Class notes for February 22, 24, 2022 and Homework 6 – Math 287

Dr Holmes

March 1, 2022

I don't usually put up class notes, but there is a student out of class who requested them, and the second part of today's lecture addresses things which are not in the book. I still owe you an extension to the previous set of notes on logic, and working with sets may induce me to get on it and produce them.

The lecture had two parts, one extending the lecture before the test about strong induction and the kind of extension to recursion which gives the Fibonacci numbers, and one an introduction to basic concepts about sets.

1 Stuff about Strong Induction, Recursion, and Fibonacci-Like sequences, Feb 22 2022

I'm just going to present the examples and theorems I did rather than try to say more about general principles.

Definition: Define a sequence A by $A_1 = 2$, $A_2 = 5$, $A_{k+2} = 5A_{k+1} - 6A_k$.

Calculations: $A_3 = 5A_2 - 6A_1 = (5)(5) - (6)(2) = 13$

$A_4 = 5A_3 - 6A_2 = (5)(13) - (6)(5) = 35$

and so forth

Theorem: For each natural number n, $A_n = 2^n + 3^n$ (as is typical with induction proofs, we aren't told where this statements comes from)

Proof: We prove this by strong induction.

$A_1 = 2 = 1 + 1 = 2^0 + 3^0$, true for $n = 1$.

$A_2 = 5 = 1 + 1 = 2^1 + 3^1$, true for $n = 2$. (we use two pieces of information at the basis).

Let $k \geq 2$ be chosen arbitarily and assume for all m with $1 \leq m \leq k$ that $A_m = 2^m + 3^m$. We already know this for $k = 2$, the basis of our induction.

Our goal is to show that $A_{k+1} = 2^{k+1} + 3^{k+1}$.

We know by definition of the sequence A that $A_{k+1} = 5A_k - 6A_{k-1}$. Notice that this uses our assumption that $k \geq 2$.

Now by inductive hypothesis $5A_k - 6A_{k-1} = 5(2^k + 3^k) - 6(2^{k-1} + 3^{k-1})$.

$5(2^k + 3^k) - 6(2^{k-1} + 3^{k-1}) = (10)2^{k-1} + (15)3^{k-1} - 6(2^{k-1}) - 6(3^{k-1})$
$= 4(2^{k-1}) + 9(3^{k-1}) = 2^{k+1} + 3^{k+1}$

And this completes the proof.

Observation: You might ask...where does this come from? We give a hint...suppose we had a sequence B with $B_{k+2} = 5B_{k+1} - 6B_k$...and make a further guess, $B_k = r^k$ for some r.

$r^{k+2} = 5r^{k+1} - 6r^k$ is true (if $r \neq 0$) if and only if $r^2 = 5r - 6$, that is $r^2 - 5r + 6$, which has roots 2 and 3 which you can find by standard techniques. So the sequence of powers of 2 and the sequence of powers of 3 satisfy this recurrence relation, and it is straightforward to show that adding two sequences which have this property will give a sequence with this property.

Definition: Define $G_k = \sum_{i=1}^{k} F_k$.

Experiment: Compute the first eight terms of this sequence and look for patterns. Two were noticed by students: $G_{k+2} = G_k + G_{k+1} + 1$, and $G_k = F_{k+2} - 1$. I admit freely that I was expecting you all to notice the second one; the first one was a bonus.

It is surprising, perhaps that neither of these proofs needs strong induction. In the coming homework problems involving proofs about Fibonacci numbers, be ready to use strong induction, but also be ready to find that you need nothing more than ordinary induction.

Theorem: For all natural numbers n, $G_{n+2} = G_n + G_{n+1} + 1$

Proof: For $n = 1$, observe that $G_1 = 1, G_2 = 1 + 1 = 2, G_3 = 1 + 1 + 2 = 4$, and $G_3 = 4 = 1 + 2 + 1 = G_1 + G_2 + 1$.

Now fix a natural number k and assume $G_{k+2} = G_k + G_{k+1} + 1$ (ind hyp). The induction goal is to show that $G_{k+3} = G_{k+1} + G_{k+2} + 1$.

$G_{k+3} = \sum_{i=1}^{k+3} F_i = \sum_{i=1}^{k+2} F_i + F_{k+3}$ by the definition of summation
$= G_{k+2} + F_{k+3}$ by definition of G

$= G_k + G_{k+1} + 1 + F_{k+3}$ by ind hyp

$= G_k + G_{k+1} + 1 + F_{k+1} + F_{k+2}$ by definition of F

$= G_k + F_{k+1} + G_{k+1} + F_{k+2} + 1$ regrouping

$= \sum_{i=1}^{k} F_i + F_{k+1} + \sum_{i=1}^{k+1} F_i + F_{k+2} + 1$ definition of G

$= \sum_{i=1}^{k+1} F_i + \sum_{i=1}^{k+2} F_i + 1$ definition of summation

$= G_{k+1} + G_{k+2} + 1$ definition of G; which is what we needed.

Theorem: For all natural numbers n, $G_n = F_{n+2} - 1$

Proof: By induction. $G_1 = 2 - 1 = F_3 - 1$, so the statement is true for $n = 1$.

Fix an arbitrary natural number k. Assume that $G_k = F_{k+2} - 1$. Our goal is to show $G_{k+1} = F_{k+3} - 1$.

$G_{k+1} = \sum_{i=1}^{k+1} F_i$ definition of G

$= \sum_{i=1}^{k} F_i + F_{k+1}$ definition of summation

$= G_k + F_{k+1}$ definition of G

$= F_{k+2} - 1 + F_{k+1}$ ind hyp

$= F_{k+3} - 1$ regrouping and definition of F.

2 Introducing Sets, Feb 22, 2022

The book introduces basic concepts of sets at a level needed for success in more advanced mathematics. You may notice that they have already been using these concepts earlier.

I will take an approach which is a bit more explicit. Without too much logic (I hope) I am going to emulate the book's treatment of natural numbers by giving some primitive notions and axioms governing the notion of set.

Some objects in the mathematical world are sets. This is a primitive notion.

Sets have objects as elements. We write $a \in S$ for a is an element of S. The membership relation is a primitive notion.

Axiom of Members: If a membership relation $a \in S$ holds, we can deduce that S is a set. (It is equivalent to say that any object which is not a set has no elements).

It is common in foundations of mathematics to assume that everything is a set. We will not make this assumption, but neither will we explicitly assume that there are non-sets.

We introduce a familiar piece of notation $\{x, y\}$: this is the set whose only elements are x and y, an unordered pair (if x and y are distinct). We call a set $\{x, x\}$ a singleton and feel free to write $\{x\} = \{x, x\}$.

Axiom of Pairs: For any objects x, y (not necessarily distinct) there is a set $\{x, y\}$. For any z, $z \in \{x, y\}$ if and only if $z = x \vee z = y$.

This notation (which should be familiar to you) can be used to make an important point. Whatever elements are, they are not parts of the sets they belong to. Let a, b be distinct objects and consider the set $\{\{a, b\}\}$. This set has only one element $\{a, b\}$, so at least one of a, b does not belong to it: suppose wlog that $a \notin \{\{a, b\}\}$. So we have $a \in \{a, b\}$ and $\{a, b\} \in \{\{a, b\}\}$ but $a \notin \{\{a, b\}\}$: the membership relation is not transitive. So members of sets are not in general parts of sets: the relationship of part to whole is transitive.

There is another important relation between sets which is a much better candidate for the relation of part to whole between sets.

Definition: The relation $A \subseteq B$ is defined as holding if and only if $(\forall x \in A : x \in B)$: that is, if every element of A is an element of B.

Theorem: For any set A, $A \subseteq A$.

Theorem: If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

Proof: Suppose that $A \subseteq B$ and $B \subseteq C$

Let x be chosen arbitrarily. Suppose $x \in A$. Our goal is to show $x \in C$.

(can you see that this is a plan to prove the Theorem?)

Since $x \in A$ and $A \subseteq B$, it follows that $x \in B$.

Since $x \in B$ and $B \subseteq C$, it follows that $x \in C$.

So we have shown that any element of A must belong to C, which is what it means for $A \subseteq C$ to be true.

The subset relation, being transitive, is a much more reasonable implementation of the idea of a *part* of a set.

This relation can be used to state the criterion for identity of sets.

Axiom of Extensionality: If A and B are sets, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Equivalently, sets A and B are equal exactly if they have the same elements (every element of A is an element of B and every element of B is an element of A).

Example: We can now prove that $\{a, b\} = \{b, a\}$.

We introduce another interesting object.

Axiom of the Empty Set: There is a set $\emptyset$ such that $x \in \emptyset$ is false for any object x.

Theorem: For any set X with no elements and any set A, $X \subseteq A$ holds. In particular, $\emptyset \subseteq A$.

Proof: Suppose that X is a set with no elements. Then for any object x, if $x \in X$, $x \in A$, because a false statement implies anything. So all elements of X (none of them) are in A, so $X \subseteq A$. $\emptyset$ has no elements, so $\emptyset \subseteq A$ by the same argument.

Observation: This does **NOT** say that the empty set belongs to every set as an element.

Theorem: Suppose that X is a set with no elements. Then $X = \emptyset$. There is only one empty set.

Proof: By the previous Theorem, $X \subseteq \emptyset$ and $\emptyset \subseteq X$, so $X = \emptyset$ by the Axiom of Extensionality.

We have used sets already in this book, usually correlated with properties. The principle we are using can be expressed formally:

Axiom of Separation: Let S be a set and let $P(x)$ be a sentence expressing a property of x. There is a set $\{x \in S : P(x)\}$ such that for every a, $a \in \{x \in S : P(x)\}$ if and only if $a \in S$ and $P(a)$.

When we use the well-ordering principle to show that all numbers have some property, we are usually applying the axiom of separation. Suppose we are trying to prove that all numbers x have some property $P(x)$. Suppose not. Then there is some natural number n such that $\neg P(n)$, so the set $\{x \in \mathbb{N} : \neg P(x)\}$ is nonempty, so it has a smallest element (the least counterexample)...and then we reason to a contradiction.

Notice that the axiom of separation lets us define sets only if we are already given sets to carve them out of. We give some additional axioms which provide us with grist for our mill.

Axiom of Power Set: For any set A, there is a set $\mathcal{P}(A)$, called the power set of A, such that $B \in \mathcal{P}(A)$ exactly if $B \subseteq A$, for any B. $\mathcal{P}(A)$ can be called...the set of all subsets of A.

We look at familiar Venn diagram operations. $A \cap B$ can be defined as $\{x \in A : x \in B\}$, which exists by the axiom of separation. $A - B$ can be defined as $\{x \in A : x \notin B\}$, again provided by the axiom of separation. For unions, we need the

Axiom of Binary Union: For any sets A, B there is a set $A \cup B$ such that for any x, $x \in A \cup B$ if and only if either $x \in A$ or $x \in B$.

Using the axioms of pairing and binary union, we can construct all finite sets.

Definition: We are given the notation $\{x_1, x_2\}$ for a finite set with two elements. If we have defined the notation $\{x_1, \ldots, x_n\}$, we define $\{x_1, \ldots, x_n, x_{n+1}\}$ as $\{x_1, \ldots, x_n\} \cup \{x_{n+1}\}$.

We are given some infinite sets, such as $\mathbb{N}$. We can simply postulate this set and its axioms as earlier in the book.

We could also present an implementation. We give the original approach of Zermelo. Define 0 as $\emptyset$. Define $n+1$ (temporarily) as $\{n\}$.

Axiom of Infinity: There is a set $\mathcal{Z}$ such that $0 \in \mathcal{Z}$ and for every x, if $x \in \mathcal{Z}$ then $x+1 = \{x\} \in \mathcal{Z}$.

Definition: We say that a set I is *inductive* iff $0 \in I$ and for every x, if $x \in I$ then $x+1 = \{x\} \in I$. Notice that the axiom of infinity simply says that there is an inductive set.

Definition: Let $\mathcal{Z}$ be an inductive set. Define $\mathcal{Z}_0$ as the collection of all n such that for every inductive element I of $\mathcal{P}(\mathcal{Z})$, $n \in I$.

Theorem: Any element of $\mathcal{Z}_0$ belongs to *every* inductive set. And any object which belongs to all inductive sets belongs to $\mathcal{Z}_0$.

Proof: Let $n \in \mathcal{Z}_0$. Let J be an inductive set. Then $J \cap \mathcal{Z}$ is an inductive set and an element of $\mathcal{P}(\mathcal{Z})$. So $n \in J \cap \mathcal{Z}$. So $n \in J$.

If x belongs to every inductive set, of course it belongs to every inductive set in the power set of $\mathcal{Z}$, and so belongs to $\mathcal{Z}_0$.

The previous theorem shows that the set $\mathcal{Z}_0$ is the same set no matter what inductive set $\mathcal{Z}$ we start with, and so should have a name of its own. We might suggest $\mathbb{N}$ as its name, if we were comfortable with the construction $0 = \emptyset; 1 = \{0\}; 2 = \{1\}; 3 = \{2\}$, and so forth (and if we included 0 in the natural numbers).

We note that nowadays there is a standard definition of the non-negative integers as sets, a somewhat different one, which works equally well and has one nice property that Zermelo's definition does not have. Define 0 as $\emptyset$ and $n+1$ as $n \cup \{n\}$, and state the axiom of infinity using this operation instead of the singleton operation. This leads to the construction $0 = \emptyset; 1 = \{0\}; 2 = \{0,1\}; 3 = \{0,1,2\}$, and so forth. This has the nice property that the set we identify with n has n elements.

I'm not going to say that either of these is our official definition. I think it is much more interesting to notice that an implementation of the system of natural numbers using sets is possible, and also that more than one such

implementation is possible. We have given only a hint of the full implementation in either case, since one would also need to define the operations of addition and multiplication (which can certainly be done).

I could specifically assert the existence of further sets such as the set of rational numbers or the set of real numbers, but it turns out that just asserting the existence of an infinite set is enough to construct sets implementing these familiar number systems and basically all mathematical structures that you will study.

The set of axioms we have given here is hardly a complete set of axioms, but it ought to support most of the work that is described in this book. And I am again rather more interested in you being aware that axioms for the set concept can be presented than in the details.

3 More remarks on sets, from the Feb 24 Lecture

In this lecture, I worked directly from the set section of the Art of Proof. I'll record some comments in these notes whcih aren't directly from their text, or which I think are particularly interesting.

I note as important a general proof strategy (really, two of them):

To prove $A \subseteq B$: If A and B are sets, to prove that A is a subset of B, introduce an arbitarily chosen object x, assume $x \in A$, and then deduce $x \in B$.

To prove equality of two sets: If A and B are sets:

Goal: $A = B$

Part I: Let: x be arbitrarily chosen

Assume: $x \in A$

Goal: $x \in B$

proof steps $\vdots$

finishing part I: $x \in B$

Part II: Let: y be arbitrarily chosen

Assume: $y \in B$

Goal: $y \in A$

proof steps $\vdots$
finishing part II: $y \in A$

Notice that Part I shows $A \subseteq B$ and Part II shows $B \subseteq A$.

I discussed set definitions with expressions to the left of the colon. The sets we are allowed by the Axiom of Separation all have the form $\{x \in A : P(x)\}$. How do we explain a set like $\{7m+1 : m \in \mathbb{Z}\}$ in a way which makes it clear that we are allowed to assume this set?

$\{7m + 1 : m \in \mathbb{Z}\} = \{k \in \mathbb{Z} : (\exists m \in \mathbb{Z} : k = 7m + 1)\}$ is an explanation of this notation: it is clear that the second expression is given to us by the axiom of separation.

A general explanation where there is one variable to the left of the colon is, when $f(x)$ is an expression that we know will be in set A if x is in set B, then $\{f(x) : x \in B\}$ means $\{k \in A : (\exists x \in B : k = f(x))\}$.

A more complicated example could appear in a definition of the gcd. We could define $\texttt{gcd}(a, b)$ as $\{ax + by \in \mathbb{N} : x \in \mathbb{Z} \wedge y \in \mathbb{Z}\}$. This would expand to

$$\{k \in \mathbb{N} : (\exists x, y \in \mathbb{Z} : k = ax + by\}.$$

Notice that both variables appearing to the left of the colon in the first definition end up being existentially quantified in the body of the second set definition. It is interesting to observe that I proposed this example then looked back to see what the authors had done in their definition...and they had given the second form!

I believe that you have all been expected in the past and will be expected in the future to read set definitions with complex terms to the left of the colon; I think a detailed formal definition here would be threatening, but a couple of examples of how to explain these definitions, which I have given, should help you to see that this kind of set definition fits into the framework I am presenting.

I suggest reading the proof the authors give of proposition 5.2.

I discussed the difference between the two set definitions given in project 5.5 part b. The crucial thing to recognize is that m is a dummy variable in the definition of U, but a fixed number given before the set is defined in the definition of V, and this gives quite different results for what the sets look like.

The authors use definitions of the form $\{x : P(x)\}$ without a bounding set in defining intersection, union, and set difference. You will see above

that we avoid doing this, basically because we cannot assume for a general sentence $P(x)$ that there even *is* a set $\{x : P(x)\}$: we know that $\{x : x \notin x\}$ does not exist!

What I prefer to do is to define $A \cap B$ as $\{x \in A : x \in B\}$ (or equivalently $\{x \in B : x \in A\}$) and define $A - B$ as $\{x \in A : x \notin B\}$, both of which set constructions are justified by the axiom of separation, and then appeal to the axiom of binary unions above, and simply assert that for any A, B, there is a set $A \cup B$, and for any c, $c \in A \cup B$ if and only if $c \in A \vee c \in B$. The problem with union is that for completely general sets A, B we don't have an obvious way to define a bounding set X such that $\{x \in X : x \in A \vee x \in B\}$ is actually $A \cup B$ without in effect assuming an axiom that for any sets A, B, there is a set X of which both are subsets (the axiom of binary union does this, of course).

It isn't an error to use the notation $\{x : P(x)\}$ as long as one understands this is the set of all x such that $P(x)$...**if there is such a set**. This notation might be undefined for some sentences.

The use of the complement notation A^c is harmless as long as one understands that there is a fixed "universal set" X one has in mind from context: this is really $X - A$ for some set understood from context. We cannot really have a complement of a set A in the absolute sense, $A^c = \{x : x \notin A\}$. If we did, then $A \cup A^c$ would be the universal set V such that $x \in V$ for any x at all, and then the axiom of separation would give us the set $\{x \in V : x \notin x\}$, which we already know cannot exist.

I am expecting that you are all familiar with the method of Venn diagrams for giving visual demonstrations of relatively simple statements in set theory. I will do some examples in class on Tuesday.

The definition of the Cartesian product

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

presupposes that you know what an ordered pair is. You might not even notice this (the authors do not make heavy weather of it) but it is worth noting that this concept must either be postulated or explained in terms of sets.

The basic property of ordered pairs is that $(a, b) = (c, d)$ implies $a = c$ and $b = d$. Defining (a, b) as $\{a, b\}$ would not work, because if a and b are distinct, we want (a, b) and (b, a) to be distinct, and $\{a, b\}$ is the same set as $\{b, a\}$.

In fact, it is possible to define (a, b) as $\{\{a\}, \{a, b\}\}$. To justify this requires work we will not do: one has to prove that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ implies $a = b$ and $c = d$, which is a bit tricky. Other definitions of the ordered pair as a set construction are also possible.

Notice that if $a \in A$ and $b \in b$ it follows that (a, b) as we have defined it is in $\mathcal{P}(\mathcal{P}(A \cup B))$, which we will write more briefly as $\mathcal{P}^2(A \cup B)$.

This allows us to show that $A \times B$ is provided by our axioms:

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

$$= \{k \in \mathcal{P}^2(A \cup B) : (\exists a, b \in A \cup B : a \in A \wedge b \in B \wedge k = (a, b))\}.$$

This depends on (a, b) being defined in the particular way given: this determines the bounding set we use. Other definitions might involve different bounding sets, but in any case no additional axioms are required to get Cartesian products. Since I have given axioms for set theory, I should show the flag about this! You are not responsible for the details of this definition, but that doesn't mean it might not be good for you to read it.

4 Homework 6

1. Do project 5.3.

2. Do project 5.12.

3. Do project 5.16.

   In projects 5.12 and 5.16, if an equation is false, give a counterexample using specific finite sets for A, B, C; if an equation is true, give a Venn diagram illustration but also write a proof using the strategies outlined above. I'll do some similar examples on Tuesday to illustrate these instructions.

4. Give a Venn diagram illustration of the identity $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$: a formal proof is not expected.

5. Write the recursive definitions requested in project 5.17: statement and/or proof of versions of the de Morgan laws will carry extra credit (the proofs would be induction proofs).

   continued on next page!

6. Do project 5.21.

7. Prove the statement I gave in class: for any sets A, B, if $A \times B = B \times A$, then $A = B$ or one of A and B is empty.

   I will prove both parts of Proposition 5.20 in class Tuesday to give you an idea how to approach the last two problems.