VECTOR SPACES

TIM SMITS

Linear algebra arose out of trying to solve systems of linear equations. In a first course, one learns the proper way to think about solutions to a system of n linear equations in n variables is by viewing them as solutions to a certain matrix equation of the form $Ax = b$ in $\mathbb{R}^n$, and then develops the necessary theory of matrices and tools needed to solve these equations. The goal of abstract linear algebra is to capture the special properties of $\mathbb{R}^n$ and of matrices that made the theory useful in the first place, and expand it to work in larger settings. This will lead to the abstract definitions of vector spaces and linear transformations, which will be the main objects of study for us.

DEFINITIONS AND EXAMPLES

Definition 0.1. A **vector space** V over a field F is a set V with an addition operation $+$ and scalar multiplication operation $\cdot$ by elements of F that sasify the following axioms:

1. For all $x, y \in V$, $x + y = y + x$.
2. For all $x, y, z \in V$, $(x + y) + z = x + (y + z)$.
3. There exists $0 \in V$ such that $x + 0 = x$ for all $x \in V$.
4. For all $x \in V$, there exists $-x \in V$ such that $x + (-x) = 0$.
5. For all $x \in V$, $1 \cdot x = x$.
6. For all $a, b \in F$ and $x \in V$, $(a + b) \cdot x = a \cdot x + b \cdot x$.
7. For all $a, b \in F$ and $x \in V$, $(ab) \cdot x = a \cdot (b \cdot x)$.
8. For all $a \in F$ and $x, y \in V$, $a \cdot (x + y) = a \cdot x + a \cdot y$.

The elements of V are called **vectors**, and it is understood that we write cx to mean $c \cdot x$.

From the axioms above, one can deduce the usual algebraic rules are true in vector spaces:

Proposition 1. *Let V be a vector space. For $x, y, z \in V$, and $a \in F$, the following hold:*

1. *If $x + y = x + z$, then $y = z$.*
2. *The vectors 0 and $-x$ are unique.*
3. $0 \cdot x = a \cdot 0 = 0$.
4. $(-a)x = -(ax)$.

The proofs of the above all follow quickly from the vector space and field axioms, and are left as an exercise.

Definition 0.2. For a vector space V and $W \subset V$, we call W a **subspace** of V if W is vector space under the same operations as in V.

Proposition 2 (Subspace criterion)**.** *Let V be a vector space. Then $W \subset V$ is a subspace $\iff 0 \in W$, and W is closed under addition and scalar multiplication.*

Proof. The forward direction is immediate by definition of a vector space. Conversely, if W is closed under addition and scalar multiplication, since vectors in W are vectors in V, this immediately gives axioms $1, 2, 5, 6, 7, 8$. Since $0 \in W$, 3 is satisfied, and since W is closed under scalar multiplication $(-1)x = -x \in W$ so 4 is satisfied. $\square$

Example 0.3. Any field F is a vector space over itself. More generally, F^n is an F-vector space for any n with operations of addition and scalar multiplication performed componentwise, where $F^n = \{(a_1, \ldots, a_n) : a_i \in F\}$ is the set of all n-tuples with entries in F.

Example 0.4. Let $F \subset L$ be a subfield. Then L is an L-vector space because L is a field, but L is also an F-vector space, with scalar multiplication by an element of F given by performing the multiplication in L, and addition also performed in L.

Example 0.5. $M_n(F)$, the set of $n \times n$ matrices with entries in a field F, is an F-vector space, with addition and scalar multiplication done entrywise.

Example 0.6. Let S be a non-empty set, then the set of all functions from S to F, denoted $\mathcal{F}(S, F)$, is an F-vector space. A vector in $\mathcal{F}(S, F)$ is a function $f : S \to F$, and two vectors f, g are equal if $f(s) = g(s)$ for all $s \in S$. The operations are given by $(f+g)(s) = f(s)+g(s)$ and $(cf)(s) = cf(s)$.

Example 0.7. The set of polynomials of degree at most n with coefficients in F, $P_n(F)$, is a subspace of $\mathcal{F}(F, F)$.

Example 0.8. Let $C([a, b])$ be the set of continuous functions from $[a, b]$ to $\mathbb{R}$, and let $C^\infty([a, b])$ be the subset of all infinitely differentiable functions. Then both $C([a, b])$ and $C^\infty([a, b])$ are subspaces of $\mathcal{F}(\mathbb{R}, \mathbb{R})$, and $C^\infty([a, b])$ is a subspace of $C([a, b])$. Let $V = \{f \in C^\infty([a, b]) : f' = f\}$. Then V is a subspace of $C^\infty([a, b])$. This gives a connection between studying solutions to differential equations and studying the vector space $C^\infty([a, b])$.

Example 0.9. Let S be a set and set $V = 2^S$, the set of all subsets of S. Then V is a vector space over $\mathbb{Z}/2\mathbb{Z}$ with addition given by $A + B = (A \setminus B) \cup (B \setminus A)$, scalar multiplication in the obvious manner, and the 0 element being the empty set. Note the additive inverse of any set A is itself.

OPERATIONS ON VECTOR SPACES

A natural question to ask is what operations can we do on vector spaces to create new vector spaces? Below are some examples:

Proposition 3. *Let V and W be vector spaces. Then $V \cap W$ is a subspace of both V and W.*

Proof. Clearly $0 \in W \cap V$. If $x, y \in V \cap W$, then as both V, W are vector spaces $x + y$ lies in both V and W, so $x + y \in V \cap W$, and similarly for $c \in F$ we see $cx \in V \cap W$. $\square$

Proposition 4. *Let V and W be vector spaces. Then $V \cup W$ is a vector space $\iff$ $W \subset V$ or $V \subset W$.*

Proof. The backwards direct is immediate: if $W \subset V$ or $V \subset W$, then the union is equal to either V or W which is a vector space. Conversely, suppose that $V \cup W$ is a subspace and that $W \not\subset V$. Suppose for contradiction that $V \not\subset W$. Pick $w \in W \setminus V$, and $v \in V \setminus W$. Then both $w, v \in W \cup V$, so $w + v \in W \cup V$. If $w + v \in W$, then $(w + v) - w = v \in W$, a contradiction. Similarly, if $w + v \in V$ then $w \in V$, again impossible. Therefore $V \subset W$. A similar argument shows that if $V \not\subset W$ then $W \subset V$. $\square$

The above proposition says that taking unions of vector spaces won't produce anything new. However, there is a way to create a vector space that contains copies of both V and W:

Proposition 5. *Let V and W be vector spaces. Then $V \times W$ is a vector space with the operations of componentwise addition and scalar multiplication.*

Proof. Exercise. $\square$

The vector space $V \times W$ is sometimes called the **external direct sum** of V and W and is commonly denoted $V \oplus W$. However to avoid confusion with the definition below, we'll keep the notation $V \times W$. There is a way to "add" vector spaces, but only if they are both subspaces of some common vector space, so that addition of vectors makes sense.

Definition 0.10. Let W_1 and W_2 be subspace of a vector space V. The **sum** of W_1 and W_2, denoted $W_1 + W_2$ is defined as $W_1 + W_2 = \{w_1 + w_2 : w_1 \in W_1, w_2 \in W_2\}$. Further, if $W_1 \cap W_2 = \{0\}$, then we call $W_1 + W_2$ the **interal direct sum** of W_1 and W_2 and denote this $W_1 \oplus W_2$.

The difference between external and interal direct sums is that in the latter case, both spaces live internally inside a larger vector space to begin with. In an external direct sum, we create a larger vector space in which copies of V and W can be identified, namely we identify V with the subspaces $\{(v, 0) : v \in V\} = V \times \{0\}$ and W with $\{(0, w) : w \in W\} = \{0\} \times W$. A sum being internal or external is to be understood by the context, and will just be referred to as a direct sum.

Proposition 6. *For subspaces W_1, W_2 of a vector space V, W_1+W_2 (and therefore $W_1 \oplus W_2$) is a subspace of V.*

Proof. It's clear that $0 \in W_1 + W_2$ since $0 \in W_1$ and $0 \in W_2$. If $x, y \in W_1 + W_2$, then $x = w_1 + w_2$ and $y = w_1' + w_2'$ for $w_1, w_1' \in W_1$ and $w_2, w_2' \in W_2$. Therefore $x + y = (w_1 + w_1') + (w_2 + w_2')$ and $w_1 + w_1' \in W_1'$ because W_1 is a subspace of V, and $w_2 + w_2' \in W_2$ for the same reasoning. The proof that $W_1 + W_2$ is closed under scalar multiplication is similar. $\square$

The difference between being a sum of subspaces and a direct sum of subspaces is the following:

Proposition 7. *Suppose $V = W_1+W_2$ for some subspaces W_1, W_2. Then $V = W_1 \oplus W_2 \iff$ every vector x in V can be written uniquely as $x = w_1 + w_2$ for $w_1 \in W_1$ and $w_2 \in W_2$.*

Proof. If $V = W_1 \oplus W_2$, and x has two different representations as a sum of the above form, write $x = w_1 + w_2$ and $x = w_1' + w_2'$ for some $w_1, w_2, w_1', w_2' \in W$. Then $w_1 - w_1' = w_2' - w_2$, and the left hand side lives in W_1 while the right hand side lives in W_2. This says $w_1 - w_1' \in W_1 \cap W_2 = \{0\}$, so $w_1 = w_1'$. Similarly $w_2 = w_2'$ so the representation is unique. Conversely, suppose that any vector $x \in V$ can be written uniquely as $x = w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$. Then clearly, $V = W_1 + W_2$. If $x \in W_1 \cap W_2$, we can write $x = x + 0$ by taking $w_1 = x$ and $w_2 = 0$. Similarly, we can write $x = 0 + x$ by taking $w_1 = 0$ and $w_2 = x$. By uniqueness, this says $x = 0$, so that $W_1 \cap W_2 = \{0\}$ says $V = W_1 \oplus W_2$. $\square$

Example 0.11. In $\mathbb{R}^2$, set $X = \{(x, y) : y = 0\}$ and $Y = \{(x, y) : x = 0\}$. Then $\mathbb{R}^2 = X \oplus Y$. Note these subspaces are simply the x and y axes. In $\mathbb{R}^3$, set $V = \{(x, y, z) : z = 0\}$

and $W = \{(x,y,z) : x = 0\}$. Then $\mathbb{R}^3 = V + W$, but the sum is not direct because $V \cap W = \{(x,y,z) : x = z = 0\}$.

Example 0.12. Let F be a field not of characteristic 2, and let $\mathrm{Sym}_n(F), \mathrm{Skew}_n(F) \subset M_n(F)$ be the subspaces of symmetric and skew-symmetric matrices respectively. Then $M_n(F) = \mathrm{Sym}_n(F) \oplus \mathrm{Skew}_n(F)$. Any matrix $A \in M_n(F)$ can be written $A = \frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t)$, so $M_n(F) = \mathrm{Sym}_n(F) + \mathrm{Skew}_n(F)$, and if $A \in \mathrm{Sym}_n(F) \cap \mathrm{Skew}_n(F)$, we have $A = A^t$ and $A = -A^t$ so that $2A^t = 0$ says $A^t = 0$, so that the sum is direct.

There's one more common operation on subspaces that we'll study, although it is quite a bit more abstract.

Definition 0.13. Let V be a vector space, and $W \subset V$ be a subspace. For a vector $v \in V$, we define the **coset** of v, denoted $v + W$, to be $v + W = \{v + w : w \in W\}$, the set of translates of v by elements of W.

Example 0.14. Let $V = \mathbb{R}^2$, $W = \{(x, 0) : x \in \mathbb{R}\}$, and $v = (0, 1)$. What set is $v + W$? Elements of the coset $v + W$ look like $(0, 1) + w$ for different choices of vectors $w \in W$. Since an arbitrary $w \in W$ looks like $(a, 0)$ for some $a \in \mathbb{R}$, such elements look like $(a, 1)$ for some $a \in \mathbb{R}$. For any choice of a the vector $(a, 0)$ is in W, so we see that $v + W = \{(a, 1) : a \in \mathbb{R}\}$.

The point of cosets is that they give us a way of partitioning the vector space V: as an equality of sets, we have $V = \bigcup_{v \in V} (v + W)$. We'll use these cosets to construct a new vector space. Let $V/W = \{v + W : v \in V\}$. We can define addition and scalar multiplication operations on V/W as follows:

Proposition 8. *V/W is a vector space, where the operations are given by $(v+W)+(v'+W) = (v + v') + W$ and $c \cdot (v + W) = c \cdot v + W$.*

Proof. Exercise. □

Definition 0.15. The set V/W with the operations of addition and scalar multiplication as given above is known as the **quotient space** of V by W.

The idea behind the quotient space is that it "crushes" the subspace W to the 0 vector. This can be seen from the following:

Proposition 9. *Two cosets $v + W$ and $v' + W$ are equal in V/W if and only if $v - v' \in W$. In particular, $v + W = 0 + W$ in V/W if and only if $v \in W$.*

Proof. Exercise. □

Example 0.16. Consider $V = \mathbb{R}^2$ and $W = \{(x, 0) : x \in \mathbb{R}\}$, the x-axis. For any vector $v = (a, b)$, we have that $v + W = \{(a + x, b) : x \in \mathbb{R}\}$ is the horizontal line through the vector v. The quotient space V/W "crushes" each of these horizontal lines to a single point, namely the intersection of this line with the y-axis: in the quotient space, we have the equality $(a, b) + W = (0, b) + W$ because $(a, b) - (0, b) = (a, 0) \in W$. We see that points in V/W can be "identified" with points on the y-axis, so that one can "picture" V/W as the y-axis.

LINEAR INDEPENDENCE

The above discussion tells us how to create new vector spaces from subspaces of some V. How can we create subspaces of V? Starting with $S \subset V$, what is needed to build a vector space out of elements of S? By definition, such a subspace would have to be closed under scalar multiplication, so for $s \in S$ and $c \in F$ it must contain $c \cdot s$. Similarly, it would need to be closed under addition, so it needs to contain all possible finite sums of the elements of the form just mentioned. It turns out, this is enough.

Definition 0.17. A **linear combination** of vectors $v_1, \ldots, v_n$ is an expression of the form $c_1v_1 + \ldots + c_nv_n$ for some $c_i \in F$. An equation of the form $c_1v_1 + \ldots + c_nv_n = 0$ is called a **linear dependence relation**. A dependence relation is called **trivial** if the only possible solution is when all $c_i = 0$, and is called non-trivial otherwise.

Definition 0.18. Let $S \subset V$. The **span** of S denoted $\mathrm{Span}(S)$ is the set of all finite linear combinations of elements of S. That is, $\mathrm{Span}(S) = \{c_1v_1 + \ldots + c_nv_n : c_i \in F, v_i \in S, n \geq 1\}$.

Proposition 10. *Let $S \subset V$. Then Span(S) is a subspace of V.*

Proof. By convention, if $S = \emptyset$ we define $\mathrm{Span}(S) = \{0\}$. If $S \neq \emptyset$, pick $v \in S$. Then $0 = 0 \cdot v \in \mathrm{Span}(S)$. If $x, y \in \mathrm{Span}(S)$, then $x = c_1v_1 + \ldots + c_nv_n$ and $y = d_1w_1 + \ldots + d_mw_m$ for some $c_i, d_j \in F$ and $v_i, w_j \in S$. Then $x + y = c_1v_1 + \ldots + c_nv_n + d_1w_1 + \ldots + d_mw_m$ is a linear combination of the vectors $v_1, \ldots, v_n, w_1, \ldots, w_m \in S$ so $x + y \in \mathrm{Span}(S)$. Similarly for $c \in F$ we see $c \cdot v \in \mathrm{Span}(S)$, so $\mathrm{Span}(S)$ is a subspace of V. □

$\mathrm{Span}(S)$ is sometimes referred to as the subspace generated by S. If $V = \mathrm{Span}(S)$, then we call S a **generating set** for V. Observe that any subspace of V containing S must contain $\mathrm{Span}(S)$, and therefore $\mathrm{Span}(S)$ is the *smallest* subspace of V containing S.

Example 0.19. In $\mathrm{Sym}_2(F)$, any symmetric matrix is of the form $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ for some $a, b, c \in F$. We see $\mathrm{Sym}_2(F) = \mathrm{Span}\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

Example 0.20. Let $V = \mathbb{R}^3$. Then $V = \mathrm{Span}\{(1,0,0), (0,1,0), (0,0,1)\}$. We may also write $V = \mathrm{Span}\{(1,1,0), (0,1,1), (1,0,1)\})$, or $V = \mathrm{Span}\{(1,1,1), (1,0,0), (0,1,0), (0,1,1)\}$. A spanning set need not be unique, nor must any spanning set have the same cardinality.

The above example shows that a spanning set may contain "redundant" information. In the third spanning set above, notice that $(1,1,1)$ is already contained in $\mathrm{Span}\{(1,0,0), (0,1,0), (0,1,1)\}$, so removing it from S does not change $\mathrm{Span}(S)$. We give this condition a name:

Definition 0.21. Let V be a vector space. For $S \subset V$, we call S **linearly dependent** if there exist $v_1, \ldots, v_n \in S$ and $c_1, \ldots, c_n \in F$ not all 0 such that $c_1v_1 + \ldots + c_nv_n = 0$. S is called **linearly independent** if S is not linearly dependent.

If S is linearly dependent, the above says there is a non-trivial linear combination of some vectors in S that equals 0. Since some coefficient c_i must be non-zero, we can solve for v_i in terms of the remaining vectors, so another way of saying this is that some vector v_i is contained in the span of some other vectors.

Example 0.22. In the above example, the set $\{(1,0,0),(0,1,0),(0,0,1)\}$ is linearly independent. The set $\{(1,1,1),(1,0,0),(0,1,0),(0,1,1)\}$ is linearly dependent.

Example 0.23. In $C^\infty(\mathbb{R})$, the vectors $\sin(x)$ and $\cos(x)$ are linearly independent: if $c_1\sin(x)+c_2\cos(x)=0$ for all x, plugging in $x=0$ and $x=\frac{\pi}{2}$ shows that $c_1=c_2=0$. Similarly if $r\neq s$, the functions e^{rx} and e^{sx} are linearly independent.

Since linear dependence is defined in terms of a finite quantity, an easy definition of linear independence that handles the case of S being infinite is as follows:

Proposition 11. *Let V be a vector space and $S\subset V$. Then S is linearly independent if and only if all finite subsets of S are linearly independent.*

Proof. If S is linearly independent, for any $S'\subset S$, a linear dependence relation among vectors in S' is also a linear dependence relation among vectors in S, so it must be trivial. Conversely, if all finite subsets of S are linearly independent, given any vectors $v_1,\ldots,v_n$, if $c_1v_1+\ldots+c_nv_n=0$, this is a dependence relation among the vectors of the finite set $S'=\{v_1,\ldots,v_n\}$, and so must be trivial by assumption. □

Given $S\subset V$, how can we check if S is linearly independent? One way is as follows:

Proposition 12. *Let V be a vector space and $S=\{v_1,\ldots,v_n\}$ for some $v_i\in V$. Then S is linearly dependent if and only if $v_1=0$ or there exists $1\leq k<n$ such that $v_{k+1}\in$ Span$(\{v_1,\ldots,v_k\})$.*

Proof. The backwards direction is immediate, so suppose that S is linearly dependent. Then $c_1v_1+\ldots+c_nv_n=0$ for some c_i not all 0. Set $k=\max\{n:c_n\neq 0\}$, which exists since some coefficient is non-zero and there are finitely many. Notice that this says $c_i=0$ for all $k<i\leq n$. If $k=1$, this says c_1 is the only non-zero coefficient, so $c_1v_1=0$ gives $v_1=0$. Otherwise, $k>1$ so $c_1v_1+\ldots+c_nv_n=c_1v_1+\ldots+c_kv_k=0$. Since $c_k\neq 0$, this says $v_k\in\text{Span}(\{v_1,\ldots,v_{k-1}\})$, so we are done. □

This gives a method of checking if a set is linearly independent that works well for sets of small size. For example, to check if $\{v_1,v_2,v_3\}$ is linearly independent one just needs to check that $v_2\notin\text{Span}(\{v_1\})$ and $v_3\notin\text{Span}(\{v_1,v_2\})$. For sets of larger size, we will later develop more efficient methods. We end the section with an extremely useful proposition.

Proposition 13. *Let $S\subset V$ be linearly independent and $v\in V$. Then $S\cup\{v\}$ is linearly dependent if and only if $v\in$ Span(S).*

Proof. If $S\cup\{v\}$ is linearly dependent, then there are $s_1,\ldots,s_n\in S$ and $c_1,\ldots,c_{n+1}\in F$ not all 0 such that $c_1s_1+\ldots+c_ns_n+c_{n+1}v=0$. Necessarily, $c_{n+1}\neq 0$ otherwise the linear independence of S forces all $c_i=0$. Then solving for v gives $v=-\frac{1}{c_{n+1}}(c_1s_1+\ldots+c_ns_n)$ so $v\in\text{Span}(S)$. Conversely, if $v\in\text{Span}(S)$ then $v=c_1s_1+\ldots+c_ns_n$ for some $s_i\in S$ and $c_i\neq 0$. Then $c_1s_1+\ldots+c_ns_n-v=0$ is a non-trivial linear dependence relation among elements of $S\cup\{v\}$, so $S\cup\{v\}$ is linearly dependent. □

Theorem 0.24. *Let $S\subset V$ be linearly independent. If $v\neq 0\in$ Span(S), then $v=c_1v_1+\ldots+c_nv_n$ for unique distinct vectors $v_i\in S$ and unique $c_i\neq 0\in F$.*

Proof. Suppose that v has two different representations using vectors in S. Write $v=c_1s_1+\ldots+c_ns_n$ and $v=d_1t_1+\ldots+d_mt_m$ for some $c_i,d_j\neq 0\in F$ and $s_i,t_j\in S$, where we may assume none of the s_i are the same and none of the t_j are the same. Subtracting shows

$c_1s_1 + \ldots + c_ns_n - d_1t_1 - \ldots - d_mt_m = 0$. If $\{s_1, \ldots, s_n\} \neq \{t_1, \ldots, t_m\}$, then there is some i such that s_i is not equal to any of t_j. Since S is linearly independent, this forces $c_i = 0$, since there is no other term in the sum that can be grouped with c_is_i. This is a contradiction, so $n = m$ and $\{s_1, \ldots, s_n\} = \{t_1, \ldots, t_m\}$. Relabeling as necessary, we may assume that $s_i = t_i$ so that the above can be written as $(c_1 - d_1)s_1 + \ldots + (c_n - d_n)s_n = 0$, so $c_i = d_i$ for all i and therefore such a representation is unique. □

BASES AND DIMENSION

The above theorem is of critical importance: the vectors in Span(S) can then be though of as tuples of elements of F by reading off the coefficients in the corresponding linear combination. A natural question to ask is if every vector space arises as the spanning set of a linearly independent subset. The answer is yes, and is the most important result in linear algebra.

Definition 0.25. A **basis** of a vector space V is a linearly independent spanning set. The **dimension** of V is the cardinality of a basis of V.

Perhaps in more familiar terms, the above says that every vector space has a basis. The fact that the dimension of a vector space is actually well defined is a fairly non-trivial result, but the proof is a rather technical set theoretic argument that is unenlightening, so for our purposes it will be taken for granted.

Proposition 14. *Let B and B' be two bases of a vector space V. Then $|B| = |B'|$.*

Dimension is one of the most useful ideas in linear algebra: it gives us a notion of size for a vector space, and being able to translate questions about vector spaces into statements about integers makes them easier to understand. At this stage, linear algebra branches off in two directions: the study of infinite dimensional vector space, and the study of finite dimensional vector spaces, the latter of which we will focus the majority of our attention on.

FINITE DIMENSIONAL VECTOR SPACE

Throughout the rest of this section, we will assume that V is an n-dimensional vector space over a field F unless otherwise stated.

The above proof that every vector space has a basis is non-constructive – it tells us one must exist but gives us no way of finding one. In the finite dimensional case, we actually have a constructive method for finding bases of a vector space.

Theorem 0.26. *Let $S = \{v_1, \ldots, v_k\}$ be a subset of V that spans V. Then there is $B \subset S$ such that B is a basis of V.*

Proof. We may assume that the v_i are non-zero, otherwise remove them. Let m be the largest integer such that there is an m element subset B of S that is linearly independent. As $\{v_i\}$ is linearly independent for any i, and S has at most k elements, in particular B must exist and $1 \leq m \leq k$. Then Span(S) = Span(B). To see this, we show that $v_i \in$ Span(B) for all i. If $v_i \notin B$, then $B \cup \{v_i\}$ is a linearly dependent subset by definition of B, so there are $c_1, \ldots, c_{m+1} \in F$ not all 0 such that $c_1s_1 + \ldots + c_ms_m + c_{m+1}v_i = 0$. By linear independence of elements of B, necessarily $c_{m+1} \neq 0$, so we can solve for v_i in terms of s_i, giving $v_i \in$ Span(B) as desired. □

Theorem 0.27. *Let $S = \{v_1, \dots v_k\}$ be a linearly independent subset of V. Then there exist vectors $w_1, \dots, w_m \in V$ such that $\{v_1, \dots, v_k, w_1, \dots, w_m\}$ is a basis of V.*

Proof. Pick a basis $\{e_1, e_2, \dots, e_n\}$ of V. Then $\{w_1, \dots, w_k, e_1, \dots, e_n\}$ is a spanning set. Remove vectors e_i from the above set if $e_i \in \operatorname{Span}(S)$. The remaining vectors $w_1, \dots, w_m$ not removed are not contained in $\operatorname{Span}(S)$, so the set $\{v_1, \dots, v_k, w_1, \dots, w_m\}$ must be linearly independent, and it remains a spanning set of V by construction so it is a basis. □

An immediately corollary is the following:

Corollary 0.28. *Let $W \subset V$ be a subspace. Then there exists $W' \subset V$ a subspace such that $V = W \oplus W'$.*

Proof. Pick a basis $\{v_1, \dots, v_k\}$ of W and extend to a basis $\{v_1, \dots, v_k, e_1, \dots, e_m\}$ of V. Set $W' = \operatorname{Span}(\{e_1, \dots, e_m\})$. Then it's clear that $V = W + W'$, and $W \cap W' = \{0\}$ because if $x \in W \cap W'$, we can write $x = c_1 v_1 + \dots + c_k v_k$ and $x = d_1 e_1 + \dots + d_m e_m$ for $c_i, d_j \in F$, so $c_1 v_1 + \dots + c_k v_k - d_1 e_1 - \dots - d_m e_m = 0$ gives all $c_i, d_j = 0$ as these vectors are linearly independent in V. □

The subspace W' is called the complement of W in V.

In linear algebra, it's not uncommon to be interested in finding a basis with some particular choices of basis vectors, so the extension result is quite useful. The following is a translation of the above two results using the language of dimension.

Theorem 0.29. *Let $S = \{v_1, \dots, v_k\}$.*

1. *If S is linearly independent, then $k \leq n$.*
2. *If S spans V, then $k \geq n$*
3. *If $k = n$, S is linearly independent if and only if S is a spanning set.*

Proof. Items 1 and 2 are immediately corollaries of the above two results. To prove 3, If S is linearly independent and S doesn't span V, then there is $v \in V$ such that $S \cup \{v\}$ is linearly independent. But then this says $n+1 \leq n$, a contradiction. Therefore S spans V. Conversely, if S is not linearly independent, we may trim S to a basis B with $n = |B| < |S| = n$, a contradiction. □

Example 0.30. In F^n, the vectors e_i where e_i is the vector that is 1 in the i-th coordinate and 0 elsewhere form a basis. It's easy to see that if $c_1 e_1 + \dots c_n e_n = 0$, then $(c_1, \dots, c_n) = (0, \dots, 0)$ so $c_i = 0$, and it's obvious this is a spanning set. This is an n-dimensional F-vector space.

Example 0.31. In $M_n(F)$, the matrices E_{ij} where E_{ij} is the matrix with (i,j)-th entry equal to 1 and 0 elsewhere is a basis – the argument is the same as above. This is an n^2-dimensional F-vector space.

Example 0.32. In $P_n(F)$, the set $\{1, x, \dots, x^n\}$ is a basis. It's clear that this is a spanning set, so it remains to see linear independence. If $c_0 + c_1 x + \dots c_n x^n = 0$ in $P_n(F)$, then in particular, this holds true for all $x \in F$. The left hand side is a degree at most n polynomial, so it has at most n roots, while the right hand side is 0 everywhere. This is only possible if all coefficients are 0. This is an $n + 1$-dimensional F-vector space.

Example 0.33. The space of all polynomials with coefficients in F, $P(F)$ is infinite dimensional: any finite set of polynomials has a maximal degree m, so their F-span is contained in $P_m(F)$. This says no finite subset of $P(F)$ is a spanning set, so it is infinite dimensional as an F-vector space.

Example 0.34. In $\mathbb{R}^3$, the set $\{(1,0,1),(1,1,0),(0,1,1)\}$ is a basis, because it is linearly independent: one can check by hand that $(0,1,1) \notin \mathrm{Span}(\{(1,0,1),(1,1,0)\})$.

Example 0.35. Let $V = \{(x,y,z) \in \mathbb{R}^3 : x - 2y + z = 0 \text{ and } 2x - 3y + z = 0\}$. Then V is a subspace of $\mathbb{R}^3$, and has basis $\{(1,1,1)\}$.

Example 0.36. The dimension of a vector space depends on the underlying field. As a $\mathbb{C}$-vector space, $\mathbb{C}^n$ has dimension n with basis vectors e_j for $1 \leq j \leq n$. However, $\mathbb{C}$ is a 2-dimensional $\mathbb{R}$-vector space: any complex number z is of the form $z = a + bi$ for real a, b, so $\{1, i\}$ is basis. The vectors e_j, ie_j for $1 \leq j \leq n$ form a basis of $\mathbb{C}^n$ as a $2n$-dimensional $\mathbb{R}$-vector space.

Example 0.37. For $a \neq 0 \in \mathbb{R}$, the set $\{1, x-a, (x-a)^2, \ldots, (x-a)^n\}$ is a basis for $P_n(\mathbb{R})$: if $c_0 + c_1(x-a) + \ldots + c_n(x-a)^n = 0$ for all x, plugging in $x = a$ shows $c_0 = 0$, and taking derivatives and repeating the argument shows $c_i = 0$. This shows linear independence and since a basis has $n+1$ elements, this is a spanning set. Every polynomial $p(x)$ can be written in the form $p(x) = c_0 + c_1(x-a) + \ldots + c_n(x-a)^n$. One can solve for the coefficients c_i by taking derivatives as necessary and plugging in $x = a$, to see $c_k = \frac{p^{(k)}(a)}{k!}$, recovering the usual Taylor expansion around $x = a$.

To illustrate why dimension is useful, we prove a quick result, which helps us understand a vector space by understanding its subspaces.

Proposition 15. *Let $W \subset V$ be a subspace. Then $\dim(W) \leq n$. If $\dim(W) = n$, then $W = V$.*

Proof. First we show that W is finite dimensional. If $W = \{0\}$, we are done. Otherwise, pick $w_1 \neq 0 \in W$. If $W = \mathrm{Span}(\{w_1\})$, we are done, otherwise there is $w_2 \in W$ with $w_2 \notin \mathrm{Span}(\{w_1\})$, so $\{w_1, w_2\}$ is linearly independent. Continue choosing vectors $w_3, \ldots, w_k$ in this way such that $\{w_1, \ldots, w_k\}$ is a linearly independent subset of W. Since $W \subset V$, it's also a linearly independent subset of V, so this process must stop before the n-th step, and the termination of this process is equivalent to saying that $W = \mathrm{Span}(\{w_1, \ldots, w_k\})$. This says $\{w_1, \ldots, w_k\}$ is a basis of W, and we have $k \leq n$. If $k = n$, these vectors are actually a basis of V as well, so $W = V$. □

Example 0.38. Let $W \subset \mathbb{R}^3$ be a subspace. Then $\dim(W) = 0, 1, 2, 3$. If $\dim(W) = 0$, then $W = \{0\}$, and if $\dim(W) = 3$, then $W = \mathbb{R}^3$. If $\dim(W) = 1$, then $W = \mathrm{Span}(\{v\})$ for some $v \in W$, i.e. W is the line through the origin in the direction of v. If $\dim(W) = 2$, we have $W = \mathrm{Span}(\{v_1, v_2\})$ for some vectors v_1, v_2. Let $v = v_1 \times v_2$, so $x \cdot v = 0$ for all $x \in W$. This defines the equation of a plane with normal vector $v_1 \times v_2$, so that subspaces of $\mathbb{R}^3$ are either $\{0\}$, $\mathbb{R}^3$, lines through the origin or planes through the origin. The dimensions of these objects should hopefully match your own geometric intuition.

Example 0.39. Set $V = (\mathbb{Z}/p\mathbb{Z})^2$, which is a 2-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space with basis vectors $(\bar{1}, \bar{0})$ and $(\bar{0}, \bar{1})$. What are all the subspaces of V? If $W \subset V$ is a subspace, we have $\dim(W) = 0, 1, 2$. If $\dim(W) = 0$ then $W = \{0\}$, and if $\dim(W) = 2$ then $W = V$. If

$\dim(W) = 1$, then $W = \mathrm{Span}(\{v\})$ for some non-zero vector v. There are a total of p^2-1 such vectors v, and each of the $p-1$ non-zero multiples of v span the same subspace of V. Since the 1-dimensional subspaces of V partition W, we conclude there are $(p^2-1)/(p-1) = p+1$ different 1-dimensional subspaces of V, for a total of $p+3$.

We end with some useful dimension counting results:

Proposition 16. *Let be V a vector spaces and let W, W_1, W_2 be subspaces.*

(a) $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$.
(b) $\dim(W_1 \oplus W_2) = \dim(W_1) + \dim(W_2)$.
(b) $\dim(V/W) = \dim(V) - \dim(W)$.

Proof. Exercise. $\square$