MATH 296 2018 DISCUSSION 2: WHAT WE TALK ABOUT WHEN WE TALK ABOUT LINEAR ALGEBRA

BEN GOULD

Contents

1. Introduction

Rumor has it 296 has begun linear algebra, and it couldn't have come soon enough. Linear algebra is the appropriate introduction to abstract algebra for a first year class, and one of the most useful and instructive fields in mathematics. Here we will speak kind of philosophically, and talk about what the objects are that we care about in linear algebra (and hopefully, in algebra generally), how to think about them, and some things to keep in mind as you work for the rest of the semester[1].

We will present several facts of life over the course of this discussion. They will be notated with an asterisk ($*$).

2. Fields

What sets linear algebra apart from commutative algebra is (among other things) its insistence on working over *fields*, as opposed to *commutative rings*. The difference between the two, as you should know, is the existence in fields of multiplicative inverses for all non-zero elements. In arbitrary rings, such as $\mathbb{Z}$, not all elements admit multiplicative inverses. This may seem like a small distinction, but in the end it makes a world of difference.

For one example, consider the rational number $\frac{1}{2}$. It is obviously an element of a field (pick your poison: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$), but it is equally obviously *not* an element of $\mathbb{Z}$. However we have perhaps the next best thing: $\frac{1}{2}$ is the root of a degree-one polynomial with coefficients in $\mathbb{Z}$, namely $2x - 1$. (A degree-n polynomial with coefficients in a ring R is just a polynomial

[1]That title sounds funny...

(*not a polynomial function, a polynomial*) with maximal exponent n on the x term). We might ask the question: is $\frac{1}{2}$ the root of a polynomial over $\mathbb{Z}$ with coefficient 1 in front of the leading (highest-order) term? Such a polynomial is called *monic*. This is not an uninteresting question, and I encourage you to think about it until you come up with an answer that you can prove. I will include the correct answer on my homepage (with proof), but I will only tell you where it is if you give me an argument that you can support.

Whatever the answer is, I will tell you that it will rely on the (non-)existence of inverses in $\mathbb{Z}$. Indeed, this and many other easily-posed questions which are trivial in fields fail to be trivial in arbitrary rings. This should suggest the following fact of life to you:

Working over fields is nice. $(*)$

But what exactly do we mean by "working over" a field? That is, what objects in linear algebra exist "over fields"? These are precisely the main objects of study in linear algebra: vector spaces.

3. Groups and vector spaces

For a field k, a *k-vector space* is a set V equipped with a binary operation $+$ such that $(V, k, +)$ satisfies the following axioms:

(1) Please
(2) fill
(3) this
(4) list
(5) yourself.
(6) (If you fail to remember one of these axioms, look it up and write it down. Then tomorrow, do the same exercise. Continue until every axiom is memorized.)

Once we have an axiom system, we can pretend that we understand what is going on. But it's worth, you know, actually learning what these things mean. So: what *do* these axioms actually mean?

We recall the notion of an *abelian group*. A *group*, we remember, is a set G equipped with an associative binary operation $\cdot$ such that: G is closed under $\cdot$, there is an element $e \in G$ such that for every $g \in G$, $e \cdot g = g \cdot e = g$ (e is the *identity element* of G), and such that for each $g \in G$, there is $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1}g = e$; g^{-1} is called the *inverse* of g in G. Such an inverse is necessarily unique, as I hope you have checked. A group is called *abelian* whenever $a \cdot b = b \cdot a$ for all $a, b \in G$. In this case, the binary operation defining G is often notated by $+$, and inverses are denoted by $-g$, highly suggestively. We recall some examples for your curiosity and peace of mind.

Example. All fields form abelian groups under $+$. Prove or disprove: all fields form abelian groups under $\cdot$. If not, do they form non-abelian groups? If not, does there exist a multiplicative subgroup of a field? If so, does there exists a largest such group?

Example. The integers $\mathbb{Z}$ form an abelian group under $+$. What about $\cdot$?

Example. The cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ forms an abelian group of order n. When is $\mathbb{Z}/n\mathbb{Z}$ a field again? Recall the permuation group S_n, of bijections from a set of n elements to itself. When is S_n abelian?

Example. Let k be any field. Recalling the abelian group structure on k, give an abelian group structure on k^n for $n \in \mathbb{N}$. (If your answer doesn't restrict to the standard setting when $n = 1$, try again.)

We didn't just do that for fun, even though it was a lot of fun. In fact, we are going to use the language of abelian groups to describe vector spaces. One more piece of technical information, however: what does it mean for a group G to act on a set S? I'll let you tell me. In what follows (and often, in mathematical life), we will consider only group actions which are "compatible" with the structure of the set S in question. For example: say G is acting on another group H, with operation $+$. We will only talk about group actions which respect $+$, i.e. such that $g(h_1 + h_2) = gh_1 + gh_2$, for all $g \in G, h_i \in H$. This is not in general true for group actions, as you should note.

Now that we (hopefully) have the language of fields, groups, abelian groups, and group actions, we can come back to our main objects of interest, vector spaces. Here's a claim.

Proposition 3.1. *$(V, k, +)$ is a vector space if and only if $(V, +)$ is an abelian group equipped with a compatible k-action.*

The proof of this is mostly a string of tautologies, which are (or should be!) extremely clear from the axioms you've given above. However this gives a particular way of thinking about vector spaces:

Vector spaces are composed of a top and a bottom: on top, an abelian group, and on bottom, a field acting on that abelian group. $(*)$

This is what we mean when we say that we are working over a field. Indeed, when one chooses to work over a *ring*, things get considerably harder. See Math 494 or Math 614 for details.

I'd like to stress this characterization of vector spaces. Often you will be working with vector spaces of the form k^n (I leave it as an exercise to check that the abelian group structure you put on k^n earlier gives it a k-vector space structure), which are actually the prototypical example of finite-dimensional (whatever that means) vector spaces, but have the unfortunate consequence of blurring the line between "top" and "bottom". When thinking about vector spaces, you should put yourself in the happy place of abelian groups, and then give yourself a baseball bat in the form of a field k with which you can kick around elements of your abelian group. If this sounds like a good time, good.

Here is an idea.

Exercise. Giving an abelian group M a k-vector space structure, where k is a field, is equivalent to giving a ring homomorphism $k \to \mathrm{End}(M)$, where $\mathrm{End}(M)$ denotes the *endomorphism*

ring of M, whose elements are group homomorphisms $M \to M$, with operations $+$ (inherited from M) and $\circ$ (function composition).

You should try (and if necessary, fail!) to prove this on your own time; I'm happy to help. At least it is good experience with rings. What it says is the following:

A vector space V is an abelian group that gets kicked around by a field k. $(*)$

This is really the third time we're stating this fact, and it's ok to do so, because it's important.

4. "Linear" algebra

What do we mean by "linear algebra"? Or, posed another way, what do we talk about when we talk about linear algebra? The short answer is that we talk about vector spaces, but that is often not dirty enough for the real life nuts-and-bolts of things. What you might have in mind, namely vectors (arrows?), matrices, and systems linear equations, are really the things you'll be working with. How do they come up?

Exercise. Give a(n additive) group isomorphisms between k^{n^2} and the set of $n \times n$ matrices with entries in k, with entry-wise addition as a group operation. Note that there is a big choice needed in writing such an isomorphism down!

Excellent. We have at least now exhibited matrices – real life objects! – as vector spaces. But let's go further. Suppose we have the simultaneous equations

$$ax + by = c$$
$$dx + ey = f$$
$$gx + hy = \ell,$$

where all letters lie in some field k. Attempt the following exercise if and only if you don't know what you're doing.

Exercise (Hard). Think up a way to multiply a matrix by a vector (an $(n \times 1)$-dimensional matrix) that makes sense. Write down the above system as a matrix multiplied by a vector.

If you honestly attempt this exercise and fail, I will gladly help you with it. This is the origin of the word "linear" in linear algebra: we are concerned with the common solutions of *linear*, that is, order 1, polynomials with coefficients in a field[2]. This is not easy, but the field structure, as noted above, gives us many tools to help. We have the following parting fact of life, which may be the most important:

The abstract notions of vector spaces and fields are used in linear algebra to *solve problems*, but only problems that can be written as the attempt to find common solutions to systems of linear polynomials with entries in a field. $(*)$

END.

[2]You might ask what changes when we no longer insist that the polynomials are linear. The field concerned with these questions is algebraic geometry, and it is very hard. Give it a Google.