MATH 215: TIPS AND TECHNIQUES

JAMES FREITAG AND ERIC RIEDL

Abstract. This document contains some tips and techniques for Math 215: Introduction to Advanced Mathematics. The document is far from comprehensive, and it will change throughout the semester to reflect new techniques which we learn.

1. Basic proof techniques

1.1. **Reversing a proof.** In the first part of the course, we are often establishing equalities and inequalities for the real numbers. For instance, lets look at establishing the following result:

Proposition 1.1. *For any real numbers a, b,*

$$4ab < (a+b)^2.$$

Before we write the proof, lets talk about how to figure out the technique of the proof. Here is the first tip: **start with the expression you hope to prove, and try to do some valid algebraic operations** (which don't change whether the inequality is true or not) and work towards getting an inequality that you know to be true.

What kinds of inequalities do we know to be true? We, one example is that for any real number c, $c^2 \geq 0$. This comes up quite a lot - **if you can write an expression as the square of some other real expression, then your original expression is nonnegative.**

But, how can we get our inequality into the form where we can exploit the fact that squares are nonnegative? If you don't see anything more obvious, then a good technique for inequalities is to **move all of the terms to one side so that only a** 0 **remains on the other side**. Doing this, we have

$$4ab \leq (a+b)^2 \tag{1}$$

$$0 \leq a^2 + 2ab + b^2 - 4ab \tag{2}$$

$$0 \leq a^2 - 2ab + b^2 \tag{3}$$

$$0 \leq (a-b)^2 \tag{4}$$

And now we can see that this last inequality is certainly true, since if $c = a - b$, then $c^2 \geq 0$. Now we have the idea of the proof, but we need to carefully write it down. Notice that we have essentially done things backwards here - we ended with a statement we know to be true, after beginning with what we want to prove. This is **not the order you should write your proofs**. Things will go much more smoothly if you write your proofs beginning with inequalities you can justify and end with your goal. Here is an example of a correct proof of Proposition 1.1:

Proof. For any $a, b \in \mathbb{R}$, we have $0 \leq (a-b)^2$, since the square of any number (for instance $a - b$ is nonnegative). So, expanding the expression on the right hand side of the inequality, we see

$$0 \leq a^2 - 2ab + b^2.$$

So,

$$0 \leq a^2 - 2ab + b^2 = a^2 + 2ab + b^2 - 4ab$$

and we may add $4ab$ to both sides of the inequality, obtaining:

$$4ab \leq a^2 + 2ab + b^2.$$

After factoring the right hand side, we obtain:

$$4ab \leq (a+b)^2,$$

completing our proof. □

1.2. **Proofs by contradiction.** To prove certain statements, direct proofs either don't work or are difficult. Sometimes a different technique, called *proof by contradiction* makes things easier. The general idea is: assume that the statement, P which you are trying to prove is false. Then, show from this assumption that some statement that you know to be wrong must hold. You can then conclude that P must have been true. Lets see an example:

Proposition 1.2. *Suppose that $a, b, c \in \mathbb{R}$ with $a > b$ and $ac \leq bc$. Then $c \leq 0$.*

Proof. Suppose that the conditions above on a, b, c hold ($a > b$ and $ac \leq bc$). *Assume that* $c > 0$. We assumed that $a > b$ and $c > 0$, so it follows that $ac > bc$, but this is a contradiction to the fact that $ac \leq bc$. So, our assumption must be wrong, and $c \leq 0$. □

1.3. **The integers.** We denote the set of integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, with the symbol $\mathbb{Z}$. You know the next couple of definitions, but it is useful to formalize your thinking in order to do certain proofs.

Definition 1.3. Let $a, b \in \mathbb{Z}$. We say that a divides b if there is $c \in \mathbb{Z}$ such that $ac = b$.

Definition 1.4. We say $a \in \mathbb{Z}$ is even if 2 divides a. We say a is odd if a is not even.

Proposition 1.5. 7 *does not divide* 15*.*

We gave proofs similar to this in class, proving, for instance, that 2 does not divide 101.

Again, there is a slight question about standards for proofs, since later in the course, we will not ask you to prove something like this, or perhaps if we did, we would provide instructions like "prove the previous proposition using only basic axioms for the real numbers and the definition of the integers."

Often when discussing divisors, we implicitly only consider positive integers - that is, if you are asked to list the divisors of 15, you might say $1, 3, 5, 15$, but of course each $-1, -3, -5, -15$ is also a divisor according to the above definition.

1.4. **The rational numbers.** We denote the rational numbers by $\mathbb{Q}$, and remind you that

$$\mathbb{Q} := \{\frac{m}{n} \mid m, n \in \mathbb{Z},\, n \neq 0\}.$$

As you are familiar with, every rational number can be written in lowest terms, something we will not prove right now:

Fact 1.6. *Any rational number can be written as $\frac{m}{n}$ such that m and n share no common divisors except* 1.

The real numbers which are not rational are called the irrational numbers.

Proposition 1.7. *The real number $\sqrt{2}$ is irrational.*

Proof. We will prove the proposition by contradiction. So, assume that $\sqrt{2}$ is rational. This means that we can write $\sqrt{2} = \frac{m}{n}$ where m, n have no common divisor. It follows that $2 = \frac{m^2}{n^2}$, and so

$$2n^2 = m^2.$$

This implies that m^2 is even, and by work we did in class, this implies that m is even (this was easy to prove). That means we can write $m = 2k$ for some $k \in \mathbb{Z}$. But then plugging $2k$ in place of m in our previously established equation $2n^2 = m^2$, we have that

$$2n^2 = (2k)^2.$$

Expanding the right hand side, we have that $2n^2 = 4k^2$. So, after dividing both sides of the equation by 2, we obtain $n^2 = 2k^2$. Now, by the same argument as earlier in the proof, we must have that n is even. But now we have shown that both m and n are even, which contradicts the fact that m and n have no common divisor besides 1. Our assumption, therefore, must have been wrong, and thus $\sqrt{2}$ is irrational. $\square$

You should study the previous proof as it employs a strategy which is very commonly useful for proving that certain numbers are irrational.

2. Sets

We started the course with real numbers and moved to the natural numbers, integers and rationals in large part because those mathematical objects are familiar to you, but in the next part of the course, we study *sets*, a topic which might include quite a few terms you are unfamiliar with. This section contains the basic definitions from our introduction to set theory, but acquainting yourself with the subject requires doing the exercises from class, in large part because the material is likely to be somewhat unfamiliar to you compared to our earlier topics.

Definition 2.1. For our course, a *set* is simply a collection of objects.[1]

We denote sets containing some objects (usually letters or numbers) inside of curly braces. For instance,

$$\{a, b, c, d\}$$

[1]There are some nuances to defining exactly what a set is, and this definition is problematic if one goes deeply into the subject, but it will work for our purposes. To see what precisely the problems with this definition are, look up Russell's Paradox.

denotes the collection which includes a, b, c, d and no other elements. The set which contains no elements is called the *empty set* and is denoted $\emptyset$. We almost always name our sets with capital letters, like A, B, C, D. Many sets used in our course so far contain infinitely many elements, for instance, $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$.

When we want to talk about the elements in a set, the symbol $\in$ is often useful. The expression $a \in A$ means that the element a is contained in the set A. For instance, $17 \in \mathbb{N}$.

Putting vertical bars around a set:

$$|A|$$

denotes the *cardinality* of the set A, which, when the set A is finite is simply the number of elements in the set. For instance,

$$|\{a, b, c, d\}| = 4.$$

This notion is also defined for infinite sets, but there things are more complicated (as we will see later in the course).

After introducing sets, we almost immediately begin asking about maps between sets. A *function* from set A to set B is a map which takes in any elements $a \in A$ and outputs one element $b \in B$. Usually we name functions, for instance, f, writing $f : A \to B$ to denote that f is a function from A to B. The output of f on input a is denoted by $f(a)$. The next two special properties of functions play a big role in set theory.

Definition 2.2. A function $f : A \to B$ is *injective* if whenever $a_1, a_2 \in A$ with $a_1 \neq a_2$ we have that $f(a_1) \neq f(a_2)$. [2]

Definition 2.3. A function $f : A \to B$ is *surjective*[3] if for all $b \in B$, there is $a \in A$ such that $f(a) = b$.

Definition 2.4. A function $f : A \to B$ is *bijective* if it is both injective and surjective.

Lets begin with a couple of simple examples - first we will consider functions $f : \mathbb{N} \to \mathbb{N}$. If $f(x) = x + 3$, then the function is injective, but not surjective. To check injectivity, assume that $a \neq b$. Then $f(a) = a + 3 \neq b + 3 = f(b)$. To see that f is not surjective. Notice that there is no $a \in \mathbb{N}$ such that $f(a) = 2$.

Often I find that students get confused about the definition of a function and whether a function is surjective. Think of things this way - a function from A to B is a rule which tells you how to get exactly one element of B whenever you are given an element of A. The function is injective if whenever you are given distinct inputs, your rule produces distinct outputs. Often, for sets like $\mathbb{N}$ or $\mathbb{Z}$, we write the the functions with familiar mathematical notation. For instance,

$$f(x) = |x|$$

defines a surjective function from $\mathbb{Z}$ to $\mathbb{N}$. The function is not injective, because $f(3) = f(-3) = 3$. The two distinct inputs produce the same output in this case.

[2]Sometimes injective is also called *one-to-one*. One can also state the condition for injectivity in the following manner: if $f(a_1) = f(a_2)$ when $a_1 = a_2$. It is easy to see this condition is equivalent to the one given in the definition - usually I find the one in the definition somewhat easier to work with.

[3]*Onto* is sometimes used in place of surjective.

It is important to keep in mind that surjectivity and injectivity are not just a properties of the expression $f(x) = |x|$, but also depend on specifying between which sets we consider the map. For instance,

$$f(x) = |x|$$

defines a map from $\mathbb{R}$ to $\mathbb{R}$. This map is neither injective (for the same reason as in the previous paragraph) nor surjective (there is no $r \in \mathbb{R}$ such that $f(r) = -17$). So, be careful - a function is more than simply a mathematical expression - to define a function you need to define which sets the function maps between. Sometimes, when $f : A \to B$ is a map, we will refer to A as the *domain* of f and B as the *codomain* of f.

Example 2.5. Find a bijection from

(1) $\mathbb{N}$ to $2\mathbb{N}$. $2\mathbb{N}$ denotes the set of even numbers $\{0, 2, 4, 6, 8, \ldots\}$.
(2) $\mathbb{Z}$ to $\mathbb{N}$.
(3) $\mathbb{N}$ to $\mathbb{Z}$.
(4) $\mathbb{N}$ to $\mathbb{N}\times\mathbb{N}$. The set $\mathbb{N}\times\mathbb{N}$ denotes the collection of pairs of natural numbers $\{(n_1, n_2) \mid n_1, n_2 \in \mathbb{N}\}$.
(5) $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$.

It is not the case that one can always write down a mathematical expression with the standard mathematical functions we know (say polynomials, rational functions, and even exponentials, trignometric functions, etc) which gives a formula for a function in which we are interested. For instance, Let $\mathbb{P}$ be the set of prime numbers, and let $\psi : \mathbb{N} \setminus \{0\} \to \mathbb{P}$ be the function which sets $\phi(n)$ equal to the n^{th} prime number. This is clearly a well-defined bijection between $\mathbb{N}$ and $\mathbb{P}$, but there is no known expression in terms of standard mathematical functions for giving a formula for the n^{th} prime number. You could certainly write a computer program to calculate $\psi(n)$, and mathematicians have proved a great may things about this map even without writing down a specific formula.

2.1. **More set theoretic constructions.** This document didn't cover a few of the most common set theoretic operations which you likely know quite well - intersection and union, but there are a few other natural constructions which you might not be quite as familiar with - at least not in a formal sense. The first is the *direct product* of two sets.

Let A, B be sets. The direct product (often shortened to product) of A and B is denoted

$$A \times B = \{(a, b) \mid a \in A,\, b \in B\}.$$

So, you should think of the product of two sets as the collection of pairs of elements, one from the first set and one from the second. We write A^2 for $A \times A$ and

$$A^n = \underbrace{A \times A \ldots \times A}_{n \text{ times}}.$$

It is not hard to see that the number of elements in $A \times B$ where A and B are finite, is $|A| \cdot |B|$. (If you don't see why this is so, write out an example with A and B fairly small sets).

Another common set theoretic construction was mentioned in class - the *power set*. Given a set A, the power set of A, denoted $\mathcal{P}(A)$ (and sometimes 2^A) is the collection of all subsets of the set A. So, if $A = \{a, b\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

In class, we proved that the cardinality of $\mathcal{P}(A)$ is $2^{|A|}$ whenever A is finite. (To see this, count the number of ways to pick a subset - hint: every element can either be in or out so there are $|A|$ many choices to make).

Thus, for finite sets, A finite, $|\mathcal{P}(A)| > |A|$. It turns out that a version of this is true also for infinite sets, but it is much trickier to prove (later in the course, we will).

Department of Mathematics, UIC, Chicago IL
E-mail address: freitagj@gmail.com

Department of Mathematics, UIC, Chicago IL
E-mail address: ebriedl@uic.edu