Math 24: Winter 2021
Lecture 1

Dana P. Williams

Dartmouth College

January 8, 2021

The Ground Rules

1. We should always start each session by making sure we are recording.
2. Everyone should be sure to familiarize themselves with our web page: `math.dartmouth.edu/~m24w21/`
3. In this pandemic world, it is just a fact of life that we may have to adapt to circumstances and the term evolves. Hence details and requirements for the course may change. It is your responsibility to keep apprised of any changes.

What Are We Doing Here

1. First and foremost, this is a class on Linear Algebra.
2. But is also a course stressing mathematical formalism and proof. Proof writing will be a new experience for many of you. The best way to learn is by doing (and asking questions during class and especially in office hours).
3. We will start by seeing that the basic properties we use with directed line segments—called vectors in Physics and/or Math 8 at Dartmouth—can be abstracted in a structure we will call a vector space. Then general properties of abstract vector spaces can be used to study many mathematical concepts such as polynomials and differential equations.
4. But let's not get too far ahead of ourselves and begin with a review of where we come from.

The Cast of Characters

Let's recall that sorts of numbers we've worked with in our calculus courses up until now.

- The natural numbers $\mathbf{N} = \{1, 2, 3, \dots\}$. The choice not to include 0 in $\mathbf{N}$ is a controversial one. Computer scientists would object.
- 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) $x(y + z) = xy + yz$.

return

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. In Math 24, we will accept that $\mathbb{F}_4$ is a field. return

The Point

1. Honestly, we won't worry too much about strange objects like $\mathbb{F}_4$ in this course. I introduced it just to illustrate that there are lots more mathematical structures out there which we might not imagine are fields at first blush.
2. Therefore, if we are faced with question "Is it always true the $0 \cdot a = 0$ in any field?", then we have to decide if this is always true in any field $\mathbf{F}$. Is it?
3. In a different course, we might worry about the following.

In a Different Course

Proposition

Let $\mathbf{F}$ *be a field. If* $a \in \mathbf{F}$*, then the "additive inverse"* $-a$ *is unique. That is, if* $x + a = 0$*, then* $x = -a$*. In particular,* $(-1) \cdot a = -a$ *for all* $a \in \mathbf{F}$*.*

Proof.

Suppose that $x + a = 0$. Then $-a + (x + a) = -a + 0$. Now since 0 is the additive identity and addition is commutative, $-a + (a + x) = -a$. Since addition is associative, $-a = (-a + a) + x = 0 + x = x$.
This proves the first assertion. Then
$(-1)a + a = (-1)a + (1)a = (-1 + 1)a = 0 \cdot a = 0$. Thus by the first part, $(-1)a = -a$. □

Question

If $x \in \mathbb{F}_4$, what is $-x$? ▸ Recall

Ordered Fields

As our example of a field with 4 elements shows, there is more to the "good old arithmetic" we're used to than just the algebraic axioms of a field. In many applications, we want more 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

If a is an element in an ordered field, either a is positive, $-a$ is positive, or $a = 0$. Alternatively, 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?

Not a Rational World

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.

- The rationals were fine for middle school, but we quickly see that there are numbers like $\sqrt{3}$, e, and π that are not rational.
- Thus if we want to model the real world, we need to enlarge $\mathbf{Q}$ so that, for example, every cubic polynomial crosses the x-axis (that is, has a root). We also want to write down a formula for the area of a circle of radius one, or to describe exponential growth, and generally perform many other tasks that take us outside of the "rational" world.
- Since we still want to do arithmetic using the usual axioms that make $\mathbf{Q}$ a field, we want a field $\mathbf{R}$ that contains not only all the fractions in $\mathbf{Q}$ but all the other "numbers" we need to model the world we live in. That is, the "real" world.

Remark

Without much fanfare in High school, it was asserted that there was a field $\mathbf{R}$—called the field of Real numbers—such that $\mathbf{Q} \subset \mathbf{R}$ and "everything we wanted' was in $\mathbf{R}$. Formally, we want $\mathbf{R}$ to be a complete ordered field in that it satisfies the following property: Given a non-empty set $S \subset \mathbf{R}$ such that there is a $b \in \mathbf{R}$ (called an upper bound for S) such that $s \leq b$ for all $s \in S$, then there is a $u \in \mathbf{R}$ such that

1. $s \leq u$ for all $s \in S$, and
2. if $s \leq t$ for all $s \in S$, then $u \leq t$.

Then u is called the least upper bound of S. We write $u = \text{lub}(S)$.

Complete is the Thing

Example

Let

$$S = \{ r \in \mathbf{Q} : r^2 < 3 \}.$$

Then S is bounded above and $\sqrt{3} = \text{lub}(S)$. The real point of this example—no pun intended—is that in the field $\mathbf{Q}$, the set S is still bounded above, but it has no least upper bound.

Remark

Remarkably, the completeness axiom tells us that $\mathbf{R}$ has to contain just about everything we want. Just as in all the courses that have come before, we just assume that the real numbers exist, are a complete ordered field, and that they form the playground we are used to.

An Example

Proposition

Let $\mathbf{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \in \mathbf{R} : a, b \in \mathbf{Q} \}$. *Note that* $0, 1 \in \mathbf{Q}(\sqrt{2})$. *Then* $\mathbf{Q}(\sqrt{2})$ *is a field with the operations inherited from* $\mathbf{R}$. *Since* $\mathbf{Q}(\sqrt{2}) \subset \mathbf{R}$, *we say that is is a subfield of* $\mathbf{R}$.

Proof.

It is straightforward to check that $\mathbf{Q}(\sqrt{2})$ is closed under addition and multiplication. For example,
$(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + a'b)\sqrt{2} \in \mathbf{Q}(\sqrt{2})$.
Since $\mathbf{Q}(\sqrt{2}) \subset \mathbf{R}$ and $0, 1 \in \mathbf{Q}(\sqrt{2})$, it is clear that all the axioms of a field are satisfied with the exception of 4) and 4′). But
$-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in \mathbf{Q}(\sqrt{2})$ so 4) is easy. But if
$a + b\sqrt{2} \neq 0$, then $a^2 - 2b^2 \neq 0$ (since $\sqrt{2} \notin \mathbf{Q}$) and

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

is also in $\mathbf{Q}(\sqrt{2})$. Therefore $\mathbf{Q}(\sqrt{2})$ is a field. □

Sometimes You Want it All

Remark

Sometimes even the real numbers are not enough. For example, the equation $x^2 = -1$ has no solution in $\mathbf{R}$. So we invent a solution and call it i. Then the complex numbers are the set of formal sums

$$\mathbf{C} = \mathbf{R}(i) = \{ x + iy : x, y \in \mathbf{R} \}$$

equipped with the operations

$$(x + iy)(x' + iy') = (x + x') + i(y + y') \quad \text{and}$$
$$(x + iy)(x' + iy') = xx' - yy' + i(xy' + x'y).$$

We accept the fiction that our high schools taught us that $\mathbf{C}$ is field containing $\mathbf{R}$ as a subfield (via $x \mapsto x + i0$). Since it may have been a while since you thought about complex numbers, it might be wise to skim Appendix D in our text.

Chill Folks

Remark

In Math 24, we are primarily concerned with the usual fields $\mathbf{F}$ where $\mathbf{F}$ is either $\mathbf{Q}$, $\mathbf{R}$, or sometimes $\mathbf{C}$. Even so, we need to be aware that even in this rarefied domian, there are subfields like $\mathbf{Q}(\sqrt{2})$ out there. For more on fields, see Appendix C.

Enough for one Go

With all due apologies to Scott Adams, perhaps it is time to take a break.

Back At It

1. It is my plan to break up our lectures into two or three bits.
2. This not only gives us a chance to rest and/or ask questions, but it also breaks the videos up.
3. But I will need to be reminded from time to time to restart the recording.

Definition

A vector space over a field $\mathbf{F}$ is a set V together with operations $(x, y) \mapsto x + y$ from $V \times V$ to V (called addition) and $(a, v) \mapsto a \cdot v$ from $\mathbf{F} \times V \to V$ (called scalar multiplication) such that the following axioms hold for all $x, y, z \in V$ and $a, b \in \mathbf{F}$.

vs1: $x + y = y + x$.

vs2: $(x + y) + z = x + (y + z)$.

vs3: There is an element $0 \in V$ such that $x + 0 = x$ for all x.

vs4: For each $x \in V$ there is a $-x \in V$ such that $-x + x = 0$.

vs5: For all $x \in V$, $1 \cdot x = x$.

vs6: $(ab) \cdot x = a \cdot (b \cdot x)$.

vs7: $a \cdot (x + y) = a \cdot x + a \cdot y$.

vs8: $(a + b) \cdot x = a \cdot x + b \cdot x$.

Remark

Just as for the abstract notion of a field, a vector space is just an abstraction of a well known toy from our old mathematical playpen.

Let $V = \mathbf{R}^2 = \{ (x, y) : x, y \in \mathbf{R} \}$ and $\mathbf{F} = \mathbf{R}$. Then we defined "vector addition" and "scalar multiplication" by $(x, y) + (x', y') = (x + x', y + y')$ and $a \cdot (x, y) = (ax, ay)$. If we agree to think of V as directed line segments in the plane, then V is just the set of 2-vectors with vector addition and scalar multiplication as defined in Math 8. Surely your previous instructors observed that axioms VS1–VS8 are satisfied for V while you ignored him or her.

The Example

Example

Let $\mathbf{F}$ be a field and $n \in \mathbf{N}$. Then the set of n-tuples $\mathbf{F}^n = \{ (a_1, a_2, \ldots, a_n) : a_k \in \mathbf{F} \}$ is a vector space with the operations $(a_1, \ldots, a_n) + (a'_1, \ldots, a'_n) = (a_1 + a'_1, \ldots, a_n + a'_n)$ and $a \cdot (a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)$.

Remark

Checking that the axioms VS1–VS8 hold isn't either hard or interesting. When $\mathbf{F} = \mathbf{R}$ and $n = 2$, then we can draw pretty pictures as in §1.1 of the text. But if $\mathbf{F} \neq \mathbf{R}$ or $n > 3$, then we just get an algebraic object. While the vector space $V = \mathbf{F}^n$ is a very concrete and very common example of a vector space over $\mathbf{F}$, it is not the only example we will work with.

Example

Let $\mathbf{F}$ be a field. Then $M_{m\times n}(\mathbf{F})$ is the set of $m \times n$ matrices

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

with each $a_{ij} \in \mathbf{F}$. If $A \in M_{m\times n}(\mathbf{F})$ then we let A_{ij} be the entry in the i^{th}-row and j^{th}-column. It is easy, but again tedious, to check that we can make $M_{m\times n}(\mathbf{F})$ into a vector space over $\mathbf{F}$ by $(A+B)_{ij} = A_{ij} + B_{ij}$ and $(rA)_{ij} = rA_{ij}$. The zero element O is the zero matrix: $O_{ij} = 0$ for all i and j. If $m = n$, then elements of $M_{n\times n}(\mathbf{F})$ are called square matrices.

Example

If $\mathbf{F}$ is a field, then let $\mathrm{P}(\mathbf{F})$ the set of formal expressions $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ with $n \in \mathbf{N} \cup \{0\}$ and each $a_k \in \mathbf{F}$. (Here, x^k is just symbol that acts as a place holder.) If $a_n \neq 0$, then we say that $f(x)$ is a polynomial of degree n with coefficients in $\mathbf{F}$. We call a_k the coefficient of x^k. If all the $a_k = 0$, then $f(x)$ is called the zero polynomial and we define its degree to be -1. We declare two polynomials to be equal if their nonzero coefficients are equal. In particular, of $f(x)$ and $g(x)$ are in $\mathrm{P}(\mathbf{F})$, we can assume $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x^1 + \cdots + b_nx^n$ (by adding zero coefficients if necessary) and define $(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x^1 + \cdots (a_n + b_n)x^n$. and $(af)(x) = aa_0 + aa_1x^1 + \cdots + aa_nx^n$. Then $\mathrm{P}(\mathbf{F})$ becomes a vector space over $\mathbf{F}$.

What? I Know What a Polynomial Is!

Remark

If we are working over a reasonable ground field, like $\mathbf{F} = \mathbf{R}$ or $\mathbf{F} = \mathbf{C}$, then there is no harm in thinking of a polynomial as a function of the form $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. This is because two polynomial functions that agree everywhere must be the zero function. Why? But if $\mathbf{F} = \mathbb{F}_4$, then you can check that for all $s \in \mathbb{F}_4$, $s^4 = s$. Since we already saw that $s + s = 0$ in $\mathbb{F}_4$, the polynomial $f(x) = x + x^4$ is the zero function when viewed as a the function $s \mapsto s + s^4$ from $\mathbb{F}_4$ to itself. But $f(x)$ is is a polynomial of degree 4 in $\mathrm{P}(\mathbb{F}_4)$ and is not the zero element in the vector space $\mathrm{P}(\mathbb{F}_4)$. Fortunately, this is not the kind of thing we are going to emphasize in Math 24.

Example

Let $\mathscr{F}(X, \mathbf{F})$ be the set of all functions from a set X to the field $\mathbf{F}$. Then the $\mathscr{F}(X, \mathbf{F})$ is a vector space over $\mathbf{F}$ with respect to the operations $(f+g)(x) = f(x) + g(x)$ and $(af)(x) = af(x)$ for all $x \in X$ and $a \in \mathbf{F}$. The zero element is the zero function: $f(x) = 0$ for all $x \in X$.

Example

An element $\sigma \in \mathscr{F}(\mathbf{N}, \mathbf{F})$ is called a sequence in $\mathbf{F}$. If $a_n = \sigma(n)$, then we usually write (a_n) in place of σ. Thus the set V of sequences in $\mathbf{F}$ is a vector space over $\mathbf{F}$ with $(a_n) + (b_n) = (a_n + b_n)$ and $a \cdot (a_n) = (aa_n)$. Note that the zero element here is just the zero sequence (a_n) with $a_n = 0$ for all $n \geq 0$

Enough

1. That is enough for today.