LECTURE 2

Subspaces and Linear Independence

Last time we defined the notion of a field $\mathbb{F}$ as a generalization of the set of real numbers, and the notion of a vector space over a field $\mathbb{F}$ as a generalization of the vector space $\mathbb{R}^n$ (or any other vector space studied in Math 3013). Today we continue to translate ideas developed in Math 3013 to the setting of a vector space over a field $\mathbb{F}$. In so doing, none of the definitions change much, all we really do is substitute $\mathbb{F}$ for $\mathbb{R}$ in the old definitions. But we'll proceed anyway, since it affords us an opportunity to simultaneously review the development in Math 3013 as we substantiate the setting of Math 4063.

DEFINITION 2.1. *We say that a set S is **closed under an operation** $*$ if the outcome of applying the operation $*$ to elements of S is another element of S.*

Thus, for example, the set of real numbers is closed under addition and multiplication; because whenever you add two real numbers you get another real number, and whenever you multiply two real numbers you get another real number.

DEFINITION 2.2. *Let V be a vector space over a field $\mathbb{F}$ and let U be a subset of the elements of V. We say that U is a **subspace** of V if U is closed under the operations of scalar multiplicaition and vector addition: In other words, U is a subspace if*

$$(u \in U \quad and \quad \alpha \in \mathbb{F}) \quad \Rightarrow \quad \alpha u \in U \tag{1}$$

$$u_1, u_2 \in U \quad \Rightarrow \quad u_1 + u_2 \in U \tag{2}$$

REMARK 2.3. While there are two separate conditions to check in order to confirm that a given subset is a subspace, one can check both conditions simultaneously via

$$U \text{ is a subspace} \quad \Longleftrightarrow \quad \alpha u_1 + \beta u_2 \in U \text{ for all } \alpha, \beta \in \mathbb{F} \text{ and all } u_1, u_2 \in U$$

By the way, when V is a vector space over a field $\mathbb{F}$, we will refer to expressions of the form $\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_k u_k$ with $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ and $u_1, \ldots, u_k \in V$ as a **linear combination** of elements of V.

This equivalence by the way is easy to prove; I'll prove this statement and it's generalization below.

EXAMPLE 2.4. Let $\mathcal{C}(\mathbb{R})$ be the set of real-valued functions on the real line. Show that the subset S consisting of functions vanishing at $x = 0$ is a subspace of $\mathcal{C}(\mathbb{R})$.

- We want to check that $\alpha f + \beta g \in S$ for any real numbers α, β and any functions $f, g \in S$. Now for a function $h(x)$ to belong to S simply requires $h(0) = 0$. So the question is does $\alpha f + \beta g$ evaluated at 0 always equal 0?

  $$0 =^? (\alpha f + \beta g)(0) = \alpha f(0) + \beta g(0) = \alpha \cdot 0 + \beta \cdot 0 = 0$$

  So, indeed, S is a subspace of $\mathcal{C}(\mathbb{R})$.

EXAMPLE 2.5. Let $\mathcal{C}(\mathbb{R})$ again be the set of real-valued functions on the real line and let T be the set of functions whose value at $x = 0$ is 1. Is T a subspace of $\mathcal{C}(\mathbb{R})$?

- Well, proceeding as before, we need to check that the function $\alpha f + \beta g$ evaluates to 1 at $x = 0$ whenever $f, g \in T$ and $\alpha, \beta \in \mathbb{R}$. But

  $$1 =^? (\alpha f + \beta g)(0) = \alpha f(0) + \beta g(0) = \alpha \cdot 1 + \beta \cdot 1 = \alpha + \beta \neq 1 \text{ in general}$$

So T is not a subspace of $\mathcal{C}(\mathbb{R})$.

By the way, here is a simple necessary condition for a subset S of a vector space V to be a subspace.

PROPOSITION 2.6. *If S is a subspace of a vector space V, then $\mathbf{0}_V \in S$.*

Proof. A subspace S will be closed under scalar multiplication by elements of the underlying field $\mathbb{F}$, in particular, S will be closed under scalar multiplication by $0_{\mathbb{F}}$. But

$$0_{\mathbb{F}} \cdot v = \mathbf{0}_V \text{ for all } v \in V$$

When $v \in S$ we still have $0_{\mathbb{F}} \cdot v = \mathbf{0}_V$ and we also have $\mathbf{0}_V = 0_{\mathbb{F}} \cdot v \in S$ because S is closed under scalar multiplication. □

Here another prototypical example of a subspace. Let $\mathbf{A}$ be an $n \times n$ matrix and let S be the solution set of $\mathbf{Ax} = \mathbf{0}$;

$$S = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{Ax} = \mathbf{0}\}$$

Then S is a subspace of $\mathbb{R}^n$.

- Indeed, suppose $\mathbf{x}, \mathbf{y} \in S$ are solutions and $\alpha, \beta \in \mathbb{R}$. We want to show that any linear combination of the form $\alpha\mathbf{x} + \beta\mathbf{y}$ is also a solution. We have

$$\mathbf{A}(\alpha\mathbf{x} + \beta\mathbf{y}) = \mathbf{A}(\alpha\mathbf{x}) + \mathbf{A}(\beta\mathbf{y})$$

because matrix multiplication distributes over vector addition. Then

$$= \alpha\mathbf{Ax} + \beta\mathbf{Ay}$$

because matrix multiplication commutes with scalar multiplication. Then

$$= \alpha\mathbf{0} + \beta\mathbf{0}$$

because $\mathbf{x}, \mathbf{y}$ are, by hypothesis, solutions of $\mathbf{Ax} = \mathbf{0}$. Since any scalar muliple of the $\mathbf{0}$ vector is the $\mathbf{0}$ vector, we reach the desired conclusion:

$$\mathbf{A}(\alpha\mathbf{x} + \beta\mathbf{y}) = \mathbf{0} \quad \Rightarrow \quad \alpha\mathbf{x} + \beta\mathbf{y} \in \mathbf{S}$$

Since every linear combinations of two elements of S is an an element of S, S is a subspace.

PROPOSITION 2.7. *A subset S of a vector space V over a field $\mathbb{F}$ is a subspace if and only if every linear combination of the form $\alpha v + \beta u$ with $\alpha, \beta \in \mathbb{F}$, $v, u \in S$ is in S.*

Proof.

$\Rightarrow$. Suppose S is a subspace of V, $\alpha, \beta \in \mathbb{F}$, and $u, v \in S$. Then αv and βu are both in S, since subspaces are closed under scalar multiplication. But then $\alpha v + \beta u \in S$ since subspaces are also closed under vector addition.

$\Longleftarrow$. Suppose $\alpha v + \beta u \in S$ for every $\alpha, \beta \in \mathbb{F}$ and every $u, v \in S$. Then we have in particular $0_V \in S$ when we specialize $\alpha = \beta = 0_{\mathbb{F}}$. And then when we specialize to $\beta = 0_{\mho}$ we have

$$S \ni \alpha v + 0_F u = \alpha v + 0_V = \alpha v$$

so S is closed under scalar multiplication. Specializing to $\alpha = 1_{\mathbb{F}}$ and $\beta = 1_{\mathbb{F}}$ we have

$$S \in \alpha v + \beta u = 1_{\mathbb{F}} v + 1_{\mathbb{F}} u = v + u$$

so S is also closed under vector addition. Since S is closed under scalar multiplication and vector addition, S is a subspace of V. □

Below I will give also an easy corollary; primarily for the purpose of demonstrating an inductive proof. But first let me remind you all how a proof by induction works. Suppose you have not one statement, but a whole series of special cases to prove

$$\begin{array}{ccc} P_1 & \Rightarrow & Q_1 \\ P_2 & \Rightarrow & Q_2 \\ P_3 & \Rightarrow & Q_3 \\ & \vdots & \end{array}$$

If circumstances allow one can do do this both effectively and efficiently by employing a proof by induction. This works as follows:

- First. prove that $P_1 \quad \Rightarrow \quad Q_1$ is true.
- Secondly, prove that if $P_n \quad \Rightarrow \quad Q_n$ is true then necessarily the next subsequent statement $P_{n+r} \quad \Rightarrow \quad Q_{n+1}$ is true.

If you can accomplish these two steps, you have succeeded in proving $P_k \quad \Rightarrow \quad Q_k$ for all k in $\{1,2,3,\ldots\}$

COROLLARY 2.8. *If S is a subspace, then any linear combination $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$ of elements of V is also in S.*

Proof. We will use proof by induction. We wil regard the intial case to prove as being

$$S \text{ is a subpace} \quad \Rightarrow \quad \alpha_1 v_1 \in S \qquad \text{for all } \ \alpha_1 \in \mathbb{F} \text{ and for all } v_1 \in S$$

and that the k^{th} special case as being

$$S \text{ is a subspace} \quad \Rightarrow \quad \alpha_1 v_1 + \cdots + \alpha_k v_k \in S \qquad \text{for all } \alpha_1, \ldots, \alpha_k \in \mathbb{F} \text{ and for all } v_1, \ldots, v_k \in S$$

The statement of the initial case is true by the definition of a subspace (the part about closure under scalar mulitplication). This accomplishes the first step of an inductive proof.

Now are to prove that

$$(\text{the truth of } P_k \quad \Rightarrow \quad Q_i) \quad \Rightarrow \quad (\text{the truth of } P_{k+1} \quad \Rightarrow \quad Q_{k+1})$$

So assume the k^{th} special case is true

$$\alpha_1 v_1 + \cdots + \alpha_k v_k \in S \qquad \text{for all } \alpha_1, \ldots, \alpha_k \in \mathbb{F} \text{ and for all } v_1, \ldots, v_k \in S$$

Now $\alpha_{k+1} v_{k+1}$ is also in S for any $\alpha_{k+1} \in \mathbb{F}$ and any $v_{k+1} \in S$. And then since both $\alpha_1 v_1 + \cdots + a_k v_k \in S$ and $\alpha_{k+1} v_{k+1} \in S$, and because the subspace S is closed under vector addition it must be that

$$\alpha_1 v_1 + \cdots + \alpha_k v_k + \alpha_{k+1} v_{k+1} \in S \qquad \text{for all } \alpha_1, \ldots, \alpha_k, \alpha_{k+1} \in \mathbb{F} \text{ and for all } v_1, \ldots, v_k, v_{k+1} \in S$$

And so the $(k+1)^{th}$ statement is also true. This then completes the inductive proof. □

Here is another standard construction of a subspace.

DEFINITION 2.9. *Let $\{v_1, \ldots, v_k\}$ be a set of vectors in a vector space V. Then the set*

$$span_{\mathbb{F}}(v_1, \ldots, v_k) := \{\alpha_1 v_1 + \cdots + \alpha_k v_k \mid \alpha_1, \ldots, \alpha_k \in \mathbb{F}\}$$

*(where the coefficients $\alpha_1, \ldots, \alpha_k$ vary over all possible element of $\mathbb{F}$) is called the **span** of the vectors $\{v_1, \ldots, v_n\}$.*

PROPOSITION 2.10. *The span of a set of vectors in V is a subspace of V.*

Proof.

It suffices to show that any linear combination of two elements of $span_{\mathbb{F}}(v_1,\ldots,v_k)$ is again an element of $span_{\mathbb{F}}(v_1,\ldots,v_k)$. Let

$$\begin{aligned} u &= \alpha_1 v_1 + \cdots + \alpha_k v_k \\ v &= \beta_1 v_1 + \cdots + \beta_k v_k \end{aligned}$$

be arbitary elements of the span, and let α and β be arbitrary eleements of $\mathbb{F}$. Then

$$\begin{aligned} \alpha u + \beta v &= \alpha(\alpha_1 v_1 + \cdots + \alpha_k v_k) + \beta(\beta_1 v_1 + \cdots + \beta_k v_k) \\ &= (\alpha\alpha_1) v_1 + (\beta\beta_1) v_1 + \cdots + (\alpha\alpha_k) v_k + (\beta\beta_k) v_k \\ &= (\alpha\alpha_1 + \beta\beta_1) v_1 + \cdots + (\alpha\alpha_k + \beta\beta_k) v_k \\ &\in span_{\mathbb{F}}(v_1,\ldots,v_k) \end{aligned}$$

□

This construction of a subspace arises very frequently. So frequently, we may as well introduce some corresponding terminology.

Definition 2.11. *The subspace $span_{\mathbb{F}}(v_1,\ldots,v_k)$ is the* ***subspace generated by vectors*** *$v_1,\ldots,v_k$. A subspace S is said to be* ***finitely generated*** *whenever there exists a finite set of vectors $\{v_1,\ldots,v_k\}$ such that $S = span_{\mathbb{F}}(v_1,\ldots,v_k)$.*

1. Linear Dependence

We now come to a fundamental idea. Just above, we have constructed subspaces by taking linear combinations of vectors. On the other hand, we have also seen that when you take a linear combination of vectors that lie within a subspace, you don't leave a subspace. This means that whenever

$$v_{k+1} \in span(v_1, v_2, \ldots, v_k)$$

the subspace $span(v_1,\ldots,v_k,v_{k+1})$ coincides with the subspace $span(v_1,\ldots,v_k)$. But thinking of a vector in $span(v_1,\ldots,v_k)$ as a linear combination of $k+1$ vectors is making things more complicated rather than simpler. So if you have a subspace $S = span(v_1,\ldots,v_k)$ it should make matters simpler if we can reduce the number of generators needed to produce $span(v_1,\ldots,v_,)$. This we can do by removing any generator that can be expressed as a linear combination of the other generators.

Proposition 2.12. *$span(v_1,\ldots v_{k+1}) = span(v_1,\ldots,v_k)$ if and only $v_{k+1} \in span(v_1,\ldots,v_k)$.*

Proof. Let $S = span(v_1,\ldots,v_k)$. An element of $span(v_1,\ldots,v_k,v_{k+1})$ is just an element of S plus a scalar multiple of v_{k+1}. But if v_{k+1} is a linear combination of $v_1,\ldots,v_k$, then v_{k+1} and all of its scalar multiples are also in the subspace S. Since S is closed under vector addition we conclude that $S = span(v_1,\ldots,v_k,v_{k+1})$.

On the other hand, if $span(v_1,\ldots,v_k) = span(v_1,\ldots,v_k,v_{k+1})$ then since v_{k+1} itself lies in $span(v_1,\ldots,v_k,v_{k+1}) = span(v_1,\ldots,v_k)$, v_k can be written as a linear combination of the $v_1,\ldots,v_k$. □

What makes this sort of situation especially problematic is that it's not alway easy to tell (at least by inspection alone) when one vector is expressible in terms of another. Or even which vector to toss out! For example, if

$$v_3 = 2v_1 - v_2$$

we also have

$$v_2 = 2v_1 - v_3$$

and

$$v_1 = \frac{1}{2}v_2 + \frac{1}{2}v_3$$

Thus,

$$span\,(v_1, v_2, v_3) = span\,(v_1, v_2) = span\,(v_1, v_3) = span\,(v_2, v_3)$$

The following definition is meant to *democratize* the ambiguity exhibited in preceding example.

DEFINITION 2.13. *A set of vectors $v_1, \ldots, v_k$ is said to be* ***linearly dependent*** *if the vectors satisfy an equation of the form*

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \mathbf{0} \tag{1}$$

with at least one coefficient $\alpha_i \neq 0$. An equation of the form (1) (with at least one non-zero coefficient) is a called a ***dependence relation*** *(amongst the vectors $v_1, \ldots, v_k$).*

If

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \mathbf{0}$$

is a dependence relation, the stipulation that at least one coefficient, say α_i, is non-zero, allows us to scalar muliply the dependence relation by $\frac{1}{\alpha_i}$ to get

$$\frac{\alpha_1}{\alpha i} v_1 + \frac{\alpha_2}{\alpha_i} v_2 + \cdots + \frac{\alpha_{i-1}}{\alpha_i} v_{i-1} + v_i + \frac{\alpha_{i+1}}{\alpha_i} v_{i+1} + \cdots + \frac{\alpha_k}{\alpha_i} v_k = \mathbf{0}$$

or

$$v_i = -\frac{\alpha_1}{\alpha_i} v_1 - \cdots - \frac{\alpha_{i-1}}{\alpha_i} v_{i-1} - \frac{\alpha_{i+1}}{\alpha_i} v_{i+1} - \cdots - \frac{\alpha_k}{\alpha_i} v_k \in span\,(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k)$$

Thus, whenever we have a dependence relation amongst vectors $v_1, \ldots, v_k$ we can reduce the set of generating vectors for $S = span\,(v_1, \ldots, v_k)$ by one member. The procedure is just to remove a vector that has a non-zero coefficient in the dependence relation.

If we have lots of dependence relations then we can remove lots of generators our initial set. But eventually this process has to terminate (the subspace generated is staying the same, we are only removing superfluous generators). One must finally reach a point where there is no longer a viable dependence relation. That final condition we formulate as follows.

DEFINITION 2.14. *A set of vectors $v_1, \ldots, v_k$ is said to be* ***linearly independent*** *if the only way of satisfying*

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \mathbf{0}$$

is to take all the coefficients $a_1, \ldots, a_k$ equal to 0_F.

REMARK 2.15. I'd like to point out that the discussion above is kind of typical for this course in the following sense. We started with a simple notion (a subspace) and simple way of constructing such things (taking linear combinations of vectors). Then I pointed out that unfortunately the same subspace can produced in lots of different ways and that it's hard to tell when two such constructions give the same result (in other words, it's hard to check equalities between subspaces). So we found a simple way to make matters simpler (tossing out superfluous vectors). But that too introduced some ambiguity (which vectors do we toss out?). To accommodate and indeed better reflect this ambiguity we figured out the essential thing that had to happen if we were to remove a generator without changing the subspace. That's how we arrived at the definition of linear independence.

What I want to point out is that the idea of linear independence is not particularly well encapsulated by its definition (Definition 2.13). Rather to get a good grasp of the notion of linear independence you need to keep in mind the flow of ideas from which it sprung; this grasp will improve, as we move on, when you also keep in mind the ideas it allows you to connect.

PROPOSITION 2.16. *Let v_1, v_2 be two non-zero vectors in a vector space over a field $\mathbb{F}$. Then $\{v_1, v_2\}$ is a linearly dependent set if and only if there is a scalar non-zero $\alpha \in \mathbb{F}$ such that $v_2 = \alpha v_1$.*

Proof.

$\Rightarrow$ Suppose $\{v_1, v_2\}$ are linearly dependent. Then, by definition, there exists scalars $\alpha_1, \alpha_2 \in \mathbb{F}$ such $\alpha_1 v_1 + \alpha_2 v_2 = \mathbf{0}_V$ and for which at least one of α_1, α_2 does not equal $0_{\mathbb{F}}$. By reordering v_1 and v_2 if necessary, we can assume that $\alpha_2 \neq 0_{\mathbb{F}}$. But then $(\alpha_2)^{-1}$ exists (via the field axioms) and so

$$(\alpha_2)\ ^{-1} \cdot (\alpha_1 v_1 + \alpha_2 v_2) = (\sigma_2)^{-1} \cdot \mathbf{0}_V$$

The right hand side easily evaluates to $\mathbf{0}_V$. The left hand side evaluates to $(\alpha_2)^{-1}\alpha_1 + v_2$. So we have

$$(\alpha_2)^{-1}\alpha_1 + v_2 = \mathbf{0}_V$$

Adding $-\left((\alpha_2)^{-1}\alpha_1 v_1\right)$ to both sides we then get

$$v_2 = -(\alpha_2)^{-1}\alpha_1 v_1$$

Since $-(\alpha_2)^{-1}\alpha_1 \in \mathbb{F}$ we have demonstrated that if $\{v_1, v_2\}$ are linearly depedent then there is a $0_{\mathbb{F}} \neq \alpha \in \mathbb{F}$ such that $v_2 = \alpha v_1$.

$\Longleftarrow$ Suppose $v_2 = \alpha v_1$. Then adding $-\alpha v_1$ to both sides we have

$$-\alpha_1 v_1 + v_2 = \mathbf{0}_{\mathbb{F}}$$

Since the coefficient of v_2 in this relation can be taken to be $1_{\mathbb{F}} \neq 0$, v_1 and v_2 are linearly dependent.

. $\square$

REMARK 2.17. Notice how patient I was in presenting the proof. Every little step was explained. This was done not to insult your intelligence. Rather my purpose was two-fold. First of all, I wanted to keep reminding you of the general setting in which we are working (vector spaces over a general field - where the actual notions of vectors, scalar multiplication and vector addition could be pretty weird). Secondly, I tried to leave no step unexplained so that I didn't hide **from myself** a gap in the proof.