MATH 115A - SPRING 2022

Pablo S. Ocal

1. Fields and vector spaces

For the non-mathematician, linear algebra is the study of linear equations and linear transformations. For us, linear algebra will be the study of linear maps between vector spaces.

We should think of vector spaces as abstract objects with special structure that behaves nicely with respect to scalars, and linear maps are functions that preserve this special structure.

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

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

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 scalars.

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:

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

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:

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

$\mathbb{Z}_p = \{[0], [1], \cdots, [p-1]\}$ 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:

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

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

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

$+ : V \times V \longrightarrow V$ and $\cdot : \mathbb{F} \times V \longrightarrow V$

$(x,y) \longmapsto x+y$ $\quad$ $(a,x) \longmapsto a \cdot x$

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 $\mathbb{F}$.

Remark: 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 closed 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 real vector space. When $\mathbb{F} = \mathbb{C}$ we say that V is a complex vector space.

Examples:

1. $\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n}$ is called the real n-space.

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

   The vector addition is done componentwise:

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

   The scalar multiplication is done componentwise:

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

   Remark: 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 $f : S \to \mathbb{F}$.

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

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

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

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 $q(x_1, x_3, x_2) = x_1 + x_3 \neq q(x_1, x_2, x_3)$.

$r(x_1, x_2, x_3) = x_1 x_2 + 2x_1 x_3 + x_2 x_3$ 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:

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

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

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 $e(x) = 1$ 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 $\mathbb{F}(x)$.

* Small aside on proof techniques:

We will mainly be using four techniques:

1. Induction: this is useful when proving something for all natural numbers.

Example: Prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

This is true for $n=1$ since $1 = \frac{1\cdot(1+1)}{2}$.

Suppose this is true for n. We now prove it for n:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n\cdot(n+1)}{2} + (n+1) = \frac{n\cdot(n+1)+2\cdot(n+1)}{2} =$$

$$= \frac{(n+1)\cdot(n+2)}{2} = \frac{(n+1)\cdot((n+1)+1)}{2}. \qquad \square.$$

2. Using the definition: this is useful when we do not know much.

Example: Prove that $\mathbb{Z}_2$ is a field. We only have to check that all the axioms hold true.

3. Using theorems and other results: this is useful when we know a lot.

Example: Prove that every $p(x) \in \mathbb{C}[x]$ factors into linear terms.

Let n be the degree of $p(x)$. If $n = 0, 1$ we are done. If $n \neq 0, 1$, by the Fundamental Theorem of Algebra $p(x)$ has one root $a_1 \in \mathbb{C}$. Then $x - a_1$ divides $p(x)$ so $p(x) = (x-a_1)\cdot q(x)$ with $q(x)$ of degree $n-1$. If $n-1 = 1$ then $q(x) = x - a_2$ so $p(x) = (x-a_1)(x-a_2)$ and we are done. If $n-1 \neq 1$, apply the Fundamental Theorem of Algebra again. Since at every step we are lowering the degree by 1, we will repeat this exactly n times, so we will have $p(x) = (x-a_1)\cdots(x-a_n)$. Thus $p(x)$ factors

into linear terms, as desired. □.

4. Follow your nose: when we are given several hypothesis and we are asked to verify that a statement holds, often we have to "put all the hypothesis in a box, shake it up a bit, and our desired conclusion will fall out."

Example: Prove that $\sqrt{2}$ is not a rational number.

Suppose that $\sqrt{2}$ is rational. We could then write $\sqrt{2} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$.

Then squaring this we obtain $2 = \frac{a^2}{b^2}$ so $2b^2 = a^2$. Thus a^2 is even.

Since even times even is even, and odd times odd is odd, a is even.

Hence there exists $k \in \mathbb{Z}$ with $a = 2k$, so $2b^2 = (2k)^2 = 4k^2$. This means that $b^2 = 2k^2$, so as before b is even. All in all, we proved that if $\sqrt{2} = \frac{a}{b}$ then a and b are both even. However, rational numbers can be written in an irreducible way, that is, if $\sqrt{2} \in \mathbb{Q}$ then there are $p, q \in \mathbb{Z}$ such that p and q do not share any divisors and $\sqrt{2} = \frac{p}{q}$. This is a contradiction with what we just proved: p and q both should be divisible by 2. Thus $\sqrt{2} \notin \mathbb{Q}$. □.

End of the aside. *

We now prove some properties of vector spaces.

Theorem 1: Let V be a vector space. If $x, y, z \in V$ and $x+z = y+z$ then $x = y$.

Proof: Since $z \in V$, by axiom 4 there is $-z \in V$ with $z + (-z) = 0$. Hence:

$$x+z = y+z \Rightarrow (x+z)+(-z) = (y+z)+(-z)$$

Associativity (2) $\Rightarrow$ $x+(z+(-z)) = y+(z+(-z))$

Inverses (4) $\Rightarrow$ $x+0 = y+0$

Identity (3) $\Rightarrow$ $x = y$. $\square$.

Corollary 2: Let V be a vector space. The vector $\vec{0} \in V$ is unique.

Proof: Suppose that there is a vector $\vec{0}' \in V$ such that $z + \vec{0}' = z$ for all $z \in V$.

Now $z + \vec{0} = z = z + \vec{0}'$ so by Theorem 1 we have $\vec{0} = \vec{0}'$. Every vector in V that satisfies axiom 3 is equal to $\vec{0}$, so $\vec{0}$ is unique. $\square$.

Corollary 3: Let V be a vector space, fix $x \in V$. Then $-x \in V$ is unique.

Proof: Analogous to the above.

Given a mathematical object with structure, we always look at how that structure reappears in mathematical objects inside the original one. For sets, these are subsets. For

vector spaces, we look at vector subspaces.

Definition: Let V be a vector space over $\mathbb{F}$. A vector subspace W of V is a subset of V that is also a vector space with the addition and multiplication by scalars inherited from V.

Example:

1. Over $\mathbb{Q}$ we have $\mathbb{Q}^n \subsetneq \mathbb{R}^n \subsetneq \mathbb{C}^n$ are all subspaces of $\mathbb{C}^n$.
2. Over $\mathbb{Q}$ we have $\mathbb{Q}[x] \subsetneq \mathbb{R}[x] \subsetneq \mathbb{C}[x]$ are all subspaces of $\mathbb{C}[x]$.
3. Over $\mathbb{Q}$ we have $M_{n\times m}(\mathbb{Q}) \subsetneq M_{n\times m}(\mathbb{R}) \subsetneq M_{n\times m}(\mathbb{C})$ are all subspaces of $M_{n\times m}(\mathbb{C})$.
4. The symmetric polynomials in n variables $\mathrm{Sym}_n(\mathbb{F})$ are a subspace of the vector space of all the polynomials in n variables $\mathbb{F}[x_1, \cdots, x_n]$.

Theorem 4: Let V be a vector space. A subset W of V is a subspace of V if and only if all the following hold:

(1) $\vec{0} \in W$.

(2) $x+y \in W$ for all $x, y \in W$.

(3) $a \cdot x \in W$ for all $a \in \mathbb{F}$.

Proof: ($\Rightarrow$) Suppose that W is a subspace of V. We want to show that (1), (2), (3) hold. Since W is a vector space, there is $\vec{0}' \in W$ such that $w + \vec{0}' = w$ for all $w \in W$. Since W is a subset of V then $w \in V$ so $w + \vec{0} = w$. Now by Theorem 1 we have $\vec{0}' = \vec{0}$, so (1) holds. Since W is a vector space, (2) and (3) hold by definition.

($\Leftarrow$) Suppose that (1), (2), (3) hold. We have to verify that the following hold.

1. Commutativity of addition: it already is, $+$ is well defined by (2).

2. Associativity of addition: it already is.

3. Identity in W: $\vec{0} \in W$ by (1).

4. Inverses in W: let $w \in W$, now $(-1) \cdot w \in W$ by (3), and $-w = (-1) \cdot w$.
   why? Prove it!

5. Scalar identity: let $w \in W$, since $w \in V$ then $1 \cdot w = w$, and by (3) we have $1 \cdot w \in W$, so $1 \cdot w = w$ is an equality in W.

6. Associativity of scalar multiplication: it already is.

7. Distributivity of scalar multiplication over addition: it already is.

8. Distributivity of the sum over scalar multiplication: it already is. $\square$.

This emphasizes that W needs to be a subset of V that is closed under the same addition

and multiplication by scalars as V.

A particularly important vector space is $M_{n\times m}(\mathbb{F})$. We now recall some definitions:

1. Column vectors: $\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{F}^n$ with $a_1, \dots, a_n \in \mathbb{F}$.

2. Row vectors: $(a_1, \dots, a_n) \in \mathbb{F}^n$ with $a_1, \dots, a_n \in \mathbb{F}$.

3. Square matrices: $M_{n\times n}(\mathbb{F})$, also denoted $M_n(\mathbb{F})$.

4. Diagonal matrices: $\begin{bmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{bmatrix} \in M_{n\times n}(\mathbb{F})$ with $a_{ij}=0$ for $i\neq j$.

5. Upper triangular matrices: $\begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & & a_{nn} \end{bmatrix} \in M_{n\times n}(\mathbb{F})$ with $a_{ij}=0$ for $i>j$.

   Similarly, we have lower triangular matrices.

5.1. Strictly upper triangular matrices: we instead require $a_{ij}=0$ for $i\geq j$, so the diagonal entries are also zero.

   Similarly, we have strictly lower triangular matrices.

6. Zero matrix: $\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \in M_{n\times m}(\mathbb{F})$ with $a_{ij}=0$ for all i,j.

7. Identity matrix: $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in M_{n\times n}(\mathbb{F})$ the diagonal matrix with $a_{ii}=1$ for all i, and $a_{ij}=0$ for $i\neq j$.

8. Transpose of a matrix: Let $M = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \end{bmatrix} \in M_{n\times m}(\mathbb{F})$, its transpose is

8. Transpose of a matrix: let $M = \begin{bmatrix} \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \in M_{mxn}(\mathbb{F})$ its <u>transpose</u> is $M^t = \begin{bmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{mn} \end{bmatrix} \in M_{nxm}(\mathbb{F})$ the matrix with a_{ji} in the i-th row and j-th column.

9. Trace of a matrix: let $M = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \in M_{nxn}(\mathbb{F})$ its <u>trace</u> is:

$$tr(M) = \sum_{i=1}^{n} a_{ii}, \quad \text{the sum of the diagonal entries.}$$

<u>Examples:</u>

1. Symmetric matrices are a subspace of square matrices.

Recall that a matrix is symmetric when it is equal to its transpose.

<u>Proof:</u> We show that $\{A \in M_n(\mathbb{F}) \mid A^t = A\}$ is a subspace of $M_n(\mathbb{F})$.

(1) $0 = 0^t$ so 0 is symmetric.

(2) If A, B are symmetric then:

$$(A+B)^t = A^t + B^t = A + B \quad \text{so } A+B \text{ is symmetric.}$$

(3) If A is symmetric and $c \in \mathbb{F}$ then:

$$(cA)^t = c(A^t) = cA \quad \text{so } cA \text{ is symmetric.} \qquad \square.$$

2. Diagonal matrices are a subspace of square matrices.

3. Upper triangular matrices are a subspace of square matrices.

4. The set of the zero matrix $\{0\}$ is a subspace of $M_{n\times m}(\mathbb{F})$. We call it the zero subspace, or the trivial subspace, of $M_{n\times m}(\mathbb{F})$.

5. The set of traceless matrices, namely matrices whose trace is zero, is a subspace of square matrices.