Math 63: Winter 2021
Lecture 2

Dana P. Williams

Dartmouth College

Wednesday January 11, 2021

Getting Started

1. Please submit your practice exam/survey by 10pm tonight via `gradescope`. Our first homework assignment will be due Friday by 3pm also via `gradescope`.
2. Everyone should be sure to familiarize themselves with our web page: `math.dartmouth.edu/~m63w21/`
3. Recall that my office hours are T 2-3 and Th 10-11. The zoom details are on my web page: `math.dartmouth.edu:~dana/office_hours/`
4. We will start each lecture with an item to ensure I've remembered to start the recording.
5. This will also be an opportunity to ask questions.

A Quick Review

Definition

We let $\mathbf{N} = \{1, 2, \dots\}$.

Remark

If $A \subset \mathbf{N}$ is such that $1 \in A$ and $n \in A$ implies $n + 1 \in A$, then $A = \mathbf{N}$.

Definition

We say that a set S is finite if it is empty or if there is a $n \in \mathbf{N}$ and a bijection $f : \{1, 2, \dots, n\} \to S$. Then we say that S has n elements and sometimes write $|S| = n$. If $S = \emptyset$, then we say S has no elements. A set which is not finite is called infinite.

Definition

If X is a set, then a sequence in X is a function $a : \mathbf{N} \to X$. We generally write a_n in place of $a(n)$ and denote a by (a_n).

Proposition

If S is infinite, then there is a sequence (a_n) in S such that $a_n \neq a_m$ if $n \neq m$. Colloquially, if S is infinite then there is a sequence of distinct elements in S.

Remark

We defined this sequence inductively: we picked a_1, and showed that if had found $a_1, \dots, a_n$ distinct in S, then we could define a_{n+1}. Hence the set A of n for which a_n is defined is such that $1 \in A$ and $n \in A$ implies $n + 1 \in A$. Thus $A = \mathbf{N}$.

Now the New Stuff: Induction

Remark (Induction)

For each $n \in \mathbf{N}$, let $P(n)$ be a statement depending on n that is either true or false. Suppose that $P(1)$ is true and whenever $P(n)$ is true, then $P(n+1)$ is true. Then $P(n)$ is true for all $n \in \mathbf{N}$. (Just let $A = \{ n \in \mathbf{N} : P(n) \text{ is true} \}$. Then $1 \in A$ and $n \in A$ implies $n + 1 \in A$. Thus $A = \mathbf{N}$.) Therefore we can prove $P(n)$ is true for all n as follows.

1. Show that $P(1)$ is true.
2. Assume that $P(n)$ is true for some $n \geq 1$. (This is called the Inductive Hypothesis.)
3. Prove that $P(n+1)$ is true using the validity of $P(n)$.

Example

Example

Show that $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Solution

Here $P(n)$ is the statement that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. This is clearly true if $n = 1$. Suppose $P(n)$ holds for some $n \geq 1$. Then we have

$$\begin{aligned} 1 + 2 + \cdots + n + 1 &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + n + 1 = \frac{1}{2}(n^2 + n + 2n + 2) \\ &= \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}. \end{aligned}$$

Therefore $P(n+1)$ holds. This completes the proof.

Finite Sets Again

Proposition

Every subset of a finite set is finite and every proper subset has a strictly smaller number of elements.

Proof.

Since this is clearly true for the empty set, it will suffice to see that, for every $n \in \mathbf{N}$, the proposition holds for every set S with n elements. Since this is clearly true for $n = 1$, we can proceed by induction. Thus we assume the result is true for sets with $n \geq 1$ elements and consider a set S with $|S| = n + 1$. Suppose $S' \subset S$. If $S' = S$ then S' is finite and there is nothing left to show. So we suppose that S' is a proper subset. Hence there is some $x \in S \setminus S'$. By assumption there is a one-to-one and onto map $f : \{1, \dots, n + 1\} \to S$. We can adjust f so that $f(n + 1) = x$. Then f restricts to a one-to-one onto map of $f' : \{1, 2, \dots, n\} \to S'' = S \setminus \{x\}$ and $S' \subset S''$. Since S'' has n elements, our induction hypothesis implies S' is finite with at most n elements. This completes the proof. $\square$

Proposition

A set S is infinite if and only if there is a one-to-one map of S onto a proper subset of itself.

Proof.

Suppose S is infinite. Then by a previous result, there is a sequence (x_n) of distinct elements in S. Let $Y = S \setminus \{ x_1, x_2, \dots \}$. Since Y and $\{ x_k : k \in \mathbf{N} \}$ are disjoint and have union S, we can define $f : S \to S$ be letting $f(x_k) = x_{k+1}$ for all $k \in \mathbf{N}$, and $f(y) = y$ if $y \in Y$. It is not so hard to see that f is one-to-one. Since it maps S onto $S \setminus \{x_1\}$, this proves the first half.
Now suppose $f : S \to S$ is one-to-one and $f(S)$ is a proper subset of S. Suppose to the contrary of what we want to prove that S is finite. Then, since f is one-to-one, $|S| = |f(S)|$. But this contradicts our previous result on proper subsets of finite sets. Hence S must be infinite. $\square$

Short Break

1. Let's Take a short break for questions.

Let's Get Real

Since this is a course in "Real Analysis", it is time we agreed on what a real number is. So let's review what sort of numbers we do know about.

- We've already met the natural numbers $\mathbf{N} = \{1, 2, 3, \dots\}$.
- The integers, or the set of whole numbers, is the set $\mathbf{Z} = -\mathbf{N} \cup \{0\} \cup \mathbf{N} = \{0, \pm 1, \pm 2, \dots\}$.
- The rational numbers, or the set of fractions, is the set

$$\mathbf{Q} = \left\{ \frac{a}{b} : a \in \mathbf{Z} \text{ and } b \in \mathbf{N} \right\}.$$

Remark (A Field)

The rational numbers, $\mathbf{Q}$, are special as they form what is called a field. Informally, this means we can do all the usual arithmetic operations and stay inside $\mathbf{Q}$.

Fields

Definition

A field is a set $\mathbf{F}$ containing at least two elements 0 and 1 equipped with operations $+$ and $\cdot$ such that for all $x, y, z \in \mathbf{F}$ we have $x + y \in \mathbf{F}$ and $x \cdot y = xy \in \mathbf{F}$ and

1)	$x + y = y + x$	1)′	$xy = yx$
2)	$x + (y + z) = (x + y) + z$	2)′	$x(yz) = (xy)z$
3)	$x + 0 = x$	3)′	$x \cdot 1 = x$
4)	there exists $-x$ such that $-x + x = 0$	4)′	if $x \neq 0$ there exists x^{-1} such that $xx^{-1} = 1$, and

5) $x(y + z) = xy + yz$.

Example

Of course the rational numbers $\mathbf{Q} = \{ \frac{a}{b} : a \in \mathbf{Z} \text{ and } b \in \mathbf{N} \}$ satisfy all these familiar rules of arithmetic. Hence $\mathbf{Q}$ is a field. But there are lots of others.

A Field with Four Elements

Example

Let $\mathbb{F}_4 = \{0, 1, a, b\}$. Then define addition and multiplication as follows

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Then it is possible to show that $\mathbb{F}_4$ is a field. However in all honesty, it would be tedious beyond belief to check this directly. Fortunately, there are other techniques—from abstract algebra—that allow us to see this from general principles. Since we are interested in the field of real numbers, I am presenting this example only to see that you're are well-educated (and possibly to encourage you to take as abstract algebra). ▸ return1 ▸ return2

General Comments About Fields

1. While our text concerns itself only with the real numbers $\mathbf{R}$, I can't help just assuming we have a field $\mathbf{F}$ and seeing what sort of properties any field must have.
2. Associativity allows us to make sense of formulas like $a+b+c+d$. Since we can only add two things at a time, we have to insert parentheses. For example, $(a+b)+(c+d)$ or $a+(b+(c+d))$. Associativity says we can do this anyway we like. Similary, for multiplication: $abcd = a(b(cd))$.
3. If $a, b \in \mathbf{F}$, then the expression $a-b$ is defined to be $a+(-b)$. Note that unlike addition and multiplication, $a-b-c$ is ambiguous: $a-(b-c)$ and $(a-b)-c$ are different unless $c=-c$. Go

Low Hanging Fruit

Proposition

Suppose that $\mathbf{F}$ *is a field and* $a, b \in \mathbf{F}$. *Then the equation* $a + x = b$ *has a unique solution. In particular, the additive inverse* $-a$ *is unique—it is the only solution to* $a + x = 0$. *Similarly, the additive identity* 0 *is unique—if* $a + x = a$, *then* $x = 0$.

Proof.

Since $a + (-a + b) = (a + (-a)) + b = 0 + b = b$, it follows that $-a + b = b - a$ is a solution to $a + x = b$. On the other hand, if $a + x = b$, then $-a + (a + x) = -a + b$. Thus by associativity and commutivity, $(-a + a) + x = b - a$. This proves the first assertion. The remaining assertions are straightforward consequences of the first. □

An Amusing Corollary or Two

Corollary

If $\mathbf{F}$ *is a field and* $a \in \mathbf{F}$*, then* $0a = 0$*.*

Proof.

We have $0a = (0+0)a = 0a + 0a$. Thus $0a = 0$ by the last part of the previous proposition. (Or just add $-0a$ to both sides.) $\square$

Corollary

Suppose that $\mathbf{F}$ *is a field and* $a \in \mathbf{F}$*. Then* $-a = (-1)a$*.*

Proof.

Observe that $(-1)a + a = (-1)a + (1)a = (-1+1)a = 0a = 0$. Hence $(-1)a = -a$ by the previous proposition. $\square$

Question

How does the previous corollary manifest itself for $\mathbf{F} = \mathbb{F}_4$? Go

What About Multiplication?

1. Does $ax = b$ always have a unique solution in a field **F**?
2. You should formulate your own proposition for $ax = b$ and uniqueness statements for a^{-1} and 1 for an arbitrary field **F**.
3. Verify that in any Field we have $-(-a) = a$, $(a^{-1})^{-1} = a$ if $a \neq 0$, $(ab)^{-1} = a^{-1}b^{-1}$, and $a(-b) = (-a)b = -(ab)$.
4. In fact all the properties **F** 4–**F** 10 in the text hold for any field **F**.

Break Time

- Again time for a short break and questions.

Ordered Fields

To single out the real numbers, as our example of $\mathbb{F}_4$ shows, we are going to need additional structure.

Definition

We say that a field $\mathbf{F}$ is ordered if there is a subset $P \subset \mathbf{F} \setminus \{0\}$ such that

1. $\mathbf{F}$ is the disjoint union of P, $\{0\}$, and $-P$.
2. If $a, b \in P$, then $a + b \in P$ and $ab \in P$.

We say that $x > 0$ if $x \in P$ and $x < y$ if $y - x \in P$. We call the pair $(\mathbf{F}, P)$, or sometimes $(F, <)$ an ordered field.

Remark (Trichotomy)

If a is an element in an ordered field, then exactly one of the following holds: a is positive, $-a$ is positive, or $a = 0$. Equivalently, given a, b in an ordered field, either $a < b$, $b < a$, or $a = b$. In particular, $\mathbb{F}_4$ can't be made into an ordered field! Why not?

More on Ordered Fields

Example

Let $P = \{ \frac{a}{b} \in \mathbf{Q} : a, b \in \mathbf{N} \}$. Then $(\mathbf{Q}, P)$ is an ordered field that we've held dear to our hearts since grade school.

Proposition

Let $(\mathbf{F}, <)$ be an ordered field. If $a < 0$ and $b < 0$, then $ab > 0$. If $a > 0$ and $b < 0$, then $ab < 0$.

Proof.

Note that $(-1)^2 = (-1)(-1) = -(-1) = 1$. Why? If $a < 0$ and $b < 0$, then by the Trichotomy principle, $-a > 0$ and $-b > 0$. Therefore, since $\mathbf{F}$ is ordered,

$$0 < (-a)(-b) = (-1)(a)(-1)b = (-1)^2 ab = ab.$$

On the other hand if $a > 0$ and $b < 0$, then
$0 < a(-b) = a(-1)b = -ab$. Therefore $ab < 0$. □

Low Hanging Friut

Corollary

Let $\mathbf{F}$ *be an ordered field. Then for all* $a \in \mathbf{F}$, $a^2 \geq 0$ *with equality if and only if* $a = 0$.

Proof.

If $a = 0$, then clearly $a^2 = 0$. If $a > 0$, then $a^2 > 0$ by definition of an ordered field. But if $a < 0$, then $a^2 > 0$ by the previous result. □

Transitivity

Proposition

Suppose that $(\mathbf{F}, <)$ is an ordered field.

1. *If $a < b$ and $b < c$, then $a < c$. Hence there is no harm in writing $a < b < c$.*
2. *If $a < b$ and $c \leq d$, then $a + c < b + d$.*
3. *If $0 < a < b$ and $0 < c \leq d$, then $ac < bd$.*

Proof.

(1) By assumption $b - a > 0$ and $c - b > 0$. Hence $0 < (b - a) + (c - b) = c - a$ and $a < c$.
(3) By assumption $b - a > 0$. Since $c > 0$, $c(b - a) = cb - ca > 0$. But $d - c \geq 0$ and $b > 0$, so $(d - c)b = db - cb \geq 0$. Then $bd - ac = (bd - cb) + (cb - ac) > 0$. That is $ac < bd$.
(2) Is similar to (3), but easier. □

Absolute Value

Definition

If $\mathbf{F}$ is an ordered field and $a \in \mathbf{F}$, then we define the absolute value by

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

Proposition

If $\mathbf{F}$ is an ordered field and $a, b \in \mathbf{F}$, then

1. $|a| \geq 0$ *with equality only when* $a = 0$,
2. $|ab| = |a| \cdot |b|$,
3. $|a^2| = a^2$,
4. *(triangle inequality)* $|a + b| \leq |a| + |b|$, *and*
5. *(reverse triangle inequality)* $|a - b| \geq \big||a| - |b|\big|$.

Proof

Proof.

Items 1, 2, and 3 are fairly routine. To prove the triangle inequality, note that $a \leq |a|$ implies $a + b \leq |a| + |b|$. Similarly, $-a \leq |a|$ implies $-(a+b) = -a - b \leq |a| + |b|$. But then $|a+b| \leq |a| + |b|$ as claimed.
To prove the reverse triangle inequality, note that $|a| = |(a-b)+b| \leq |a-b| + |b|$. Hence $|a| - |b| \leq |a-b|$. Reversing the roles of a and b gives $-(|a| - |b|) = |b| - |a| \leq |b-a| = |a-b|$. But then $\big||a| - |b|\big| \leq |a-b|$. $\square$

Integral Exponents

Notation

If $\mathbf{F}$ is a field and $a, b \in \mathbf{F}$ with $b \neq 0$, then $\frac{a}{b} = ab^{-1}$.

Definition

Let $\mathbf{F}$ be a field and $a \in \mathbf{F} \setminus \{0\}$. Let $a^0 = 1$ and $a^1 = a$. For $n \in \mathbf{N}$, let $a^{n+1} = a^n a$ and $a^{-n} = \frac{1}{a^n}$. (Note that writing $a^{-n} = (a^n)^{-1}$ would be problematical here.) Thus colloquially, if $n \in \mathbf{N}$, we have $a^n = \underbrace{a \cdot \cdots \cdot a}_{n\text{-times}}$.

Proposition

Suppose that $\mathbf{F}$ *is a field and* $a, b \in \mathbf{F} \setminus \{0\}$. *Then for all* $n, m \in \mathbf{Z}$,

1. $a^n a^m = a^{n+m}$.
2. $(a^n)^m = a^{nm}$.
3. $(ab)^n = a^n b^n$.

Sketch of the Proof.

Item 1 is trivially true if $m = 0$, and true for $m = 1$ (if you consider the three cases $n \in \mathbf{N}$, $n = 0$, and $-n \in \mathbf{N}$ separately). Then we can proceed by induction:

$$a^n a^{m+1} = a^n a^m a = a^{n+m} a = a^{n+m+1}$$

to show item 1 holds for all $m \geq 0$. Now we prove $a^n a^{-m} = a^{n-m}$ for all $m \in \mathbf{N}$ similarly. Items 2 and 3 are proved similarly. $\square$

Enough

1. That is enough for today.
2. We covered most, but not all of §II.2. You'll need to read that section carefully.