MAST10007 Linear Algebra

THE UNIVERSITY OF MELBOURNE
SCHOOL OF MATHEMATICS AND STATISTICS

Summer Term, 2026

Arun Ram: Additional Slides

These slides have been made by Arun Ram, in preparation for teaching of the summer session of MAST10007 Linear Algebra at University of Melbourne in 2026. The template is from the University of Melbourne School of Mathematics and Statistics slide deck which was produced by members of the School including, in particular, huge developments by Craig Hodgson and Christine Mangelsdorf.

Lecture 12: Vector spaces and linear transformations

A field is a number system $\mathbb{F}$ that is similar to $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (the precise definition is given on slide 139-140).

The number systems $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields. There are some 'more exotic' fields like *finite fields*. For example, if p is a prime number then the p-clock number system $\mathbb{F}_p$ is a finite field.

The world of $\mathbb{F}$-vector spaces works for any field $\mathbb{F}$. But, the properties *depend* on $\mathbb{F}$. For example, with dimension of a vector space

The $\mathbb{R}$-dimension of $\mathbb{R}^3$ is 3.

The $\mathbb{C}$-dimension of $\mathbb{C}^3$ is 3.

The $\mathbb{R}$-dimension of $\mathbb{C}^3$ is 6.

The $\mathbb{Q}$-dimension of $\mathbb{R}^3$ is ∞.

We often write 'Let $\mathbb{F}$ be a field'. You are encouraged to think of $\mathbb{F}$ as $\mathbb{R}$ or $\mathbb{Q}$ (or whatever your favourite field is).

Later we may explore some cool applications of vector spaces that use finite fields (codes, fast Fourier transform, etc.).

Definition ($\mathbb{F}$-vector space)

Let $\mathbb{F}$ be a field. A *$\mathbb{F}$-vector space*, or *$\mathbb{F}$-module*, is a set V with functions

$$\begin{array}{ccc} V \times V & \to & V \\ (v_1, v_2) & \mapsto & v_1 + v_2 \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{F} \times V & \to & V \\ (c, v) & \mapsto & cv \end{array}$$

(*addition* and *scalar multiplication*) such that

(a) If $v_1, v_2, v_3 \in V$ then $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$,

(b) There exists $0 \in V$ such that if $v \in V$ then $0 + v = v$.

(c) If $v \in V$ then there exists $-v \in V$ such that $v + (-v) = 0$.

(d) If $v_1, v_2 \in V$ then $v_1 + v_2 = v_2 + v_1$,

(e) If $c \in \mathbb{F}$ and $v_1, v_2 \in V$ then $c(v_1 + v_2) = cv_1 + cv_2$,

(f) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then $(c_1 + c_2)v = c_1 v + c_2 v$,

(g) If $c_1, c_2 \in \mathbb{F}$ and $v \in V$ then $c_1(c_2 v) = (c_1 c_2)v$,

(h) If $v \in V$ then $1v = v$.

Linear transformations are for comparing vector spaces.

Definition

Let $\mathbb{F}$ be a field and let V and W be $\mathbb{F}$-vector spaces. An *$\mathbb{F}$-linear transformation from V to W* is a function $f : V \to W$ such that

(a) If $v_1, v_2 \in V$ then $f(v_1 + v_2) = f(v_1) + f(v_2)$,

(b) If $c \in \mathbb{F}$ and $v \in V$ then $f(cv) = cf(v)$.

One vector space can be a subspace of another.

Definition (Subspace)

Let V be an $\mathbb{F}$-vector space. A *subspace of W* is a subset $W \subseteq V$ such that

(a) $0 \in W$,

(b) If $w_1, w_2 \in W$ then $w_1 + w_2 \in W$,

(c) If $w \in W$ and $c \in \mathbb{F}$ then $cw \in W$.

Definition (Basis and dimension)

Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space.
Let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be a subset of V.
An *$\mathbb{F}$-linear combination* of $\mathbf{v}_1, \ldots, \mathbf{v}_k$ is an element of the set

$$\mathbb{F}\text{-span}\{\mathbf{v}_1, \ldots, \mathbf{v}_k\} = \{c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k \mid c_1, c_2, \ldots, c_k \in \mathbb{F}\}.$$

The set $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is *linearly independent over $\mathbb{F}$* if it satisfies:

$$\text{if } c_1, \ldots, c_k \in \mathbb{F} \text{ and } c_1\mathbf{v}_1 + \cdots + c_k\mathbf{v}_k = 0$$

$$\text{then } c_1 = 0,\ c_2 = 0,\ \ldots,\ c_k = 0.$$

An *$\mathbb{F}$-basis* of V is a subset $B \subseteq V$ such that

(a) $\mathbb{F}\text{-span}(B) = V$,

(b) B is linearly independent.

The *$\mathbb{F}$-dimension* of V is the number of elements of a $\mathbb{F}$-basis B of V.

Favourite vector spaces and favourite bases

1. $\mathbb{R}^n = \{|a_1, a_2, \ldots, a_n\rangle \mid a_1, a_2, \ldots, a_n \in \mathbb{R}\} = M_{n\times 1}(\mathbb{R})$ has basis

$$\{e_1, e_2, \ldots, e_n\}, \quad \text{where} \quad e_i = |0, \ldots, 0, 1, 0, \ldots, 0\rangle,$$

has 1 in the ith entry and 0 elsewhere.

2. $M_{m\times n}(\mathbb{R})$ has basis

$$\{E_{ij} \mid i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}\},$$

where E_{ij} is the matrix with 1 in the (i, j) entry and 0 elsewhere.

3. $\mathbb{R}[x]_{\leqslant n} = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_0, a_1, \ldots, a_n \in \mathbb{R}\}$

$$\text{has basis} \quad \{1, x, x^2, \ldots, x^n\}.$$

4. The vector space of polynomials with coefficients in $\mathbb{R}$ is

$\mathbb{R}[x] = \mathbb{R}\text{-span}\{1, x, x^2, x^3, \ldots\}$ which has basis $\{1, x, x^2, x^3, \ldots\}$.

Example V22. Let $v_1, v_2, v_3, v_4 \in \mathbb{R}^3$ be given by

$$v_1 = |1,2,3\rangle, \quad v_2 = |3,6,9\rangle, \quad v_3 = |-1,0,-2\rangle, \quad v_4 = |1,4,4\rangle.$$

(a) Is $\{v_1, v_2, v_3, v_4\}$ linearly independent?

(b) Express v_2 and v_4 as linear combinations of v_1 and v_3.

(c) Is $\{v_1, v_3\}$ linearly independent?

(a) Since $v_2 = 3v_1$ then $0 = 3v_1 - v_2 = 3v_1 - v_2 + 0v_3 + -v_4$.
So $c_1 = 3$, $c_2 = -1$, $c_3 = 0$, $c_4 = 0$ is a case that gives
$c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4 = 0$.
So $\{v_1, v_2, v_3, v_4\}$ is not linearly independent.

(b) Since $v_2 = 3v_1 + 0v_3$ then $v_2 \in \mathbb{R}$-span$\{v_1, v_3\}$.
Since $v_1 + v_3 = (0,2,1)$ and $v_1 + |0,2,1\rangle = |1,4,4\rangle$.
So $v_4 = 2v_1 + v_3$. So $v_4 \in \mathbb{R}$-span$\{v_1, v_3\}$.

(c) To show: If $c_1, c_2 \in \mathbb{R}$ and $c_1|1,2,3\rangle + c_2|-1,0,2\rangle = |0,0,0\rangle$ then $c_1 = 0$ and $c_2 = 0$.

Assume $c_1, c_2 \in \mathbb{R}$ and $c_1|1,2,3\rangle + c_2|-1,0,2\rangle = |0,0,0\rangle$.
Then

$$\begin{aligned} c_1 - c_2 &= 0, \\ 2c_1 + 0c_2 &= 0, \\ 3c_1 + 2c_2 &= 0. \end{aligned}$$

The first equation gives $c_1 = c_2$ and the second equation gives $2c_1 = 0$ so that $c_2 = c_1 = 0$. This system has

$$\text{only one solution:} \qquad c_1 = 0, \quad c_2 = 0.$$

So $\{v_1, v_3\}$ is linearly independent. □

A *subspace of* $\mathbb{R}^2$ is a subset $L \subseteq \mathbb{R}^2$ such that

(a) $0 \in L$,

(b) If $w_1, w_2 \in L$ then $w_1 + w_2 \in L$,

(c) If $w \in L$ and $c \in \mathbb{R}$ then $cw \in L$.

Example V7. Is the line $L = \{|x, y\rangle \in \mathbb{R}^2 \mid y = 2x + 1\}$ a subspace of $\mathbb{R}^2$?

Since $0 = |0, 0\rangle$ and $0 \neq 2 \cdot 0 + 1$ then $0 \notin L$.
So L is not a subspace of $\mathbb{R}^2$.

Example A8. Is the line $L = \{|x, y\rangle \in \mathbb{R}^2 \mid y = 2x\}$ a subspace of $\mathbb{R}^2$?
Since $|0, 0\rangle = |0, 2 \cdot 0\rangle$ then $|0, 0\rangle \in L$.
Assume $|a, 2a\rangle, |b, 2b\rangle \in L$. Then

$$|a, 2a\rangle + |b, 2b\rangle = |(a + b), 2(a + b)\rangle \in L.$$

Assume $|a, 2a\rangle \in L$ and $c \in \mathbb{R}$. Then

$$c \cdot |a, 2a\rangle = |(ca), 2(ca)\rangle \in L.$$

So L is a subspace of $\mathbb{R}^2$.

Definition (Field)

A *field* is a set $\mathbb{F}$ with functions

$$\begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & a+b \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & ab \end{array}$$

such that

(Fa) If $a, b, c \in \mathbb{F}$ then $(a+b)+c = a+(b+c)$,

(Fb) If $a, b \in \mathbb{F}$ then $a+b = b+a$,

(Fc) There exists $0 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 0+a = a \text{ and } a+0 = a,$$

(Fd) If $a \in \mathbb{F}$ then there exists $-a \in \mathbb{F}$ such that $a+(-a) = 0$ and $(-a)+a = 0$,

(Fe) If $a, b, c \in \mathbb{F}$ then $(ab)c = a(bc)$,

Definition (Field continued)

(Ff) If $a, b, c \in \mathbb{F}$ then

$$(a+b)c = ac + bc \qquad \text{and} \qquad c(a+b) = ca + cb,$$

(Fg) There exists $1 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 1 \cdot a = a \text{ and } a \cdot 1 = a,$$

(Fh) If $a \in \mathbb{F}$ and $a \neq 0$ then there exists $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$ and $a^{-1}a = 1$,

(Fi) If $a, b \in \mathbb{F}$ then $ab = ba$.