Day 4: Friday, 1/27/2017
Return chapter 1 hw

Discuss access to the answer keys to assignments and practice questions in the reading.

Take questions on homework; collect regular hw on chapter 2. Reminder: 2 quiz problems from chapter 2 will be due on Tuesday. The solutions to the homework should be available on blackboard tonight. If you have any uncertainty about the assigned homework, you may wish to check the answers before working on the quiz problems. **Reminder:** quiz problems are open note and open book, but otherwise no consultation of references or people is permitted.

Lecture Topic 1: Complete discussion of quantification.

1. Definition and meaning of $\exists$ and $\forall$ symbols
2. Notation: (quantification statement)(open sentence)
   a. This asserts the truth of the open sentence for all of the variable substitutions that are consistent with the quantification
   b. Example: $(\forall\, x \in \mathbb{R})(\, x^2 + 1 > 0\,)$ means "*For every real number x,* $x^2 + 1$ *is positive.*". To be excessively pedantic, you could say "*For every real number x, it is true that* $x^2 + 1$ *is positive.*" to emphasize that fact that you are asserting the truth of the clause in the second parenthesis, but normally we don't go to such rhetorical lengths.
   c. An open sentence in which every variable is quantified is a statement – it may be true or false. The one in the prior example is definitely true. Here is one that is false: $(\forall\, x \in \mathbb{R})(\, x^2 \geq x\,)$. To demonstrate that it is false it is enough to show a single valid x (specified by the first parenthesis) for which the second parenthesis is false. In this case $x = 1/2$ is such an example. Note that this *disproves* the statement $(\forall\, x \in \mathbb{R})(\, x^2 \geq x\,)$. This is a case where a specific example is a valid proof – it is called a counter example.
   d. There can be multiple quantification clauses. For example
      i. $(\,\exists\, x \in \mathbb{R})(\,\forall\, y \in \mathbb{R})(xy = 0)$ [This is true]
      ii. $(\,\exists\, x \in \mathbb{R})(\,\forall\, y \in \mathbb{R})(x + y = 0)$ [This is false]
      iii. $(\,\forall\, x \in \mathbb{R})(\,\exists\, y \in \mathbb{R})(x + y = 0)$ [This is true]
3. Negations of quantified statements follow a general rule of changing $\exists$'s to $\forall$'s and $\forall$'s to $\exists$'s and then negating the final statement. For example:
   a. $\neg(\exists\, x \in \mathbb{R})(x^2 + 1 = 0) \equiv (\forall\, x \in \mathbb{R})(x^2 + 1 \neq 0)$
   b. $\neg(\,\exists\, x \in \mathbb{R})(\,\forall\, y \in \mathbb{R})(xy = 0) \equiv (\,\forall\, x \in \mathbb{R})(\exists\ y \in \mathbb{R})(xy \neq 0)$
4. The negation of a quantified open sentence like the ones in examples 2b and 2c
   a. This has the form $Q = (\forall\, x \in U)(\, P(x))$
   b. Negation is $\neg Q = (\exists\, x \in U)(\, \neg P(x))$. (Means: for *some* x in U $P(x)$ is false)

c. This justifies symbolically the idea that a single counter-example disproves the statement Q.

d. For the example in 2c, $\neg(\forall x \in \mathbb{R})(x^2 \geq x) \equiv (\exists x \in \mathbb{R})(x^2 \not\geq x)$. In words, "$(\forall x \in \mathbb{R})(x^2 \geq x)$ is false if and only if $(\exists x \in \mathbb{R})(x^2 \not\geq x)$ is true". So if you demonstrate the truth of $(\exists x \in \mathbb{R})(x^2 \not\geq x)$ by exhibiting a particular value of x for which $x^2 \not\geq x$, that disproves the statement $(\forall x \in \mathbb{R})(x^2 \geq x)$

e. Negations are also used in proofs by contradiction, as we will see later. For now suffice it to say that we sometimes prove $P \rightarrow Q$ by assuming P and $\neg Q$. For this we need some facility forming negations.

f. Example. For a real function f, the definition of f being continuous at a real number a is:
$(\forall \varepsilon \in \mathbb{R}^+)(\exists \delta \in \mathbb{R}^+)(\forall x \in \mathbb{R})((|x - a| < \delta) \rightarrow (|f(x) - f(a)| < \varepsilon))$
where $\mathbb{R}^+$ denotes the set of positive reals. To prove the theorem (f differentiable at a)$\rightarrow$(f continuous at a) by contradiction, we would begin "Suppose f is differentiable at a but f is *NOT* continuous at a." That means we are assuming the negation of the definition of continuity. Using the general rule, we can immediately write that negation as
$(\exists \varepsilon \in \mathbb{R}^+)(\forall \delta \in \mathbb{R}^+)(\exists x \in \mathbb{R})((|x - a| < \delta) \not\rightarrow (|f(x) - f(a)| < \varepsilon))$

Lecture Topic 2: Chapter 3 on writing proofs

1. Overview
   a. We'll see a few simple proof structures
   b. These will be illustrated in the context of properties of the integers connected with divisors and modular arithmetic. Those topics are introduced in order to have something to write proofs about. I won't go into these in detail. Read them.
   c. There are also writing format guidelines Read these too.
2. Direct Proof
   a. Simplest proof structure for proving $P \rightarrow Q$.
   b. The proof is a set of assertions that starts with assumption that P is true, continues with a list of true statements that are derived from the starting assumption and other known information (definitions, prior results, etc), and ends with Q.
   c. Example: Sum of two even numbers is even
      i. Definition of even integer: n is an even integer if it is (evenly) divisible by 2 (in the integers).
      ii. Reformulation: n is an even integer iff $(\exists m \in \mathbb{Z})(n = 2m)$ (is true).

iii. Proof: Suppose that p and q are even integers. Then by the definition of even, there exist integers r and s for which $p = 2r$ and $q = 2s$. Therefore we have

$$m + n = 2r + 2s = 2(r+s).$$

Now define $z = r + s$, which is an integer because $\mathbb{Z}$ is closed under addition. Thus we have shown that $p + q = 2z$ where z is an integer. Therefore, by definition of even integer, $p+q$ is even.

d. Diagram showing the statements we showed were true, and the justification for each step

Statement	Reason it is true
p and q are even integers	Assumed; Hypothesis of the theorem
$(\exists\ r, s \in \mathbb{Z})((p = 2r) \wedge (q = 2s))$	Definition of even integer
$p + q = 2r + 2s = 2(r + s)$	Substitution, distributive law for integers
$r + s \in \mathbb{Z}$	Closure of $\mathbb{Z}$ under addition
$r + s = z$	Definition of the variable z
$p + q = 2z$	Substitution in an earlier equation
$p + q$ is even	Definition of even

Although this may show the proof with more clarity, it is not the way mathematics is written. Organizing your ideas like this can be a good strategy for formulating a proof. But once you are confident that your proof is correct, it has to be translated into normal written prose, as in item ciii above.

e. "Tracing" the proof.

i. Notice that each variable is defined as it is introduced in the proof.

ii. For p and q the allowable replacement set is the even integers. This is what is meant by "Let p and q be even integers." IE, we mean let them be ANY even integers.

iii. So they *might* be 8 and 32, and if so, all of the following statements have to be valid. So let's repeat the proof with those specific numbers:

iv. Suppose that p and q are the even integers 8 and 32. Then by the definition of even, there exist integers r and s for which $8 = 2r$ and $32 = 2s$. In fact, we can see that $r = 4$ and $s = 16$. [note: because r and s are defined in relation to p and q, the replacement sets for r and s are implicitly specified: r can only be $p/2$ and s can only be $q/2$.] Therefore we have

$$8 + 32 = 2\cdot4 + 2\cdot16 = 2(4+16).$$

Now define $z = 4+16 = 20$, which is an integer because $\mathbb{Z}$ is closed under addition. Thus we have shown that $8 + 32 = 2\cdot20$, and we know that 20 is an integer. Therefore, by definition of even integer, $8 + 32$ is even.

v. The fact that everything works out correctly in this way does not certify that the proof is correct. But if the logic is not correct with your specific example, that definitely means there is an error in your proof. Even if you find no error, going

through this process should contribute to your confidence, and give you deeper understanding of how the proof works. And you can use this same technique with a proof you read in the book, to get a better understanding of that proof.

3. Counter Examples
   a. We have already discussed this. If you want to refute a statement of the form $(\forall\, x \in U)(\, P(x))$ it is valid to exhibit an element of U for which P does not hold.
   b. This is often applied when you have a conjecture of the form $(\forall\, x \in U)(\, P(x))$ and are unsure whether it is true or not. If you are unable to prove it, you can try to disprove it.
   c. Example: Some mathematicians and computer scientists are interested in methods to find prime numbers. One idea is this: Take the first n primes, multiply them all together, and then add 1. For example, the first 4 primes are 2, 3, 5, and 7. Multiply them all together and you get 210. Add 1 and you get 211. Now this cannot be divisible by 2, 3, 5, or 7, because of the added 1. And in fact 211 is a prime number. This might suggest the following conjecture: Define $p_1, p_2, p_3, p_4, p_5, \ldots$ to be the positive integer primes, in increasing order. Thus $p_1, p_2, p_3, p_4, p_5, \ldots = 2, 3, 5, 7, 11, \ldots$. Then for any positive integer n, the number $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \cdots \cdot p_n + 1$ is prime. Symbolically, we can write this conjecture as $(\forall\, n \in \mathbb{Z}^+)(p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \cdots \cdot p_n + 1$ is prime). After a few unsuccessful attempts to prove this, we might start to look systematically for a counter example. With $n = 1$ we find $p_1 + 1 = 2+1 = 3$ is prime; $p_1 \cdot p_2 + 1 = 2 \cdot 3 + 1 = 7$ is prime; $p_1 \cdot p_2 \cdot p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$ is prime; and so on. With $n = 6$, we find $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ is not prime. This example disproves the conjecture.

4. Proof by Contradiction
   a. This is an alternate structure to direct proof. If we wish to prove statement P is true, we begin by assuming that P is false, then argue from that to a statement that is a contradiction. That is, a statement that cannot be true.
   b. Example: For every integer n, if n^2 is odd then n is odd. Proof: Suppose the statement is false. Then there must exist an integer n where n^2 is odd but n is not odd. That would imply that n is even. But in that case, $n = 2k$ for some integer k. And then $n^2 = (2k)^2 = (2k)(2k) = 2(k \cdot 2k)$. But this 2 times an integer, and hence even. However, we know that n^2 is even. Thus we have reached a contradiction. This proves that the original statement is true
   c. Why is this valid? Conceptually, either P is true or it is false. If we assume it is false, we are led to an impossibility. (In this specific example, assuming P is false leads to both (n^2 is odd) and (n^{2-} is even).) This shows it is impossible for P to be false, and therefore P must be true.

d. We can also argue symbolically. Our proof actually demonstrates the implication $\neg P \rightarrow C$ where C is a contradiction, and hence false under all conditions. We want to show that we can infer P from this result. In other words, we want to show that

$$[\neg P \rightarrow C] \rightarrow P.$$

We can do this with a truth table, where we allow P to be either true or false, but only allow C to be false:

P	C	$\neg P$	$\neg P \rightarrow C$	$(\neg P \rightarrow C) \rightarrow P$
T	F	F	T	T
F	F	T	F	T

[Remember that $A \rightarrow B$ is only F when A is T and B is F.] The truth table shows that we can infer P from what we proved, namely that the negation of P leads to a contradiction.

e. This is related to earlier comments about negating quantified open sentences. For the example, the statement P we want to prove can be written this way: $(\forall n \in \mathbb{Z})(\ n^2 \text{ odd} \rightarrow n \text{ odd})$. For our proof by contradiction, we assume the negation of this statement:

$$\neg(\forall n \in \mathbb{Z})(\ n^2 \text{ odd} \rightarrow n \text{ odd}) \equiv (\exists n \in \mathbb{Z})(\neg(\ n^2 \text{ odd} \rightarrow n \text{ odd}))$$

But as shown in the book, the negation of $A \rightarrow B$ is equivalent to $(A \wedge \neg B)$. Thus

$$\neg(\forall n \in \mathbb{Z})(\ n^2 \text{ odd} \rightarrow n \text{ odd}) \equiv (\exists n \in \mathbb{Z})((\ n^2 \text{ odd} \wedge n \text{ is not odd})).$$

And that is exactly what we showed in our proof by contradiction.

f. Why would proof by contradiction be useful? For one thing, we have more given information to work with – both the hypothesis of the desired statement, and also the negation of the conclusion. For another, we don't have a specific goal statement to reach. Deriving any contradictory result is sufficient to complete the proof.

5. Cases

a. In a simple proof that $P \rightarrow Q$, we assume P and then obtain a sequence of inferences leading to Q. In some cases, though, P can be true in several different ways, and the proof we give will be different for these different possibilities. This is called a proof by cases.

b. In outline form, a case argument looks like this:
asd

   i. Show that $P \rightarrow (C_1 \vee C_2 \vee C_3 \vee \cdots \vee C_n)$

   ii. Show $C_1 \rightarrow Q$. Also show $C_2 \rightarrow Q$. Also …

c. Usually there are a small number of cases (but in some famous theorems that were thousands of cases). Usually different cases are only used when different proofs are needed.

d. Example: For any integer n, $n^3 - n$ is divisible by 3.
Proof: Let n be an integer. Then either n is divisible by 3, or when n is divided by 3 the is a remainder of 1 or 2. We consider these three cases separately.

Case 1: n is divisible by 3. In this case, we must have $n/3$ is an integer, which we will call t. Thus $n/3 = t$ so $n = 3t$. Now we compute

$$n^3 - n = (3t)^3 - 3t = 27t^3 - 3t = 3(9t^3 - 1).$$

Therefore, $(n^3 - n)/3 = 9t^3 - 1$ which is an integer. This shows that $n^3 - n$ is divisible by 3.

Case 2: n leaves a remainder of 1 when it is divided by 3. In this case, $n - 1$ must be evenly divisible by 3. Therefore $n - 1 = 3t$ for some integer t, and $n = 3t+1$. As before, we compute $n^3 - n = (3t+1)^3 - (3t+1)$. Expanding the cubed term, this leads to

$$n^3 - n = 27t^3 + 27t^2 + 9t+1 - 3t - 1 = 27t^3 + 27t^2 + 6t = 3(9t^3 + 9t^2 + 2t).$$

As before, we see that $(n^3 - n)/3$ is an integer, hence $n^3 - n$ is divisible by 3.

Case 3: n leaves a remainder of 2 when divide by 3. As in case 2, we conclude that $n - 2$ is divisible by 3. But then $n - 2 + 3 = n + 1$ will also be divisible by 3. In particular, if $(n+1)/3$ is the integer t, then $n = 3t - 1$. Following the same course as before, we compute

$$\begin{aligned} n^3 - n &= (3t - 1)^3 - (3t - 1) \\ &= 27t^3 - 27t^2 + 9t - 1 - 3t + 1 \\ &= 27t^3 - 27t^2 + 6t \\ &= 3(9t^3 - 9t^2 + 2t). \end{aligned}$$

And as in the other cases, this shows that $n^3 - n$ is divisible by 3.

Thus we have shown that in all three cases $n^3 - n$ is divisible by 3. This completes the proof.

End of Day