Linear Algebra

Adam Kelly (ak2316@cam.ac.uk)

October 11, 2021

This article constitutes my notes for the 'Linear Algebra' course, held in Michaelmas 2021 at Cambridge. These notes are *not a transcription of the lectures*, and differ significantly in quite a few areas. Still, all lectured material should be covered.

Contents

§1 Vector Spaces

§1.1 Vector Spaces and Subspaces

Linear algebra is, somewhat obviously, primarily about studying objects that are *linear* in nature. The objects we really care about are *vector spaces*, settings in which we can add elements and multiply by scalars. We are also going to consider *linear maps*, functions on vector spaces which preserve that linear structure – but more on that later.

Throughout the following discussion (and this course), $\mathbb{F}$ is going to denote an arbitrary field[1]

Definition 1.1 ($\mathbb{F}$-Vector Space)

An **$\mathbb{F}$-vector space** is an abelian group $(V, +)$ together with a function $\mathbb{F} \times V \to V$, written $(\lambda, v) \mapsto \lambda v$ such that the following axioms hold:

(i) *Distributivity in V.* $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$,

(ii) *Distributivity in $\mathbb{F}$.* $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$,

(iii) *Associativity.* $\lambda(\mu v) = (\lambda\mu)v$,

(iv) *Identity.* $1v = v$.

[1] A field $\mathbb{F}$ is a set $\mathbb{F}$ equipped with two operations $+$ ('addition') and $\cdot$ ('multiplication'). We require $\mathbb{F}$ with addition to form an abelian group, and multiplication must be associative and have an identity element 1. We also require every element except 0 to have an inverse with respect to multiplication, and multiplication must be distributive over addition.

Informally, you can think of a field as something you can do arithmetic in.

We usually call elements of V **vectors** and elements of $\mathbb{F}$ **scalars**. The identity element in V is usually called the zero vector, and is written 0_V (or just 0 if the context is clear).

If $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$, we use the terms 'real vector space' and 'complex vector space', since they're so common.

Example 1.2 (Examples of Vector Spaces)

(i) The set of triples

$$\{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

forms a real vector space called $\mathbb{R}^3$, because you can add any two triples component wise.

(ii) The set

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

is a $\mathbb{Q}$-vector space, where we add elements and scale by rational numbers in the obvious way.

(iii) The set $\mathcal{C}[0, 1]$ of all continuous functions $f : [0, 1] \to \mathbb{R}$ forms a real vector space.

As with many new objects, it's helpful to be able to discuss its substructure. In the case of a vector space V, there's a pretty natural notion for what it means for a subset $U \subseteq V$ to still act like a vector space.

Definition 1.3 (Subspace)

Let V be a $\mathbb{F}$-vector space. A subset $U \subseteq V$ is a **subspace** of V if U is also an $\mathbb{F}$-vector space. If U is a subspace of V, we will write $U \leq V$.

Example 1.4 (Examples of Subspaces)

(i) The set of vectors $\{(x, y, z) \mid x, y, z \in \mathbb{R}, x + y + z = 0\}$ is a subspace of $\mathbb{R}^3$.

(ii) The set of polynomials with terms of even degree $\{a_0 + a_2x^2 + a_4x^4 + \cdots + a_{2k}x^{2k} \mid \alpha_{2i} \in \mathbb{R}, k \in \mathbb{N}\}$ is a subspace of $\mathbb{R}[X]$, the vector space of polynomials with coefficients in $\mathbb{R}$.

As you would expect, checking that something is a subspace is usually easier than checking all of the axioms for a vector space. In particular, to check that U is a subspace of an $\mathbb{F}$-vector space V, you can just check that the following hold:

- *Zero vector*[2]. $0_V \in U$,
- *Closure under addition.* $u_1, u_2 \in U$ to imply $u_1 + u_2 \in U$,
- *Closure under scaling.* $\lambda \in \mathbb{F}$ and $u \in U$ to imply $\lambda u \in U$.

There are various ways in which we can manipulate subspaces, for example we can take the intersection of two subspaces, and we will get back another subspace.

[2]You may wonder why we need to check this when we already check that we are closed under scaling. To see why, notice that we still have to ensure U is non-empty!

Proposition 1.5 (Intersecting Subspaces)
Let $U, W \leq V$. Then $U \cap W \leq V$.

Proof. Since U and V are both subspaces of V, we have $0_V \in U \cap V$, and also since they are both closed under addition and scaling, $u_1, u_2 \in U \cap W$ implies that $u_1 + u_2 \in U \cap W$, and $\lambda \in \mathbb{F}$ implies $\lambda u \in U \cap W$. Thus $U \cap W$ is a subspace of V. □

However we can't manipulate subspaces however we want and expect magic. For example, the union of two subspaces is generally *not* a subspace, as it is typically not closed under addition. In fact, the union is only ever a subspace if one of the subspaces is contained in the other.[3]

We can however try to 'complete' the union so that it becomes a subspace.

Definition 1.6 (Sum of Subspaces)
Let V be a vector space over $\mathbb{F}$, and let $U, W \leq V$. We define the **sum** of U and W to be the set

$$U + W = \{u + w \mid u \in U, w \in W\}.$$

This definition immediately forces $U + W \leq V$, and indeed it is the minimal such space (in that any subspace of V containing both U and W must also contain $U + W$).

§1.2 Quotient Spaces

Since a vector space V forms an abelian group $(V, +)$, we are able to take the quotient by any subspace $U \leq V$.

Definition 1.7 (Quotient Space)
Let V an $\mathbb{F}$-vector space, and let $U \leq V$. The **quotient space** V/U is the abelian group V/U equipped with the scalar multiplication $F \times V/U \to V/U$ written $(\lambda, v + U) \mapsto \lambda v + U$.

With this definition, we need to check that this scalar multiplication operation is well defined. Indeed, if $v_1 + U = v_2 + U$ then

$$\begin{aligned} & v_1 - v_2 \in U \\ \implies & \lambda(v_1 - v_2) \in U \\ \implies & \lambda v_1 + U = \lambda v_2 + U \in V/U, \end{aligned}$$

so our operation is indeed well defined.

As you would expect, taking a quotient gives you back a vector space.

Proposition 1.8 (Quotient Spaces are Vector Spaces)
V/U is an $\mathbb{F}$-vector space.

[3]There are some more exercises of this flavour on the example sheet.

Proof Sketch. Check definitions (most properties are inherited from V being a vector space). □

§1.3 Basis and Dimension

A familiar idea is that of *dimension*, which measures the amount of freedom in a vector space.

Definition 1.9 (Span)

Let V be a vector space over $\mathbb{F}$, and let $S \subset V$. We define the **span** of S, $\langle S \rangle$ to be the set of finite combinations of elements of S.

Remark. By convention, we also take $\langle \emptyset \rangle = \{0\}$.

The span of S, $\langle S \rangle$ is the smallest vector subspace of V that contains S.

Example 1.10

If $V = \mathbb{R}^3$, and $S = \{(1, 0, 0), (0, 1, 2), (3, -2, -4)\}$, then $\langle S \rangle = \{(a, b, 2b) \mid a, b \in \mathbb{R}\}$.

Definition 1.11 (Spanning Set)

Let V be a vector space over $\mathbb{F}$, and let $S \subset V$. We say that S **spans** V if $\langle S \rangle = V$.

Definition 1.12 (Finite Dimension)

Let V be a vector space over $\mathbb{F}$. We say that V is **finite dimensional** if it is spanned by a finite set.

Example 1.13 (Finite and Infinite Dimensional Vector Spaces)

The space $\mathbb{R}[X]$ of polynomials with coefficients in $\mathbb{R}$ is infinite dimensional, but the space $\mathbb{R}_n[X]$ of polynomials of degree at most n is finite dimensional, and is spanned by the set $\{1, X, X^2, \dots, X^n\}$.

Definition 1.14 (Linear Independence)

We say that $\{v_1, \dots, v_n\} \in V$ are **linearly independent** if

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$$

implies that $\lambda_1 = \cdots = \lambda_n = 0$.

If a set of vectors is *not* linearly independent, then one of the vectors in the set can be written as a linear combination of the others.

Remark. If $\{v_1, \dots, v_n\}$ are linearly independent, then $v_i \neq 0$ for all i.

Definition 1.15 (Basis)

A subset S of V is a **basis** of V if S is a set of linearly independent vectors that span V.

Remark. When S spans V, we say that S is a **generating family** of V.

Example 1.16 (Canonical Basis for $\mathbb{R}^n$)

$\mathbb{R}^n$ has a basis $\{(1,0,\dots,0),(0,1,\dots,0),\dots,(0,0,\dots,1)\}$, which is known as the **canonical basis**.

Lemma 1.17 (Unique Representations with a Basis)

Let V be a vector space over $\mathbb{F}$. Then $\{v_1,\dots,v_n\}$ is a basis of V if and only if any vector $v \in V$ can be written uniquely as a linear combination of $\{v_1,\dots,v_n\}$.

Proof. If $v \in V$ can't be written as such a linear combination, then $\{v_1,\dots,v_n\}$ does not span V and is thus not a basis. Also, if v can be written as such a combination but it is non unique, then taking

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n.$$

where $\lambda_i \neq \mu_i$ for at least one value of i, we'd have $0 = v - v = (\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_n - \mu_n)v_n$, and at least one of these coefficients must be non-zero, thus $\{v_1,\dots,v_n\}$ is not a linearly independent set.

Other direction is an exercise. $\square$

Lemma 1.18 (Spanning Sets Contain a Basis)

If $\{v_1,\dots,v_n\}$ spans V, then some subset of this family is a basis of V.

Proof. If $\{v_1,\dots,v_n\}$ is linearly independent, then we are done. If it's not, then (up to reordering) we have $v_n \in \langle\{v_1,\dots,v_{n-1}\}\rangle$. But then $\langle\{v_1,\dots,v_n\}\rangle = \langle\{v_1,\dots,v_{n-1}\}\rangle$. Removing elements in this way repeatedly, since there is finitely many elements in this set we must eventually get a linearly independent set that still spans V. $\square$

Theorem 1.19 (Steinitz Exchange Lemma)

Let V be a finite dimensional vector space over $\mathbb{F}$. Suppose that $\{v_1,\dots,v_m\}$ is a linearly independent set and that $\{w_1,\dots,w_n\}$ spans V. Then

(i) $m \leq n$,

(ii) Up to reordering $\{v-1,\dots,v_m,w_{m+1},\dots,w_n\}$ spans V.

Proof. Suppose that we've replaced l of the w_i, and that $\langle v_1,\dots,v_l,w_{l+1},\dots,w_n\rangle = V$. If $m = l$ then we are done. Otherwise if $l < m$ then $v_{l+1} \in V$ implies we can write

$$v_{l+1} = \sum_{i \leq l} \alpha_i v_i + \sum_{i > l} \beta_i w_i.$$

Since $\{v_1, \ldots, v_m\}$ is linearly independent, then one of the β_i has to be non-zero.

Finish after the lecture. $\square$