Elements of Algebraic Structures 06^{th} September, 2019

Lecture 11: Spanning set, Linear Independence and Basis

Instructor: Sujata Ghosh *Scribe: Ankit Gupta*

First, revisit the definition of field which we have discussed in the last class.

A field is a set F, along with 2 operations i.e. $(F, +, .)$ with the following properties :

1. (F,+) forms an abelian group with 0 as an identity element and $-a$ as an inverse element of a where $0, a, -a \in F$
2. (F-{0},.) forms an abelian group with 1 as an identity element and a^{-1} as inverse element of a with $a^{-1} = \frac{1}{a}$, where $a, a^{-1}, 1 \in F$

   Binary operations which are defined on this field F can be anything. The important thing is that we should have 2 abelian groups(additive and multiplicative) to get a field. Here, in multiplicative abelian group, every non-zero element must have a multiplicative inverse and additive & multiplication laws must be compatible over this field F which means distributive law i.e. $a.(b + c) = (a.b) + (a.c)$ should also be followed here.

Now, when we say vector space V is defined over a field F, it means :

- $(V, +)$ forms an abelian group, where + is defined as :

  $$+ : V \times V \to V$$

  It means, it takes any 2 vectors say v and w from vector space V and generates a new vector $v + w$

- Vector space V should follow scalar multiplication(.) over a field F, where . is defined as :

  $$. : F \times V \to V$$

  It means, it takes a vector, say, v from vector space V and a scalar 'c' from field F and gives a new vector $c.v$ which is also an element of vector space V
  i.e.

  $$v \mapsto c.v$$

  Now, comes to the concept of Spanning set, Linear Independence and Basis. Suppose, we have a vector space V over a fixed field F.

1 Span of a set

If we have a set of vectors $S = \{v_1, v_2, ..., v_n\}$ in a vector space V and if we can express a vector $w \in V$ as :

$$w = a_1.v_1 + a_2.v_2 + ... + a_n.v_n$$
$$\forall i, \;\; a_i \in F$$

Then all such linear combinations (or) all such w's form the span of S. So, basically, the span of a set S is the set of all linear combinations of the vectors in S. It is denoted by $span(S)$.

$$span(S) = span\{v_1, v_2, ...v_n\} = \{a_1v_1 + a_2v_2 + ... + a_nv_n \mid a_1, a_2, ..., a_n \in F\}.$$

Span(S) is basically a subspace of V.

Spanning Set of a Vector Space: if set $S = \{v_1, v_2, ...v_n\}$ be a subset of a vector space V. Then set S is called a spanning set of V if **every** vector in V can be written as a linear combination of vectors in S. In such cases, it is said that S spans V and consequently, we say, V is finite dimensional.

2 Linear Independence

A set of vectors $\{v_1, v_2, ..., v_n\}$ is called linearly independent if

$$a_1.v_1 + a_2.v_2 + ... + a_n.v_n = 0_V$$

where, $\forall i, \;\; a_i \in F$ and $a_1 = a_2 = ... = a_n = 0$

Example: Suppose, we have a vector space $V = \mathbb{R}^3$ and set of vectors $\{v_1, v_2, v_3\}$ where $v_1 = (1, 0, 0)$, $v_2 = (1, 1, 0)$, $v_3 = (1, 2, 3)$
Now, here, $span\{v_1, v_2\}$ makes the subspace which contains vectors of the form $(a, b, 0)$, where, $a, b \in \mathbb{R}$
Also, set $\{v_1, v_2, v_3\}$ is linearly independent if $a_1 = a_2 = a_3 = 0$ in $a_1v_1 + a_2v_2 + a_3v_3 = 0$.
Let's test it whether they are linearly independent or not.

$$\begin{gathered} a_1v_1 + a_2v_2 + a_3v_3 = 0_V \\ a_1(1, 0, 0) + a_2(1, 1, 0) + a_3(1, 2, 3) = (0, 0, 0) \\ (a_1, 0, 0) + (a_2, a_2, 0) + (a_3, 2a_3, 3a_3) = (0, 0, 0) \\ (a_1 + a_2 + a_3, a_2 + 2a_3, 3a_3) = (0, 0, 0) \\ \Rightarrow a_1 + a_2 + a_3 = 0,\; a_2 + 2a_3 = 0,\; 3a_3 = 0 \\ \Rightarrow a_1 = 0, a_2 = 0, a_3 = 0 \end{gathered}$$

Hence, $\{v_1, v_2, v_3\}$ is a linearly independent set. Actually $\{v_1, v_2, v_3\}$ is a basis of $\mathbb{R}^3$. We will see basis in next section.

3 Basis

For vector space V over field F, an ordered set $(v_1, v_2, ..., v_n)$ is said to be a basis of V if it spans V and is linearly independent.
It means every vector $w \in V$ is uniquely expressed as a linear combination i.e.

$$w = a_1v_1 + a_2v_2 + ... + a_nv_n$$

Proof. Let, vector w can be expressed in 2 different ways as:

$$w = a_1v_1 + a_2v_2 + ... + a_nv_n \rightarrow (1)$$
$$w = b_1v_1 + b_2v_2 + ... + b_nv_n \rightarrow (2)$$

Now, subtract (2) from (1),

$$0_V = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + ... + (a_n - b_n)v_n$$

Since, vectors $v_1, v_2, ..., v_n$ are linearly independent.
So, $a_1 - b_1 = 0$, $a_2 - b_2 = 0$,.....,$a_n - b_n = 0$
$\Rightarrow \ a_1 = b_1, a_2 = b_2, ..., a_n = b_n$
Hence, every vector $w \in V$ can be uniquely expressed. ∎

- **A basis of V gives an isomorphism from V to $\mathbf{F^n}$ i.e. $\mathbf{f : V \rightarrow F^n}$ where $\mathbf{f(w) = (a_1, a_2, ..., a_n), w \in V}$**

Proof. : Here, f is homomorphism because if we add 2 vectors w and w' where $w = a_1v_1 + a_2v_2 + ... + a_nv_n$ and $w' = b_1v_1 + b_2v_2 + ... + b_nv_n$ then
$f(w + w') = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n) = f(w) + f(w')$
& $f(cw) = (ca_1, ca_2, ..., ca_n) = cf(w)$
Now, f is onto because if we have n tuples of scalers in F^n then we can make 'w' by multiplying those scalers with our vectors.
f is one-one also because let,

$$\begin{gathered} f(w) = f(w') \\ \Rightarrow \ (a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n) \\ \Rightarrow \ a_1 = b_1, a_2 = b_2, ...a_n = b_n \\ \Rightarrow \ w = w' \end{gathered}$$

So, f is one-one. ∎

Theorem: **If V is a finite dimensional vector space over a field F then if S is a finite set that spans V, there is a subset of S which forms a basis for V**

Proof. : If S is a linearly independent set then we are done because by definition, S is linearly independent set and spans V , So, it forms a basis.
Suppose, if not, i.e. S is a linearly dependent set.
Now, consider the set $S = \{v_1, v_2, ..., v_n\}$ and relation:
$a_1v_1 + a_2v_2 + ... + a_nv_n = 0 \to (1)$
with some $a_i \neq 0$
Now, without loss of generality,
Suppose, $a_n \neq 0$
Then, from equation (1),
$a_nv_n = -(a_1v_1 + a_2v_2 + ... + a_{n-1}v_{n-1}) \in V$
Now, use the fact that we are in a field and we have a non-zero element in the field, So, we can write its multiplicative inverse. So, a_n^{-1} exists.
Then, $v_n = \frac{-1}{a_n}(a_1v_1 + a_2v_2 + ... + a_{n-1}v_{n-1})$
It means $v_n \in span(v_1, v_2, ...v_{n-1})$
It means, if we could write something in n things then we could also write it in $(n-1)$ things.
So,$span(v_1, v_2, ..., v_n) = span(v_1, v_2, ..., v_{n-1}) = V$
Now, if this set $\{v_1, v_2, ..., v_{n-1}\}$ is linearly independent then we are done and if not, repeat this process finitely many times because we have started with a finite set S. At the end, we may get an empty set which is a basis for $\{0\}$ vector space.
This completes the proof. ■

Theorem: If $L = \{\mathbf{w_1}, \mathbf{w_2}, ..., \mathbf{w_n}\}$ is a linearly independent set in V then L can be extended to a set which will form a basis of V.

Proof. : 1) If L spans V, we are done because according to definition, set L is linearly independent and spans V, so it will definitely form a basis.
2) If not,
Let S is a finite set which spans V. Now, assume, there exists a vector $v \in S$ such that $v \notin span(L)$ because if everything in S is written as a linear combination of things which are in L and everything in V can be written as a linear combination of things which are in S then we would have written everything in V as a linear combination of things in L but here L did not span V. So, there must be some vector in S which is not in the span of L. Then,
Claim: $L \cup \{v\}$ is linearly independent set. Now, consider the relation,

$$\sum_{i=1}^{m} a_iw_i + bv = 0$$

Here, 'b' should be zero otherwise 'v' will be in the span of L because $v = \frac{-1}{b}(\sum_{i=1}^{m} a_iw_i)$ but we assume v is not in $span(L)$
Hence, $\sum_{i=1}^{m} a_iw_i = 0$, So, all $a_i = 0$ for $1 \leq i \leq m$.
Let, $L' = L \cup \{v\}$
If L' spans S, we are done otherwise repeat this procedure finite number of times because S is finite and we will get a basis for V.
This completes the proof. ■

Theorem: **If $\mathbf{S} = \{\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_n}\}$ spans $\boldsymbol{V}$ & $\mathbf{L} = \{\mathbf{w_1}, \mathbf{w_2}, ..., \mathbf{w_m}\}$ is a linearly independent set in $\boldsymbol{V}$.**
Then, $\mathbf{n \geq m}$
i.e. spanning sets are bigger than or equal to linearly independent sets.

Proof. : Since, S spans V, we have

$$w_j = \sum_{i=1}^{n} a_{ij} v_i$$

Now, L is linearly independent set, So,

$$0 = \sum_{j=1}^{m} c_j w_j$$

Now, replace the value of w_j,we get,

$$\begin{aligned} 0 &= \sum_{j=1}^{m} c_j \left(\sum_{i=1}^{n} a_{ij} v_i\right) \\ &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} c_j\right) v_i \end{aligned}$$

Now, if we have that $\sum_{j=1}^{m} a_{ij} c_j = 0$ for all i with some $c_j \neq 0$ then the set L could not be linearly independent because set L will be linearly independent if all c_j are zero and then $\sum_{j=1}^{m} a_{ij} c_j = 0$
Now, here in $\sum_{j=1}^{m} a_{ij} c_j = 0$ with $1 \leq i \leq n$, we have n equations and m unknowns in system of simultaneous linear equations i.e.

$$\begin{gathered} a_{11}c_1 + a_{12}c_2 + ... + a_{1m}c_m = 0 \\ a_{21}c_1 + a_{22}c_2 + ... + a_{2m}c_m = 0 \\ ..... \\ ..... \\ a_{n1}c_1 + a_{n2}c_2 + ... + a_{nm}c_m = 0 \end{gathered}$$

Now, as we know, If we have more unknowns than equations ($m > n$) then we can always find a non-trivial solution. It means, it is possible that c_j ($j = 1, 2, ..., m$) will be non-zero. So, for $m > n$, it contradicts our hypothesis that set $L = \{w_1, w_2, ..., w_m\}$ is linearly independent because in that case all c_j must be zero. So, in case of $m > n$, we get the contradiction.
Hence, $m \leq n$
This completes the proof. ■

Corollary:
1) All the bases of $\boldsymbol{V}$ have the same no. of elements & number of elements in the basis is called the dimension of $\boldsymbol{V}$. The elements of a basis are called **basis vectors**. For every vector space, there exists a basis. If the dimension of V is finite then V is finite-dimensional otherwise infinite-dimensional.

Proof. : Let, we have 2 bases B and B'. Since, B spans and B' is linearly independent.
So, from previous theorem,
Number of elements in $B \geq$ Number of elements in B'
Similarly,
Since, B' spans and B is linearly independent. So,
Number of elements in B' $\geq$ Number of elements in B
So, from the above 2 facts,
Number of elements in $B =$ Number of elements in B' ■

2) If S is a spanning set then no. of elements in $S \geq \dim(V)$
As we have seen previously, we can reduce the spanning set to get a basis. So, no. of elements in S should be atleast the no. of elements in a basis.

3) If L is a linearly independent set then no. of elements in $L \leq \dim(V)$
As we have seen previously, we can always increase a linearly independent set to get a basis. So, no. of elements in L should be $\leq$ number of elements in basis(dim(V)).

- **Suppose, $W \subseteq V$ and let $W = \{\mathbf{w_1}, \mathbf{w_2}, ..., \mathbf{w_m}\}$ is a basis for W then $\{\mathbf{w_1}, \mathbf{w_2}, ..., \mathbf{w_m}, \mathbf{v_{m+1}}, ..., \mathbf{v_n}\}$ will form a basis of V which means any basis of W can be extended to form a basis of V.**

  Proof. : Since, original set $\{w_1, w_2, ..., w_n\}$ is a linearly independent set in V & spans W. As we have seen previously, we can always take a linearly independent set and extend it to a basis.
  This completes the proof. ■

- Consider a map,

$$f \colon V \to V/W$$

such that

$$v \mapsto v + W$$

f is called the **canonical map**.
Here, $\{\mathbf{f(v_{m+1})}, \mathbf{f(v_{m+2})}, ..., \mathbf{f(v_n)}\}$ **forms a basis of quotient space V/W.**

Proof. : Here, we need to prove 2 things :
1) set $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ spans V/W
2) set $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ is linearly independent
Here, W is a subspace of V.
Let, set $R = \{w_1, w_2, ..., w_m\}$ is a basis for W and
set $S = \{w_1, w_2, ..., w_m, v_{m+1}, v_{m+2}, ..., v_n\}$ is a basis for V because if we have $\{w_1, w_2, ..., w_m\}$ is a basis for W then we can extend it to get a basis for V

Let, $x \in V/W$ and $x = v + W$, where, $v \in V$
We can write $x = v + W$ as :
$x = a_1w_1 + a_2w_2 + ... + a_mw_m + a_{m+1}v_{m+1} + ... + a_nv_n + W$ [Since,S is a basis]
Since, $a_1w_1 + a_2w_2 + ... + a_mw_m = 0$ [Since, R is a basis]
So, $x = a_{m+1}v_{m+1} + a_{m+2}v_{m+2} + ... + a_nv_n + W$
$\Rightarrow x = a_{m+1}v_{m+1} + W + a_{m+2}v_{m+2} + W + ... + a_nv_n + W$
$\Rightarrow x = a_{m+1}(v_{m+1} + W) + a_{m+2}(v_{m+2} + W) + ... + a_n(v_n + W)$
$\Rightarrow x = a_{m+1}f(v_{m+1}) + a_{m+2}f(v_{m+2}) + ... + a_nf(v_n + W)$
So, $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ spans V/W
Now, we will prove that set $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ is linearly independent.
Consider, $\{c_1f(v_{m+1})+c_2f(v_{m+2})+....+c_nf(v_n) = 0'\}$ where $0' \in W$ and $c_1, c_2, ..., c_n \in F$
$\Rightarrow c_1(v_{m+1} + W) + c_2(v_{m+1} + W) + ... + c_n(v_n + W) = 0'$
$\Rightarrow c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n + W = 0'$
$\Rightarrow c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n + W = 0 + W$
$\Rightarrow c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n \in W$
Let, $w = c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n$ Since, set R forms a basis for W and w is in W. So, w can also be written as :
$w = a_1w_1 + a_2w_2 + ... + a_mw_m$
So, $c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n = a_1w_1 + a_2w_2 + ... + a_mw_m$
$\Rightarrow c_1v_{m+1} + c_2v_{m+1} + ... + c_nv_n - a_1w_1 - a_2w_2 - ..... - a_mw_m = 0$ Since, set S is a basis.
So, $c_1 = 0, c_2 = 0, ...c_n = 0$ which implies set $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ is linearly independent.
Hence, $\{f(v_{m+1}), f(v_{m+2}), ..., f(v_n)\}$ forms a basis of quotient space V/W. ■

- **If subspace of V is $\mathbf{W' = span\{v_{m+1}, ..., v_n\}}$ then W' is isomorphic to V/W.**
  Here, quotient space V/W sits within vector space V.

- **If W is a subspace of V spanned by $\{\mathbf{w_1, w_2, ...w_m}\}$ and W' is another subspace which is spanned by $\{\mathbf{v_{m+1}, v_{m+2}, ..., v_n}\}$**
  Then $W \cap W' = \mathbf{0_V}$

Proof. :
Suppose, $w \in W$ and $w' \in W'$ then we can write w and w' as :
$w = a_1w_1 + a_2w_2 + ... + a_nw_m \rightarrow (1)$
$w' = a_{m+1}v_{m+1} + a_{m+2}v_{m+2} + ... + a_nv_n \rightarrow (2)$
Now, suppose $w = w'$ means there is a common vector in sub-spaces W and W'. Now, We will show that this common vector must be only zero vector 0_V
Subtract equation (2) from equation (1),
$0 = w - w'$
$0 = a_1w_1 + a_2w_2 + ... + a_nw_m - a_{m+1}v_{m+1} - a_{m+2}v_{m+2} + ... - a_nv_n$
Since, set $\{w_1, w_2, ...w_m, v_{m+1}, v_{m+2}, ..., v_n\}$ is linearly independent set and forms a basis for V.

So, each $a_i = 0$.From equation (1) and (2),
$\Rightarrow w = w' = 0$
This completes the proof. ■

- **We have an isomorphism between $\boldsymbol{W} \times \boldsymbol{W'}$ and $\boldsymbol{V}$ i.e.**

$$W \times W' = \text{(w,w'); w} \in W \text{ \& w'} \in W'$$

more natural map for this will be :

$$\text{(w,w')} \mapsto \text{w+w'}$$

Proof. First, we will show that there is a homomorphism/ linear map/linear transformation which means :

$$\text{f(s+t) = f(s) + f(t) \&}$$
$$\text{f(cs) = cf(s)}$$

where s, t are vectors in vector space and 'c' is a scalar from field. Here, map is like :

$$(w_1, w_1') + (w_2, w_2') = (w_1 + w_2, w_1' + w_2')$$
$$c(w, w') = (cw, cw')$$

where, let $w_1, w_2 \in W$ and $w_1', w_2' \in W'$
It is clearly a linear map. Now, to show bijections in Vector Spaces, always relate injections with linear independence and surjections with span.
Here, it shows surjectivity because $\{v_1, ..., v_n\}$ spans V. So, everything in V can be written as a linear combination of $\{v_1, ..., v_n\}$. So, if we take 1^{st} part of linear combination from w and 2^{nd} part from w' and add up these, we will get whatever vector we want in vector space V. So, surjectivity follows from spanning.
Now, Injectivity comes from linear independence.
Suppose, $f(w_1, w_1') = f(w_2, w_2')$
$\Rightarrow w_1 + w_1' = w_2 + w_2'$
$\Rightarrow w_1 - w_2 = w_1' - w_2'$
Since, $w_1 - w_2 \in W$ and $w_1' - w_2' \in W'$
Let, common vector is v. So, $w_1 - w_2 = v$ and $w_1' - w_2' = v$
So, $v \in W \cap W'$ which implies $v = 0_V$
Hence, $w_1 - w_2 = 0 \Rightarrow w_1 = w_2$ and $w_1' - w_2' = 0 \Rightarrow w_1' = w_2'$
This completes the proof. ■

- **Suppose, $\boldsymbol{W}$ is a subspace of $\boldsymbol{V}$ and there is another subspace $\boldsymbol{W'}$ of $\boldsymbol{V}$ such that the composition map**

$$W' \to V \to V/W$$

i.e.

$$w' \mapsto w' \mapsto w' + W$$

gives a linear isomorphism from *W'* to *V/W*

- ***V* is isomorphic to *W* $\times$ *V/W***
  i.e.

$$V \cong W \times V/W$$

Now, $dim(V) = dim(W) + dim(V/W)$ or we can also write it as : $dim(V) = dim(Ker(f)) + dim(Im(f))$.