\alpha^2 + 2\alpha r + 4\beta^2 + 2\beta s$.

If r and s were both even or both odd, then $r^2 + s^2$ would be even, so h would be even. Hence one of r, s is even, and the other one is odd. Suppose r is even and s is odd. Then $r = 0$ or $r = 2$. Suppose $r = 0$. Then $s = 1$ or $s = 3$. If $s = 1$ then $r^2 + s^2 = 1$, so $h = 4\ell + 1$ for some integer ℓ, since can just take $\ell = \kappa$. If $s = 3$ then $r^2 + s^2 = 9 = 2 \times 4 + 1$, so $h = 4\ell + 1$ for some integer ℓ, since can just take $\ell = \kappa + 2$. Next suppose $r = 2$. Then $s = 1$ or $s = 3$. If $s = 1$ then $r^2 + s^2 = 5 = 4 \times 1 + 1$, so $h = 4\ell + 1$ for some integer ℓ, since can just take $\ell = \kappa + 1$. If $s = 3$ then $r^2 + s^2 = 13 = 4 \times 4 + 1$, so $h = 4\ell + 1$ for some integer ℓ, since can just take $\ell = \kappa + 4$. So we see that in all cases the remainder of dividing h by 4 is 1. But this is impossible, because the remainder is fact 3. **END OF PROOF**

Comment. If you think about it carefully, you will discover that the two arguments that I have given you above are basically the same: in both cases, the proof really amounts to saying that what we would like to do cannot be done because it cannot be done modulo 4.

13.4 Solution to Problem D

This statement is true. Here is a proof.

Let a, b be integers each one of which is the sum of two squares. Then we can pick integers $\alpha, \beta, \gamma, \delta$ such that

$$a = \alpha^2 + \beta^2 \qquad \text{and} \qquad b = \gamma^2 + \delta^2\,.$$

Let

$$\mu = \alpha\gamma - \beta\delta\,, \qquad \nu = \alpha\delta + \beta\gamma\,.$$

Then

$$\begin{aligned}
\mu^2 + \nu^2 &= (\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2 \\
&= \alpha^2\gamma^2 + \beta^2\delta^2 - 2\alpha\gamma\beta\delta + \alpha^2\delta^2 + \beta^2\gamma^2 + 2\alpha\delta\beta\gamma \\
&= \alpha^2\gamma^2 + \beta^2\delta^2 + \alpha^2\delta^2 + \beta^2\gamma^2 \\
&= \alpha^2(\gamma^2 + \delta^2) + \beta^2(\gamma^2 + \delta^2) \\
&= (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) \\
&= a \cdot b\,,
\end{aligned}$$

so $a \cdot b$ is the sum of two squares. **END OF PROOF**

Comment. You may be wondering "how on Earth did he figure this out? Where did he get the idea of making this particular choice of μ and ν?"

Here is how I figured it out. If you work with complex numbers $x + iy$ (remembering that $i = \sqrt{-1}$, so $i^2 = -1$), then you can write

$$a = \alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i)\,, \qquad \text{and} \qquad b = \gamma^2 + \delta^2 = (\gamma + \delta i)(\gamma - \delta i)\,.$$

Then

$$\begin{aligned}
a \cdot b &= (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) \\
&= (\alpha + \beta i)(\alpha - \beta i)(\gamma + \delta i)(\gamma - \delta i) \\
&= (\alpha + \beta i)(\gamma + \delta i)(\alpha - \beta i)(\gamma - \delta i) \\
&= \Big(\alpha\gamma - \beta\delta + (\alpha\delta + \beta\gamma)i\Big)\Big(\alpha\gamma - \beta\delta - (\alpha\delta + \beta\gamma)i\Big) \\
&= (\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2\,.
\end{aligned}$$

Naturally, once you have found the formulas for μ and ν you can forget about complex numbers and write the proof as I did.

Problem E is identical to Problem D, so obviously this is just a mistake in the handout, and I will not repeat the solution to Problem D again.

13.5 Solution to Problem F

This statement is false, so it cannot be proved. Here is a proof that it is false.

Let $a = 3$, $b = 5$. Then both a and b are sums of three squares, because $a = 1 + 1 + 1 = 1^2 + 1^2 + 1^2$ and $b = 0 + 1 + 4 = 0^2 + 1^2 + 2^2$. But the product $a \cdot b$ is *not* the sum of three squares, because $a \cdot b = 15$ and 15 is not the sum of three squares. (Reason: the only squares ≤ 15 are 0, 1, 4 and 9. For the sum of three of these to be 15, we need a 9, because otherwise the sum would be at most $4 + 4 + 4$, i.e., 12. So, if one of the squares is going to be 9, the sum of the other two must be 6. But the only squares ≤ 6 are 0, 1, and 4. If the sum of two of these is going to be 6, then one of them has to be 4, but then the other one would be 2, which is not a square.)

13.6 Solution to Problem G

This statement cannot be proved, because it does not follow from the premisses. Here is a proof.

Suppose Olivia is a giraffe, Dolly is a sheep, and there are no cows (i.e., the set of cows is empty). And suppose all giraffes (including Olivia) are very tiny and all sheep (including Dolly) are huge, so sheep are taller than giraffes (and in particular Dolly is taller than Olivia). Then all the premissses would be true. (Premiss (1) would be true vacuously, since there are no cows, so the statement "if x is a cow and y is a sheep then x is taller than y" is true no matter what x and y are, because the premiss "x is a cow and y is a sheep" is false—since "x is a cow" is necessarily false no matter what x is, because there are no cows—and then the implication "if x is cow and y is a sheep then x is taller than y" is true. Premiss (2) is also true for the same reason. Premiss (3) is clearly true. So are (4) and (5).) But the conclusion is false. So ***the conclusion cannot be proved from the premisses, because the conclusion could be false even when the premisses are true.***

COMMENTS. (NOTE: *these comments only apply to you if you got the problem wrong, and wrote a proof that Olivia is taller than Dolly. If you got it right, then my only comment for you is "congratulations!!!!!!"*)

You must be very angry and feeling "cheated." Let me show to you why you should not feel that way at all. Instead, you should feel enriched by the learning experience you have just gone through.

First of all, **you really should have thought that in this problem there was a "catch."** Otherwise, if the problem really was as simple as you thought it was, then why do you think I would have have assigned such a stupid thing to you? The only possible explanation is that something here wasn't as obvious as it seemed!! And you cannot complain that you had not been warned! **You were warned repeatedly about "banana peels,"** i.e., about the possibility that maybe there is something that isn't quite what it appears to be.

Second, I claim that if you really had written the proof carefully, trying to apply the rules *as given in class*, without cheating, then you would have realized that the proof did not work. Let me show you. Here is an attempt to write a proof being very careful and precise. You will see that there is one step where you cannot make the proof go through, because the only way to make it work is to cheat. (By "cheating" I mean "doing something that is not permitted by the rules." It's very much like cheating when you play solitaire.)

An attempted (but of course incorrect) positive solution to problem G, in which we "prove" that under the given premisses Olivia is taller than Dolly:

1. Pick a cow and call her Clarabella. (Note: you could call the cow "Mimi," or "Deirdre," or "Theodora," or "x", if you prefer.)

2. Since Olivia is a giraffe, Clarabella is a cow, and giraffes are taller than cows, Olivia is taller than Clarabella.

3. Since Clarabella is a cow, Dolly is a sheep, and cows are taller than sheep, Clarabella is taller than Dolly.

4. Since Olivia is taller than Clarabella and Clarabella is taller than Dolly, Premiss (3) implies that Olivia is taller than Dolly. **END OF PROOF.**

This a valiant attempt to write a correct proof. However, precisely because it is so good, and in particular so clear and precise, this attempted proof shows clearly where it goes wrong. The mistake is, of course, in Step 1. As we explained in class, *you can pick an object (in this case, a cow) and give it a name provided that you have established before that at least one such object exists.* You are *not* allowed to introduce an object that may fail to exist and give it a name. (We discussed this in class. I showed to you that if you allow that then you can get things like the **Peano paradox**, that is, a "proof" of the obviously false statement that 1 is the largest integer.)

Now, you may have written something that looks more like "let x be an arbitrary cow" rather than "pick a cow and give her a name." And you may think that this is fine, because you have been told that you can write "let x be an arbitrary object such that $blahblahblah(x)$" and you don't need to prove that there exists an x such that $blahblahblah(x)$. And this is indeed true. In fact, to prove that "$\emptyset \subseteq A$ for every set A" we did say "let x be an arbitrary member of $\emptyset$," and then moved on to prove that $x \in A$. Doesn't this appear to justify your "let x be an arbitrary cow" beginning?

The answer is "yes, indeed, it is perfectly legitimate to start a proof with 'let x be an arbitrary cow'. But if you do it carefully, you will still be unable to prove that Olivia is taller than Dolly." Let us try.

1. Let x be an arbitrary cow.
2. Since Olivia is a giraffe, x is a cow, and giraffes are taller than cows, Olivia is taller than x.
3. Since x is a cow, Dolly is a sheep, and cows are taller than sheep, x is taller than Dolly.
4. Since Olivia is taller than x and x is taller than Dolly, Premiss (3) implies that Olivia is taller than Dolly. **END OF PROOF.**

Is this O.K.? **NO!!!!!!!** We have not proved that "Olivia is taller than Dolly." *We have proved that "Olivia is taller than Dolly"* **under the assumption that x is an arbitrary cow**. *The only conclusion that we are allowed to derive from this is*

$$\forall x, (x \text{ is a cow} \Longrightarrow \text{Olivia is taller than Dolly}).$$

In other words, "if you give me a cow, then Olivia is taller than Dolly." To be able to conclude from this that that "Olivia is taller than Dolly" you still need a cow!!! And if there are no cows you certainly will not be able to find one. And there is no way on Earth that you are going to prove that there are cows from the given premisses. (If you knew that there exists a cow, i.e., that $\exists x, x$ is a cow, then you could pick one and call her a—or Clarabella, or Deirdre—so now you would have "a is a cow." Then you could use the specialization rule $\forall_{out}$, explained below, to conclude that

$$a \text{ is a cow} \Longrightarrow \text{Olivia is taller than Dolly}.$$

And since you have "a is a cow", you can use Modus Ponens (Rule $\Longrightarrow_{out}$) to conclude that Olivia is taller than Dolly.)

Here is the question that you should ask yourself. ***Where did I make a mistake? Which step of my "proof" is wrong?*** In many cases, I was unable to figure this out, because what the students wrote was so vague and imprecise that I couldn't tell what the argument was. The two examples of wrong proofs that I have given you above at least have the virtue of being clear and precise, and for that reason I can tell you exactly where they go wrong.

Here is a general principle that you should start thinking about: ***your proofs should be clear enough that I can figure out what each step is and how it is justified. This way, if you make a mistake, e.g. by getting one step wrong, then at least I will be able to tell you where the mistake is.***

Here is a concrete example to illustrate how this principle works: ***many students got Problem B wrong, and actually "proved" that even if you reorder the months there will still necessarily have to be a Friday the 13th.*** All these "proofs" have to be wrong, because I have shown to you that the conclusion is false. However, ***in most cases I was unable to find the mistake***, because the proof was so confusing that I just could not tell what on Earth the argument was supposed to be. (For example, a student wrote that "reordering the months does not make any difference, because there are 7 days and $\mathbb{Z}_7$ is a field." Frankly, I have not idea how the fact that $\mathbb{Z}_7$ is a field could have anything to do with this question. Do you?)

Finally, let me address the question that many of you must be asking. You are probably thinking that

*Q. Of course cows do exist. Everybody knows that there are cows. So the fact that cows exist **is** true, so why cannot I use it?*

This question misses the main point of the problem. The problem was not about proving that a giraffe is taller than a sheep. The problem was about ***proving it from the given assumptions.*** These two things are not at all the same. There are millions of examples of things that are true but ***do not follow*** from other things, even if those other things are also true.

For example, consider the following examples of "logical reasoning":

1. George W. Bush is a former governor of Texas.
2. George W. Bush is the son of a U.S. president.
3. George W. Bush is married to Laura Bush.

CONCLUSION: George W. Bush is president.

1. H. J. Sussmann is a Rutgers professor.
2. H. J. Sussmann is a mathematician.

CONCLUSION: H. J. Sussmann is teaching Math 300.

In these two examples, we have exactly the same situation as in our giraffes-cows-sheep problem: ***the premisses are true, the conclusion is true, but the conclusion does not follow logically (i.e., cannot be proved) from the premisses.*** So my answer to Question Q is:

*A. Sure, everybody knows that G. W. Bush is president, and that H. J. Sussmann is teaching Math 300. But neither of these true statements follows from the premisses listed above. In exactly the same way, we know that if the premisses of Problem G are true, then Olivia is taller than Dolly, but this fact cannot be proved from the premisses alone, without using an extra piece of information that is **not** given, namely, that there exists at least one cow.*

14 More information about the first midterm

The first midterm will be on ***Thursday March 4***. The ***topics covered*** are: chapters 1 and 2 of the book (except for the Russell Paradox) and the notes, Parts 1, 2, 3.

14.1 Questions that will appear in the first midterm test

In the test there will be, ***for sure***, questions of the following kind:

1. ***Translations*** from symbolic language to plain English and back (for example, say "$\forall x \in \mathbb{R}, (x \geq 0 \Longrightarrow \exists y \in \mathbb{R}, y^2 = x)$", or "$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y > x$", or "$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y > x$", in plain English, with words, without using any mathematical symbols and any letter variables; another example: say "every nonnegative integer is the sum of the squares of four integers" in symbolic language; or: say "every member of the set of integers modulo 323 is both even and odd in the integers modulo 323" in symbolic language without using the predicates "even" and "odd').

2. ***Definitions*** of such concepts as even, odd, divisible, prime, tautology, contradiction (see below), union, intersection, empty set, set difference, symmetric difference, subset, power set.

3. ***Truth table problems***, in which you will be asked to write the truth table for some propositional forms, or you will be given some propositional forms and will be asked to tell whether they are tautologies, contradictions, or neither.

4. ***A few informal proofs***, of statements involving integers, or integers modulo n, or sets, of the kind we have done in the course or are done in the book, chapters 1 and 2. This includes, for example, the proof that $\sqrt{2}$ is irrational, i.e., that there exists no rational number whose square is 2. You may be asked to do something similar, e.g., prove that $\sqrt{3}$ is irrational, i.e., that there exists no rational number whose square is 3. Or to prove that a propositional form such as $A \vee B(\Longrightarrow C)$ or $((P \vee Q) \wedge \sim Q) \Longrightarrow (P \vee Q)$ or $((P \vee Q) \wedge (\sim Q))(\Longrightarrow (P \vee Q))$is not well formed. (You would be given the definition of "well formed formula.") Or to prove that the product of two irrational numbers is irrational, or that with the formula for ISBN numbers modulo 11 detects transposition errors. Or to prove that $\forall x \in \mathbb{Z}, x^2 \geq x$, or that $\forall x \in \mathbb{R}, x^2 \geq x$, or that $\forall x \in \mathbb{Z}, x^3 \geq x$, or that union distributes with respect to intersection, or that $\mathcal{P}(A \backslash B) = \mathcal{P}(A) \backslash \mathcal{P}(B)$. ***Don't forget that when you are asked to prove something the answer could be "it's not true, so it cannot be proved; here is a proof that it is not true"***.

5. ***At least one formal proof***, of something simple, for example, that the product of two odd integers is odd, or that the empty set is a subset of every set, or that "if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$."

There will not be any questions about the Russell paradox. The Russell paradox is ***very*** important, but I am not going to ask questions about it in the first midterm, because I want to have time to discuss it in class first. **There will definitely be questions on the Russell paradox in the second midterm and in the final.**

14.2 The definitions of "tautology" and "contradiction"

Recall that we have given a precise defintion of "propositional form" (also known as "sentence form," or "statement form") in the notes, Part 2. As explained there, a propositional form contains letters known as *propositional variables*, and if you give truth values (T or F) to each such variable then the propositional form has a truth value.

Definition 1. A ***tautology*** is a propositional form $\mathcal{F}$ such that $\mathcal{F}$ has the truth value T for every possible way of assigning truth values to the propositional variables that occur in $\mathcal{F}$.

Definition 2. A ***contradiction*** is a propositional form $\mathcal{F}$ such that $\mathcal{F}$ has the truth value F for every possible way of assigning truth values to the propositional variables that occur in $\mathcal{F}$.

14.3 Review: Proof that $\sqrt{2}$ is irrational

Recall that a ***rational number*** is a real number r having the property that there exist integers m, n such that $n \neq 0$ and $r = \frac{m}{n}$. An ***irrational number*** is a real number that is not rational.

We want to prove that there does not exist a rational number r such that $r^2 = 2$. In other words, we want to prove that there do not exist integers m, n such that $n \neq 0$ and $\left(\frac{m}{n}\right)^2 = 2$. Equivalently, we must prove that there do not exist integers m, n such that $n \neq 0$ and $m^2 = 2n^2$. We do the proof by contradiction. Suppose such integers exist. Pick m, n such that $m^2 = 2n^2$, and call them μ, ν, so μ, ν are integers, $\nu \neq 0$, and $\mu^2 = 2\nu^2$. (If you want to call them m and n that's O.K. with me. I don't like it very much, but I will accept it.) If μ is negative, we can change μ to $-\mu$, and the condition $\mu^2 = 2\nu^2$ will still hold with the new μ. So we can assume that $\mu \geq 0$. Simiarly, if ν is negative, we can change ν to $-\nu$, and the condition $\mu^2 = 2\nu^2$ will still hold with the new ν. So we can assume that $\nu > 0$. If both μ and ν are even, then we can divide both of them by 2 (that is, replace μ by $\frac{\mu}{2}$ and ν by $\frac{\nu}{2}$) and we get smaller μ and ν for which the equation $\mu^2 = 2\nu^2$ still holds. If these new μ, ν are still even, we can divide by 2 again, and we can keep doing this until we get μ and ν that are not both even. (That is, one of them is odd, or both are odd.) Now, if μ was odd, μ^2 would be odd, which is not the case, because $\mu^2 = 2\nu^2$. So μ has to be even.

But then we can pick an integer k such that $\mu = 2k$. It folows that

$$2\nu^2 = \mu^2 = 4k^2 \,.$$

So $\nu^2 = 2k^2$. So ν^2 is even. So ν is even, because if ν was odd then ν^2 would have to be odd.

So now we have found that (a) μ and ν are not both even, and (b) μ and ν are both even. These two things together are impossible. So the assumption that there exist integers m, n such that $n \neq 0$ and $m^2 = 2n^2$ has led us to an impossible conclusion. Hence m and n do not exist. **END OF PROOF**

15 Beware of mock turtles!

Many students have repeatedly talked, in the homework, about "the set $A \wedge B$" (in a situation where A and B were two given sets), or "the number $\sim x$" (in a situation where x was some given number, e.g., an integer or a real number).

This is something you should ***never*** do. "$\wedge$" is a *binary logical connective*: it connects two *sentences.* It does not connect things, such as numbers or sets. Similarly, "$\sim$" is a *unary logical connective*: it applies to one *sentence.* not to a thing such as a number or a set. There is no such thing as "the set $A \wedge B$" or "the number $\sim x$"

I think the confusion arises from the following situations: students often see sentences such as "x belongs to A and B", or "$\sim x = 5$", and somehow think that there exists a set called "A and B" to which x belongs, or a number "$\sim x$" which is equal to 5. The cause of the confusion is ***incorrect grouping of words or symbols.***

The classical example of such incorrect grouping is Lewis Carroll's invention of a fictional character called "The Mock Turtle," based on children's common misreading of the words "mock turtle soup" as "(mock turtle) soup", that is, "a soup made of mock turtle", which would require the existence of an animal called "mock turtle" that this soup would be made of. The correct reading is, of course, "mock (turtle soup)", that is, a turtle soup (or, better, a soup which is like turtle soup) but is really an imitation turtle soup. (Actually, "mock turtle soup" is a soup made from a calf's head to resemble turtle soup.)

Similarly, the correct reading of "$\sim x = 5$" is "$\sim (x = 5)$", that is, "x is not equal to 5", or "it's nottrue that $x = 5$." (We don't write the parentheses because they are not needed, since there is no other possible way to read "$\sim x = 5$". You might think that it can be read as "$(\sim x) = 5$", but this would not make any sense, because "$\sim x$" is not anymore real than a mock turtle!

16 Definitions: why they matter and how you should write them.

We have already seen examples of why definitions are important. In Problem 2 of Page 9 of Part 1 of these notes, we asked the question "how many solutions does Problem 1 have?" We reached the conclusion that we could not answer the question because we did not know exactly what the precise meaning of "solution of Problem 1"

If we are asked "is the number 23 small?", we have the same difficulty. I have no idea how to answer this question, because I do not know what "small" means. (Do you? If you think you do, please tell me!) I know what "smaller than" means, but that's a totally different thing!

On the other hand, if we are asked "is the number 18 even?", then we can answer, because we have a precise definition of "even":

> DEFINITION OF "EVEN"
>
> Let n be an integer. We say that n is ***even*** if there exists an integer k such that $n = 2k$.

We can also say this (but we don't have to) using symbolic language:

$$\forall n \in \mathbb{Z}, (n \text{ is } \mathbf{even} \iff \exists k \in \mathbb{Z}, n = 2.k),$$

or, if we have already somehow stipulated that our letter variables take values in the set $\mathbb{Z}$ of all integers:

$$\forall n, (n \text{ is } \mathbf{even} \iff \exists k, n = 2.k),$$

To prove that 18 is even we apply the definition. Since the n of the definition is an ***arbitrary*** integer, we can certainly take $n = 18$. Then we conclude that "18 is even provided that there is an integer k such that $2k = 18$." So now all we need is to prove that "there is an integer k such that $2k = 18$." That is, we have to prove that $\exists k \in \mathbb{Z}, 2k = 18$. (Notice that here k is a ***dummy variable***, because it is ***bound variable***, occurring in a quantified statement under the scope of a quantifier. We could equally well have written this statement as $\exists x \in \mathbb{Z}, 2x = 18$, or $\exists a \in \mathbb{Z}, 2a = 18$, or $\exists q \in \mathbb{Z}, 2q = 18$, or $\exists \alpha \in \mathbb{Z}, 2\alpha = 18$, or $\exists \diamondsuit \in \mathbb{Z}, 2\diamondsuit = 18$, or $\exists \clubsuit \in \mathbb{Z}, 2\clubsuit = 18$, or $\exists \aleph \in \mathbb{Z}, 2\aleph = 18$, or $\exists something \in \mathbb{Z}, 2something = 18$, or $\exists gnu \in \mathbb{Z}, 2gnu = 18$. The predicate "$\exists k, n = 2.k$" is a ***one variable predicate***—the variable being n—because in order to decide whether "$\exists k, n = 2.k$" is true you need to ask me what n is. And the predicate "$\exists k, 18 = 2.k$" is a ***zero variables predicate***—i.e., a statement—because in order to decide whether "$\exists k, 18 = 2.k$" is true you don't need to ask me anything, because you can figure out whether the sentence is true or not all by yourself.)

Now recall our Rule $\exists_{in}$:

> **To prove that there exists a thing such that something involving this thing happens, you show one (that is, you exhibit a witness).**
>
> For example: to prove that there exists a town in New Jersey with a population larger that 10,000, you say "for instance, Piscataway has more than 10,000 people." (Naturally, you could also have used Trenton, or Princeton, or New Brunswick.)

So, to prove that $\exists k \in \mathbb{Z}, 2c = 18$ you must exhibit an integer k such that $2k = 18$. The obvious choice (in fact the only choice) is 9. Since $2.9 = 18$, and 9 is an integer, it is true that $\exists k \in \mathbb{Z}, 2k = 18$. So 18 is even.

This definition takes care, in a completely unambiguous way, of questions that students sometimes ask in class. For example, students sometimes ask "is 0 even?", or "is 0 considered even?" My answer to that question is "if the definition of even implies that 0 is even then 0 is even; if the definition of even implies that 0 is not even then 0 is not even; to decide whether 0 is or is not even, apply the definition." So, you see, *having a precise definition of "even" enables you to settle the question whether something is even in cases* *when you are in doubt.* (I should have said "even in cases when you are in doubt," but that would have looked bad, wouldn't it?)

Now consider the definition of "prime." Is 3 prime? Is 6 prime? Is 1 prime? Students often say vague, fuzzy things such as "a prime number is a number that has no factors." Now, *this purported definition is either wrong or so vague that you cannot work with it.* Actually, every integer has "factors", since, for example, every integer is divisible by itself and by 1. So if one takes the definition literally, then no integer is prime, and the definition is wrong, because this is obviously, not what you want! So maybe you didn't quite mean that. So, what ***did*** you mean? Maybe when you said "no factors" you meant "no factors other than itself and 1." But then, again, that would not work, because every integer is also divisible by -1. So maybe you mean "a prime number is a natural number that has no natural number factors other than 1 and itself." Now, this is a precise definition, but turns out not to be a good one, because according to this definition 1 would be prime, and there are millions of reasons why we do not want to count 1 as prime. (For example: we want every natural number > 1 to be uniquely expressible as a prime or a product of primes. If 1 was a prime, then we would have $6 = 2.3$, but also $6 = 1.2.3$, and $6 = 1.1.1.1.1.1.1.1.1.2.3$, and this would violate the uniqueness of the factorization.)

So, the usual ways of defining "prime" that students are used to are too vague to be useful. That's why we give a precise definition:

DEFINITION OF "PRIME"

Let n be an integer. We say that n is ***prime*** if $n > 1$ and there do not exist integers p, q such that $n = p.q$ and $1 < p < n$.

We can also say this (but we don't have to) using symbolic language:

$$\forall n \in \mathbb{Z}, \Big(n \text{ is } \textbf{prime} \iff (n > 1 \wedge \sim \exists p \in \mathbb{Z}, \exists q \in \mathbb{Z}, (n = p.q \wedge 1 < p < n))\Big),$$

or, if we have already somehow stipulated that our letter variables take values in the set $\mathbb{Z}$ of all integers:

$$\forall n, \Big(n \text{ is } \textbf{prime} \iff (n > 1 \wedge \sim \exists p, \exists q, (n = p.q \wedge 1 < p < n))\Big).$$

This definition is truly useful, in the sense that you can work with it. If I give you any integer, you can actually use the definition and decide whethet the given integer is or is not prime.

Similarly, if I am asked whether Star Trek's Mr. Spock has a brother, then I need a definition of "brother" that I can work with. And, when I try to write down such a definition, I am faced with the problem that the word "brother," as is commonly used, is ambiguous, because sometimes we want to allow half brothers to count as brothers and sometimes don't. (And we also have to decide whether we are just dealing with human beings or we also count animals. Here, for simplicity, I will just work with humans.) So we have two possible "formal" definitions of "brother":

> FIRST DEFINITION OF "BROTHER"
>
> Let n, m be human beings. We say that n is a ***brother*** of m if n is male, $n \neq m$, and the two parents of n are also the parents of m.

We can also say this using symbolic language, if we write $\mathbb{P}$ for "the set of all human beings":

$$\forall n \in \mathbb{P}, \forall m \in \mathbb{P}, \Big(n \text{ is a } \textbf{brother} \text{ of } m \Longleftrightarrow ((n \text{ is male}$$

$$\wedge n \neq m) \wedge \forall k \in \mathbb{P}, (k \text{ is a parent of } n \Longrightarrow k \text{ is a parent of } m))\Big)$$

> SECOND DEFINITION OF "BROTHER"
>
> Let n, m be human beings. We say that n is a ***brother*** of m if n is male, $n \neq m$, and at least one of the two parents of n is also a parent of m.

Again, we can athis using symbolic language:

$$\forall n \in \mathbb{P}, \forall m \in \mathbb{P}, \Big(n \text{ is a } \textbf{brother} \text{ of } m \Longleftrightarrow ((n \text{ is male}$$

$$\wedge n \neq m) \wedge \exists k \in \mathbb{P}, (k \text{ is a parent of } n \wedge k \text{ is a parent of } m))\Big)$$

These definitions are truly useful. And now we can decide whether Mr. Spock has a brother: if we adopt the first definition, he does not, but if we use the second definition he does. (To be even more precise: everybody knows that Mr. Spock has an evil half-brother, so he does have a "brother" in the sense of the second definition. But I am not aware of Mr. Spock having a brother in the sense of the first definition.)

Similarly, suppose I have to answer the question "Are John Kerry and Laura Bush married?" If I try to understand what this means, precisely, I run into the fact that the predicate "married" is ambiguous, because when you are talking about two people, "being married" could mean "being married to each other," or "being married each one separately." So the ambiguity here arises because, *there really are two predicates "married": one is the one-variable predicated "begin married to somebody", and the other one is the two-variable predicate "being married to each other."* Let us call these predicates "married$_1$" and "married$_2$". Then we can give formal definitions:

DEFINITION OF "MARRIED$_2$"

Let n, m be human beings. We say that n and m are ***married***$_2$ if they have been legally declared spouses of each other.

DEFINITION OF "MARRIED$_1$"

Let n be a human being. We say that n is ***married***$_1$ if there exists m such that n and m are married$_2$.

16.1 Definitions and arguments

From the previous examples, you can see that

Predicates have ***arguments***, so when you define a predicate you have to begin by specifying what the arguments are, and in particular it has to be clear from your definition how many arguments there are. These arguments connect the definition with the rest of the world. For example, the definitions of "even," "prime," and "married$_1$" have **one** argument each, so they enable you to plug in **one** object and get a true-false conclusion. The definitions of "divisible," "brother," and "married$_2$ " have **two** arguments. You plug in **two** things to get a true-false conclusion.

When you write a definition you should first of all figure out how many arguments will be involved, and then you should make sure that the definition begins by introducing these arguments.

Example 9. Let us figure out on our own, step by step, how to define "divisible." First of all, "divisible" is a word that talks about two numbers. (We do not talk about one number being "divisible." We talk about one number being "divisible" by another number.) So if we set out to write a definition of "divisible" we have to start by introducing our two arguments: "Let a and b be numbers." Moreover, the "numbers" involved, cannot just be any numbers. They have to be *integers*. So we really have to start with "Let a and b be integers." Now that we know who we are talking about (that is, we have properly introduced our two arguments) we are ready to say what we want to say. We want to explain what it means for a to be divisible by b. So we write "We say that a is *divisible* by b if (or 'provided that') XXXXXXXXXXX." Now what is missing is XXXXXXXXXXX. We already have the *structure* of our definition:

> Let a and b be integers. We say that a is *divisible* by b if XXXXXXXXXXX.

and we have to fill in the contents.

So far, all that mattered is that "divisible" is something about two integers. Now we have to say what that "something" is. In our case, the thing to put in the XXXXXXXXX slot is "$\exists c \in \mathbb{Z}, bc = a$," and we end up with

Let a and b be integers. We say that a is
divisible by b if $\exists c \in \mathbb{Z}, bc = a$.

Example 10. Let us figure out on our own, step by step, how to define "grandson" for the benefit of someone who knows what "father," "mother" and "male" mean. First of all, "grandson" is a word that talks about two people. (We do not talk about one person being "a grandson." We talk about one person being another person's "grandson.") So if we set out to write a definition of "grandson" we have to start by introducing our two arguments: "Let a and b be persons." Now that we know who we are talking about (that is, we have introduced our two arguments) we are ready to say what we want to say. We want to explain what it means for a to be a grandson of b. So we write "We say that a is a *grandson* of b if (or 'provided that') XXXXXXXXX." Now what is missing is XXXXXXXXX. We already have the *structure* of our definition:

Let a and b be persons. We say that a is a *grandson* of b
if XXXXXXXX.

and we have to fill in the contents. (So far, all that mattered is that "grandson" is something about two persons. Now we must say what that "something" is.)

In our case, the thing to put in the XXXXXX slot seems to be "b is a parent of someone who is a parent of a," that is,

"$\exists c, (c$ is a person and c is a parent of a and b is a parent of c)."

But a moment's thought shows that this is not enough. We are trying to define *grandson*, not *grandchild*. So we have to make sure that a is male.

The final result is

Let a and b be persons. We say that a is a *grandson* of b if
a is male and
$\exists c, (c$ is a person and c is a parent of a and b is a parent of c).

16.2 Always highlight the definiendum

When you write a definition, you are defining a particular word or phrase. That word or phrase is called the *definiendum*. (This just means "the thing being defined.") **The definiendum should always be highlighted.** In books, the authors do this by using Italics, or Boldface. (Look, for example, at any definitions you want in our textboook) When you write your homework or your exams, or when I write on the blackboard, it's hard to do Italics, so we use underlining instead.

16.3 More than two variables?

As you probably have guessed by now, there are three-variable predicates, four-variable predicates, and so on. For example, "common divisor" is a three-variable predicate: let a, b, c be integers; we say that a is a ***comon divisor*** of b and c if b is divisible by a and c is divisible by a. (Note: I could have said "b and c are divisible by a," but then someone who believes in the existence of the Mock Turtle might have drawn from this the wrong conclusion that there is a number called "b and c.")

17 Integer Arithmetic

17.1 The basic vocabulary of integer arithmetic

I. The **logical connectives:**

1. The **propositional connectives:**
   a. the *negation symbol* ("$\sim$ ...", read as "not ...", or "it is not the case that ..."),
   b. the *conjunction symbol* ("... $\wedge$ ...", read as "... and ..."),
   c. the *disjunction symbol* ("... $\vee$ ...", read as "... or ..."),
   d. the *implication symbol* ("... $\Longrightarrow$ ...", read as "... implies ...", or "if,... then ..."),
   e. the *biconditional symbol* ("... $\Longleftrightarrow$ ...", read as "... if and only if ..."),
2. The **quantifiers:**
   a. the *existential quantifier* ("$\exists$ ...", read as "there exists ... such that");
   b. the *universal quantifier* ("$\forall$ ...", read as "for all ...");
3. The **right and left parentheses and the comma.**

II. The **letter variables:** a, b, ..., i, j, k, ..., m, n, p, q, ..., x, y, z, ... (In principle, any symbol can be used as a variable, provided you declare it as such. This includes Greek letters such as α, β, etc., Hebrew or Arabic letters, weird symbols such as $\diamondsuit$ or $\clubsuit$,

II. **The arithmetical symbols:**

a. the *constants* "0" ("zero") and "1" ("one"),

b. the *symbols for the arithmetical operations*: "+" ("plus") and "$\cdot$" ("times", sometimes written "$\times$"),

c. the *minus* (or *negative*) *symbol*: "$-$" (read "minus", or "negative"),

d. the *predicates:* "=" ("is equal to", or "equals") , "<" ("is less than", or "is smaller than"), ">" ("is larger than"), "$\leq$" ("is less than or equal to", or "is not greater than"), "$\geq$" ("is greater than or equal to", or "is not smaller than").

If you want, you can also include the predicates "$\in \mathbb{N}$" ("belongs to $\mathbb{N}$", or "is a natural number", or "is a nonnegative integer") and "$\in \mathbb{Z}$" ("belongs to $\mathbb{Z}$", or "is an integer"). This, however, is not necessary, strictly speaking, because

A. If it is clear that we are just talking about the integers, then *everything is an integer*, so there is not need to say "x is an integer" every time we bring in an object x, because x couldn't possibly be anything other than an integer. So if this is the case then "$\in \mathbb{Z}$" is not needed.

B. The predicate "$\in \mathbb{N}$" is unnecessary, because instead of saying "$x \in \mathbb{N}$" you could just say "$x > 0$", or "$0 < x$."

On the other hand,

C. If you include the predicate "$\in \mathbb{N}$" then you do not need to include the predicates $<$, $>$, $\leq$, and $\geq$, because you can *define* them in terms of the other symbols together with "$\in \mathbb{N}$". (This is what Problem 4 of page 5 of the book is about.)

D. If you want to talk about integers and also things that are not integers (e.g., sets, lists, integers modulo n), then you need the predicate "$\in \mathbb{Z}$ to specify when the things you are talking about are supposed to be integers.

Here are four versions of the basic vocabulary. Version I is used if the universe of discourse is $\mathbb{Z}$, i.e., if we are talking about integers only. Version II can be substituted for Version I. Version III is used if the universe of discourse contains $\mathbb{Z}$ and other things as well, i.e., if we are talking about integers and also other things. Version IV can be substituted for Version III.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION I

$$\sim \quad \wedge \quad \vee \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad < \quad > \quad \leq \quad \geq \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION II

$$\sim \quad \wedge \quad \vee \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad \in \mathbb{N} \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION III

$$\sim \quad \wedge \quad \vee \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad < \quad > \quad \leq \quad \geq \quad \in \mathbb{Z} \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE BASIC VOCABULARY OF INTEGER ARITHMETIC, VERSION IV

$$\sim \quad \wedge \quad \vee \Longrightarrow \quad \Longleftrightarrow \quad \exists \quad \forall \quad (\quad) \quad ,$$

$$= \quad \in \mathbb{N} \quad \in \mathbb{Z} \quad 0 \quad 1 \quad + \quad - \quad \cdot$$

and the variables.

THE AXIOMS OF INTEGER ARITHMETIC

RING AXIOMS

RA1. $\forall x, \forall y, x + y = y + x.$

RA2. $\forall x, \forall y, x.y = y.x.$

RA3. $\forall x, \forall y, \forall z, (x + y) + z = x + (y + z).$

RA4. $\forall x, \forall y, \forall z, (x.y).z = x.(y.z).$

RA5. $\forall x, \forall y, \forall z, (x + y).z = x.z + y.z.$

RA6. $\forall x, x + 0 = x.$

RA7. $\forall x, x + (-x) = 0.$

RA8. $\forall x, x.1 = x.$

RA9. $\forall x, \forall y, \forall z, \Big((y.x = z.x \wedge \sim x = 0) \Longrightarrow y = z\Big).$

RA10. $\sim 1 = 0.$

ORDER AXIOMS

OA1. $\forall x, \forall y, (x > y \Longleftrightarrow y < x)$

OA2. $\forall x, \forall y, (x \leq y \Longleftrightarrow (x < y \vee x = y))$

OA3. $\forall x, \forall y, (x \geq y \Longleftrightarrow (x > y \vee x = y))$

OA4. $\forall x, \forall y, ((0 < x \wedge 0 < y) \Longrightarrow 0 < x + y)$

OA5. $\forall x, \forall y, ((0 < x \wedge 0 < y) \Longrightarrow 0 < x.y)$

OA6. $\forall x, \forall y, (x < y \Longleftrightarrow 0 < y + (-x))$

OA7. $\forall x, (0 \leq x \vee x \leq 0)$

OA8. $\sim 0 < 0$

THE PRINCIPLE OF MATHEMATICAL INDUCTION

PMI. Let u be a variable, and let $p(u)$ be a formula that contains no u-quantifiers. Then

$$\Big(p(1) \wedge \forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u+1))\Big) \Longrightarrow \forall u, (u > 0 \Longrightarrow p(u)).$$

THEOREM T1. $-0 = 0$.

PROOF.

$$-0 = (-0) + 0 \qquad \boxed{\text{RA6}}$$

and

$$(-0) + 0 = 0 \qquad \boxed{\text{RA7}}$$

So $-0 = 0$. **THE END**

DEFINITION D1. $2 = 1 + 1$.

DEFINITION D2. $3 = 2 + 1$.

DEFINITION D3. $4 = 3 + 1$.

THEOREM T2. $2 + 2 = 4$.

PROOF.

$$\begin{aligned} 2 + 2 &= 2 + (1 + 1) && \boxed{\text{D1}} \\ &= (2 + 1) + 1) && \boxed{\text{RA3}} \\ &= 3 + 1) && \boxed{\text{D2}} \\ &= 4 && \boxed{\text{D3}} \end{aligned}$$

THE END

THEOREM T3. $2.2 = 4$.

PROOF.

$$\begin{aligned} 2.2 &= 2.(1 + 1) && \boxed{\text{D1}} \\ &= 2.1 + 2.1 && \boxed{\text{RA5}} \\ &= 2 + 2 && \boxed{\text{RA8}} \\ &= 4 && \boxed{\text{T2}} \end{aligned}$$

THE END

THEOREM T4. $\forall x, x.0 = 0$.

PROOF. Let x be arbitrary. Then

$$\begin{aligned} x.0 &= x.0 + 0 && \boxed{\phantom{\text{RA0}}} \\ &= x.0 + (x.0 + (-(x.0))) && \boxed{\phantom{\text{RA0}}} \\ &= (x.0 + x.0) + (-(x.0)) && \boxed{\phantom{\text{RA0}}} \\ &= x.(0 + 0) + (-(x.0)) && \boxed{\phantom{\text{RA0}}} \\ &= x.0 + (-(x.0)) && \boxed{\phantom{\text{RA0}}} \\ &= 0 && \boxed{\phantom{\text{RA0}}} \end{aligned}$$

THE END

THEOREM T5. $\forall x, \forall y, \forall z, x.(y+z) = x.y + x.z.$

PROOF. Let x, y, z be arbitrary. Then

$$\begin{aligned} x.(y+z) &= (y+z).x && \boxed{\text{RA2}} \\ &= y.x + z.x && \boxed{\text{RA5}} \\ &= x.y + x.z && \boxed{\text{RA2}} \end{aligned}$$

THE END

THEOREM T6. $(-1).(-1) = 1.$

PROOF.

$$\begin{aligned} (-1).(-1) &= (-1).(-1) + 0 \\ &= (-1).(-1) + (1 + (-1)) \\ &= (-1).(-1) + (1 + (-1).1) \\ &= (-1).(-1) + ((-1).1 + 1) \\ &= ((-1).(-1) + (-1).1) + 1 \\ &= (-1).((-1) + 1) + 1 \\ &= (-1).(1 + (-1)) + 1 \\ &= (-1).0 + 1 \\ &= 0 + 1 \\ &= 1 + 0 \\ &= 1 \end{aligned}$$

THE END

THEOREM T7. $\forall x, (-1).x = -x.$

PROOF. Let x be arbitrary. Then

$$\begin{aligned} (-1).x &= (-1).x + 0 \\ &= (-1).x + (x + (-x)) \\ &= ((-1).x + x) + (-x) \\ &= (x.(-1) + x) + (-x) \\ &= (x.(-1) + x.1) + (-x) \\ &= x.((-1) + 1) + (-x) \\ &= x.(1 + (-1)) + (-x) \\ &= x.0 + (-x) \\ &= 0 + (-x) \\ &= (-x) + 0 \\ &= -x\,. \end{aligned}$$

THE END

THEOREM T8. $\forall x, x.(-1) = -x$.

PROOF. Let x be arbitrary. Then $x.(-1) = (-1).x = -x$.

THEOREM T9. $\forall x, -(-x) = x$.

PROOF. Let x be arbitrary. Then

$$\begin{aligned} -(-x) &= (-x).(-1) \\ &= (x.(-1)).(-1) \\ &= x.((-1).(-1)) \\ &= x.1 \\ &= x \end{aligned}$$

THE END

THEOREM T10. $\forall x, \forall y, -(x+y) = (-x) + (-y)$.

PROOF. Let x, y be arbitrary. Then

$$\begin{aligned} -(x+y) &= (x+y).(-1) \\ &= x.(-1) + y.(-1) \\ &= (-x) + (-y) \end{aligned}$$

THE END

DEFINITION D4. $\forall x, \forall y, x - y = x + (-y)$.

THEOREM T11. $\forall x, \forall y, \forall z, (x - y = z \Longleftrightarrow x = y + z)$.

PROOF. Let x, y, z be arbitrary. Assume $x - y = z$. Then

$$\begin{aligned} x &= x + 0 \\ &= x + (y + (-y)) \\ &= x + ((-y) + y) \\ &= (x + (-y)) + y \\ &= (x - y) + y \\ &= z + y \\ &= y + z \end{aligned}$$

So $x - y = z \Longrightarrow x = y + z$.

Now suppose $x = y + z$. Then

$$\begin{aligned} x - y &= x + (-y) \\ &= (y + z) + (-y) \\ &= (z + y) + (-y) \\ &= z + (y + (-y)) \\ &= z + 0 \end{aligned}$$

$$= z$$

So $x = y + z \Longrightarrow x - y = z$. **THE END**

THEOREM T12. $\forall x, \forall y, -(x - y) = y - x$.

PROOF. Let x, y be arbitrary. Then

$$\begin{aligned}
-(x - y) &= (x - y).(-1) \\
&= (x + (-y)).(-1) \\
&= x.(-1) + (-y).(-1) \\
&= x.(-1) + ((y.(-1)).(-1)) \\
&= (-x) + y.((-1).(-1)) \\
&= (-x) + y.1 \\
&= (-x) + y \\
&= y + (-x) \\
&= y - x
\end{aligned}$$

THE END

DEFINITION D5. $\forall x, (x \text{ is even } \Longleftrightarrow \exists y, x = 2.y)$.

DEFINITION D6. $\forall x, (x \text{ is odd } \Longleftrightarrow \exists y, x = 2.y + 1)$.

THEOREM T13. $\forall x, \forall y, ((x \text{ is even } \wedge y \text{ is even }) \Longrightarrow x + y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x and y are even. Since x is even, $\exists u, x = 2.u$. Pick one such u and call it a. Since y is even, $\exists u, y = 2.u$. Pick one such u and call it b. Then $x = 2.a$ and $y = 2.b$. So $x + y = 2.(a + b)$. So $\exists u, x + y = 2.u$. So $x + y$ is even. **THE END**

THEOREM T14. $\forall x, \forall y, ((x \text{ is even } \wedge y \text{ is odd }) \Longrightarrow x + y \text{ is odd })$

PROOF. Let x, y be arbitrary. Suppose x is even and y is odd. Since x is even, $\exists u, x = 2.u$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u + 1$. Pick one such u and call it b. Then $x = 2a$ and $y = 2.b + 1$. So $x + y = 2.(a + b) + 1$. So $\exists u, x + y = 2.u + 1$. So $x + y$ is odd. **THE END**

THEOREM T15. $\forall x, \forall y, ((x \text{ is odd } \wedge y \text{ is odd }) \Longrightarrow x + y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x and y are odd. Since x is odd, $\exists u, x = 2.u + 1$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u + 1$. Pick one such u and call it b. Then $x = 2a + 1$ and $y = 2.b + 1$. So $x + y = (2.a + 1) + (2.b + 1) = 2.(a + b + 1)$. So $\exists u, x + y = 2.u$. So $x + y$ is even. **THE END**

THEOREM T16. $\forall x, \forall y, (x \text{ is even } \Longrightarrow x.y \text{ is even })$

PROOF. Let x, y be arbitrary. Suppose x is even. Then $\exists u, x = 2.u$. Pick one such u and call it a. Then $x = 2.a$. So $x.y = (2.a).y = 2.(x.y)$. So $\exists u, x.y = 2.u$. So $x.y$ is even. **THE END**

THEOREM T17. $\forall x, \forall y, ((x \text{ is odd } \wedge y \text{ is odd }) \Longrightarrow x.y \text{ is odd })$

PROOF. Let x, y be arbitrary. Suppose x and y are odd. Since x is odd, $\exists u, x = 2.u+1$. Pick one such u and call it a. Since y is odd, $\exists u, y = 2.u+1$. Pick one such u and call it b. Then $x = 2a + 1$ and $y = 2.b + 1$. So $x.y = (2.a + 1).(2.b + 1) = 4.a.b + 2.a + 2.b + 1 = 2(2.a.b + a + b) + 1$. So $\exists u, x.y = 2.u + 1$. So $x.y$ is odd. **THE END**

THEOREM T18. $\forall x, (x \text{ is odd } \Longleftrightarrow x + 1 \text{ is even })$

PROOF. Let x be arbitrary. Suppose x is odd. Then $\exists u, x = 2.u + 1$. Pick one such u and call it a. Then $x + 1 = (2.a + 1) + 1 = 2.(a + 1)$. So $\exists u, x + 1 = 2.u$. So $x + 1$ is even.

Now suppose $x + 1$ is even. Then $\exists u, x + 1 = 2.u$. Pick one such u and call it a. Then $x + 1 = 2.a$. Therefore $x = 2.a - 1 = 2.(a - 1) + 1$. So $\exists u, x = 2.u + 1$. So x is odd. **THE END**

THEOREM T19. $\forall x, x \leq x$.

PROOF. Let x be arbitrary. Then $x \leq x \Longleftrightarrow (x < x \vee x = x)$ by OA2. But $x = x$, so "$x < x \vee x = x$" is true, and then $x \leq x$. **THE END**

THEOREM T20. $\forall x, \forall y, (x < y \Longleftrightarrow 0 < y - x)$.

PROOF. This follows trivially from OA6 and D4. **THE END**

THEOREM T21. $\forall x, \forall y, (x \leq y \Longleftrightarrow 0 \leq y - x)$.

PROOF. Let x, y be arbitrary. Suppose $x \leq y$. Then $x < y \vee x = y$ by OA2. If $x < y$ then $0 < y+(-x)$ by OA6, and $y+(-x) = y-x$ by D4, so $0 < y-x$, and then $0 \leq y - x$ by OA2. If $x = y$ then $y - x = x - x = x + (-x) = 0$, so $\leq y - x$, because $0 \leq 0$ by T19. So in both cases $(x < y$ and $x = y)$ the conclusion $0 \leq y - x$ follows. Therefore $x \leq y \Longrightarrow 0 \leq y - x$.

Now suppose $0 \leq y - x$. Then $0 < y - x \vee 0 = y - x$ by OA2. If $0 = y - x$ then

$$y = y + 0 = y + (x + (-x)) = y + ((-x) + x) = (y + (-x)) + x$$

$$= (y - x) + x = 0 + x = x + 0 = x\,,$$

so $y = x$. Then $x \leq y$ by OA2. If $0 < y - x$, then $0 < y + (-x)$, so $x < y$ by OA6, and then $x \leq y$ by OA2. So in both cases $(0 < y - x$ and $0 = y - x)$ the conclusion $x \leq y$ follows. Therefore $0 \leq y - x \Longrightarrow x \leq y$.

Since $x \leq y \Longrightarrow 0 \leq y - x$ and $0 \leq y - x \Longrightarrow x \leq y$, the conclusion $x \leq y \Longrightarrow 0 \leq y - x$ follows. **THE END**

THEOREM T22. $\forall x, \forall y, ((0 \leq x \wedge 0 < y) \Longrightarrow 0 < x + y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 < y$. Then $0 = x$ or $0 < x$ by OA2. If $0 = x$ then $x + y = 0 + y = y + 0 = y$, so the fact that $0 < y$ implies that $0 < x + y$. If $0 < x$ then OA5 implies $0 < x + y$. **THE END**

THEOREM T23. $\forall x, \forall y, ((0 \leq x \wedge 0 \leq y) \Longrightarrow 0 \leq x + y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 \leq y$. If $0 < x$ or $0 < y$ we can use T22 and conclude that $0 < x + y$, so $0 \leq x + y$. If $x = 0$ and $y = 0$ then $x + y = 0 + 0 = 0$, so $0 \leq x + y$. **THE END**

THEOREM T24. $\forall x, \forall y, \forall z, \forall u, ((x \leq y \wedge z < u) \Longrightarrow x + z < y + u)$.

PROOF. Let x, y, z, u be arbitrary. Assume that $x \leq y \wedge z < u$. Then $0 \leq y - x$ by T20, and $0 < u - z$ by T21. So $0 < (y - x) + (u - z)$ by T22. But $(y - x) + (u - z) = (y + u) - (x + z)$. So $0 < (y + u) - (x + z)$, and then $x + z < y + u$ by T14. **THE END**

THEOREM T25. $\forall x, \forall y, \forall z, \forall u, ((x \leq y \wedge z \leq u) \Longrightarrow x + z \leq y + u)$.

PROOF. Let x, y, z, u be arbitrary. If $x < y$ or $z < u$ then we can apply T24 and conclude that $x + z < y + u$, so $x + z \leq y + u$. If $x = y$ and $z = u$ then $x + z = y + u$, so $x + z \leq y + u$. **THE END**

THEOREM T26. $\forall x, \forall y, ((0 \leq x \wedge 0 \leq y) \Longrightarrow 0 \leq x.y)$.

PROOF. Let x, y be arbitrary. Assume that $0 \leq x \wedge 0 \leq y$. If both $\sim x = 0$ and $\sim y = 0$, then OA2 implies that $0 < x$ and $0 < y$, so $0 < x.y$ by OA5, and then $0 \leq x.y$ by OA2. If $x = 0 \vee y = 0$ then $x.y = 0$ by T4, so $0 \leq x.y$, because $0 \leq 0$. **THE END**

THEOREM T27. $\forall x, \forall y, \forall z, ((x \leq y \wedge 0 \leq z) \Longrightarrow x.z \leq y.z)$.

PROOF. Let x, y, z be arbitrary. Assume that $x \leq y \wedge 0 \leq z$. Then $0 \leq y - x$ by T21. So $0 \leq (y - x).z$ by T26. But

$$(y - x).z = (y + (-x)).z = y.z + (-x).z = y.z + ((-1).x).y$$

$$= y.z + (-1).(x.y) = y.z + (-(x.y)) = y.z - x.y\,.$$

So $0 \leq y.z - x.z$, and then T21 tells us that $x.z \leq y.z$. **THE END**

THEOREM T28. $\forall x, \forall y, (((\sim x = 0) \wedge \sim y = 0) \Longrightarrow (\sim x.y = 0))$.

PROOF. Let x, y be arbitrary. Assume that $(\sim x = 0) \wedge \sim y = 0$. By OA7, $0 \leq x \vee x \leq 0$. If $0 \leq x$, then $0 < x$, because $0 < x \vee 0 = x$ by OA2, and $\sim 0 = x$. If $x \leq 0$, then $x < 0$, because $x < 0 \vee x = 0$ by OA2, and $\sim x = 0$, and this implies that $0 < -x$, because OA6 says that

$x < 0 \Longleftrightarrow 0 < 0 + (-x)$, and $0 + (-x) = -x$. So "$0 < x \vee 0 < -x$" is true if $0 \le x$ and also if $x \le 0$. Since $0 \le x \vee x \le 0$, we have established that $0 < x \vee 0 < -x$. Similarly, $0 < y \vee 0 < -y$.

So one of the following four possibilities hold:

(1) $0 < x \wedge 0 < y$,

(2) $0 < x \wedge 0 < -y$,

(3) $0 < -x \wedge 0 < y$,

(4) $0 < -x \wedge 0 < -y$.

If (1) holds, then $0 < x.y$ by OA5. Therefore $\sim x.y = 0$, because if $x.y = 0$ it would follow that $0 < 0$, contradicting OA8.

If (2) holds, then $0 < x.(-y)$ by OA5. Therefore $\sim x.(-y) = 0$, because if $x.(-y) = 0$ it would follow that $0 < 0$, contradicting OA8. Then $\sim x.y = 0$, because if $x.y = 0$ we would have $x.(-y) = x.((-1).y) = (x.(-1)).y = ((-1).x).y) = (-1).(x.y) = -(x.y) = -0 = 0$, contradicting the fact that $\sim x.(-y) = 0$.

Cases (3) and (4) are handled similarly. **THE END**

THEOREM T29. $\forall x, \forall y, ((x \le y \wedge y \le x) \Longrightarrow x = y)$.

PROOF. Let x, y be arbitrary. Suppose $x \le y \wedge y \le x$. We prove that $x = y$ by contradiction. Suppose $\sim x = y$. Then OA2 tells us that $x < y \vee x = y$. Since $\sim x = y$, we have $x < y$. Then OA6 and D4 imply that $0 < y - x$. Similarly, $0 < x - y$. Then OA4 implies that $0 < (y - x) + (x - y)$, and a simple calculation shows that $(y - x) + (x - y) = 0$. So $0 < 0$, contradicting OA8. **THE END**

THEOREM T30. $\forall x, \forall y, \forall z, ((x \le y \wedge y \le z) \Longrightarrow x \le z)$.

PROOF. Let x, y, z be arbitrary. Suppose $x \le y \wedge y \le z$. Then $0 \le y - x$ and $0 \le z - y$ by T21. So $0 \le (y-x)+(z-y)$ by T23. But $(y-x)+(z-y) = z-x$. So $0 \le z - x$, and then T21 implies $x \le z$. **THE END**

THEOREM T31. $0 < 1$.

PROOF. OA7 tells us that $0 \le 1 \vee 1 \le 0$. We consider separately the two cases $0 \le 1$ and $1 \le 0$, and show that $0 < 1$ in each case.

First suppose that $0 \le 1$. Then $0 < 1 \vee 0 = 1$ by OA2. But $\sim 0 = 1$ by RA10. So $0 < 1$, as desired.

Now suppose that $1 \le 0$. Then $1 < 0 \vee 1 = 0$ by OA2. But $\sim 1 = 0$ by RA10. So $1 < 0$. But OA6 tells us that $1 < 0 \Longleftrightarrow 0 < 0 + (-1)$. So $0 < 0+(-1)$, and then $0 < -1$. It then follows from OA4 that $0 < (-1).(-1)$. But $(-1).(-1) = 1$ by T6. So $0 < 1$, as desired. **THE END**

THEOREM T32. $-1 < 0$.

PROOF. OA6 implies that $-1 < 0 \Longleftrightarrow 0 < 0 + (-(-1))$. But $-(-1) = 1$ by T9. So $-1 < 0 \Longleftrightarrow 0 < 1$. Since $0 < 1$ by T31, we have $-1 < 0$. **THE END**

THEOREM T33. $0 < 2$.

PROOF. Since $0 < 1$ by T31, OA5 implies that $0 < 1 + 1$, i.e., that $0 < 2$. **THE END**

THEOREM T34. $2 \neq 0$.

PROOF. Since $0 < 2$ by T33, OA8 implies that $2 \neq 0$, because if $2 = 0$ then "$0 = 0$" would be true, contradicting OA8. **THE END**

THEOREM T35. $\forall x, (x \leq 0 \vee 1 \leq x)$.

PROOF. Let x be arbitrary. Suppose $\sim x \leq 0$. We will prove that $1 \leq x$.

By OA7, $x \leq 0 \vee 0 \leq x$. Since $\sim x \leq 0$, we have $0 \leq x$. Therefore $0 = x \vee 0 < x$ by OA2. But "$0 = x$" isn't true, because if $0 = x$ it would follow that $x \leq 0$, and we are assuming that $\sim x \leq 0$. So $0 < x$.

We want to prove that $1 \leq x$. We will do it by using the PMI. Let $p(u)$ be the predicate "$1 \leq u$". Then $p(1)$ is true, because of T19. Let us prove that $\forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u+1))$, i.e., that $\forall u, ((u > 0 \wedge 1 \leq u) \Longrightarrow 1 \leq u+1)$.

Let u be arbitrary. We want to prove $(u > 0 \wedge 1 \leq u) \Longrightarrow 1 \leq u + 1$. Assume $u > 0 \wedge 1 \leq u$. We want to prove $1 \leq u + 1$. T24 implies that $(1 \leq u \wedge 0 < 1) \Longrightarrow 1 + 0 < u + 1$. Since $u > 0 \wedge 1 \leq u$, we have $1 \leq u$. T31 tells us that $0 < 1$. Hence $1 \leq u \wedge 0 < 1$. So $1 + 0 < u + 1$ by $\Longrightarrow_{out}$. But $1 + 0 = 1$ by RA6 specialized to $x = 1$. So $1 < u + 1$. Now, OA2 (specialized to $x = 1$, $y = u + 1$), implies $1 \leq u + 1 \Longleftrightarrow (1 < u + 1 \vee 1 = u + 1)$. Since we already have $1 < u + 1$, we can conclude that $1 < u + 1 \vee 1 = u + 1$. But then $1 \leq u + 1$. So we have proved $1 \leq u + 1$ under the assumption that $u > 0 \wedge 1 \leq u$. Hence $(u > 0 \wedge 1 \leq u) \Longrightarrow 1 \leq u + 1$. This has been proved for an arbitrary u. So $\forall u, ((u > 0 \wedge 1 \leq u) \Longrightarrow 1 \leq u + 1)$. That is, $\forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u + 1))$.

By the PMI,

$$\Big(p(1) \wedge \forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u + 1))\Big) \Longrightarrow \forall u, (u > 0 \Longrightarrow p(u)) .$$

We have already established $p(1)$ and $\forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u + 1))$. Therefore we have $p(1) \wedge \forall u, ((u > 0 \wedge p(u)) \Longrightarrow p(u+1))$, so we can conclude that $\forall u, (u > 0 \Longrightarrow p(u))$.

Now specialize to $u = x$. Then $x > 0 \Longrightarrow p(x)$. But we have $0 < x$, so using OA1 we can conclude that $x > 0$. Then we have $p(x)$, that is, $1 \leq x$. This was proved under the assumption that $\sim x \leq 0$. So we can conclude $\sim x \leq 0 \Longrightarrow 1 \leq x$. But $(\sim x \leq 0 \Longrightarrow 1 \leq x) \Longrightarrow (x \leq 0 \vee 1 \leq x)$ is an

instance of a tautology. So we can go to $x \leq 0 \vee 1 \leq x$. This was proved for an arbitrary x. Hence
$$\forall x, (x \leq 0 \vee 1 \leq x).$$

THE END

THEOREM T36. $\forall x, \forall y, (x \leq y \vee y+1 \leq x)$.

PROOF. Let x, y be arbitrary. Suppose $\sim x \leq y$. Using T35, we find that $x-y \leq 0 \vee 1 \leq x-y$. If $x-y \leq 0$, then T25 would imply $x \leq y$, contradicting the assumption that $\sim x \leq y$. So $\sim x-y \leq 0$. Therefore $1 \leq x-y$. Then T25 implies $y+1 \leq x$. **THE END**

THEOREM T37. $\forall x, (x \leq 0 \vee x = 1 \vee 2 \leq x)$.

PROOF. Let x be arbitrary. Suppose $\sim x \leq 0$. Then T35 implies $1 \leq x$, and T36 implies $x \leq 1 \vee 1+1 \leq x$. If $x \leq 1$, then T29 implies $x = 1$, since $1 \leq x$ and $x \leq 1$. If $1+1 \leq x$, then $2 \leq x$. **THE END**

THEOREM T38. $\forall x, (x \text{ is even } \vee \ x \text{ is odd})$.

PROOF. Let $q(u)$ be the statement

We will first prove that $\forall u, (u > 0 \Longrightarrow q(u))$ We do this using the PMI. For this purpose, we have to prove $q(1) \wedge \forall u, \Big((u > 0 \wedge q(u)) \Longrightarrow q(u+1)\Big)$.

To prove $q(1)$, we observe that "1 is even $\vee$ 1 is odd" is true because 1 is odd. (Proof that 1 is odd: $\forall x, (x \text{ is odd} \Longleftrightarrow \exists y, x = 2y+1)$ by Definition D6. So $1 \text{ is odd} \Longleftrightarrow \exists y, 1 = 2y+1)$ by Rule $\forall_{out}$. Now: $2.0 = 0$ by T4 specialized to $x = 0$. So $1 = 1+0 = 0+1 = 2.0+1$, i.e., $1 = 2.0+1$, showing that $\exists y, 1 = 2y+1$. Then 1 is odd.

Now we prove that $\forall u, \Big((u > 0 \wedge q(u)) \Longrightarrow q(u+1)\Big)$ Let u be arbitrary. Suppose $u > 0 \wedge q(u)$. Then $u > 0$. Also, $q(u)$, that is, u is even$\wedge\, u$ is odd. We want to prove $q(u+1)$, i.e., $u+1$ is even$\wedge\, u+1$ is odd. Since we know that "u is even$\wedge\, u$ is odd", we are in a position to do a proof by cases.

So consider first the case when u is even. In that case, $\exists y, u = 2y$ by Definition D5. (Actually, Definition D5 says $\forall x, (x \text{ is even} \Longleftrightarrow \exists y, x = 2y)$. Specializing to $x = u$ we get $u \text{ is even} \Longleftrightarrow \exists y, u = 2y$. Since we are working under the assumption that u is even, we can go to $\exists y, u = 2y$ by Rule $\Longleftrightarrow_{out}$.) Pick a y such that $u = 2y$ and call it k. Then $u = 2k$. So $u+1 = 2k+1$. So $\exists y, u+1 = 2y+1$ (witness: $y = k$). So $u+1$ is odd, So $u+1$ is even$\vee u+1$ is odd, by Rule $\vee_{out}$.

Now consider the case when u is odd. In that case, $\exists y, u = 2y+1$ by Definition D6. (Actually, Definition D5 says $\forall x, (x \text{ is odd} \Longleftrightarrow \exists y, x = 2y+1)$. Specializing to $x = u$ we get $u \text{ is odd} \Longleftrightarrow \exists y, u = 2y+1$. Since we are working under the assumption that u is odd, we can go to $\exists y, u = 2y+1$ by Rule $\Longleftrightarrow_{out}$.) Pick a y such that $u = 2y+1$ and call it k. Then $u = 2k+1$.

So $u+1 = 2k+2 = 2(k+1)$. So $\exists y, u+1 = 2y$ (witness: $y = k+1$). So $u+1$ is even, So $u+1$ is even$\vee u+1$ is odd, by Rule $\vee_{out}$.

So we have proved that "$u+1$ is even$\vee u+1$ is odd" in both cases, when y is even and when u is odd. Since we are assuming that "u is even$\wedge\, u$ is odd", we can conclude that "$u+1$ is even$\vee u+1$ is odd", i.e., that $q(u+1)$.

The conclusion $q(u+1)$ was proved under the assumption that $u > 0 \wedge q(u)$. So we can conclude that $(u > 0 \wedge q(u)) \Longrightarrow q(u+1)$.

The conclusion that "$(u > 0 \wedge q(u)) \Longrightarrow q(u+1)$" has been proved for an arbitrary u. Hence we can conclude that

$$\forall u, \Big((u > 0 \wedge q(u)) \Longrightarrow q(u+1)\Big).$$

So we have proved $q(1)$ and $\forall u, \Big((u > 0 \wedge q(u)) \Longrightarrow q(u+1)\Big)$. It then follows from the PMI that $\forall u, (u > 0 \Longrightarrow q(u))$, i.e., that

$$\forall u, (u > 0 \Longrightarrow (u \text{ is even } \vee\, u \text{ is odd})),$$

or, equivalently,

$$\forall x, (x > 0 \Longrightarrow (x \text{ is even } \vee\, x \text{ is odd})).$$

That is, we have shown that every $x \in \mathbb{Z}$ which is positive is either even or odd.

Now we want to show that every $x \in \mathbb{Z}$ is either even or odd, i.e., that $\forall x, (x \text{ is even } \vee\, x \text{ is odd})$.

Let u be arbitrary. We want to prove that u is even $\vee\, u$ is odd. Axiom OA7 implies that $0 \leq u \vee u \leq 0$. Now that we know that $0 \leq u \vee u \leq 0$, we can do a proof by cases.

Consider first the case when $0 \leq u$. Axiom OA2 implies $0 \leq u \Longleftrightarrow (0 < u \vee 0 = u)$. So we can conclude that $0 < u \vee 0 = u$. Again, we do a proof by cases (within our proof by cases.) Consider the case when $0 < u$. Then $u > 0$ by OA1, and since we already know that $\forall x, (x > 0 \Longrightarrow (x \text{ is even } \vee\, x \text{ is odd}))$, we can specialize to $x = u$ and get $u > 0 \Longrightarrow (u \text{ is even } \vee\, u \text{ is odd})$. Since $u > 0$, Rule $\Longrightarrow_{out}$ implies u is even $\vee\, u$ is odd.

Next consider the case when $0 = u$. Then $u = 2.0$, so u is even. So u is even $\vee\, u$ is odd in this case as well.

All this was for the case when $0 \leq u$. Now look at the case when $u \leq 0$. Then $u < 0 \vee u = 0$ by OA2. Consider the case $u < 0$. Then $u + (-u) < 0 + (-u)$, i.e., $0 < -u$. Since we already know that $\forall x, (x > 0 \Longrightarrow (x \text{ is even} \vee x \text{ is odd}))$, we can conclude that $-u$ is even $\vee -u$ is odd. Now we do a proof by cases. Let us do it in very abbreviated form. If $-u$ is even then we can write $-u = 2k$ for some k, so $u = -2k = 2.(-k)$, so u is even, so u is even $\vee\, u$ is odd. If $-u$ is odd then we can write $-u = 2k+1$ for some k, so $u = -2k-1 = 2.(-k-1)+1$, so u is odd, so u is even $\vee\, u$ is odd. If

$-u$ is even then we can write $-u = 2k$ for some k, so $u = -2k = 2.(-k)$, so u is even, so u is even $\vee u$ is odd. So we have shown that "u is even $\vee u$ is odd" both under the assumption that $-u$ is even and under the assumption that $-u$ is odd. Since we have $-u$ is even $\vee$ $-u$ is odd, we can conclude that "u is even $\vee$ u is odd". This was proven under the assumption that $u < 0$. The case when $u = 0$ has already been handled before, and we proved that "u is even $\vee$ u is odd" in this case as well.So we have proved "u is even $\vee$ u is odd" under the assumption that $u \leq 0$.

To conclude: we have shown that "u is even $\vee u$ is odd" in the case when $0 \leq u$ and also in thecase when $u \leq 0$. Sowe have established "u is even $\vee$ u is odd" in all cases. Since u was arbitrary, we have proved: "$\forall x(x$ is even $\vee$ x, is odd)". **THE END**

THEOREM T39. $\sim \exists k, 2.k = 1$.

PROOF. Suppose $\exists k, 2.k = 1$. Pick one such k and call it a. Then $2.a = 1$.

By T35, $a \leq 0 \vee 1 \leq a$. If $a \leq 0$, then $0 \leq -a$ by T25. Since $0 < 2$ by T30, it follows from T27 that $0 \leq 2.(-a)$. But $2.(-a) = 2.((-1).a) = (2.(-1)).a = ((-1).2).a = (-1).(2.a) = (-1).1 = -1$. So $0 \leq -1$. Then $1 \leq 0$ by T25. Since $0 < 1$ by T31, we have $0 < 0$, contradiciting OA8. Therefore $\sim\ a \leq 0$.

It follows that $1 \leq a$. Then T25 implies that $1 + 1 \leq a + a$, i.e., that $2 \leq 2.a$. Since $2.a = 1$, we have $2 \leq 1$. Since $1 < 2$, we have $2 < 2$. Therefore $0 < 0$, contradicting OA8. **THE END**

THEOREM T40. $\forall x, \sim$ (x is even $\wedge$ x is odd).

PROOF. Let x be arbitrary. Suppose x is even $\wedge$ x is odd. Then

$$\exists k, x = 2.k\,.$$

Pick one such k and call it a. Also,

$$\exists k, x = 2.k + 1\,.$$

Pick one such k and call it b. Then

$$x = 2.a \qquad \text{and} \qquad x = 2.b + 1\,.$$

Subtracting, we get

$$1 = 2.(b - a)\,.$$

So $\exists k, 2.k = 1$. But this contradicts T39.

It follows that $\sim$ (x is even $\wedge$ x is odd). **THE END**

18 More on homework

18.1 Homework due on Thursday, March 11

I. Give a completely formal proof of the conclusion stated below from the four given hypotheses.

Hypotheses:
(1) $\forall x, (x$ is a student $\Longrightarrow x$ does not understand Math 300)
(2) $\forall x, (x$ is a student $\Longrightarrow x$ is not able to fool me)
(3) $\forall x, \Big(x$ will pass Math 300 $\Longrightarrow (x$ understands Math 300$\vee x$ is able to fool me$)\Big)$
(4) $\exists x, x$ is a student

Conclusion:
$\exists x, x$ will not pass Math 300.

(You are allowed to introduce abbreviations, such as for example using "uM300" for "understands Math 300", "iafm" for "is able to fool me", and so on.)

REMARK: This proof took me about 20 steps. If your proof is a lot shorter, e.g. 10 steps, you should not believe it.

II. Give a completely formal proof of each of the following statements, or show that such a proof cannot exist.

(1) $(\forall x, (x$ is a borogove$\wedge x$ is mimsy$)) \Longleftrightarrow (\forall x, x$ is a borogove$\wedge \forall x, x$ is mimsy$)$

(2) $(\forall x, (x$ is a borogove$\vee x$ is mimsy$)) \Longrightarrow (\forall x, x$ is a borogove$\vee \forall x, x$ is mimsy$)$

(3) $(\forall x, x$ is a borogove $\vee\ \forall x, x$ is mimsy$) \Longrightarrow (\forall x, (x$ is a borogove $\vee$ x is mimsy$))$

III. Give a completely formal proof of the result of Problem 3, Part II, of the first midterm, using a format similar to the proof given in the solutions handout, but *without using Rules* $\wedge_{in}$*,* $\wedge_{out}$*,* $\Longleftrightarrow_{in}$*, and* $\Longleftrightarrow_{out}$.

IV. Prove that $\sqrt{5}$ is irrational.

V. Prove that $\sqrt{6}$ is irrational.

VI. Determine the set of real numbers α that have the property that

$$\forall n \in \mathbb{N}, \alpha^n \geq n\,.$$

18.2 Homework due on Thursday, April 1

I. Problems from the book: 3.2.3, 3.2.6, 3.3.2, 3.3.4.

In the following problems, there appear several summation symbols. Here is the inductive definition of summation:

$$\sum_{k=1}^{1} a_k = a_1 \,,$$

and

$$\forall n \in \mathbb{N},\ \sum_{k=1}^{n+1} a_k = a_{n+1} + \sum_{k=1}^{n} a_k \ .$$

II. Prove the following using the Principle of Mathematical Induction:

(1) $\forall n \in \mathbb{N}, \left(\sum_{k=1}^{n}(2k-1) = n^2\right)$.

For comparison, here is an argument that does *not* use induction. Write

$$S_n = 1 + 3 + \cdots + 2n - 1\,, \qquad \text{i.e.,} \quad S_n = \sum_{k=1}^{n}(2k-1)\,.$$

Then

$$\begin{array}{rcl} S_n & = & 1 + \quad 3 + \cdots + 2n - 3 + 2n - 1\,, \\ S_n & = & 2n - 1 + 2n - 3 + \cdots + \quad 3 + \quad 1\,, \\ 2S_n & = & 2n + 2n + \cdots + 2n + 2n \qquad (n \text{ times})\,, \end{array}$$

and then $2S_n = n.(2n) = 2n^2$, so $S_n = n^2$.

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

(3) For every $n \in \mathbb{N}$, the sum $\sum_{k=1}^{n} k^3$ is the square of an integer. (Hint: to do this problem, you have to find a formula for $\sum_{k=1}^{n} k^3$, prove your formula by induction, and then from the formula get the desired conclusion. How do you find the formula? By guessing, but then of course you have to **prove** that your guess is right, so if you didn't guess correctly then you will not be able to prove it. How do you go about making the right guess? One possibility would be to try several examples until you think that you "see the pattern.")

(4) For every $n \in \mathbb{N}$ such that $n \geq 5$: $2^n > n^2$. (Hint: prove the following by induction: $\forall n \in \mathbb{N}, (n \geq 5 \Longrightarrow 2^n > n^2)$. For this purpose, use the predicate "$n \geq 5 \Longrightarrow 2^n > n^2$" as your $p(n)$, and make sure you take into account properly the fact that $p(n)$ is an implication.)

II. Prove the following using the Principle of Complete Mathematical Induction:

(1) Every natural number n such that $n > 1$ has a prime factor. That is:
$\forall n \in \mathbb{N}, (n > 1 \Longrightarrow \exists p \in \mathbb{N}, \exists q \in \mathbb{N}, (p \text{ is prime} \wedge n = p.q))$.

(2) Every natural number n such that $n > 1$ can be written as $7^k q$, where $k \in \mathbb{Z}$, $k \geq 0$, and q is not divisible by 7. (Note: here is the definition of "divisible": Let $n, m \in \mathbb{Z}$. We say that n is **divisible** by m if there exists $q \in \mathbb{Z}$ such that $n = m.q$. And, in case you ask, as you should, "what is the definition of n^k?", here is an inductive definition: let $n \in \mathbb{Z}$, then $n^0 = 1$ and $\forall k \in \mathbb{N}, n^k = n.n^{k-1}$.)

18.3 Solution of Problem 1, Section 18.1

In the proof, I use the abbreviations "uM300" for "understands Math 300", "iafm" for "is able to fool me", "iss" for "is a student", and "wpM300" for "will pass Math 300".

PROOF:

1. $\exists x, x$ iss
2. Pick a such that a iss.
3. $\forall x, \Big(x \text{ iss} \Longrightarrow (\sim x \text{ uM300})\Big)$
4. $a \text{ iss} \Longrightarrow (\sim a \text{ uM300})$
5. $\sim a$ uM300
6. $\forall x, \Big(x \text{ iss} \Longrightarrow (\sim x \text{ iafm})\Big)$
7. $a \text{ iss} \Longrightarrow (\sim a \text{ iafm})$
8. $\sim a$ iafm
9. $\sim a \text{ uM300} \wedge \sim a \text{ iafm}$
10. Assume a wpM300.
11. $\forall x, \Big(x \text{ wpM300} \Longrightarrow (x \text{ uM300} \vee x \text{ iafm})\Big)$
12. $a \text{ wpM300} \Longrightarrow (a \text{ uM300} \vee a \text{ iafm})$
13. $a \text{ uM300} \vee a \text{ iafm}$
14. $(\sim a \text{ uM300} \wedge \sim a \text{ iafm}) \wedge (a \text{ uM300} \vee a \text{ iafm})$
15. $\Big((\sim a \text{ uM300} \wedge \sim a \text{ iafm}) \wedge (a \text{ uM300} \vee a \text{ iafm})\Big) \Longrightarrow (\sim a \text{ wpM300})$
16. $\sim a$ wpM300
17. $a \text{ wpM300} \Longrightarrow (\sim a \text{ wpM300})$
18. $\Big(a \text{ wpM300} \Longrightarrow (\sim a \text{ wpM300})\Big) \Longrightarrow (\sim a \text{ wpM300})$
19. $\sim a$ wpM300
20. $\exists x, \sim x$ wpM300
21. $\exists x, \sim x$ wpM300

18.4 Homework assignment due on Thursday, April 8

I. Prove, using the Well Ordering Principle, that

If $m, n \in \mathbb{Z}$, $m \neq 0$ and $n \neq 0$, then

$\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, (m.b = a.n \wedge \sim \exists c \in \mathbb{Z}, ((c|a \wedge c|b) \wedge c > 1))$.

II. Book, Problems 4.1.10, 4.2.4.

III. (See book, footnote on page 65.) *NOTE: This problem was assigned on April 6, with the proviso that you could hand it in on April 8 or on April 15, as you wish.*

A good definition of the "ordered pair" (a, b) of two objects a, b, is a definition for which the following is true:

$$\forall a, \forall b, \forall c, \forall d, \Big((a, b) = (c, d) \Longleftrightarrow (a = c \wedge b = d)\Big)\,.$$

III.a. Prove that the following definition of "ordered pair" is good:

DEFINITION: The **ordered pair** of two objects a, b, is the set (a, b) given by

$$(a, b) = \{\{a\}, \{a, b\}\}\,.$$

III.b. Prove that the following definition of "ordered pair" is not good:

DEFINITION: The **ordered pair** of two objects a, b, is the set (a, b) given by

$$(a, b) = \{a, b\}\,.$$

III.c. Prove or disprove that the following definition of "ordered pair" is good:

DEFINITION: The **ordered pair** of two objects a, b, is the set (a, b) given by

$$(a, b) = \{\{a\}, \{\{b\}\}\}\,.$$

18.5 Homework assignment due on Thursday, April 15

I. Problems from the book: 4.3.5, 4.3.7, 4.3.10, 4.3.11, 4.3.23.

II. *The purpose of this problem is to show you how we mathematicians like to construct the system $\mathbb{Q}$ of rational numbers if we are given the system $\mathbb{Z}$ of integers. The idea is this: a rational numbers should be a "fraction" such as $3/5$ or $-7/12$ or $723/5$. We do not know what a fraction "really is", but we can write it down anyhow, as we just did. So we would like to say that a "fraction", whatever that may really be, "is" (or, if you prefer, "is given by," or "is determined by," or "is specified by") two integers m, n, called the "numerator" and "denominator" of the fraction. So we could try saying that* *a "fraction" is an ordered pair (m, n) of integers. This, however, is not good for a number of reasons. To begin with, we know that we are not supposed to divide by zero. So we should not allow the denominator to be 0. That is, we should not allow "fractions" such as $(3, 0)$. We take care of this problem by amending our tentative definition of "fraction" as follows: a "fraction" is an ordered pair (m, n) of integers such that $n \neq 0$. That is, we let Ω be the set of all ordered pairs (m, n) of integers such that $n \neq 0$, and we tentatively propose to define a "rational number," or "fraction," to be a member of Ω. And we plan to use the expression "m/n" as just an alternative notation for the pair (m, n) so that, for example, "$3/5$" is just another way of writing "$(3, 5)$" This, however, is not good yet, because there is still something happening here that should not happen. We want the "fractions" $3/5$ and $6/10$ to be "the same," whatever that means. But if we think of $3/5$ and $6/10$ as the ordered pairs $(3, 5)$ and $(6, 10)$, respectively, then $3/5$ and $6/10$ are most definitely not the same. So we have to do something, and it is here that equivalence relations come in handy. We introduce an equivalence relation $\sim$ on Ω in such a way that the pairs $(3, 5)$ and $(6, 10)$ are "the same," in the sense that $(3, 5) \sim (6, 10)$. In general, we would like two "fractions" (m, n), (μ, ν) to be "the same" if "the quotients m/n and μ/ν are equal". But, since we do not know yet what "m/n" and "μ/ν" mean, we rewrite the desired equality $m/n = \mu/\nu$ in a form that makes sense to us, because it only involves integers and the basic arithmetic operations on the set of integers. So, instead of "$m/n = \mu/\nu$", we write "$m.\nu = n.\mu$". The way out of our difficulties is then as follows: we start with the set Ω of ordered pairs (m, n) as above, but we do* **not** *call these pairs "fractions." We declare two pairs (m, n), (μ, ν) to be "the same" (that is, related by the relation $\sim$) if $m.\nu = n.\mu$. We then have to prove that $\sim$ is an equivalence relation. Once we have done that, we reject the original idea of calling the members of Ω "fractions," and we call them "prefractions" instead. We then define a* **rational number***, or* **fraction***, to be an equivalence class of the relation $\sim$, that is, a member of the set $\Omega_\sim$. And, for any prefraction (m, n), we write m/n to denote the equivalence class of (m, n). Now, with these definitions and notations, it is rigorously true that, for example, $3/5 = 6/10$, because the equality "$3/5 = 6/10$" means "the prefractions $(3, 5)$ and $(6, 10)$ belong to the same equivalence class of $\sim$," that is, "$(3, 5) \sim (6, 10)$", which is indeed true because, according to the definition of $\sim$, "$(3, 5) \sim (6, 10)$" means "$3.10 = 5.6$", which is true, since $3.10 = 30$ and $5.6 = 30$.*

Let Ω be the set of all ordered pairs (m, n) of integers such that $n \neq 0$. (In symbols,

$$\Omega = \Big\{(m, n) \in \mathbb{Z} \times \mathbb{Z} : n \neq 0\Big\},$$

so $\Omega \subseteq \mathbb{Z} \times \mathbb{Z}$.) Define a relation $\sim$ on A by letting

$$\sim = \Big\{\Big((m, n), (\mu, \nu)\Big) \in A : m.\nu = n.\mu\Big\}.$$

(In other words, we declare two pairs (m, n), (μ, ν) to be "related" if $m.\nu = n.\mu$. That is, $(m, n) \sim (\mu, \nu) \Longleftrightarrow m.\nu = n.\mu$.)

(**II.a**) Prove that $\sim$ is an equivalence relation on Ω.

(**II.b**) The equivalence classes of $\sim$ are the **rational numbers**. We use $\mathbb{Q}$ to denote the set of all rational numbers, so $\mathbb{Q} = \Omega_\sim$ by definition. Here are three attempts to define operations on $\mathbb{Q}$:

$$\frac{m}{n} \oplus \frac{\mu}{\nu} = \frac{m+\mu}{n+\nu},$$

$$\frac{m}{n} + \frac{\mu}{\nu} = \frac{m.\nu + n.\mu}{n.\nu},$$

$$\frac{m}{n} \times \frac{\mu}{\nu} = \frac{m.\mu}{n.\nu}.$$

Two of these are acceptable, one is not. (The meaning of "acceptable" is explained in the remark below.) Determine which are the two that are acceptable, and which is the one that is not, and in each of the three cases prove your statement.

REMARK: "Acceptable" means "such that the equivalence class in the right-hand side is the same no matter which members (m, n), (μ, ν) you pick for the equivalence classes in the left-hand side." For example, it would not be acceptable to define an operation # on $\mathbb{Q}$ by letting

$$\frac{m}{n} \# \frac{\mu}{\nu} = \frac{m}{\nu},$$

because, if you take $m = 3$, $n = 5$, $\mu = 2$, $\nu = 7$, that would yield $\frac{3}{5} \# \frac{2}{7} = \frac{3}{7}$, but you could also take $m = 6$, $n = 10$, $\mu = 8$, $\nu = 28$, and then you would get $\frac{6}{10} \# \frac{8}{28} = \frac{6}{28}$. But $\frac{3}{5} = \frac{6}{10}$, and $\frac{2}{7} \# \frac{8}{28}$. Let us give names to these two equivalence classes: use r to denote the class $\frac{3}{5}$, so $r = \frac{3}{5} = \frac{6}{10}$, and use s to denote the class $\frac{2}{7}$, so $s = \frac{2}{7} = \frac{8}{28}$. For our definition of the operation # to be acceptable it would have to be the case that $r \# s$ is a well-defined rational number, i.e., a well-defined equivalence class. In other words, $r \# s$ would have to be the same class no matter which prefraction we use to represent r and which prefraction we use to represent s. But we have done the calculation using $(3, 5)$ for r and $(2, 7)$ for s, and got the result $r \# s = \frac{3}{7}$. And we have also done the calculation using $(6, 10)$ for r and $(8, 28)$ for s, and got the result $r \# s = \frac{6}{28}$. But **it is not true** that $\frac{3}{7} = \frac{6}{28}$. (Indeed, for this to be true, the prefractions $(3, 7)$ and $(6, 28)$ would have to be equivalent, that is, we would have to have $(3, 7) \sim (6, 28)$. But this is not true, because "$(3, 7) \sim (6, 28)$" means "$3.28 = 7.6$", which is false, becase $3.28 = 84$ and $7.6 = 42$.) So # is **not** acceptable.

18.6 Answers to the questions of the first midterm exam.

1. i. Define "prime number." **ANSWER.** A **prime number** is an integer n such that $n > 1$ and there do not exist integers p, q such that $p \cdot q = n$ and $1 < p < n$.

ii. Define "tautology." **ANSWER.** A **tautology** is a propositional form $\mathcal{F}$ such that $\mathcal{F}$ has the truth value "true" for all possible ways of assigning truth values to the propositional variables that occur in $\mathcal{F}$.

iii. Define "union" of two sets. **ANSWER.** Let A, B be sets. The **union** of A and B is the set of all x such that x belongs to A and x belongs to B. In symbols, using "$\cup$" to denote union: $A \cup B = \{x : x \in A \vee x \in B\}$.

iv. Define "union" of a collection of sets. **ANSWER.** Let $\{C_\alpha\}_{\alpha \in A}$ be a collection of sets. The **union** of the C_α is the set $\bigcup_{\alpha \in A} C_\alpha$ given by

$$\bigcup_{\alpha \in A} C_\alpha = \{x : \exists \alpha \in A, x \in C_\alpha\}\,.$$

v. Define "power set." **ANSWER.** Let A be a set. The **power set** of A is the set of all subsets of A.

2. Prove each of the following (informal proofs O.K.).

(i) If A, B, C are sets and $A \subseteq B \cup C$ then $A \subseteq B$ or $A \subseteq C$.

ANSWER. This cannot be proved because it is not true. PROOF THAT THE STATEMENT IS NOT TRUE. Let A be the set of all U.S. Senators, let B be the set of all Democratic U.S. Senators, let C be the set of all Republican U.S. Senators. Then $A \subseteq B \cup C$ but it's not true that $A \subseteq B$ or $A \subseteq C$.

(ii) If A, B, C are sets and $A \subseteq B \cap C$ then $A \subseteq B$ and $A \subseteq C$.

ANSWER. This is true. Here is a proof. Suppose $A \subseteq B \cap C$. Pick an arbitrary a. Suppose $a \in A$. Then $a \in B \cap C$, because $A \subseteq B \cap C$. So $a \in B$ and $a \in C$. So we have proved, for an arbitrary a, that $a \in A \Longrightarrow a \in B$, and $a \in A \Longrightarrow a \in C$. So $\forall x, (x \in A \Longrightarrow x \in B)$, and $\forall x, (x \in A \Longrightarrow x \in C)$. Therefore $A \subseteq B$ and $A \subseteq C$. **END OF PROOF**

(iii) If A, B are sets then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

ANSWER. This is true. Here is a proof. First, we must prove that if $A \subseteq B$ then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Suppose $A \subseteq B$. Let us prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Let $X \in \mathcal{P}(A)$ be arbitrary. Then $X \subseteq A$. Since $A \subseteq B$, $X \subseteq B$. So $X \in \mathcal{P}(B)$. Since X was an arbitrary member of $\mathcal{P}(A)$ we have shown that $\forall X, (X \in \mathcal{P}(A) \Longrightarrow X \in \mathcal{P}(B))$, i.e., that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Now we must prove that if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ then $A \subseteq B$. Assume $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We will prove that $A \subseteq B$. Let $x \in A$ be arbitrary. Then the set

$\{x\}$ is a subset of A, so $\{x\}$ is a member of $\mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we can conclude that $\{x\} \in \mathcal{P}(B)$. So $\{x\} \subseteq B$. But then every member of $\{x\}$ belongs to B. So in particular $x \in B$. We have shown that $x \in A \Longrightarrow x \in B$ for an arbitrary x. Hence $A \subseteq B$. **END OF PROOF**

3. Give completely formal proofs (with a full justification of each step) of each of the following two statements:

I. If A is a set then $\emptyset \subseteq A$.

II. If A, B, C are sets, $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

ANSWER. Proof of I: We are going to prove that $\emptyset \subseteq A$, i.e., that $\forall x, (x \in \emptyset \Longrightarrow x \in A)$.

(1) $\forall x, (\sim x \in \emptyset)$ [Characterization of $\emptyset$]
(2) Let a be arbitrary. [Preparation to apply Rule $\forall_{in}$]
(3) Assume $a \in \emptyset$. [Preparation to apply Rule $\Longrightarrow_{in}$]
(4) $\sim a \in \emptyset$. [From (1) by Rule $\forall_{out}$]
(5) $a \in \emptyset \wedge (\sim a \in \emptyset)$. [From (3) and (4) by Rule $\wedge_{in}$]
(6) $(a \in \emptyset \wedge (\sim a \in \emptyset)) \Longrightarrow a \in A$. [Tautology $(\alpha \wedge (\sim \alpha) \Longrightarrow \beta$]
(7) $a \in A$. [From (5) and (6) by Rule $\Longrightarrow_{out}$]
(8) $a \in \emptyset \Longrightarrow a \in A$. [From (3) and (7) by Rule $\Longrightarrow_{in}$]
(9) $\forall x, (x \in \emptyset \Longrightarrow x \in A)$. [From (2) and (8) by Rule $\forall_{in}$]

END OF PROOOF

And now here is a proof of II.
(1) A is a set. [Hypothesis]
(2) B is a set. [Hypothesis]
(3) C is a set. [Hypothesis]
(4) $A \subseteq B$. [Hypothesis]
(5) $B \subseteq C$. [Hypothesis]
(6) $\forall X, \forall Y, \Big((X \text{ is a set} \wedge Y \text{ is a set}) \Longrightarrow$
$(X \subseteq Y \Longleftrightarrow \forall x, (x \in X \Longrightarrow x \in Y))\Big)$. [Hypothesis]
(7) $\forall Y, \Big((A \text{ is a set} \wedge Y \text{ is a set}) \Longrightarrow$
$(A \subseteq Y \Longleftrightarrow \forall x, (x \in A \Longrightarrow x \in Y))\Big)$. [From (6) by Rule $\forall_{out}$]
(8) $\forall Y, \Big((B \text{ is a set} \wedge Y \text{ is a set}) \Longrightarrow$
$(B \subseteq Y \Longleftrightarrow \forall x, (x \in B \Longrightarrow x \in Y))\Big)$. [From (6) by Rule $\forall_{out}$]
(9) $(A \text{ is a set} \wedge B \text{ is a set}) \Longrightarrow (A \subseteq B \Longleftrightarrow \forall x, (x \in A \Longrightarrow x \in B))\Big)$.
[From (7) by Rule $\forall_{out}$]

(10) A is a set$\wedge$ B is a set. [From (1) and (2) by Rule $\wedge_{in}$]
(11) $A \subseteq B \iff \forall x, (x \in A \Longrightarrow x \in B))$ [From (9) and (10) by Rule $\Longrightarrow_{out}$]
(12) $(B \text{ is a set} \wedge C \text{ is a set}) \Longrightarrow \Big(B \subseteq C \iff \forall x, (x \in B \Longrightarrow x \in C)\Big)$. [From (8) by Rule$\forall_{out}$]
(13) B is a set$\wedge$ C is a set. [From (2) and (3) by Rule $\wedge_{in}$]
(14) $B \subseteq C \iff \forall x, (x \in B \Longrightarrow x \in C))$. [From (12) and (13) by Rule $\Longrightarrow_{out}$]
(15) $\forall x, (x \in A \Longrightarrow x \in B)$. [From (4) and (11) by Rule $\iff_{out}$]
(16) $\forall x, (x \in B \Longrightarrow x \in C)$. [From (5) and (14) by Rule $\iff_{out}$]
(17) Let u be arbitrary. [Preparation to apply Rule $\forall_{out}$]
(18) Assume $u \in A$. [Preparation to apply Rule $\Longrightarrow_{out}$]
(19) $u \in A \Longrightarrow u \in B$. [From (15) by Rule $\forall_{out}$]
(20) $u \in B$. [From (18) and (19) by Rule $\Longrightarrow_{out}$]
(21) $u \in B \Longrightarrow u \in C$. [From (16) by Rule $\forall_{out}$]
(22) $u \in C$. [From (20) and (21) by Rule $\Longrightarrow_{out}$]
(23) $u \in A \Longrightarrow u \in C$. [From (18) and (22) by Rule $\Longrightarrow_{in}$]
(24) $\forall x, (x \in A \Longrightarrow x \in C)$. [From (18) and (23) by Rule $\forall_{in}$]
(25) $(A \text{ is a set} \wedge C \text{ is a set}) \Longrightarrow \Big(A \subseteq C \iff \forall x, (x \in A \Longrightarrow x \in C)\Big)$. [From (7) by Rule $\forall_{out}$]
(26) A is a set $\wedge$ C is a set. [From (1) and (3) by Rule $\wedge_{out}$]
(27) $A \subseteq C \iff \forall x, (x \in A \Longrightarrow x \in C)$. [From (25) and (26) by Rule $\Longrightarrow_{out}$]
(28) $A \subseteq C$. [From (24) and (27) by Rule $\iff_{out}$]

END OF PROOF

4. Prove each of the following. (Informal proofs O.K.)

(i) $$\Big((\exists x, x \text{ is a borogove}) \wedge (\exists x, x \text{ is mimsy})\Big) \Longrightarrow \Big(\exists x, (x \text{ is a borogove} \wedge x \text{ is mimsy})\Big).$$

ANSWER. This cannot be proved, because it need not be true. For example, suppose "is a borogove" means "is an elephant" and "is mimsy" means "is a giraffe." Then our statement asserts that if there exist elephants and there exist giraffes it follows that there exist animals that are both elephants and giraffes. This is obviously not true.

(ii) $$\Big((\exists x, x \text{ is a borogove}) \vee (\exists x, x \text{ is mimsy})\Big) \Longrightarrow \Big(\exists x, (x \text{ is a borogove} \vee x \text{ is mimsy})\Big).$$

ANSWER. Here is a proof. Assume $(\exists x, x \text{ is a borogove}) \vee (\exists x, x \text{ is mimsy})$. Consider first the case when $\exists x, x$ is a borogove. Pick a borogove and call it

a. Then (a is a borogove)$\vee$(a is mimsy). So

$$(\exists x, (x \text{ is a borogove} \vee x \text{ is mimsy})\,.$$

Next consider the case when $\exists x, x$ is mimsy. Pick a mimsy thing and call it a. Then (a is a borogove)$\vee$(a is mimsy). So $\exists x, (x$ is a borogove $\vee\, x$ is mimsy$)$. So we have proved that $\exists x, (x$ is a borogove $\vee\, x$ is mimsy) in both cases.

(iii) $$\Big((\forall x, x \text{ is a borogove}) \Longrightarrow (\forall x, x \text{ is mimsy})\Big) \Longrightarrow \Big(\forall x, (x \text{ is a borogove} \Longrightarrow x \text{ is mimsy})\Big)\,.$$

ANSWER. This cannot be proved, because it need not be true. For example, suppose "is a borogove" means "is an elephant" and "is mimsy" means "is a giraffe." Then the premiss "$(\forall x, x$ is a borogove$) \Longrightarrow (\forall x, x$ is mimsy$)$" says that "if everything is an elephant then everything is a giraffe." This is true, because it is not true that everything is an elephant. On the other hand, the conclusion "$\forall x, (x$ is a borogove $\Longrightarrow x$ is mimsy$)$" says that every elephant is a giraffe, which is manifestly not true. Hence our statement is an implication with a true premiss and a false conclusion, so it is false.

(iv) $$\Big(\forall x, (x \text{ is a borogove} \Longrightarrow x \text{ is mimsy})\Big) \Longrightarrow \Big((\forall x, x \text{ is a borogove}) \Longrightarrow (\forall x, x \text{ is mimsy})\Big)\,.$$

ANSWER. Here is a proof. Suppose $\forall x, (x$ is a borogove $\Longrightarrow x$ is mimsy$)$. We want to prove that $(\forall x, x$ is a borogove$) \Longrightarrow (\forall x, x$ is mimsy$)$. For this purpose, we assume that $\forall x, x$ is a borogove, and prove that $\forall x, x$ is mimsy. Let a be arbitrary. We will try to prove that a is mimsy. Since we know that $\forall x, x$ is a borogove, we can conclude that a is a borogove by the specialization rule $\forall_{out}$. Since $\forall x, (x$ is a borogove $\Longrightarrow x$ is mimsy$)$, we can conclude that a is a borogove $\Longrightarrow a$ is mimsy. Since a is a borogove, it follows that a is mimsy by Rule $\Longrightarrow_{out}$. **END OF PROOF**

5. Prove that the number 393 can be expressed as the sum of three primes.

ANSWER. $393 = 103 + 7 + 283$. The number 7 is prime. The number 103 is prime, because it is not divisible by 2 (since it ends in a 3), or by 3 (since $1 + 0 + 3 = 4 = 1$ modulo 3), or by 5 (since it ends in a 3), or by 7 (since $103 = 110 = 40 = 5$ modulo 7), or by 11 (since $1 - 0 + 3 = 4$), and we do not need to try prime factors larger than 11, since $11^2 = 121 > 103$. Finally, 283 is prime, because it is not divisible by 2 (since it ends in a 3), or by 3 (since $2 + 8 + 3 = 13 = 4 = 1$ modulo 3), or by 5 (since it ends in a 3), or by 7 (since $283 = 290 = 10 = 3$ modulo 7), or by 11 (since $2 - 8 + 3 = -3$), or by 13 (since $283 = 270 = 10$ modulo 13), or by 17 (since $283 = 300 = 130 = -40 = -6 = 11$ modulo 17), or by 19 (since $283 = 93 = 17$ modulo 19), and we do not need to try prime factors larger than 19, since $20^2 = 400 > 283$.

6. (i) For each of the following three statements: (a) rewrite the statement in plain English, without letter symbols or any mathematical symbol; (b) indicate whether the statement is true or false (no proof necessary).

1. $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, y > x$

ANSWER. For every integer there is a larger integer. This is TRUE.

2. $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, y \geq x$

ANSWER. There exists an integer which is greater than or equal to every integer. This is FALSE.

3. $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, \forall z \in \mathbb{Z}, (x \cdot z = y \cdot z \Longrightarrow x = y)$

ANSWER. If the results of multiplying two integers by a third integer are equal, then the two integers are equal. This is FALSE (because $3 \cdot 0 = 4 \cdot 0$ but $3 \neq 4$).

(ii.) For each of the following three statements: (a) rewrite the statement in formal language, using the symbols $\in \quad \mathbb{R} \quad \mathbb{Z} \quad + \quad \cdot$ (for multiplication) $= \quad >$, letter variables, the logical connectives $\exists \quad \forall \quad \wedge \quad \vee \quad \sim \quad \Longrightarrow \quad \Longleftrightarrow$, the comma, the left and right parentheses, and **nothing else**. (b) indicate whether the statement is true or false (no proof necessary).

4. Every real number has a square root.

ANSWER. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y \cdot y = x$. This is FALSE.

5. There exists a smallest nonnegative real number.

ANSWER. $\exists x \in \mathbb{R}, \forall z \in \mathbb{R}, \Big(z = z + z \Longrightarrow ((x > z \vee x = z) \wedge \forall y \in \mathbb{R}, ((y > z \vee y = z) \Longrightarrow (y > x \vee y = x)))\Big)$. This is TRUE. (Witness: $x = 0$.)

6. Every positive integer is the sum of the squares of three integers.

ANSWER. $\forall x \in \mathbb{Z}, \forall u \in \mathbb{Z}, \Big(u = u + u \Longrightarrow (x > u \Longrightarrow \exists y \in \mathbb{Z}, \exists z \in \mathbb{Z}, \exists w \in \mathbb{Z}, (x = y \cdot y + z \cdot z + w \cdot w))\Big)$.

ANSWER. This is FALSE, because if $x = 7$ then y, z, w do not exist.

7. In a propositional calculus with propositional variables P, Q, R, prove in each case that the given string of symbols is a well-formed formula.

1. $((\sim P) \wedge (Q \wedge R)) \Longrightarrow (Q \wedge Q)$

ANSWER. This string is well formed. PROOF:
The strings "P", "Q", and "R" are well formed by Rule 1.
The string "$\sim P$" is well formed by Rule 2.
The string "$Q \wedge R$" is well formed by Rule 4.

The string "$(\sim P) \wedge (Q \wedge R)$" is well formed by Rule 7.
The string "$Q \wedge Q$" is well formed by Rule 4.
The string "$((\sim P) \wedge (Q \wedge R)) \Longrightarrow (Q \wedge Q)$" is well formed by Rule 7.
END OF PROOOF

2. $(P \wedge P) \vee (Q)$

ANSWER. This string is **not** well formed. PROOF: Call our string $\mathcal{F}$. Suppose $\mathcal{F}$ was well formed. Then $\mathcal{F}$ would arise from well formed strings by applying one of the seven rules. But $\mathcal{F}$ cannot arise by applying Rules 1 or 2 or 3, because Rule 1 only produces one-letter strings, and Rules 2 and 3 only produce strings containing a $\sim$. So $\mathcal{F}$ is produce by applying Rule 4 or Rule 5 or Rule 6 or Rule 7. This means that $\mathcal{F}$ is of the form $\mathcal{U}\#\mathcal{V}$, where $\mathcal{U}$, $\mathcal{V}$ are strings and $\#$ is one of the connectives

$$\wedge \qquad \vee \qquad \Longrightarrow \qquad \Longleftrightarrow$$

The only possible ways this can happen are (a) if $\mathcal{U}$ is "$(P \wedge P)$", $\mathcal{V}$ is "(Q)", and $\#$ is $\vee$, or (b) if $\mathcal{U}$ is "$(P$", $\mathcal{V}$ is "$P) \vee (Q)$", and $\#$ is $\wedge$. In Case (a), the rule that was applied cannot be Rule 4 or Rule 6, because these two rules produce strings not ending with a right parenthesis. So it would have to be Rule 5 or Rule 7. Then the string playing the role of $\mathcal{B}$ has to be "Q", but this is impossible because if $\mathcal{B}$ consists of a single letter then Rules 5 and 7 do not apply. In Case (b), the rule that was applied cannot be Rule 4 or Rule 6, because these two rules produce strings not ending with a right parenthesis. So it would have to be Rule 5 or Rule 7. But this is impossible because these rules would produce a string with a parenthesis immediately following the $\wedge$.

8. a. Prove that the product of two irrational numbers is irrational.

ANSWER. This cannot be proved because it is FALSE since, for example, $\sqrt{2}$ is irrational and $\frac{1}{\sqrt{2}}$ is irrational but the product of $\sqrt{2}$ and $\frac{1}{\sqrt{2}}$ is 1, which is not irrational.

b. Prove that $\sqrt{3}$ is irrational.

ANSWER. Here is a proof (by contradiction).

Suppose $\sqrt{3}$ was rational. Then we would have $\sqrt{3} = \frac{m}{n}$, where m, n are integers such that $n \neq 0$. If m and n are both divisible by 3, we can cancel the common factor 3 and produce smaller m and n for which $\sqrt{3} = \frac{m}{n}$ is still true. If these new m, n are still both divisible by 3, we can cancel the common factor 3 again, and produce even smaller m and n for which $\sqrt{3} = \frac{m}{n}$ is true. Continue this process until no further cancellation is possible. Then $\sqrt{3} = \frac{m}{n}$, m, n are integers, $n \neq 0$, and m, n are not both divisible by 3. If $n < 0$ then m would have to be < 0 as well, because the quotient $\frac{m}{n}$ is positive. If this is the case, we replace m by $-m$ and n by $-n$, and now we have m, n with all the properties listed above, plus the fact that $m > 0$ and

$n > 0$. Since $\sqrt{3} = \frac{m}{n}$, we have $3 = \frac{m^2}{n^2}$, so $3n^2 = m^2$. Now, we need the fact that *if a product $a.b$ of integers is divisible by* 3*, then one of them must be divisible by* 3. (This is easy to prove: Suppose a is not divisible by 3 and b is not divisible by 3. Then there exist integers k, r, k', r' such that $a = 3k + r$, $b = 3k' + r'$, $r = 1$ or $r = 2$, and $r' = 1$ or $r' = 2$. Then

$$a.b = (3k + r)(3k' + r') = 9kk' + 3kr' + 3k'r + rr' = 3\ell + rr',$$

where $\ell = 3kk' + kr' + k'r$. Now, if $r = 1$ or $r = 2$ and $r' = 1$ or $r' = 2$, then $rr' = 1$ or $rr' = 2$ or $rr' = 4$. In each of the three cases, rr' is not divisible by 3. So $a.b$ is not divisible by 3 either, because if it was then rr' would also be, since $rr' = a.b - 3\ell$.)

Applying this fact, we see that "$3n^2 = m^2$" tells us that m^2 is divisible by 3, so m is divisible by 3. Write $m = 3s$, with $s \in \mathbb{Z}$. Then $3n^2 = m^2 = 9s^2$, so $n^2 = 3s^2$. Therefore n^2 is divisible by 3, so n is divisible by 3. Hence we have shown that both m and n are divisible by 3, But we know that they are not both divisible by 3. Hence we have reached acontradiction and our proof is complete.

9. In each of the following cases, determine of the formula is a tautology, a contradiction, or a contingency.

1. $P \Longrightarrow (Q \Longrightarrow (R \Longrightarrow (S \Longrightarrow (P \wedge Q \wedge R \wedge S))))$ **ANSWER.** This is a tautology.

2. $(P \wedge (\neg P)) \Longrightarrow Q$ **ANSWER.** This is a tautology.

3. $P \Longrightarrow (\neg P)$ **ANSWER.** This is a contingency.

4. $(P \wedge (\neg Q)) \Longrightarrow (P \Longrightarrow Q)$ **ANSWER.** This is a contingency.

5. $((\neg P) \vee (\neg Q)) \Longrightarrow (P \Longrightarrow (Q \Longrightarrow R))$ **ANSWER.** This is a tautology.

6. $((\neg P) \wedge (\neg Q)) \wedge (P \vee Q)$ **ANSWER.** This is a contradiction.