MATHEMATICS 300 — FALL 2008

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Pages 1 to 28

(November 6, 2008)

1 Information on the course

1.1 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**.

1.2 Web page

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

http://www.math.rutgers.edu/˜sussmann/math300page-Fall08.html

All the instructor's notes will be available there.

1.3 Office hours

My office is **Hill 538**. My office hours will be:

- **Wednesday, 2.00pm to 5:00pm**, in my office,
- any other time (possibly including weekends), by appointment, in my office.

1.4 Your final grade

- *Homework (and a few quizzes)* will count for about 30% of your grade.
- The *two midterms* will count—together—for about 35%.
- The *final exam* will count for the remaining 35%.

1.5 Textbook and notes

We will be using:

- the book *A Transition to Advanced Mathematics* (sixth edition), by Douglas Smith, Maurice Eggen, and Richard St. Andre;
- the notes written by the instructor.

> **The material of the instructor's 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.*

1.6 Always bring the book to class!

In the lectures, we are going to spend a lot of time looking at the book and analyzing definitions, arguments and proofs given there. So

> **Please always bring the book to class! You are going to need it.**

1.7 Readings for the first 3 weeks (September 2, 4, 9, 11, 16 and 18)

- the book's "Preface to the student,"
- the book's Chapter 1 (**all of it!**),
- the book's Chapter 2, sections 2.1 and 2.2,
- the instructor's notes dated September 4, Pages 1 to 28.

1.8 Homework assignment no. 1, due on Thursday September 11

Before you start writing your homework, read carefully the rest of this handout, in particular §1.9 on "some remarks about mathematical writing."

1. Book, Exercises 1.2 (pages 17-18-19-20): Problems 5 (non-starred items), 8 (non-starred items), and 13 (non-starred items),

2. (i) Prove or disprove: there exist integers x, y such that $x^2 - y^2 = 28$,
(ii) Prove or disprove: there exist integers x, y such that $x^2 - y^2 = 29$,
(iii) Prove or disprove: there exist integers x, y such that $x^2 - y^2 = 30$.

NOTE: to prove that an object x such that a statement $S(x)$ involving x exists, you can exhibit one. (This is called Rule $\exists_{prove}$, for reasons that will be made clear below.) For example: to prove that there exists an integer x such that $x^2 + 1 = 10$, you can just say:

Let $x = 3$. [Asssumption]
Then x is an integer. [Well-known fact[1]]
And $x^2 + 1 = 10$. [Elementary algebra]
So $\boxed{\text{there exists an integer } x \text{ such that } x^2 + 1 = 10.}$ [Rule $\exists_{prove}$]

END OF PROOF

To prove that an object x such that a statement $S(x)$ involving x does *not* exist, you can do it by contradiction. For example, to prove that there does not exist an integer x such that $x^2 + 1 = 9$, you can just say:

Assume there exists an integer x such that $x^2 + 1 = 9$. [Assumption]
Then that integer x must satisfy $x^2 = 8$. [Elementary algebra]
So $x = 2\sqrt{2}$ or $x = -2\sqrt{2}$. [Elementary algebra]
So $2\sqrt{2}$ is an integer. [Because x is an integer and $2\sqrt{2} = x$ or $2\sqrt{2} = -x$]
But $2\sqrt{2}$ is not an integer. [Well known fact]
Therefore $\boxed{\text{there does not exist an integer } x \text{ such that } x^2 + 1 = 9.}$
[Proof by contradiction rule]

END OF PROOF

[1] If this justification bothers you, we will see later how this fact follows from the axioms

3. Consider the statement

(S) If $x \in \mathbb{R}$ then if $|x^2 - 11| < 5$ and $x > 0$ then $x < 4$ and $x > 2$.

(a) Translate (S) into symbolic language (using the connectives $\sim$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$).

(b) Prove (S).

4. Consider the statement

(S) $x \in \mathbb{R} \Rightarrow (|x - 6| > 4 \Rightarrow (x > 10 \vee x < 4))$

(a) Translate (S) into non-symbolic language (using the words 'if', 'then', 'and', 'or", etc.).

(b) Prove (S).

1.9 Some remarks about mathematical writing

1.9.1 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 who 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[2], because you have not said what "a," "b," and "c" are supposed to be.[3]

- Avoid exaggerated or incorrect use of cryptic mathematical notation.
- Explain what you are doing.
- Make sure that letter "variables" are used correctly, that is that 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 will also be explained later in these notes.
- 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. (Here are two very entertaining books about punctuation that I recommend to you: (1) *Eats, Shoots and Leaves; the Zero Tolerance Approach to Punctuation*, by Lynne Truss, (2) *Eats, Shoots and Leaves; why Commas Really Do Make a Difference!*, by Lynne Truss and Bonnie Timmons.)
- 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.

[2]Of course, your teacher will know what you are trying to say, and anybody who already knows the statement of Pythagoras' theorem will know. But when you are asked to state a theorem or a definition **you should write it as if you were talking to somebody who does not know yet what the theorem or the definition say.**

[3]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 $a^2 + b^2 = c^2$.*

- *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.

1.9.2 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.
  - 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.)

  - 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.

- 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 **numbered**.

If you hand in a homework assignment that has 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 unstapled sheets,**
- **it has unnumbered sheets,**
- **it has sheets that 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 you will lose points. If it has two or more of those flaws, then the assignment will be marked "unacceptable" and returned unread and, from Assignment No. 3 on, you will not get a chance to redo it and hand it in again.

2 Some logical rules

- **Rule** $\wedge_{use}$ says:

From	$P \wedge Q$
you can go to	P ,

and

From	$P \wedge Q$
you can go to	Q .

- **Rule** $\wedge_{prove}$ says:

From	P
and	Q
you can go to	$P \wedge Q$.

- **Rule** $\vee_{use}$ (proof by cases) says:

From	$P \vee Q$
and	$P \Rightarrow R$
and	$Q \Rightarrow R$
you can go to	R .

- **Rule** $\vee_{prove}$ says:

From	P
you can go to	$P \vee Q$,

and

From	Q
you can go to	$P \vee Q$.

- **Rule** $\Rightarrow_{use}$ (Modus Ponens) says:

From	$P \Rightarrow Q$
and	P
you can go to	Q .

- **Rule** $\Rightarrow_{prove}$ (also known as the *deduction rule*) says: If you start a subproof with 'Assume P' and prove Q, then in the main proof you can go to $P \Rightarrow Q$.

- The **proof by contradiction** rule says:

  a. If you start a subproof with 'Assume P' and prove Q, and also $\sim Q$, then yo can go to $\sim P$.

  b. If you start a subproof with 'Assume $\sim P$' and prove Q, and also Q, then yo can go to P.

3 An example of a proof

Theorem. If $x \in \mathbb{R}$ then if $|x-5| < 1$ then $4 < x$.

This theorem says that $\boxed{x \in \mathbb{R} \Rightarrow (|x-5| < 1 \Rightarrow 4 < x)}$.

Proof.

Assume $x \in \mathbb{R}$. [Assumption]

Assume $|x-5| < 1$. [Assumption]

Then $-1 < x-5 < 1$. [because if $|u| < v$ then $-v < u < v$]

So $4 < x < 6$. [adding 5 to each of the terms in the previous inequality]

Therefore $4 < x \wedge x < 6$. [because '$a < b < c$' means '$a < b \wedge b < c$']

Hence $4 < x$. [Rule $\wedge_{use}$]

So $|x-5| < 1 \Rightarrow 4 < x$. [Rule $\Rightarrow_{prove}$]

Hence $\boxed{x \in \mathbb{R} \Rightarrow (|x-5| < 1 \Rightarrow 4 < x)}$. [Rule $\Rightarrow_{prove}$]

END OF PROOF.

4 The precise definition of the notion of "propositional form"

Suppose we are given an *alphabet* $\mathcal{A}$, that is, a set of letters or letter-like symbols that will be called "propositional variables." For example, $\mathcal{A}$ could be $\{A, B, C\}$ (that is, the set consisting of the three letters A, B, C). Or $\mathcal{A}$ could be $\{A, B, C, D, E, F\}$. Or $\mathcal{A}$ could be $\{P, Q, R, S, T, U, V, W\}$. Or $\mathcal{A}$ could be an infinite set, say, the set consisting of the symbols P_1, P_2, P_3, and so on, so that P_n is a member of $\mathcal{A}$ for every natural number $\mathbb{N}$.

Using the alphabet $\mathcal{A}$, we define "propositional strings" as follows: a **propositional string** with variables in $\mathcal{A}$ is a string S of symbols such that each symbol in S is either (a) a member of $\mathcal{A}$, or (b) one of the propositional connectives $\sim$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, or (c) a left parenthesis or a right parenthesis. For example, if $\mathcal{A} = \{A, B, C\}$, then the following are propositional strings:

$$\begin{array}{ll}
A & BAB)))((A\wedge \Rightarrow \\
A \wedge B & \sim A \\
AB\wedge & \sim A \wedge B \\
(A \wedge B \wedge C) \vee D & \sim (A \wedge B) \\
((A \wedge B) \wedge C) \vee D & (\sim A) \wedge B \\
\wedge\vee \sim (BA \Rightarrow & (\sim A)(\wedge B\,.
\end{array}$$

We now want to specify exactly how to distinguish those propositional strings that are "well-formed" (that is, are acceptable representations of sentences) from those that are not well-formed. (For example, the strings

$$\begin{array}{l}
A \\
A \wedge B \\
(A \wedge B \wedge C) \vee D \\
((A \wedge B) \wedge C) \vee D \\
\sim A \\
\sim (A \wedge B) \\
(\sim A) \wedge B
\end{array}$$

are well-formed, but the strings

$$\begin{array}{l}
AB\wedge \\
\wedge\vee \sim (BA \Rightarrow \\
BAB)))((A\wedge \Rightarrow \\
\sim A \wedge B \\
(\sim A)(\wedge B
\end{array}$$

are not.)

In order to do this, we have to deal with a difficulty. When, for example, we combine the strings A and $B \wedge C$ by means of the connective $\vee$, we write $A \vee (B \wedge C)$. But when we combine $A \Rightarrow B$ and $B \wedge C$ by means of $\vee$, we write $(A \Rightarrow B) \vee (B \wedge C)$. In other words, when a string S is combined with other strings, then S remains unchanged if it is just a letter, but it is surrounded by parentheses if it is a string such as $A \Rightarrow B$, consisting of more than just one letter.

To make this precise, we introduce the following notation: if S is a propositional string consisting of a single symbol in $\mathcal{A}$, then S^* will stand for S. And if S is any other propositional string, then S^* will stand for (S). For example, if S is A then S^* is A, but if S is $A \wedge B$ then S^* is $(A \wedge B)$.

Now, here are the rules defining "well-formed formula" (wff):

WFF1. If S consists of a single letter in $\mathcal{A}$, then S is a wff.

WFF2. If S is a wff then $\sim S^*$ is a wff.

WFF3. If S and T are wff's then $S^* \Rightarrow T^*$ and $S^* \Leftrightarrow T^*$ are wff's.

WFF4. If n is a natural number, $n > 1$, and $S_1, S_2, \cdots, S_n$ are wff's, then $S_1^* \wedge S_2^* \wedge \cdots \wedge S_n^*$ and $S_1^* \vee S_2^* \vee \cdots \vee S_n^*$ are wff's.

WFF5. Only those strings that are obtainable by repeated applications of WFF1, WFF2, WFF3 and WFF4 are wff's.

Example 1. Let $\mathcal{S}$ be the string $\sim (P \wedge Q)$. Let us prove that $\mathcal{S}$ is well-formed.

1. By Rule WFF1, the one-letter strings P, Q, are well-formed. (*At this point, we know that P and Q are well-formed.*)

2. By Rule WFF4 (with $n = 2$), the string $P \wedge Q$ is well-formed, because P and Q are well-formed. (*At this point, we know that P, Q, and $P \wedge Q$ are well-formed.*)

3. By Rule WFF2 the string $\sim (P \wedge Q)$ is well-formed, because $P \wedge Q$ is well-formed. (*At this point, we have found out that $\mathcal{S}$ is well-formed, so our proof is complete.*)

Example 2. Let $\mathcal{S}$ be the string

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

Let us prove that $\mathcal{S}$ is well-formed.

1. By Rule WFF1, the one-letter strings P, Q, R are well-formed. (*At this point, we know that P, Q, R are well-formed.*)
2. By Rule WFF3 the strings $P \Rightarrow Q$ and $P \Rightarrow R$ are well-formed, because P, Q and R are well-formed. (*At this point, we know that P, Q, R, $P \Rightarrow Q$, and $P \Rightarrow R$ are well-formed.*)
3. By Rule WFF4 (with $n = 2$), the string $P \wedge Q$ is well-formed, because P and Q are well-formed. (*At this point, we know that P, Q, R, $P \Rightarrow Q$, $P \Rightarrow R$, and $P \wedge Q$ are well-formed.*)
4. By Rule WFF2, the string $\sim R$ and the string $\sim (P \wedge Q)$ are well-formed, because R and $P \wedge Q$ are well-formed. (*At this point, we know that P, Q, R, $P \Rightarrow Q$, $P \Rightarrow R$, $P \wedge Q$, $\sim R$, and $\sim (P \wedge Q)$ are well-formed.*)
5. By Rule WFF3, the string $Q \Rightarrow (\sim R)$ is well-formed, because Q and $\sim R$ are well-formed. (*At this point, we know that P, Q, R, $P \Rightarrow Q$, $P \Rightarrow R$, $P \wedge Q$, $\sim R$, $\sim (P \wedge Q)$, and $Q \Rightarrow (\sim R)$ are well-formed.*)
6. By Rule WFF4, with $n = 3$, the string
$$(P \Rightarrow Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow (\sim R))$$
is well-formed, because $P \Rightarrow Q$, $P \Rightarrow R$, and $Q \Rightarrow (\sim R)$ are well-formed. (*At this point, we know that P, Q, R, $P \Rightarrow Q$, $P \Rightarrow R$, $P \wedge Q$, $\sim R$, $\sim (P \wedge Q)$, $Q \Rightarrow (\sim R)$, and $(P \Rightarrow Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow (\sim R))$ are well-formed.*)
7. By Rule WFF3, the string
$$((P \Rightarrow Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow (\sim R))) \Rightarrow (\sim (P \vee Q))$$
is well-formed, because $(P \Rightarrow Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow (\sim R))$ and $\sim (P \vee Q)$ are well-formed. (*At this point, we have finally shown that $\mathcal{S}$ is well-formed, so our proof is finished*)

Question for you to think about. Let $\mathcal{S}$ be the string
$$((P \Rightarrow Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow (\sim R)) \Rightarrow (\sim (P \vee Q)) \ .$$
How would you prove that $\mathcal{S}$ is *not* well-formed? (*This is not easy. You need a clever idea. Think of how the number of left parentheses in a wff compares with the number of right parentheses.*)

5 More logical rules

- **Rule** $\Leftrightarrow_{use}$ says:

From	$P \Leftrightarrow Q$
you can go to	$P \Rightarrow Q$,

and

From	$P \Leftrightarrow Q$
you can go to	$Q \Rightarrow P$,

- **Rule** $\Leftrightarrow_{prove}$ says:

From	$P \Rightarrow Q$
and	$Q \Rightarrow P$
you can go to	$P \Leftrightarrow Q$.

- **Rule** $\forall_{use}$ (also known as the *specialization rule*) says:

(1) If a is any constant term, then

From	$(\forall x)P(x)$
you can go to	$P(a)$.

(2) If a is any constant term, then

From	$(\forall x \in U)P(x)$
and	$a \in U$
you can go to	$P(a)$.

Example. If you have

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

and you take $a = 0.8$, then you can go to

$$0.8 > 0 \Rightarrow 0.8 + \frac{1}{0.8} \geq 2$$

by the specialization rule. Since, in addition, it is true that $0.8 > 0$, we can use Modus Ponens and conclude that

$$0.8 + \frac{1}{0.8} \geq 2\,.$$

(Incidentally, you can verify directly that $0.8+\frac{1}{0.8} \geq 2$. Indeed, $0.8 = \frac{8}{10}$ and $\frac{1}{0.8} = \frac{10}{8}$, so $0.8 + \frac{1}{0.8} = \frac{8}{10} + \frac{10}{8} = \frac{64+100}{80}\frac{164}{80} > \frac{160}{80} = 2$.)

- **Rule** $\exists_{use}$ says:
  (1) If you have $(\exists x)P(x)$ then you can pick an x such that $P(x)$ and give it a name. (For example, you could say "Pick an x such that $P(x)$ and call it c, so $P(c)$ is true," or even "Pick an x such that $P(x)$ and call it x, so $P(x)$ is true.")
  (2) If you have $(\exists x \in U)P(x)$ then you can pick an $x \in U$ such that $P(x)$ and give it a name. (For example, you could say "Pick an $x \in U$ such that $P(x)$ and call it c, so $c \in U$ and $P(c)$ are true," or even "Pick an $x \in U$ such that $P(x)$ and call it x, so $x \in U$ and $P(x)$ are true.")

In both cases, **the name you choose for the x you pick cannot be something already in use**. For example, if you know that a is even and b is even, this means that $(\exists x \in \mathbb{Z})a = 2x$ and $(\exists x \in \mathbb{Z})b = 2x$, so you can say "pick an x such that $2x = a$ and call it x" but then you cannot say "pick an x such that $2x = b$ and call it x," because 'x' is already in use as the 'x' you have picked for a.

Example. Let me show you what horrible mistakes one can mak e if one does not respect the above restriction. Let us "prove" that "if a is even and b is even then $a + b$ is divisible by 4." *"Proof."* Since a is even, $(\exists x \in \mathbb{Z})a = 2x$, so we may pick x such that $a = 2x$. Since b is even, $(\exists x \in \mathbb{Z})b = 2x$, so we may pick x such that $b = 2x$. Then $a+b = 2x+2x = 4x$, so $a+b$ is divisible by 4. So **we have "proved" something false!!!** (Of couse, the statement "if a is even and b is even then $a+b$ is divisible by 4" is false! If this is not clear to you, just try $a = 4$ and $b = 2$ and see what happens.) What is wrong? **What is wrong is that we picked an x twice and both times we called it x.** If you do things correctly, you would have to write

> Since a is even, $(\exists x \in \mathbb{Z})a = 2x$, so we may pick x such that $a = 2x$. Since b is even, $(\exists x \in \mathbb{Z})b = 2x$, so we may pick x such that $b = 2x$ and call it y. Then $a + b = 2x + 2y$.

and now *you cannot conclude that* $a + b$ *is divisible by* 4.

My own recommendation. When you pick an x such that $P(x)$, do not call it x[4]. Call it k, or j, or any letter or symbol you want which is not in use. And then, if you have to pick another x, use a new letter. For example, when you pick x such that $a = 2x$, call it k, or call it x_a ("the x corresponding to a") and then when you pick your second x (i.e., an x such that $b = 2x$), call it j, or x_b.

- **Rule** $\exists_{prove}$ (also known as the *witness rule*) says:

  (1) If you have produced an object a such that $P(a)$, then you can go to $(\exists x)P(x)$.

  (2) If you have produced an object a such that $a \in U$ and $P(a)$, then you can go to $(\exists x \in U)P(x)$.

  Example. Let us prove that $(\exists x \in \mathbb{Z})x^2 = 4$. *Proof.* Let $a = 2$. Then $a^2 = 2^2 = 4$. So $(\exists x \in \mathbb{Z})x^2 = 4$ by the witness rule.

- The **tautology proof rule** says that *you can bring in an instance of a tautology any time you want.*

  Example. Let us show that if A, B are sentences, and you have $A \vee B$, $A \Rightarrow C$, and $B \Rightarrow C$, then you can go to C. (This is the proof by cases rule, so what I am saying here is that you do not need the proof by cases rule, because you can achieve the same thing using just the tautology rule and Modus Ponens.)

  Here is how you do it:

[4] If you call it x, it would be like picking a cow—knowing that there are cows—and calling her "cow". You are free to do it, but it's not a good idea. Especially, because if you then go and pick a second cow, you cannot also call it "cow". since then you would have two different things with the same name, which in mathematics is forbidden. A cow should called Daisy, or Suzy, or Clarabella, but not "cow."

(1) $A \vee B$
(2) $A \Rightarrow C$
(3) $B \Rightarrow C$
(4) $(A \vee B) \Rightarrow)(((A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow C)$ [instance of tautology]
(5) $((A \Rightarrow C) \wedge (B \Rightarrow C)) \Rightarrow C$ [Modus Ponens, from (1) and (4)]
(6) $(A \Rightarrow C) \wedge (B \Rightarrow C)$ [Rule $\wedge_{prove}$, from (2) and (3)]
(7) C [Modus Ponens, from (5) and (6)]

6 More examples of proofs

In the next two examples, I am showing you some proofs with lots of details and justifications. **You are not expected to write your proofs like this, with so much detail.** But I still want your proofs to have the kind of structure you see in these examples. In particular, your proofs should have clearly identifialble **steps**, and it should be possible to justify each step, even if you do not write down the justification. (My advice: write as many justifications as you can.) In particular, it should be clear where you are using your hypothesis to justify a step or steps. (For example, in the first proof below, pay attention to where we used the hypothesis that $x > 0$.)

Theorem. For any positive real number x, the inequality $x + \frac{1}{x} \geq 2$ holds. (Symbolically: $(\forall x \in \mathbb{R})(x > 0 \Rightarrow x + \frac{1}{x} \geq 2)$.) *Proof.*

Let $x \in \mathbb{R}$ be arbitrary. [Assumption]
Assume $x > 0$. [Assumption]
Assume $\sim x + \frac{1}{x} \geq 2$. [Assumption]
Then $x + \frac{1}{x} < 2$. [Because if $\sim a \geq b$ then $a < b$]
Then $(x + \frac{1}{x})^2 < 4$. [Because $x > 0$, so $x + \frac{1}{x} > 0$]
So $x^2 + \frac{1}{x^2} + 2 < 4$. [Because $(x + \frac{1}{x})^2 = x^2 + \frac{1}{x^2} + 2$]
Therefore $x^2 + \frac{1}{x^2} - 2 < 0$. [Subtracting 4 from both sides]
Hence $(x - \frac{1}{x})^2 < 0$. [Because $(x - \frac{1}{x})^2 = x^2 + \frac{1}{x^2} - 2$]
So $\sim (x - \frac{1}{x})^2 \geq 0$. [Because if $a < 0$ then $\sim a \geq 0$]
But $(x - \frac{1}{x})^2 \geq 0$. [Because if $a \in \mathbb{R}$ then $a^2 \geq 0$]
So $x + \frac{1}{x} \geq 2$. [Proof by contradiction rule]
Hence $x > 0 \Rightarrow x + \frac{1}{x} \geq 2$. [Deduction rule]
Therefore $\boxed{(\forall x \in \mathbb{R})(x > 0 \Rightarrow x + \frac{1}{x} \geq 2)}$. [Generalization rule]

END OF PROOF

Theorem. There is a real number with the property that for any two larger numbers there is another real number that is larger than the sum of the two numbers and less than their product. (Symbolically:
$(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((y > x \wedge z > x) \Rightarrow (\exists w \in \mathbb{R})(w > y + z \wedge w < yz)).$)

Proof.

Let $x = 2$ [Assumption]
Let $y \in \mathbb{R}$ [Assumption]
Let $z \in \mathbb{R}$ [Assumption]
Assume $y > x \wedge z > x$ [Assumption]
Then $y > 2 \wedge z > 2$ [Because $x = 2$]
Also, $y \geq z \vee z \geq y$ [Because if $a, b \in \mathbb{R}$ then $a \geq b \vee b \geq a$]
Assume $y \geq z$ [Assumption]
Then $y + z \leq 2y < yz$ [Because $2 < z$]
So $y + z < yz$ [Consequence of previous step]
Hence $y \geq z \Rightarrow y + z < yz$ [Deduction rule]
Assume $z \geq y$ [Assumption]
Then $y + z \leq 2z < yz$ [Because $2 < y$]
So $y + z < yz$ [Consequence of previous step]
Hence $z \geq y \Rightarrow y + z < yz$ [Deduction rule]
So $y + z < yz$ [Proof by cases rule]
Let $w = \frac{y+z+yz}{2}$ [Assumption]
Then $w > \frac{y+z+y+z}{2} = y + z$ [Because $yz > y + z$]
And $w < \frac{yz+yz}{2} = yz$ [Because $y + z < yz$]
So $w > y + z \wedge w < yz$ [Rule $\wedge_{prove}$]
So $(\exists w \in \mathbb{R})(w > y + z \wedge w < yz)$ [Rule $\exists_{prove}$]
Therefore $(y > x \wedge z > x) \Rightarrow (\exists w \in \mathbb{R})(w > y + z \wedge w < yz)$
[Deduction rule]
So $(\forall z \in \mathbb{R})((y > x \wedge z > x) \Rightarrow (\exists w \in \mathbb{R})(w > y + z \wedge w < yz))$
[Rule $\forall_{prove}$]
So $(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((y > x \wedge z > x) \Rightarrow (\exists w \in \mathbb{R})(w > y + z \wedge w < yz))$
[Rule $\forall_{prove}$]

Hence

$$\boxed{(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})((y > x \wedge z > x) \Rightarrow (\exists w \in \mathbb{R})(w > y + z \wedge w < yz))}$$

[Rule $\exists_{prove}$]

END OF PROOF

7 Homework assignments no. 2, due on Thursday September 18, and no. 3, due on Thursday September 25.

Homework No. 2:

1. Book, Exercises 1.4 (pages 37, 38, 39). Problem 2, Problem 5(b),(c), Problem 6(a),(d),(e), Problem 8, Problem 11(b).

2. Book, Exercises 1.5 (pages 44, 45, 46). Problem 6(a), Problem 11.

3. Book, Exercises 1.6 (pages 53, 54, 55, 56). Problem 1(e),(h), Problem 2(a), Problem 5(a),(d),(g), Problem 7(b),(i),(j), Problem 8(e),(f),)h).

Homework No. 3:

1. Book, Exercises 2.1 (pages 76, 77, 78). Problem 1(b),(e),(f)' Problem 3(b),(d),(f),(h),(j), Problem 4(b),(d),(f),(h),(j),(l), Problem 6(b),(d),(e), Problem 7(b),(d),(e),(f), Problem 19(a),(b),(d),(h),(f),(g).

2. Book, Exercises 2.2 (pages 83, 84, 85, 86). Problem 10(b),(f),(g), Problem 13(b),(c), . Problem 14(d),(f), Problem 15(a),(b),(c),(d), Problem 17(b),(c),(f),(h).

8 The first midterm exam

The first midterm exam will be on **Tuesday, October 14**.

9 Homework assignment no. 4, due on Thursday October 2

1. Book, Exercises 2.5 (pages 116, 117, 118). Problem 8. (Do not use the division theorem proved in class, but give a proof similar to the one we gave in class.)

In the following problems, we use "$a|b$" to indicate that a divides b. (The definition of "divides" is in the book, page xii.) A **rational number** is a real number x such that $x = \frac{m}{n}$ for some integers m, n such that $n \neq 0$. We write $\mathbb{Q}$ to denote the set of all rational numbers, and $\mathbb{R}$ to denote the set of all real numbers. Then

$$(\forall x \in \mathbb{R})\Big(x \in \mathbb{Q} \Leftrightarrow (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(n \neq 0 \wedge x = \frac{m}{n}\ )\Big)\,.$$

A rational number can be expressed in many ways as a quotient of integers. For example, 3.6 is equal to $\frac{36}{10}$, and also to $\frac{72}{20}$, to $\frac{-36}{-10}$, and to $\frac{18}{5}$. A **coprime fractional expression** of a rational number x is an expression of x as $\frac{m}{n}$, where m, n are integers, $n \neq 0$, and in addition m and n have no common factors greater than 1 (that is $\sim (\exists k \in \mathbb{N})(k > 1 \wedge k|m \wedge k|n)$). For example, if we write $3.6 = \frac{36}{10}$, then this is not a coprime fractional expression of 3.6, because 36 and 10 are both divisible by 2, but $3.6 = \frac{18}{5}$ is a coprime fractional expression of 3.6, because 18 and 5 have no common factors.

2. Prove that every rational number has a coprime fractional expression. (Hint: consider all possible ways of writing $x = \frac{m}{n}$ with $m \in \mathbb{Z}$, $n \in \mathbb{N}$, and then use the WOP to pick one with the smallest possible value of n.)

3. Prove that if x, y are integers such that $3|x$ and $5|y$ then $15|xy$.

4. Prove that if x is an integer such that $3|x$ and $5|x$ then $15|x$. Do **not** use the theorem that says that every integer is a product of primes in a unique way. (Hint: write $1 = 10 - 9$ and multiply both sides by x.)

10 Homework assignment no. 5, due on Thursday October 9

In this assignment, the rules of the game are slightly changed. If you are asked to prove something, the answer could be "It cannot be proved because it isn't true," followed by a proof that the statement isn't true. For example, if you are asked to prove that the equation $x^2 + 1 = 0$ *has a real solution (i.e., that* $(\exists x \in \mathbb{R})x^2 + 1 = 0$*), the answer should be "I cannot prove this because it isn't true. Here is a proof that the statement isn't true, i.e., that the equation* $x^2 + 1 = 0$ *does not have a real solution: suppose there exists an* $x \in \mathbb{R}$ *such that* $x^2 + 1 = 0$*; pick one such* x *and fix it from now on; then* $x^2 \geq 0$*, because the square of any real number is* ≥ 0*; so* $x^2 + 1 > 0$*, because* $1 > 0$*, so* $x^2 + 1 > x^2 \geq 0$*; but* $x^2 + 1 = 0$*, so* $0 > 0$*; on the other hand,* $\sim 0 > 0$*; so we got a contradiction. Hence* $\sim (\exists x \in \mathbb{R})x^2 + 1 = 0$*."*

Recall that

$$\mathbb{Q} = \{x \in \mathbb{R} : x \text{ is rational}\},$$

that is

$$\mathbb{Q} = \left\{x \in \mathbb{R} : (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(n \neq 0 \wedge x = \frac{m}{n})\right\}.$$

1. Prove each of the following statements:

   1. i. If x, y are rational numbers then $x + y$ is rational.
   1. ii. If x, y are rational numbers then $x \cdot y$ is rational.
   1. iii. If x, y are rational numbers then $x - y$ is rational.
   1. iv. If x, y are rational numbers and $y \neq 0$ then $\frac{x}{y}$ is rational.
   1. v. If x is a rational number and y is irrational then $x + y$ is irrational.
   1. vi. If x is a rational number and y is irrational then $x \cdot y$ is irrational.
   1. vii. If x, y are irrational numbers then $x + y$ is irrational.
   1.viii. If x, y are irrational numbers then $x \cdot y$ is irrational.

2. Prove that $\sqrt{5} \notin \mathbb{Q}$. You are allowed to use the result of Homework No. 4, Problem 2, and the FTA (Fundamental Theorem of Arithmetic), stated below. You may also use, instead of the FTA, the following: if a, b, p are integers, p is prime, and p divides ab, then p divides a or p divides b.

3. Prove that $\sqrt{3}+\sqrt{5} \notin \mathbb{Q}$.
4. Prove that $\sqrt{2}+\sqrt{3}+\sqrt{5} \notin \mathbb{Q}$.
5. Book, page 65, problem 8. (In addition to Parts (a), (b) and (c), add Part (d): $a = 112$, $b = 53$.)
6. Book, page 65, problem 10.
7. Book, page 117, Problem 11. (Naturally, in order to do this problem you have to read Problem 14 on Page 109, but you do not have to do that problem.)

STATEMENT OF THE FUNDAMENTAL THEOREM OF ARITHMETIC. Let $n \in \mathbb{N}$ be such that $n > 1$. Then there exist $m \in \mathbb{N}$ and prime numbers $p_1, p_2, \ldots, p_m$ such that

a. $p_1 \leq p_2 \leq \cdots \leq p_m$,

b. $n = p_1 p_2 \cdots p_m$,

c. if $\tilde{m} \in \mathbb{N}$ and $\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_{\tilde{m}}$ are prime numbers such that

$$\tilde{p}_1 \leq \tilde{p}_2 \leq \cdots \leq \tilde{p}_{\tilde{m}} \text{ and } n = \tilde{p}_1 \tilde{p}_2 \cdots \tilde{p}_{\tilde{m}} .$$

then $\tilde{m} = m$ and in addition $\tilde{p}_1 = p_1$, $\tilde{p}_2 = p_2$, ..., $\tilde{p}_m = p_m$.

11 Homework assignment no. 6, due on Thursday October 16

This assignment is very short, because you have the first midterm test on Tuesday, October 14.

Recall that

$$\mathbb{Q} = \{x \in \mathbb{R} : x \text{ is rational}\},$$

that is

$$\mathbb{Q} = \left\{x \in \mathbb{R} : (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(n \neq 0 \wedge x = \frac{m}{n})\right\} .$$

1. Prove that $11^{1/2} + 11^{1/3} \notin \mathbb{Q}$. You are allowed to use the result of Homework No. 4, Problem 2, and the FTA (Fundamental Theorem of Arithmetic). (You may also use, instead of the FTA, the following: if a, b, p are integers, p is prime, and p divides ab, then p divides a or p divides b.) You are also allowed to use any of the results of Problem 1 of Homework assignment No. 5, as long as they are true. (Recall that Homework assignment No. 5 some of the statements could be false.)

2. Prove that if $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and $\sim (a = 0 \wedge b = 0)$, then there exist integers α, β such that $\alpha a + \beta b > 0$.

12 Homework assignment no. 7, due on Thursday October 23

1. Book, Exercises 2.2 (pages 83, 84, 85, 86). Problem 16.

2. Book, Exercises 1.7 (pages 64 to 67). Problem 1(a),(b),(c).

3. Prove that

i. If S is a subset of $\mathbb{R}$ such that there exists a smallest member of S—that is, $(\exists s)(s \in S \wedge (\forall t)(t \in S \Longrightarrow s \leq t))$—then there exists a unique smallest member of S; that is

$$(\exists! s)(s \in S \wedge (\forall t)(t \in S \Longrightarrow s \leq t)) .$$

ii. If S is a subset of $\mathbb{R}$ such that there exists a largest member of S—that is, $(\exists s)(s \in S \wedge (\forall t)(t \in S \Longrightarrow s \geq t))$— then there exists a unique largest member of S; that is

$$(\exists! s)(s \in S \wedge (\forall t)(t \in S \Longrightarrow s \geq t)) .$$

iii. The set $\mathbb{Z}$ does not have a smallest member and does not have a largest member.

iv. The set $\mathbb{N}$ has a smallest member but does not have a largest member.

v. Let $S = \{x \in \mathbb{R} : x > 0\}$. Then S does not have a smallest member.

4. Prove that if S is a nonempty set of integers which is bounded below then S has a smallest member. (A set S of integers is **bounded below** if there exists an integer n such that $n \leq s$ for every $s \in S$.) *Hint for the proof*: Pick an integer $\bar{n}$ such that $\bar{n} \leq s$ for every $s \in S$, and consider the set T of all the numbers $s + 1 - \bar{n}$, for $s \in S$. (That is, $T = \{t \in \mathbb{Z} : (\exists s \in S)t = s+1-\bar{n}\}$.) Apply the WOP to get a smallest member $\bar{t}$ of T. (To be able to do this, you need to show that $T \subseteq \mathbb{N}$ and $T \neq \emptyset$.) Then let $\bar{s} = t + \bar{n} - 1$, and show that $\bar{s}$ is a smallest member of S.

5. Prove that if S is a nonempty set of integers which is bounded above then S has a largest member. (A set S of integers is **bounded above** if there exists an integer n such that $n \geq s$ for every $s \in S$.) *Hint for the proof*: Pick an integer $\bar{n}$ such that $\bar{n} \geq s$ for every $s \in S$, and consider the set T of all the numbers $\bar{n} + 1 - s$, for $s \in S$. (That is, $T = \{t \in \mathbb{Z} : (\exists s \in S)t = \bar{n} + 1 - s\}$.) Apply the WOP to get a smallest member $\bar{t}$ of T. (To be able to do this, you need to show that $T \subseteq \mathbb{N}$ and $T \neq \emptyset$.) Then let $\bar{s} = \bar{n}+1-\bar{t}$, and show that $\bar{s}$ is a largest member of S.

6. Prove or disprove each of the following:

i. $(\exists! x \in \mathbb{R})x^3 = 2x$,

ii. $(\exists! x \in \mathbb{Z})x^3 = 2x$.

13 Homework assignment no. 8, due on Thursday October 30

1. Let S be the statement "If a is an arbitrary integer, then there exists an integer k such that $a = 4k$ or $a = 4k+1$ or $a = 4k+2$ or $a = 4k+3$."

1.i. Rewrite S in formal language.

1.ii. Prove S.

2. Prove that if n is an odd integer then there exists an integer k such that $n^2 = 4k + 1$.

3. Prove that if m, n are integers such that $m^2 + n^2$ is odd then there exists an integer k such that $m^2 + n^2 = 4k + 1$.

4. Prove that the number $2,370,863$ cannot be the sum of two squares of integers. (That is, prove that

$$\sim (\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})m^2 + n^2 = 2,370,863\,. \qquad)$$

5. Two integers p, q are **coprime** if $\sim (\exists k \in \mathbb{Z})(k > 1 \wedge k|p \wedge k|q)$. Prove: if p, q are integers such that $p \neq 0$ or $q \neq 0$, then p and q are coprime if and only if 1 is an integer linear combination of p and q. (Recall that an **integer linear combination** of p and q is an integer c such that $(\exists \alpha \in \mathbb{Z})(\exists \beta \in \mathbb{Z})c = \alpha p + \beta q$.)

6. Prove: If two integers p, q are prime, then p and q are coprime if and only if $p \neq q$.

7. Prove: If two integers p, q are such that p is prime and p does not divide q, then p and q are coprime.

8. Prove: If two integers p, q are coprime then, whenever a is an integer such that $p|a$ and $q|a$, it follows that $pq|a$. (Hint: express 1 as an integer linear combination of p and q and multiply both sides by a.)

9. Prove that the result of Problem 8 can fail to be true if p and q are not required to be coprime.

14 Homework assignment no. 9, due on Thursday November 6

This assignment consists of a single, long problem. Try to do as many parts as you can, but do not worry if you do not do everything.

Try to structure your proofs as in the model solutions. given below. Make sure that in the problems involving sums and products of finite families of numbers, you use the inductive definitions given below.

The problem is **Problem 8, on Pages 106-107 of the book, all nonstarred part except Part (e).**

Examples of inductive definitions.

Example 1. *Inductive definition of the sum of a finite family of numbers.*

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

Remark. One often writes

$$a_1 + a_2 + \cdots + a_n$$

instead of $\sum_{k=1}^{n} a_k$.

Example 2. *Inductive definition of the product of a finite family of numbers.*

$$\begin{aligned}\prod_{k=1}^{1} a_k &= a_1\,,\\ \prod_{k=1}^{n+1} a_k &= \Big(\prod_{k=1}^{n} a_k\Big) \cdot a_{n+1} \quad \text{for all} \quad n \in \mathbb{N}\,.\end{aligned}$$

Example 3. *Inductive definition of the factorial.*

$$\begin{aligned}1! &= 1\,,\\ (n+1)!k &= n! \cdot (n+1) \quad \text{for all} \quad n \in \mathbb{N}\,.\end{aligned}$$

Remarks.

1. The inductive definition of the factorial is usually extended by also defining the factorial of zero. By definition,
$$0! = 1\,.$$

2. Naturally, one could also define the factorial by the formula
$$n! = \prod_{k=1}^{n} k \qquad\qquad \text{for all} \;\; n \in \mathbb{N}\,.$$

Two model solutions

Example 1. Prove that $4^n = 1$ is divisible by 3 for every natural number 2 (i.e., that $(\forall n \in \mathbb{N})3|4^n - 1$.

Answer. Let $P(n)$ be the statement " $3|4^n - 1$".
We want to prove that $(\forall n \in \mathbb{N})P(n)$. We do it by induction.
In the *basis step*, we have to prove $P(1)$. Now, the statement $P(1)$ says that 3 divides $4 - 1$, which is true, since $4 - 1 = 3$.
In the *inductive step*, we have to prove that $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$.
Here is the proof:
Let $n \in \mathbb{N}$ be arbitrary.
Assume $P(n)$.
Then $3|4^n - 1$.
Pick an integer k such that $4^n - 1 = 3k$.
Then $4^{n+1}-1=4^{n+1}-4^n+4^n-1=4^n(4-1)+3k=4^n\cdot 3+3k = 3(4^n+k)$.
So $4^{n+1} - 1 = 3(4^n + k)$.
Therefore 3 divides $4^{n+1} - 1$.
So $P(n + 1)$ holds.
Hence $P(n) \Rightarrow P(n + 1)$.
So $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n + 1))$, completing the inductive step.
Therefore the PMI implies that $(\forall n \in \mathbb{N})P(n)$, i.e. that $\boxed{(\forall n \in \mathbb{N})3|4^n - 1}$.

Example 2. Prove that
$$\sum_{k=1}^{n} k^3 = \Big(\frac{n(n+1)}{2}\Big)^2 \quad \text{for all} \;\; n \in \mathbb{N}\,.$$

Answer. Let $P(n)$ be the statement " $\sum_{k=1}^{n} k^3 = \Big(\frac{n(n+1)}{2}\Big)^2$ ".

We want to prove that $(\forall n \in \mathbb{N})P(n)$. We do it by induction.
In the *basis step*, we have to prove $P(1)$. Now, the statement $P(1)$ says that $\sum_{k=1}^{1} k^3 = \left(\frac{1(1+1)}{2}\right)^2$, that is, that $1 = 1$, which is true.
In the *inductive step*, we have to prove that

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

Here is the proof:

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

Assume $P(n)$.

Then $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Using the inductive definition of the summation, we have

$$\sum_{k=1}^{n+1} k^3 = \left(\sum_{k=1}^{n} k^3\right) + (n+1)^3\,.$$

Since $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$, we have

$$\sum_{k=1}^{n+1} k^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3\,.$$

Also
$$\begin{aligned}\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 &= \frac{n^2(n+1)^2}{4} + (n+1)^3 \\ &= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\ &= \frac{(n^2 + 4(n+1))(n+1)^2}{4} \\ &= \frac{n^2 + 4n + 4)(n+1)^2}{4} \\ &= \frac{(n+2)^2(n+1)^2}{4} \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2.\end{aligned}$$

Therefore
$$\sum_{k=1}^{n+1} k^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2.$$

So $P(n+1)$ holds.

Hence $P(n) \Rightarrow P(n+1)$.

So $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$, completing the inductive step.

Therefore the PMI implies that $(\forall n \in \mathbb{N})P(n)$, i.e. that $\boxed{(\forall n \in \mathbb{N}) \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2}$.

15 Homework assignment no. 10, due on Thursday November 13

- Book, Page 116, Problem 6(a)(b)(c).
- Book, Pages 127-8-9, Problems 3, 10, 11(c)(d), 15, 18(c).