MATH 33A – SPRING 2022

Pablo S. Ocal

1. Fields and vector spaces

For the non-mathematician, linear algebra is the study of <u>linear equations</u> and <u>linear transformations</u>. For us, linear algebra will be the study of <u>linear maps</u> between <u>vector spaces</u>. We should think of vector spaces as abstract objects with special structure that behaves nicely with respect to <u>scalars</u>, and linear maps are functions that preserve this special structure.

<u>Definition</u>: A <u>field</u> $\mathbb{F}$ is a set with two operations

$$+ : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} \qquad \text{and} \qquad \cdot : \mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F}$$
$$(a,b) \longmapsto a+b \qquad\qquad\qquad (a,b) \longmapsto a \cdot b$$

called sum and product respectively, such that for all $a,b,c \in \mathbb{F}$ we have:

(1) Commutativity: $a+b = b+a$ and $a \cdot b = b \cdot a$.

(2) Associativity: $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(3) Identity: there exist $0, 1 \in \mathbb{F}$ with $a+0 = a$ and $a \cdot 1 = a$.

(4) Inverses: when $a \neq 0$ there exist $-a, a^{-1} \in \mathbb{F}$ with $a+(-a) = 0$ and $a a^{-1} = 1$.

(5) Distributivity: $a \cdot (b+c) = a \cdot b + a \cdot c$.

The elements of a field are called <u>scalars</u>.

Example:

1. Some number sets are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

2. Some number sets are not fields: $\mathbb{N}$, $\mathbb{Z}$. (why?)

3. There are weird fields:

$$\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$$

$\mathbb{Z}_2 = \{[0], [1]\}$ is the field of integers mod 2, having:

$$0+1=1, \quad 0+0=0, \quad 1+1=0, \quad 0\cdot 1=0, \quad 1\cdot 1=1.$$

We can think of $\mathbb{Z}_2$ as $\mathbb{Z}$ where we have declared that all even numbers are the same, and also that all odd numbers are the same:

$$2k \equiv 0 \quad \text{and} \quad 2k+1 \equiv 0 \quad \text{for all } k \in \mathbb{Z}.$$

$\mathbb{Z}_p = \{[0], [1], \dots, [p-1]\}$ for $p \in \mathbb{N}$ prime is the field of integers mod p.

We can think of $\mathbb{Z}_p$ as $\mathbb{Z}$ where we declare that two numbers are equal if and only if they have the same remainder when divided by p:

$$p\cdot k + j \equiv j \quad \text{for all } 0 \leq j < p \text{ and all } k \in \mathbb{Z}, \text{ so}$$

$$[j] = \{\text{integers with remainder } j \text{ upon division by } p\}.$$

Definition: A <u>vector space</u> V over a field $\mathbb{F}$ is a set with two operations:

$$+ : V \times V \longrightarrow V \qquad \text{and} \qquad \cdot : \mathbb{F} \times V \longrightarrow V$$
$$(x,y) \longmapsto x+y \qquad\qquad (a,x) \longmapsto a\cdot x$$

called addition and scalar multiplication respectively, such that for all $x, y, z \in V$ and $a, b \in \mathbb{F}$:

(1) Commutativity of addition: $x+y = y+x$.

(2) Associativity of addition: $(x+y)+z = x+(y+z)$.

(3) Identity in V: there exists $\vec{0} \in V$ with $x + \vec{0} = \vec{0}$.

(4) Inverses in V: there exists $-x \in V$ with $x+(-x) = \vec{0}$.

(5) Scalar identity: $1 \cdot x = x$. (do we have multiplicative inverses x^{-1} in V?)

(6) Associativity of scalar multiplication: $a\cdot(b\cdot x) = (a\cdot b)\cdot x$.

(7) Distributivity of scalar multiplication over addition: $a\cdot(x+y) = a\cdot x + a\cdot y$.

(8) Distributivity of the sum over scalar multiplication: $(a+b)\cdot x = a\cdot x + b\cdot x$.

These properties are saying that the addition and multiplication by scalars in V behave well with respect to the sum and product in $\mathbb{F}$.

<u>Remark:</u> Alternatively, we could say that a vector space is a commutative group under addition with associative and distributive scalar multiplication.

In particular, vector spaces are <u>closed</u> under finite sums and scalar multiplication: if $x_1, \dots, x_n \in V$ and $a_1, \dots, a_n \in \mathbb{F}$, then $a_1 x_1 + \cdots + a_n x_n \in V$.

When $\mathbb{F} = \mathbb{R}$, we say that V is a <u>real vector space</u>. When $\mathbb{F} = \mathbb{C}$ we say that V is a <u>complex vector space</u>.

<u>Examples:</u>

1. $\mathbb{R}^n = \overbrace{\mathbb{R} \times \cdots \times \mathbb{R}}^{n}$ is called the <u>real n-space</u>.

   The elements in $\mathbb{R}^n$ are n-tuples $(r_1, \dots, r_n)$ with $r_1, \dots, r_n \in \mathbb{R}$.

   The vector addition is done componentwise:

   $$(r_1, \dots, r_n) + (s_1, \dots, s_n) = (r_1 + s_1, \dots, r_n + s_n)$$

   The scalar multiplication is done componentwise:

   $$a \cdot (r_1, \dots, r_n) = (a \cdot r_1, \dots, a \cdot r_n)$$

   <u>Remark:</u> Here we could replace the field $\mathbb{R}$ by $\mathbb{Q}$, and everything would still make sense. It is important to specify over which field we are working.

   In fact, if we replace $\mathbb{R}$ by $\mathbb{Z}$, things still make sense. When we work over a ring instead of a field, we generalize vector spaces to the notion of modules.

2. Let $\mathbb{F}$ be a field, let S be a set, let V be the set of functions from S to $\mathbb{F}$.

   Namely elements $f \in V$ are functions of sets $f: S \longrightarrow \mathbb{F}$.

   The scalar multiplication $a \cdot f$ is the function satisfying $(a \cdot f)(x) = a \cdot f(x)$.

$$a\cdot f : S \longrightarrow \mathbb{F}$$
$$x \longmapsto a\cdot f(x)$$

The addition $f+g$ is the function satisfying $(f+g)(x) = f(x) + g(x)$.

Many important examples arise in this way.

2.1. Let V be the set of continuous functions over $\mathbb{R}$ or over $\mathbb{C}$, denoted $\mathcal{C}(\mathbb{R})$ or $\mathcal{C}(\mathbb{C})$.

2.2. Let V be the set of polynomials with coefficients in $\mathbb{F}$, denoted $\mathbb{F}[x]$. Recall that $p(x) \in \mathbb{F}[x]$ has the form $p(x) = a_n x^n + \cdots + a_1 x + a_0$ for $a_n, \ldots, a_0 \in \mathbb{F}$.

2.3. Let V be the set of symmetric polynomials in n-variables, denoted $\mathrm{Sym}_n(\mathbb{F})$.

The elements are polynomials in the variables $x_1, \ldots, x_n$ such that:

$$p(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = p(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n) \quad \text{for all } i,j \in \{1, \ldots, n\}.$$

That is, exchanging two variables does not change the polynomial.

Fix $n=3$, then:

$p(x_1, x_2, x_3) = x_1 + x_2 + x_3$ is symmetric,

$q(x_1, x_2, x_3) = x_1 + x_2$ is not symmetric since $q(x_1, x_3, x_2) = x_1 + x_3 \neq q(x_1, x_2, x_3)$.

$r(x_1, x_2, x_3) = x_1x_2 + 2x_1x_3 + x_2x_3$ is not symmetric,

$s(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ is symmetric.

3. Let $\mathbb{F}$ be a field, let V be the set of $n \times m$ matrices with entries in $\mathbb{F}$, denoted $M_{n\times m}(\mathbb{F})$. The matrix addition and scalar multiplication are both defined componentwise.

$$\begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & \cdots & a_{1m}+b_{1m} \\ \vdots & & \vdots \\ a_{n1}+b_{n1} & \cdots & a_{nm}+b_{nm} \end{bmatrix}$$

$$a \cdot \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} = \begin{bmatrix} a\cdot a_{11} & \cdots & a\cdot a_{1m} \\ \vdots & & \vdots \\ a\cdot a_{n1} & \cdots & a\cdot a_{nm} \end{bmatrix}$$

The zero vector is the zero matrix.

$$\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}$$

In general, $M_{n\times m}(\mathbb{F})$ is not a field since we cannot multiply two $n\times m$ matrices.

4. Let V be the field of rational functions over $\mathbb{F}$, denoted $\mathbb{F}(x)$. Elements in $\mathbb{F}(x)$ are fractions of polynomials, namely $\frac{p(x)}{q(x)}$ with $p(x), q(x) \in \mathbb{F}[x]$. Now $\mathbb{F}[x]$ is a vector space over $\mathbb{F}$, and $\mathbb{F}[x]$ is also a field on its own.

The vector addition is:

$$p(x) \quad + \quad r(x) \quad = \quad p(x)\,s(x) + q(x)\,r(x)$$

$$\frac{\quad}{q(x)} + \frac{\quad}{s(x)} = \frac{\quad}{q(x)\,s(x)}.$$

The scalar multiplication is:

$$a \cdot \frac{p(x)}{q(x)} = \frac{a \cdot p(x)}{q(x)}.$$

With these two operations, $\mathbb{F}(x)$ is a vector space over $\mathbb{F}$. Consider the sum:

$$\frac{p(x)}{q(x)} + \frac{r(x)}{s(x)} = \frac{p(x)\,s(x) + q(x)\,r(x)}{q(x)\,s(x)}$$

and the product:

$$\frac{p(x)}{q(x)} \cdot \frac{r(x)}{s(x)} = \frac{p(x)\,r(x)}{q(x)\,s(x)}.$$

With these two operations, $\mathbb{F}(x)$ is a field. The identities of $\mathbb{F}(x)$ are:

$z(x) = 0$ the zero, and $\varepsilon(x) = 1$ the one.

Note that $\mathbb{F}(x)$ is closed since the sum and product give rational functions.

In fact, $\mathbb{F}(x)$ is also a vector space over $\mathbb{F}(x)$. The difference is that here the scalars have changed from $\mathbb{F}$ to $\mathbb{F}(x)$.