Lecture 3:
Fields
Vector spaces

Warmup: Last time, we thought about $\mathbb{R}^n$ as a set of vectors, written either as lists/n-tuples or as column vectors. We defined addition and scaling of vectors, and explored their meaning a little *geometrically*. Today our job is going to be a bit of *algebraic* abstraction on $\mathbb{R}^n$—isolating the properties of $\mathbb{R}^n$ that we care about as algebraists, so that we can think more generally about their consequences and behavior.

Some language:
A binary operation on a set X is a function that takes in a pair (x, y) in $X \times X$ and returns a single element of X (**bi**nary because a pair has **two** things).

[Ex: $+$ is a binary op. on $\mathbb{R}$]

An action of a set A on a set X is a function that takes in a pair (a, x) in $A \times X$ and returns a single element of X. [Ex: scaling is an action of $\mathbb{R}$ on $\mathbb{R}^n$.]

Brainstorm:

1. Besides addition on $\mathbb{R}$ and $\mathbb{R}^n$, what other sets and binary operations have you seen? What sets have multiple familiar binary operations?
2. Besides $\mathbb{R}$ acting on $\mathbb{R}^n$, what other examples of actions have you seen?
3. For the binary operations, what are some properties you've come to care about? What are some examples and non-examples? [e.g. the commutative property]
4. Are there any circumstances where a function can be a binary operation *and* an action?

Fields

A "field" is essentially a number system that is most like $\mathbb{R}$ and $\mathbb{C}$ in an algebraic sense: you can add, subtract, multiply, and divide (except by 0).

Namely, for a set F, we define the binary operations

$$+: \; F \times F \to F, \quad (\alpha, \beta) \mapsto \alpha + \beta, \qquad \times: \; F \times F \to F, \quad (\alpha, \beta) \mapsto \alpha\beta.$$

We require that both are associative, and commutative, and that multiplication distributes across addition. We also assume that the are identity elements 0 and 1 such that

$$a + 0 = a \quad \text{and} \quad a1 = a \quad \text{for all } a \in F,$$

and that addition and multiplications are (mostly) invertible: for all $a \in F$ there exist $-a$ and a^{-1} (unless $a = 0$) such that

$$a + (-a) = 0 \quad \text{and} \quad a(a^{-1}) = 1$$

i.e. subtraction and division (by non-zero elements) are well-defined. The result is called a field. [See *Topic: Fields* at the end of Ch. Two.]

Examples: Non-examples:

Finite fields

The field $\mathbb{F}_2$ is the set $\{0, 1\}$ with multiplication as usual, but with $1 + 1 := 0$.

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

On your own: verify the field axioms.

Next semester: For any prime $p \geqslant 2$, the set $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ is a field, where addition and multiplication are defined modulo p (divide by p and report the remainder).

Vector spaces

Now we abstract $\mathbb{R}^n$...

Let F be a field. A vector space (over F) is a set V with a binary operation

$$+ : V \times V \to V \qquad \text{(vector addition)}$$

and an action

$$\cdot : F \times V \to V \qquad \text{(scalar multiplication/scaling)}$$

that satisfy the following:

addition

- commutative
- associative
- has an identity element $\mathbf{0}$: $\mathbf{0} + \mathbf{v} = \mathbf{v} = \mathbf{v} + \mathbf{0}$ for all $\mathbf{v} \in V$
- invertible: for all $\mathbf{v} \in V$ there exists $-\mathbf{v} \in \mathbb{V}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$

scaling

- associative: $a \cdot (b \cdot \mathbf{v}) = (ab) \cdot \mathbf{v}$ for all $a, b \in F$ and $\mathbf{v} \in V$
- $1 \in \mathbb{F}$ acts nicely: $1 \cdot \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$
- distributes across scalar and vector addition: for all $a, b \in F$ and $\mathbf{u}, \mathbf{v} \in V$, $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$ and $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$

It can be *very* helpful to think of these axioms as *preserving structure*.

Examples of vector spaces

Let F be a field. (Think: $F = \mathbb{R}$.)

Ex. Let

$$F^n = \left\{ \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \;\middle|\; u_i \in F \text{ for } i = 1, \dots, n \right\}.$$

Then F^n is a vector space over F with

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix} \quad \text{and} \quad a \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} au_1 \\ \vdots \\ au_n \end{pmatrix}.$$

Note: The case where $n = 1$ says that $F^1 \cong F$ is also a vector space ($\mathbb{R}$ is a vector space). What about F^0?

Ex. Polynomials $F[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in F\}$ with regular polynomial addition and scaling. "F adjoin x"

Ex. F-valued functions $V = \{f \mid f : F \to F\}$ where addition and scaling are defined *point-wise*: for all $f, g \in V$ and $a, x \in F$,

$$(f + g)(x) := f(x) + g(x) \quad \text{and} \quad (a \cdot f)(x) := a \cdot (f(x)).$$

Examples of vector spaces

Let F be a field. (Think: $F = \mathbb{R}$.)

Ex. **Matrices**!

Let $M_{m,n}(F) = \{m \times n$ matrices with coefficients in F $\}$. Define addition and scaling coordinate-wise:

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} + \begin{pmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,n} \end{pmatrix}$$

$$= \begin{pmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix}, \quad \text{and}$$

$$c \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} = \begin{pmatrix} ca_{1,1} & \cdots & ca_{1,n} \\ \vdots & \ddots & \vdots \\ ca_{m,1} & \cdots & ca_{m,n} \end{pmatrix}.$$

You try:

1. For each of the four examples of vector spaces V we just explored, what is the additive identity element in V?
2. Pick one of the four example, and briefly try to convince yourself it *is actually a vector space*. Namely, walk through the axioms and try to check that they hold for the example.
3. Consider
$$V = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \middle| \ x, y, z \in \mathbb{R}, x + y + z = 0 \right\}$$
as a subset of $\mathbb{R}^3$. **Claim:** V is a vector space.
   (a) Check that V is closed under the vector addition and scaling by $\mathbb{R}$ coming from $\mathbb{R}^3$ (meaning that if $\mathbf{u}, \mathbf{v} \in V$ and $c \in \mathbb{R}$, then $\mathbf{u} + \mathbf{v} \in V$ and $c\mathbf{u} \in V$.
   (b) Check $V \neq \varnothing$.
   (c) Check that for all $\mathbf{v} \in V$, we have $0 \cdot \mathbf{v} = \mathbf{0}$, so that $\mathbf{0} \in V$ by part (a).
   (d) Check that for all $\mathbf{v} \in V$, we have $(-1) \cdot \mathbf{v}$ is the additive inverse of $\mathbb{V}$, so that $-\mathbf{v} = (-1) \cdot \mathbf{v} \in V$ by part (a).
   [*Careful!* A priori, $(-1) \cdot \mathbf{v}$ means "scale $\mathbf{v}$ by scalar $-1 \in \mathbb{R}$" and $-\mathbf{v}$ means "the thing that adds to $\mathbf{v}$ to get $\mathbf{0}$"; you're checking that these do, indeed, mean the same thing here.]
   (e) Convince yourself that the rest of the axioms of vector spaces now come for free, inherited from $\mathbb{R}^3$ being a vector space.

Epilog: Some tips for translating between lecture and the book.

- The book only works over $F = \mathbb{R}$ for now, but everything in Two.I can be done over any field as we have done.
- The book uses notation $\vec{v}$ to mean a vector in F^n; we've been using $\mathbf{v}$. LaTeX: `\mathbf{v}`, or `\vv` if you use my preamble shortcuts.
- $\mathcal{P}_n = \{f \in \mathbb{R}[x] \mid \deg(f) \leqslant n\} = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{R}\}$ is the set of polynomials of degree $\leqslant n$.

  More general: $\mathcal{P}_n(F) = \{f \in F[x] \mid \deg(f) \leqslant n\}$.
- The book uses $\mathcal{M}_{m \times n}$ to mean $M_{m,n}(\mathbb{R})$, and sometimes calls it "the space $m \times n$".
- As we used in the exercise above, "closure" is about addition and scaling being well-defined functions. Namely, a function $f : A \to B$ is well-defined if it satisfies both
  1. the image of f really is in B: for all $a \in A$, we have $f(a) = b$; and
  2. each element $a \in A$ has *exactly one* image in B: $f(a) = b$ and $f(a) = b'$ implies $b = b'$.

  Now, we say V is closed under addition if $\mathbf{u} + \mathbf{v} \in V$ for all $\mathbf{u}, \mathbf{v} \in V$. But *we* embedded this in the fact that $+ : V \times V \to V$ is a *function* (otherwise it would not have satisfied the first criterion of well-defined).
- We will see next time that if V is a vector space and $U \subseteq V$ is also a vector space under the same operations (like in problem 3 above), U is called a subspace of V.