

Test I Math 287 Spring 2023

Dr Holmes

March 2, 2023

This is a takehome exam. The main rule is that you may not consult any person other than myself about it. This is difficult for me to enforce, but if I see suspiciously similar work on different student papers, or improbably sophisticated work that they are not likely to have produced on their own, we may move to more strenuous proctoring approaches, which will give you far less time to do an exam, for subsequent exams.

Proofs on this exam should be written in a two column format: the left column a series of statements, and the right column the justifications of those statements.

A reference sheet with axioms, propositions and definitions you need is the last page of the exam. You may tear it off for reference. The book and the manual of logical style are of course also available for reference.

1. The FOIL identity you learned in school is

$$(a + b) \cdot (c + d) = (a \cdot c + a \cdot d) + (b \cdot c + a \cdot d)$$

(First, Outer, Inner, Last). We supply the parentheses for precision.

Use the axioms (parts of Axiom 1.1, listed in the attachments to the paper, which you may tear off for reference) to give a detailed step by step proof of FOIL.

Each step should be justified by a single axiom.

You may use references to parts of the axiom using the exact phrases I give, and be aware that the phrase distributive law refers to exactly the form in the axioms (the left distributive law is the one you will use): you need to change things to apply it on the other side.

2. Prove $a \cdot (-b) = -(a \cdot b)$ using Proposition 1.9 and the axioms from chapter 1 in the reference sheet. Remember that the axioms do not give you any relationship between the additive inverse and multiplication directly; this is what you are proving here. The strategy here is very like the strategy for proving 1.14: add the right thing to both sides so that you can apply Proposition 1.9.

A step should be a hypothesis of the argument, or should be justified by nothing other than axioms, proposition 1.9 and/or previous steps in the proof.

3. Prove using the definition of divisibility (on the reference sheet) and algebra (you may be more informal about the algebra than in problems 1 and 2) that if a, b, x, y are integers, $d|a$ and $d|b$, it follows that

$$d|(a \cdot x + b \cdot y).$$

Your proof will start: Let a, b, d be integers and assume that $d|a$ and $d|b$...because $d|a$, there is an integer u such that $a = d \cdot u$...carry on from there.

4. Prove, using the axioms for \mathbf{N} (the set of positive integers: axiom 2.1 on the reference sheet) and the definition of $<$ given on the reference sheet and algebra of equations with addition, subtraction and multiplication (about which you may be informal [single steps may be justified by ‘algebra’ which would be many steps using chapter 1 axioms] but be quite formal about applying the axioms for the positive integers (referencing the correct part of axiom 2.1) and the definition of $<$) that if $0 < x < y$ then $x^2 < y^2$ (where for any integer z , we define z^2 as $z \cdot z$). Also prove that if $x < y < 0$, that $x^2 > y^2$ (which will also need the definition of $>$).

Your proof will begin “Let x, y be integers. Suppose that $0 < x$ and $x < y$. By the hypotheses and the definition of $<$, [something]...(carry on from there).

5. An arithmetic sequence is a sequence of the form $x_i = a + di$, where a and d are fixed integers.

The standard method of adding the sum of a finite arithmetic sequence is to add the first and the last terms, take their average, and multiply by the number of terms.

Compute

$$\sum_{i=0}^n (a + di)$$

by this rule (what is the first term? what is the last term? how many terms are there?). There is something very slightly tricky here: make sure you write out an example sum in full to catch it.

Then prove by induction that this formula for $\sum_{i=0}^n (a + di)$ is correct.

6. A sequence a_1 is defined recursively: $a_1 = 9$, $a_{k+1} = 10a_k + 9$.

Compute the first six terms of this sequence.

Prove by induction that for each natural number k , $a_k = 10^k - 1$.

- (a) Prove the theorem $((A \rightarrow C) \vee (B \rightarrow C)) \rightarrow ((A \wedge B) \rightarrow C)$ using the rules in the manual of logical style.

You will need to use proof by cases.

- (b) Two arguments are given. One of them is valid and one of them is not. Show by truth table methods that one is valid and show by truth table methods that the other is invalid. Just giving the table is not enough: you need to say something about each table to make your point.

i.

$$\frac{\begin{array}{c} P \\ \neg P \vee Q \end{array}}{Q}$$

ii. (eight lines in this table!)

$$\frac{(A \wedge B) \rightarrow C}{A \rightarrow C}$$

7. Format induction proofs carefully. In all induction proofs, two column format will force you to mention where the induction hypothesis is used!
- (a) Prove by induction that for an arbitrary sequence x_i and $n > 1$, $\sum_{i=1}^n x_i = x_1 + \sum_{i=2}^n x_i$ (we can pull out the first term of a sequence instead of the last; you might remember that this was used in the proof of the Binomial Theorem).

- (b) Prove by induction that for arbitrary $a \leq b$ and sequences x_i and y_i ,

$$\sum_{i=m}^n (x_i - y_i) = \left(\sum_{i=m}^n x_i \right) - \left(\sum_{i=m}^n y_i \right).$$

You have done something very similar to this in homework, and I did something very similar in lecture. The point is to write it out very carefully. Prove this by induction on n with basis $n = m$.

1 Reference sheet

Axiom 1.1. If m , n , and p are integers, then

- (a) $m + n = n + m$. (commutativity of addition)
- (b) $(m + n) + p = m + (n + p)$. (associativity of addition)
- (c) $m \cdot (n + p) = m \cdot n + m \cdot p$. (distributivity)
- (d) $m \cdot n = n \cdot m$. (commutativity of multiplication)
- (e) $(m \cdot n) \cdot p = m \cdot (n \cdot p)$. (associativity of multiplication)

Axiom 1.2. There exists an integer 0 such that whenever $m \in \mathbb{Z}$, $m + 0 = m$. (identity element for addition)

Axiom 1.3. There exists an integer 1 such that $1 \neq 0$ and whenever $m \in \mathbb{Z}$, $m \cdot 1 = m$. (identity element for multiplication)

Axiom 1.4. For each $m \in \mathbb{Z}$, there exists an integer, denoted by $-m$, such that $m + (-m) = 0$. (additive inverse)

Axiom 1.5. Let m , n , and p be integers. If $m \cdot n = m \cdot p$ and $m \neq 0$, then $n = p$. (cancellation).

Proposition 1.9. Let m , n , and p be integers. If $m + n = m + p$, then $n = p$

Axiom 2.1. There exists a subset $N \subseteq \mathbb{Z}$ with the following properties:

- (a) If $m, n \in N$ then $m + n \in N$.
- (b) If $m, n \in N$ then $mn \in N$.
- (c) $0 \notin N$.
- (d) For every $m \in \mathbb{Z}$, we have $m \in N$ or $m = 0$ or $-m \in N$.

Definition: The statements $m < n$ (m is less than n) and $n > m$ (n is greater than m) both mean that $n - m \in N$.

Definition: When m and n are integers, we say m is divisible by n (or alternatively, n divides m) Do not confuse this with the notations n/m and n/m for fractions. if there exists $j \in \mathbb{Z}$ such that $m = jn$. We use the notation $n \mid m$.