MATH 3333–INTERMEDIATE ANALYSIS–BLECHER NOTES

This course has two goals. First, we learn how to prove things in mathematics. This requires a talent for logic (to be able to follow very detailed chains of logical implications). Don't take this course if you usually lose arguments! It also requires the ability to think very abstractly, manipulate mathematical symbols, and to be able to find simple examples and use them to 'see what is going on', and then to construct a formal proof. Most of this is learned by experience, and this and Math 3325 (Transitions) are the courses in which we begin to learn this. It is very very different to earlier courses, such as calculus, and because of this you may dislike it very much for a while, or may decide that this is not where you want to go with your life. Learning new skills is often unpleasant at first! You are going to have to completely immerse yourself in the material to absorb it. The second goal of the course is to rigorously develop the basic facts about the real numbers and functions of one real variable, and to actually prove many of the facts you took for granted in Calculus I and II. This will require us to really understand ϵ-δ arguments and definitions, the basic 'topology' of the real number line (limits, sequences, continuity), and why the basic results in calculus work. One only really appreciates many mathematical ideas and techniques when you understand their proofs.

You will be expected to reread and digest these typed notes after class, line by line, trying to follow why the line is true, for example how it follows from previous lines. I suggest you add a check mark after you have read and understood the line, add extra explanation or pictures to yourself if needed. Add a question mark next to any line you cannot follow, and ask me or the TA about it. That is why I have given wide margins on every page. Also memorize 'definitions' as you read. The best advice I can give to ensure success in this class is to do this reading properly. In my experience, the class becomes much much more difficult if you do not do it. This kind of detailed reading is not without pain, but it will help reconfigure your brain to internalize the kind of logic/thinking/proof skills that are needed in this subject (and in other math 'proof' courses). And remember the universal college rule: 3 hours study outside of class for every hour in class. The way I will monitor if you are doing all this is to give an 'easy-quiz' once a week, named as such because it will be easy for anyone who has been reading the notes as suggested.

Some encouragement from a great mathematician: "Mathematics is a process of staring hard enough with enough perseverance at the fog of muddle and confusion to eventually break through to improved clarity. I'm happy when I can admit ... that my thinking is muddled, and I try to overcome the embarassment that I might reveal ignorance or confusion [and ask for help! (DB)] ... this has helped me develop clarity..." Thurston

(These lines will be of great use here, or if you are going on to other higher level math classes.)

Up to and including Section 3.2 of the textbook 5th Edition (Section 11 of 3rd or 4th edition), are preliminaries. Most of this will be familiar to some, and so we will move quickly. If you are not familiar with parts of this material before Section 3.3 in the textbook 5th Edition (Section 12 in the 4th Ed, or Section 3.3 of these typed notes), then they are very important, and you may have to work harder than some other students here, and use the textbook and outside sources like wikipedia liberally.

1. Logic and deductive reasoning (Chapter 1, Lay)

The following will be a review for most (or who have 3325), so we will move quickly. You probably will need to read it carefully several times. Depending on your background, you might have to read Chapter 1 in the textbook too for additional discussion/examples, or to supplement the following. You could also look up several of these topics on wikipedia. Also, Math 3325 and 3336 is in large part devoted to this kind of thing, and if you have taken any other math courses with proofs (such as some linear algebra or abstract algebra courses) you will have met it there too.

- **Statement:** a phrase that is either true or false, but not both. Mathematics consists entirely of statements, and is thus either right or wrong. Be sure that your 'statements' are properly written, and have meaning (make sense).

  A statement which is true is also sometimes said 'to hold', or we say 'it holds', or more rarely is called 'valid'.
- Example of a statement: 'Seven is an even number'. Example of a non-statement: 'This sentence is false'. Or: 'Houston is a nice place to live'.
- Sometimes we give a statement a name. For example, let Q be the statement: Seven is an odd number. Or, if x is a real number, let $P(x)$ be the statement: $x^2 - 5x + 3 \geq 0$. Note $P(0)$ is true here, but $P(1)$ is false.
- **Where things live:** In mathematics, it is very important to keep remembering 'where things live'. By this I mean, what exactly are the objects we are talking about. This is where most students get into trouble. For example, if you are trying to prove something about a sphere in 3-space, you will get into big trouble if you forget that your variable x is a point

on the sphere, and start using it as if it were a real number, or a rational number. Obviously you cannot take the square root of a point on the sphere, and you cannot apply results that work for real numbers to points on the sphere. This is just an example, I'm just trying to say that one gets into trouble if you confuse the role of things, and forget what something is supposed to be. This is true in real life too!!

- **Negation:** If P is a statement, then $\sim P$ or $\neg P$ is its *negation*. For example, if $P(x)$ is as above, then $\sim P(x)$ is the statement: $x^2 - 5x + 3 < 0$.
- **Connectives:** 'and' ($\wedge$), 'or' (that is, the inclusive 'or' $\vee$). Thus $A \vee B$ means A is true, or B is true, or both are true (see text).
- **Implication:** If P then Q. Also sometimes written as '$P \Rightarrow Q$', or 'P implies Q'. We sometimes call P the *hypothesis* and Q the *conclusion*.
- **Deduction words:** 'Thus', 'therefore', 'hence', 'consequently', 'this implies that ...', and so on. Also sometimes written as $\therefore$, or $\Rightarrow$.
- **Converse:** The converse of '$P \Rightarrow Q$' is '$Q \Rightarrow P$' or '$P \Leftarrow Q$'.
- **Contrapositive:** $P \Rightarrow Q$ is the same as $(\sim Q) \Rightarrow (\sim P)$. The latter may be easier!

  For example, the contrapositive of (If $n \in \{1, 2, 3, \cdots\}$ then $2n$ is even), is: (If $2n$ is not even then $n \notin \{1, 2, 3, \cdots\}$.
- **Equivalence:** P if and only if Q. Also written as: 'P is equivalent to Q', 'P iff Q', or '$P \iff Q$'. To prove that $P \iff Q$, we need to prove both that $P \Rightarrow Q$, and its converse $Q \Rightarrow P$. To prove an equivalence we often first prove one of these, and then say 'Conversely,...' and then go on to show the other. Or sometimes you will see an 'if and only if' proof set up as follows:

Proposition 1.1. *P if and only if Q.*

Proof. $(P \Rightarrow Q)$: Suppose that P holds. Then ... chain of reasoning ... so that Q is true.

$(Q \Rightarrow P)$: Conversely, suppose that Q holds. Then ... chain of reasoning ... so P is true. □

or this may appear as:

Proof. $(\Rightarrow)$: Suppose that P holds. Then ... chain of reasoning ... so that Q is true.

$(\Leftarrow)$: Conversely, suppose that Q holds. Then ... chain of reasoning ... so P is true. □

Sometimes proving an equivalence is not done directly; for example to show $P \iff Q$, it is enough to prove that $P \Rightarrow Q$ and $(\sim P) \Rightarrow (\sim Q)$.

- If we have more than two statements which are to be proved equivalent, we often use 'T.F.A.E.' ('the following are equivalent'). A typical result of this kind may look as follows:

Theorem 1.2. *Let .... . Then T.F.A.E.:*
(i) P ,
(ii) Q ,
(iii) R.

Proof. (i) $\Rightarrow$ (iii) Suppose that P holds. Then ... chain of reasoning ... so that (iii) holds.

(iii) $\Rightarrow$ (ii) Suppose that R holds. Then ... chain of reasoning ... so that Q holds.

(ii) $\Rightarrow$ (i) Finally, suppose that (ii) holds. Then ... chain of reasoning ... so that P holds. $\square$

- $\forall$ **quantifier:** 'For all', 'for every', 'whenever', ... For example, $\forall x \geq 2, x^2 - 5x + 10 \geq 0$. Also acceptable here: $x^2 - 5x + 10 \geq 0, \forall x \geq 2$ (BEWARE: in general, do not move quantifiers around, see below), or even
$$x^2 - 5x + 10 \geq 0, \qquad x \geq 2,$$
or
$$x^2 - 5x + 10 \geq 0, \qquad (x \geq 2).$$
Proving a 'for all' statement usually means taking an arbitrary or generic member x from the system under consideration (in the example above, we would need to take an arbitrary real number $x \geq 2$), and show that the statement asserted about x is true.
- $\exists$ **quantifier:** 'There exists', 'there is at least one'. For example, $\exists x$ such that $x^2 - 5x + 3 \leq -1$. (Often 'such that' is written s.t. or $\ni$.) Proving a 'there exists statement' usually means finding a clever choice of a particular x that works (e.g. $x = 1$ in the last example). Thus we have to 'construct' (maybe by guesswork, or intuition) an example satisfying the required condition. However, sometimes a 'there exists statement' may be proved in other ways, for example by contradiction (assume its negation, which is a 'for all' statement, and show that this leads to a contradiction). We'll talk more about proofs by contradiction later.
- Practice exercise from text: Rewrite using the symbols $\exists, \forall$:

(a) There exists a positive number x such that $x^2 = 5$. [Answer: $\exists x > 0$ s.t. $x^2 = 5$.]

(b) For every positive number N there is a positive number M such that $N < 1/M$. [Answer: $\forall N > 0, \exists M > 0$ s.t. $N < 1/M$.]

(c) If $n \geq N$, then $|f_n(x) - f(x)| \leq 3$ for all x in A. [Answer: $\forall n \geq N, \forall x \in A, |f_n(x) - f(x)| \leq 3$.]

- **Order of quantifiers, etc., matters:** so be careful! '$\forall x, \exists y$ s.t. $y > x$' is not the same statement as '$\exists y$ s.t. $\forall x, y > x$'. (See end of Section 1.2 text 5th Edition (Section 2 of 4th edition).
- **Negations of statements with quantifiers:** A rough guide, when negating statements with quantifiers, is that $\forall$'s become $\exists$, $\exists$'s become $\forall$, and inequalities in 'conclusions' reverse. More precisely, the negation of '$\forall x, P(x)$' is '$\exists x$ s.t. $(\sim P(x))$', and the negation of '$\exists x$ s.t. $P(x)$' is '$\forall x, (\sim P(x))$'. Thus the negation of 'Everyone in the room is asleep', or equivalently the negation of '$\forall x$ in room, x is asleep', is '$\exists x$ in room s.t. x is asleep'. That was a good test if you were awake. Also, the negation of $P \wedge Q$ is $(\sim P) \vee (\sim Q)$, and the negation of $P \vee Q$ is $(\sim P) \wedge (\sim Q)$.
- Examples from this section of the text. What are the negations of the following statements:

(a) For every $x \in A$, $f(x) > 5$. [Answer: $\exists x \in A$ s.t. $\sim [f(x) > 5]$, or $\exists x \in A$ s.t. $f(x) \leq 5$.]

(b) There exists a positive number y such that $0 < g(y) \leq 1$. [Answer: $\forall y > 0, \sim [0 < g(y) \leq 1]$. Since $0 < g(y) \leq 1$ represents $(0 < g(y)) \wedge (g(y) \leq 1)$, its negation is $(0 \geq g(y)) \vee (g(y) > 1)$. So the final answer is: $\forall y > 0, (0 \geq g(y)) \vee (g(y) > 1)$, which in English reads: For every $y > 0$, either $0 \geq g(y)$ or $g(y) > 1$.]

(c) $\forall \epsilon > 0\ \exists N$ s.t. $|f_n(x) - f(x)| < \epsilon$ whenever $n \geq N, x \in A$. [Answer: We can do this one step at a time:

$$\sim [\forall \epsilon > 0, \exists N \text{ s.t. } \forall n \geq N, x \in A, |f_n(x) - f(x)| < \epsilon]$$

$$\iff \exists \epsilon > 0 \text{ s.t. } \sim [\exists N \text{ s.t. } \forall n \geq N, x \in A, |f_n(x) - f(x)| < \epsilon]$$

$$\iff \exists \epsilon > 0 \text{ s.t. } \forall N, \sim [\forall n \geq N, \forall x \in A, |f_n(x) - f(x)| < \epsilon]$$

$$\iff \exists \epsilon > 0 \text{ s.t. } \forall N, \exists n \geq N \text{ s.t. } \sim [\forall x \in A, |f_n(x) - f(x)| < \epsilon]$$

$$\iff \exists \epsilon > 0 \text{ s.t. } \forall N, \exists n \geq N, \exists x \in A \text{ s.t. } \sim [|f_n(x) - f(x)| < \epsilon]$$

$$\iff \exists \epsilon > 0 \text{ s.t. } \forall N, \exists n \geq N, \text{ and } \exists x \in A \text{ s.t. } |f_n(x) - f(x)| \geq \epsilon.$$

(Note that you can always test if a line like one of the last few lines is correct by comparing it with the previous line, and see if they are saying the same thing logically, maybe by turning them partly back into English.)

- Some 'phrases' in a math statement, just like in an English statement, should be treated as 'molecules' and not be split up into its individual atoms. For example, if you were to negate the statement "there is a guy in the class whose name is Sam", you would treat 'guy in the class' as a single compound object, a molecule, so we will not be negating the atoms 'guy' or 'class'. The negation is: 'for every (guy in the class), their name is not Sam'. Another example: if we were to negate 'there exist real numbers x and y with sum z', that is $\exists x \in \mathbb{R}$ and $y \in \mathbb{R}$ s.t. $x + y = z$, we treat '$x \in \mathbb{R}$ and $y \in \mathbb{R}$ as a molecule, and do not split them and change the 'and' to an 'or'. The negation is: 'for all $x \in \mathbb{R}$ and $y \in \mathbb{R}$, $x + y \neq z$.
- **Respectively's:** Often to save writing an only slightly changed sentence, we use the word 'respectively'. For example: 'The function $f(x)$ is strictly increasing (resp. strictly decreasing) if $f'(x) > 0$ (resp. $f'(x) < 0$) for all x'. You are supposed to read the statement twice, once without reading the words in parentheses, and then again with the words before the parentheses replaced by the words in parentheses. Similarly, if a sentence is only slightly changed more than once. For example: 'The function $f(x)$ is strictly increasing (resp. strictly decreasing, constant) if $f'(x) > 0$ (resp. $f'(x) < 0$, $f'(x) = 0$) for all x'.
- **Techniques of proof: Deductive reasoning.** Suppose you are trying to prove that P implies Q. As explained in Section 1.3 of the text 5th Edition (Section 3 of 4th edition), this usually boils down to building a bridge of logical statements, to connect the hypothesis P to the conclusion Q. The building blocks of the bridge consist of:
  - **Definitions** (the basic meanings of the words used, usually of the key words contained in P and Q),
  - Theorems or facts that have been previously established as true (look for those using the key words contained in P and Q),
  - Statements that are logically implied by earlier statements in the proof,
  - Axioms. These occur less frequently in proofs, they are the basic assumptions one makes at the beginning of a theory, and one does not usually discuss them too much after the first few days of class.

  The MOST IMPORTANT, and most frequently useful, technique for proving results in this class is to GO BACK TO THE DEFINITION.

  When actually building the bridge, it may not be at all obvious (at least to a beginning bridge-builder), which blocks to use, and the order to use them in. This comes with experience, perseverance, intuition, good logical abilities, and sometimes good luck.

In trying to prove $P \Rightarrow Q$, the text suggests starting at both ends and working to the middle. Ask: "What does P imply?" Answering this is usually just a matter of looking up the definitions of the words in P, and seeing what then must obviously follow. Often it entails looking back in your notes to see what previously established Theorems or facts we can bring to bear on P. Suppose then that we realize that $P \Rightarrow P_1$ (actually there may be several things that P implies). Then ask what P_1 implies, using a similar process to the one we just went through. Continue this process until you build a chain (or chains) of deductions, and you can go no further. If you havent reached Q yet, start to work backwards from Q, asking "What statement would imply Q?" Again, answering this is usually just a matter of looking up the definitions of the words in Q and using your head, or looking back in your notes to see what previously established Theorems or facts we can use to get Q. Once we have realized that $Q_1 \Rightarrow Q$, we repeat the process, to find Q_2 with $Q_2 \Rightarrow Q_1$. Hopefully the two parts of the bridge meet in the middle. This is **deductive reasoning**. When one gets good at it, it becomes pretty automatic, like eating popcorn: you reach automatically and quickly for the definition or fact you need to add to the bridge, and the bridge is built in seconds. It is a messy process sometimes (cramming a lot of popcorn in your mouth), but once a shoddy bridge is built one can then write it again economically, and so that it reads nicely.

Example of working backwards: Suppose that you were asked to prove the following

Theorem 1.3. *For every $\epsilon > 0$ there exists a $\delta > 0$ such that*

$$1 - \delta < x < 1 + \delta \text{ implies that } 5 - \epsilon < 2x + 3 < 5 + \epsilon.$$

Note that here we want $5 - \epsilon < 2x + 3 < 5 + \epsilon$. Subtracting 3, the above is equivalent to $2 - \epsilon < 2x < 2 + \epsilon$. Dividing by 2, the last inequality is equivalent to $1 - \epsilon/2 < x < 1 + \epsilon/2$. Thus if we choose $\delta = \epsilon/2$, then indeed $1 - \delta < x < 1 + \delta$ implies that $5 - \epsilon < 2x + 3 < 5 + \epsilon$.

We can now tidy up, and write the proof economically, and so that it reads nicely:

Proof. Given any number $\epsilon > 0$, set $\delta = \epsilon/2$. Then $\delta > 0$. If $1 - \delta < x < 1 + \delta$, then $1 - \epsilon/2 < x < 1 + \epsilon/2$. Multiplying this inequality through by 2, and then adding 3, we obtain $5 - \epsilon < 2x + 3 < 5 + \epsilon$. This is what was required. □

- **Proof by cases:** Many proofs divide naturally up into different cases, each of which need to be dealt with separately. For example, this occurs frequently when one has to divide by a certain quantity in a proof. One cannot divide by 0, so one has to break the proof into two cases, first the case where the quantity is not zero, and second, the case where the quantity is zero. In the latter case, we cannot divide through by the zero quantity, and the proof has to be finished in another way. Another example: read Example in the text (Ex 4.5 in 4th Edition).

- **Proof by contradiction:** One way to prove a statement P is to assume that it was false, that is, we assume that $\sim P$ is true, and then use deductive reasoning to deduce a statement Q, where Q is clearly false. Such a proof is often written beginning with the words "BWOC suppose that P is false. ..."; BWOC stands for 'By way of contradiction'. Then one continues the proof until one arrives at something riduculous. This is *proof by contradiction*, or *reductio ad absurdum*. Or, if we want to prove that $P \Rightarrow Q$, it suffices to show that $P \wedge (\sim Q)$ leads to a contradiction.
- **Techniques of disproof:** Disproving a false statement is often harder than proving a true statement, because it often means finding a **counterexample**. A counterexample is an example showing that a statement is false. Finding examples is sometimes hard. Here is one that is not so hard, it just takes a few minutes of perseverance: Show that the statement 'n^2+n+17 is a prime number for all positive integers n' is false. [Solution: $n = 16$ is a counterexample.]

  Another way to disprove a statement P is to assume that it was true, and then use deductive reasoning to show that $P \Rightarrow Q$, where Q is clearly false. This is also *proof by contradiction*.
- **General advice:** Write down all your reasoning, particularly if you are new at this, or if you want a good grade. Don't say 'it is clear', if it would not be clear to a classmate.

Homework for Chapter 1.

5th Edition numbers: 1.1 Ex 2, 1.2 Ex 3, 11, 13, 15, 17, 18, 22. 1.3 Ex 2, 3, 6a-f, 7. 1.4 Ex 1, 9, 11, 19c, 23, 24. (4th & 3rd Edition numbers: Numbers in parentheses refer to the equivalent problems in the third edition of the text: Exercises 1.2, 2.3, 2.5 (not f), 2.11 (2.7), 2.13 (2.9), 2.15 (2.11), 2.16 (2.12), 2.20 (2.16), 3.2, 3.3, 3.6a-f, 3.7 (3.8), 4.1, 4.3, 4.5, 4.13c (4.7), 4.17 (4.11), 4.18 (4.12).)

You do not need to do them all. They will be collected in class on the date listed on the website, but the grade will be essentially just for turning something in. Instead, there will be a 10 minute quiz on that date containing some of these problems.

2. Sets and functions (Chapter 2 Lay)

Please read Chapter 2 yourself, Sections 1, 2, 3 in the 5th edition of the text (5, 6, 7 in the 4th Ed). You can omit the later Sections of Chapter 2).

Some important notations for this course and for these notes:

- A set, naively, is a collection of objects (elements, members). For example we may write $A = \{1, 2, 3\}$. We write $x \in A$ if x is an element of set A, and $x \notin B$ if x is not an element of set B.
- In this course/these notes we will write $\mathbb{N}$ for the *natural numbers* $\mathbb{N} = \{1, 2, 3, \cdots\}$, and $\mathbb{N}_0$ for the *whole numbers* $\mathbb{N}_0 = \{0, 1, 2, 3, \cdots\}$, and $\mathbb{Z}$ for the *integers* $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$. We usually reserve the symbols n, m for natural numbers or integers. The *rational numbers* are $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}$. The *real numbers* are written as $\mathbb{R}$, and $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$. Of course the *irrational numbers* are $\{x \in \mathbb{R} : x \notin \mathbb{Q}\}$. The notation $A \setminus B$ means $\{x \in A : x \notin B\}$ (called the *set-difference*). Thus the irrational numbers are $\mathbb{R} \setminus \mathbb{Q}$.
- Most of the sets we look at will be *intervals*: that is is a subset of $\mathbb{R}$ of one of the 9 types: $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}, [a, b) = \{x \in \mathbb{R} : a \leq x < b\}, (a, b] = \{x \in \mathbb{R} : a < x \leq b\}, (a, b) = \{x \in \mathbb{R} : a < x < b\}, [a, \infty) = \{x \in \mathbb{R} : a \leq x\}, (a, \infty) = \{x \in \mathbb{R} : a < x\}, (-\infty, b] = \{x \in \mathbb{R} : x \leq b\}, (-\infty, b) = \{x \in \mathbb{R} : x < b\}, (-\infty, \infty) = \mathbb{R}$. Here a, b are real numbers with $a < b$ (except in the first of these 9 types where $a \leq b$). [Pictures drawn in class.]
- $\emptyset$ denotes the empty set (no members). The simplest kind of set after the empty set is a set with only one element (number), this is called a *singleton set*. A set A is called *finite* iff $\exists n \in \mathbb{N}$ such that A can be written as $A = \{x_1, x_2, \cdots, x_n\}$, for some $x_1, x_2, \cdots x_n \in A$. If the x_i here are all different (distinct), then n is called the *cardinality* of A. So a singleton set has cardinality 1. A set is called *infinite* if it is not finite. Intervals are infinite sets (except $[a, a]$).
- The notation $A \subseteq B$ or $A \subset B$ means that A is a subset of set B, (that is, $x \in A \ \Rightarrow \ x \in B$). Of course $A = B$ if $A \subset B$ and $B \subset A$ (that is, $x \in A \ \Leftrightarrow \ x \in B$).

  Example: $5 \in \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}, \qquad \{1, 2, 3, 4\} = \{2, 4, 1, 3\} = \{1, 2, 3, 2, 4, 2\}$.
- Unions: $A \cup B = \{x : (x \in A) \vee (x \in B)\}$

  Intersections: $A \cap B = \{x : (x \in A) \wedge (x \in B)\}$

  We will talk about unions and intersections of infinitely many sets later
- Complement: $A^c = \{x : x \notin A\}$
- We say that sets A and B are *disjoint* if $A \cap B = \emptyset$ (no common elements).
- Examples: $A = \{1, 2, 3, 4\}, \quad B = \{2, 4, 6\}, \quad A \cup B = \{1, 2, 3, 4, 6\}$

$$A \cap B = \{2, 4\}, \quad A \backslash B = \{1, 3\}, \quad (A \cap B) \cup (A \backslash B) = \{1, 2, 3, 4\} = A$$

- **Functions:** $f : A \to B$ means that f is a function from domain A into the codomain B. Most of the following you will have met in other courses such as Calculus II:
- The default domain of f in this course is the largest subset of numbers x in $\mathbb{R}$ for which $f(x)$ is a real number or makes sense. For example the default domain of $1/\sqrt{2-x}$ is $(-\infty, 2)$.
- Image: if $C \subseteq A$, and $f : A \to B$, then $f(C) = \{f(x) : x \in C\}$. This is a subset of the codomain of f, called the *image* of C under f
- Pre-image: If $f : A \to B$, and $D \subseteq B$, then $f^{-1}(D) = \{x \in A : f(x) \in D\}$. This is called the *pre-image* of D under f
- I did an example in class of finding the image and pre-image: here A was the set of all students in class today, $B = \{n \in \mathbb{N} : n \leq 12\}$, and $f(x)$ is the number of the birthmonth of student x. I asked $f^{-1}(\{2, 3, 7\})$ to stand up. I also asked what $f(B)$ was if B were the students in class today wearing red shirts.
- We say that $f : A \to B$ is *surjective*, or *onto* if $f(A) = B$. That is, $\forall b \in B \; \exists a \in A$ s.t. $f(a) = b$.
- We say that $f : A \to B$ is *injective*, or *one-to-one* if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. We sometimes write f is 1-1 in this case.
- We say that $f : A \to B$ is *bijective* if it is one-to-one and onto. In this case there is an inverse function $f^{-1} : B \to A$ with $f^{-1}(y) = x$ iff $f(x) = y$, for $x \in A, y \in B$. Actually there exists an inverse function if f is merely injective (and not onto), but the domain of f^{-1} in that case is $f(A)$.
- Composition of functions: If $f : A \to B$ and $g : B \to C$ then $g \circ f : A \to C$ is such that $(g \circ f)(a) = g(f(a))$ for $a \in A$

3. The real numbers

3.1. **Mathematical induction.** Axiom: [Well-ordering property of $\mathbb{N}$]. Let $S \neq \emptyset$ be a subset of $\mathbb{N}$. Then $\exists m \in S$ s.t. $m \leq k, \ \forall k \in S$. (Note: $m = \min(S)$).

We will go through the following quickly, since many of you already know it. See also wikipedia.

Theorem 3.1. [Principle of Mathematical Induction] *Let $P(n)$ be a statement $\forall n \in \mathbb{N}$. Suppose that*

(a) *$P(1)$ is true, and*
(b) *$\forall k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is true.*

Then $P(n)$ is true $\forall n \in \mathbb{N}$.

Remark: Sometimes the assumption that $P(k)$ is true in statement (b) is called the *inductive hypothesis*.

Proof. By contradiction. Suppose that the statements (a) and (b) hold, but $P(n)$ is false for some $n \in \mathbb{N}$. That is, the set $S = \{n \in \mathbb{N} : P(n) \text{ is false}\}$ is not the empty set. By the well-ordering axiom, $\exists m \in S$ s.t. $m \leq k, \ \forall k \in S$. Since $P(1)$ is true by (a), $1 \notin S$, so that $m > 1$. Then $m - 1 \in \mathbb{N}$, and $m - 1 \notin S$ (since m is the least element). Thus, $P(m-1)$ is true, and so $P(m)$ is true by (b), so $m \notin S$, which contradicts the definition of m. Thus $S = \emptyset$, and $P(n)$ is true $\forall n \in \mathbb{N}$. □

It is best to always have certain words in every mathematical induction proof. Otherwise you may lose points. I have underlined such words in the examples below.

Example: Prove that $1 + 2 + \cdots + n = \frac{1}{2}n(n+1), \ \forall n \in \mathbb{N}$.

Solution. <u>We use Mathematical Induction. First we check that the statement is true for $n = 1$:</u>

$$1 = \frac{1}{2}(1)(1+1),$$

<u>which is true. Next assume that the statement is true for $n = k$, that is:</u>

$$1 + 2 + \cdots + k = \frac{1}{2}k(k+1).$$

<u>We need to prove that the statement is true for $n = k+1$, that is, we need to check if:</u>

$$1 + 2 + \cdots + k + (k+1) = \frac{1}{2}(k+1)[(k+1)+1].$$

The left side of the last formula, <u>by the inductive hypothesis</u>, equals:

$$\frac{1}{2}k(k+1) + (k+1) = (k+1)(\frac{1}{2}k + 1) = (k+1)(\frac{1}{2}k + \frac{1}{2} \cdot 2) = \frac{1}{2}(k+1)(k+2).$$

The right side of the formula we are checking, is:

$$\frac{1}{2}(k+1)[(k+1)+1] = \frac{1}{2}(k+1)(k+2).$$

Since the left side equals the right side, we have proved that the statement is true for $n = k+1$. By mathematical induction, it is true for all $n \in \mathbb{N}$. $\square$.

Modified induction: Instead of proving that $P(n)$ is true for all $n \in \mathbb{N}$, we may be asked to prove $P(n)$ for $n \geq m$. Here m is some fixed 'starting point' integer. For example, we may be asked to prove $P(0), P(1), P(2), \ldots$; or we may want to prove $P(5), P(6), P(7), \ldots$ (indeed $P(4)$ may not be true). Here the theorem is: Suppose that (a) $P(m)$ is true, and (b) for all integers $k \geq m$, if $P(k)$ is true then $P(k+1)$ is true. Then $P(n)$ is true for all $n \in \mathbb{N}, n \geq m$.

Example: Prove that $2^n > n^2$ for all natural numbers $n \geq 5$.

Solution. We use Mathematical Induction. First we check that the statement is true for $n = 5$:

$$2^5 = 32 > 25 = 5^2,$$

which is true. Next assume that the statement is true for an integer $n = k \geq 5$, that is:

$$2^k > k^2.$$

We need to prove that the statement is true for $n = k+1$, that is, we need to check if:

$$2^{k+1} > (k+1)^2.$$

The left side of the last formula, by the inductive hypothesis, equals:

$$2 \cdot 2^k > 2 \cdot k^2.$$

The right side of the formula we are checking, is:

$$(k+1)^2 = k^2 + 2k + 1.$$

Thus we are done if $2 \cdot k^2 > k^2 + 2k + 1$, that is if $2k^2 - (k^2 + 2k + 1) = k^2 - 2k - 1 > 0$ for $k \geq 5$. By College Algebra or Calculus I it is easy to see that $k^2 - 2k - 1 > 0$ if $k \geq 5$ (indeed the quadratic $x^2 - 2x - 1$ has its biggest root at $\frac{-b+\sqrt{b^2-4ac}}{2a} = \frac{2+\sqrt{8}}{2} = 1 + \sqrt{2} < 5$. See picture drawn in class). Thus the left side of the formula we are checking is greater than the right side, and so we have proved that the statement is true for $n = k+1$.
By (modified) induction, it is true for all $n \in \mathbb{N}, n \geq 5$. $\square$.

3.2. **Ordered fields.** We are moving towards trying to define the real numbers. We will define them by their properties: we will make a long list of 'sensible properties', and the real numbers will be the only thing that satisfies all of this long list. All other so-called 'well-known facts' about real numbers can be deduced from this list!

You do not need to memorize the following definitions:

A *field* is any set $\mathbb{F}$ with an addition $+$ and a multiplication $\cdot$ such that

- A1 $\forall x, y \in \mathbb{F},\ x + y \in \mathbb{F}$
- A2 $x + y = y + x$
- A3 $x + (y + z) = (x + y) + z$
- A4 $\exists$ unique element in $\mathbb{F}$, written 0, s.t. $0 + x = x,\ \forall x \in \mathbb{F}$
- A5 $\forall x \in \mathbb{F}, \exists w \in \mathbb{F}$ s.t. $x + w = 0$
- M1 $\forall x, y \in \mathbb{F},\ x \cdot y \in \mathbb{F}$
- M2 $x \cdot y = y \cdot x$
- M3 $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- M4 $\exists$ unique element in $\mathbb{F}$, written 1, s.t. $1 \cdot x = x,\ \forall x \in \mathbb{F}$
- M5 $\forall x \in \mathbb{F},\ x \neq 0,\ \exists\ z \in \mathbb{F}$ s.t. $\quad x \cdot z = 1$.
- DL $x \cdot (y + z) = x \cdot y + x \cdot z$

Items (A2,A3,M2,M3,DL) must hold for all $x, y, z \in \mathbb{F}$.

The number 0 in (A4) is called the *zero*, the number 1 in (M4) is called the *one* or *identity*, the number w in (A5) is called the *negative* of x and is written as $-x$, and the number z in (M5) is called the *inverse* or *reciprocal* of x and is written as $\frac{1}{x}$ or x^{-1}.

An *ordered field* is a field $\mathbb{F}$ with a relation/ordering $<$ such that

- O1 $\forall x, y \in \mathbb{F}$ exactly one of the relations $x < y$, $y < x$, or $y = x$ holds
- O2 if $x < y$ and $y < z$, then $x < z$
- O3 if $x < y$, then $x + z < y + z$
- O4 if $x < y$ and $z > 0$, then $xz < yz$

Here of course, $x, y, z \in \mathbb{F}$.

Examples. The set $\mathbb{Q}$ is an ordered field, that is it obeys these 11 + 4 axioms.

The following are "examples of proving the obvious". Why do we want to do this? Answer: 1) they are examples of showing how all properties we know about numbers, and say are obvious, are actually derivable from the dozen or so rules (A1, A2, $\cdots$) above, and 2) for practice at proving things and using mathematical logic.

Theorem 3.2. *Let x, y, z be in an ordered field $\mathbb{F}$.*

(a) *If* $x + z = y + z$, *then* $x = y$,
(b) $x \cdot 0 = 0$,
(c) $(-1) \cdot x = -x$,
(d) $xy = 0 \iff x = 0$ *or* $y = 0$,
(e) $x < y \iff -y < -x$,
(f) *If* $x < y$ *and* $z < 0$, *then* $xz > yz$
(g) *If* $xz = yz$, *and* $z \neq 0$ *then* $x = y$.

Proof. (a) If $x+z = y+z$, then adding $-z$, we get $(x+z)+(-z) = (y+z)+(-z)$. Now $(x+z)+(-z) = x+(z+(-z))$ by (A3), which equals $x+0$ by (A5), which equals $0+x$ by (A2) and (A4). So $(x+z)+(-z) = x$ and similarly $(y+z)+(-z) = y$. So $x = y$.

(b) By A4, $x \cdot 0 = x \cdot (0+0) \overset{DL}{=} x \cdot 0 + x \cdot 0$. By A4 again, $0 + x \cdot 0 = x \cdot 0 + x \cdot 0$. So by (a), $0 = x \cdot 0$.

(c) By M2, we have

$$x + (-1) \cdot x = x + x \cdot (-1) \overset{M4}{=} x \cdot 1 + x \cdot (-1) \overset{DL}{=} x \cdot [1 + (-1)] \overset{A5}{=} x \cdot 0 \overset{(b)}{=} 0.$$

By A5, $(-1) \cdot x = -x$

(d) ($\Leftarrow$) If $y = 0$, then $xy = x \cdot 0 \overset{(b)}{=} 0$. If $x = 0$, then $xy = 0 \cdot y \overset{M2}{=} y \cdot 0 \overset{(b)}{=} 0$.

($\Rightarrow$) Suppose that $xy = 0$ and $x \neq 0$. We prove that $y = 0$. Since $x \neq 0$, there is an inverse $\frac{1}{x}$ s.t. $\left(\frac{1}{x}\right) \cdot x \overset{M2}{=} x \cdot \left(\frac{1}{x}\right) \overset{M5}{=} 1$. Thus

$$0 \overset{(b)}{=} \left(\frac{1}{x}\right) \cdot (xy) \overset{M3}{=} \left(\frac{1}{x} \cdot x\right) \cdot y = 1 \cdot y \overset{M4}{=} y.$$

So $y = 0$.

(e) ($\Rightarrow$) $x < y \overset{O3}{\Rightarrow} x + [(-x)+(-y)] < y + [(-x)+(-y)] \overset{A2}{\Rightarrow} x + [(-x)+(-y)] < y + [(-y)+(-x)] \overset{A3}{\Rightarrow} [x+(-x)] + (-y) < [y+(-y)] + (-x) \overset{A5}{\Rightarrow} 0 + (-y) < 0 + (-x) \overset{A2,A4}{\Rightarrow} -y < -x$.

($\Leftarrow$) is similar.

(f) If $z < 0$, then $-0 < -z$ by (e). Since $0 + 0 = 0$ by A4, and $0 + (-0) = 0$ by A5, we have $-0 = 0$ and $0 < -z$. Thus if $x < y$ then by O4 we have $x(-z) < y(-z)$. Now $-z = (-1)z$ by (c), and so

$$x(-z) = x[(-1)z] \overset{M3}{=} [x(-1)]z \overset{M2}{=} [(-1)x]z \overset{M3}{=} (-1)(xz) \overset{(c)}{=} -(xz).$$

Similarly, $y(-z) = -(yz)$. Thus, $-(xz) < -(yz)$, and then (e) gives $yz < xz$.

(g) Similar to (a) but using the product rather than $+$, and 1 rather than 0 and $1/z$ rather than z. $\square$

From Calculus (or before) we recall the *absolute value* of a number:

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

Some also call this the *modulus* or mod x.

Theorem 3.3. (a) $|x| \geq 0$,
(b) *If* $a \geq 0$ *then* $|x| \leq a \;\Leftrightarrow\; -a \leq x \leq a$*; and in particular* $-|x| \leq x \leq |x|$,
(c) $|xy| = |x| \cdot |y|$,
(d) $|x+y| \leq |x| + |y|$ *("triangle inequality")*
(e) $|-x| = |x|$ *and* $|x-y| = |y-x|$.
(f) $||x| - |y|| \leq |x-y|$.

Proof. (a) If $x \geq 0$ then $|x| = x \geq 0$. If $x < 0$, then $|x| = -x > 0$, as we saw in the last proof somewhere. So in both cases, $|x| \geq 0$.

(b) ($\Rightarrow$) If $|x| \leq a$ and $x \geq 0$, then $-a \leq 0 \leq x = |x| \leq a$. If $x < 0$, then $-x = |x| \leq a \;\Rightarrow x \geq -a$. Thus, $-a \leq x < 0 \leq a$.

($\Leftarrow$) Suppose $-a \leq x \leq a$. If $x \geq 0$, then $x = |x| \leq a$. If $x < 0$, $a \geq -x = |x|$.

(c) Do as an exercise (Hint: consider four cases depending on whether x and y are both positive, both negative, or have opposite signs. For example, if $x \geq 0, y < 0$ then $xy \leq 0$ and so $|xy| = -(xy) = x(-y) = |x| \cdot |y|$).

(d) By (b) we have $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$. Adding these together: $-(|x|+|y|) \leq x+y \leq |x|+|y|$. Hence, by (b) again (but used in the other direction), $|x+y| \leq |x| + |y|$.

(e) The first follows from (c) with $y = -1$, the second follows from the first with x replaced by $y - x$ (of course $-(y-x) = x - y$).

(f) $|x| = |x-y+y| \leq |x-y|+|y|$ by the triangle inequality. So $|x|-|y| \leq |x-y|$. Similarly, $|y| - |x| \leq |y-x| = |x-y|$ (using (e) too), so mulyiplying by -1 we get $|x| - |y| \geq -|x-y|$. So $-|x-y| \leq |x| - |y| \leq |x-y|$; hence $||x| - |y|| \leq |x-y|$ by (b). $\square$

Another useful form: $|a-b| \leq |a-c| + |c-b|$. This follows from the triangle inequality: $|a-b| = |a-c+c-b| \leq |a-c| + |c-b|$.

We will prove later that square roots exist. For now let us just take it on faith.

Proposition 3.4. $\sqrt{2}$ *is irrational.*

Proof. We will use the 'prime factorization' from earlier courses: any $n \in \mathbb{N}$ may be uniquely written as $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ where $1 < p_1 < p_2 < \cdots < p_k$ are primes, and $m_k \in \mathbb{N}$. Such primes $p_1, \cdots, p_k$ are called the prime factors of n. Note that then $n^2 = p_1^{2m_1} p_2^{2m_2} \cdots p_k^{2m_k}$; from which one can deduce that n and n^2 have exactly the same prime factors. BWOC, suppose $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ and $n \neq 0$ and m and n have no common prime factors. Then $2 = \frac{m^2}{n^2}$, so that $2n^2 = m^2$. Thus m^2 is 'divisible' by 2; that is 2 is one of its prime factors. Hence 2 must be one of the prime factors of m (Why?). Thus, $m = 2k$ for some $k \in \mathbb{Z}$. But then $2n^2 = (2k)^2 = 2^2k^2$, so that $n^2 = 2k^2$. So 2 is a prime factor of n^2, hence

2 is a prime factor of n. This contradicts the fact that m and n have no common prime factors. $\square$

Remark A similar proof shows that $\sqrt{p}$ is irrational for any prime number p.

Homework 1.

See course webpage.

3.3. **The completeness axiom.** The next bit you also saw in Calculus I and it is in the official syllabus for the "Transitions" course:

Definitions Let S be a nonempty subset of $\mathbb{F}$. A number $M \in \mathbb{F}$ is called an *upper bound* for S if $\quad x \leq M, \quad \forall x \in S$. If there exists an upper bound for S then we say that S is *bounded above*, otherwise S is *unbounded above.*

Similarly, a number $m \in \mathbb{F}$ is a *lower bound for S*, and the set S is *bounded below*, if $\quad m \leq x, \quad \forall x \in S$. Otherwise S is *unbounded below.*

The set S is *bounded* if it is bounded below and above.

An upper bound β of the subset S, which has the property that $\beta \leq M$ for every upper bound M for S, is called the *least upper bound* or *supremum* of S. It is denoted by $lub(S)$ or $\sup(S)$.

Similarly, a lower bound α of S, which has the property that $\alpha \geq m$ for every lower bound m for S, is called the *greatest lower bound* or *infimum* of S. It is denoted by $glb(S)$ or $\inf(S)$.

If an upper bound M is an element of S, then it is called the *maximum* of S (largest element), denoted by $\max(S)$. Clearly this is the least upper bound of S, since any other upper bound of S is $\geq \max(S)$ (because $\max(S) \in S$). So $\max(S) = \sup(S)$ in this case. If no upper bounds of S are in S we say that S has *no maximum*, or that *no maximum exists.*

Similarly, if a lower bound m is an element of S, then it is called the *minimum* (least element), denoted by $\min(S)$. Clearly this is the greatest lower bound of S, so $\min(S) = \inf(S)$ in this case.

Remarks. 1) It is not obvious that least upper bounds or greatest lower bounds exist. In fact they do not in the field $\mathbb{F} = \mathbb{Q}$.

2) Any nonempty subset T of a bounded set S is bounded. Proof: If M is an upper bound for S, it is also an upper bound for $T \subset S$. The same holds for lower bounds.

We say that an ordered field $\mathbb{F}$ has the *completeness property* (CP) if every nonempty subset S of $\mathbb{F}$ which is bounded above, has a least upper bound in $\mathbb{F}$.

Theorem 3.5. *There exists one and only one ordered field that satisfies the completeness property (CP).*

We **define** the real numbers $\mathbb{R}$ to be the one and only one complete ordered field in the last theorem. A *real number* is a member, or element, of this one and only one complete ordered field. We will not prove this theorem (due to Dedekind and Cantor), it is too lengthy. In practice this means that we take the completeness property (CP) as an *axiom*, we are taking it on faith. It also means that all the properties of the real numbers that we learned in high school, are deducible, or can be proved, from the 16 properties above (A1–A5,M1–M5, DL, O1-O4, CP). We did some of this in Theorem 3.2 above.

- It is easy to prove from (CP) that every nonempty subset of $\mathbb{R}$ which is bounded below has a greatest lower bound or inf. Indeed in Homework 2 you will prove that if S is a nonempty set, then S is bounded below iff $T = \{-x : x \in S\}$ is bounded above, and in this case $\inf(S) = -\sup(T)$.
- A moments thought shows that a nonempty set in $\mathbb{R}$ which is bounded above (resp. below) has a maximum (resp. minimum) iff $\sup(S) \in S$ (resp. $\inf(S) \in S$).

Examples:

(a) The finite set $S = \{2, 4, 6, 8\}$ is bounded. The upper bounds of this set, are all numbers $x \geq 8$. Since the upper bound 8 is in S, we have $\max(S) = \sup(S) = 8$. Similarly, the lower bounds of this set, are all numbers $x \leq 2$, and $\min(S) = \inf(S) = 2$.

By the same argument, any finite set is bounded, and has a maximum and a minimum, which equal the sup and inf respectively.

(b) The interval $S = [1, \infty)$ has no upper bounds, but is bounded below. Since one of its lower bounds, namely 1, is in S, we have $\min(S) = \inf(S) = 1$.

(c) The interval $S = (0, 4]$ is bounded. The upper bound 4 is in S, so $\max(S) = \sup(S) = 4$. The lower bound 0 is not in the set S. Indeed the set has no minimum. To see that $0 = \inf(S)$, BWOC (by way of contradiction) suppose that there existed a lower bound m of S with $m > 0$. Since m is a lower bound, $m \leq 4$, and so $0 < \frac{m}{2} < m \leq 4$. Hence $\frac{m}{2} \in S$. But this contradicts the fact that m is a lower bound of S (since $m > \frac{m}{2} \in S$). Hence 0 is the greatest lower bound: that is, $0 = \inf(S)$.

(d) The interval $S = [1, 2)$. As in (b) we have $1 = \min(S) = \inf(S)$. Clearly 2 is an upper bound of S. BWOC, suppose that there existed an upper bound M of S with $M < 2$. Since M is an upper bound of S we have $M \geq 1$. If one draws a picture of the number line one sees the problem: if $M < 2$ then numbers between M and 2 like the average $\frac{M+2}{2}$, are in S