115A , Winter 2023

Lecture 8

Fr, Jan 27

• We talked about how important it is to identify subsets S of a vector space V that generate (span) V and are in some sense "minimal" (or most efficient) with this property.

Today we'll study more in depth such sets, proving that such "minimal generating sets" S are automatically linearly independent, and have the remarkable property that any vector in V can be uniquely written as a linear combination of vectors in S.

We'll call such S, basis for V

8.1 Definition A linearly independent subset S of a vector space V that generates (spans) V is called a basis for V

8.2 Example Let $V = \mathbb{R}^3$ and

$S = \{(1,0,0), (0,1,0), (0,0,1)\}$

Then S is a basis for V

Indeed: we already showed that $(1,0,0), (0,1,0), (0,0,1)$ are linearly independent vectors in $\mathbb{R}^3$. And if $v = (a,b,c) \in \mathbb{R}^3$ is an arbitrary vector, then $v = a(1,0,0) + b(0,1,0) + c(0,0,1)$. Thus, S spans V as well

8.3 Exercise Let $V = M_{2\times 2}(\mathbb{R})$ and consider the set

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Show that S is a basis for V.

Solution We already showed in an exercise on Monday (see 6.13) that S spans V. If

we would have $a\begin{pmatrix}1&0\\0&0\end{pmatrix}+b\begin{pmatrix}0&1\\0&0\end{pmatrix}$
$+c\begin{pmatrix}0&0\\1&0\end{pmatrix}+d\begin{pmatrix}0&0\\0&1\end{pmatrix}=0$

then this entails

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

so $a=0$, $b=0$, $c=0$, $d=0$
showing that S is lin. indep.

$\boxtimes$

$\boxed{8.4 \text{ Example}}$ if F is a field and $V=F[X]$ is the vector space over F of all polynomials in undetermined X and coefficients in F
then $S=\{1, X, X^2, X^3, \dots\}$ is a basis for V.

indeed, we already showed that $\mathrm{span}(S)=V$. if $a_0, a_1, \dots \in F$ are so that $a_0\cdot 1+a_1X+a_2X^2+\dots+a_nX^n$
$=0$

then by the definition of the polynomials we must have $a_0 = 0, a_1 = 0, \dots, a_n = 0$ showing that S is lin. indep. as well

8.5. Theorem. Let V be a vector space. A set $S = \{v_1, \dots, v_n\} \subset V$ is a basis for V iff any vector $v \in V$ can be uniquely expressed as a linear combination of elements in S, i.e., there exist unique scalars $c_1, c_2, \dots, c_n \in F$ such that $v = c_1 v_1 + c_2 v_2 + \dots + c_n v_n$

$\boxed{\text{Proof}}$, "$\Rightarrow$" if $S = \{v_1, \dots, v_n\}$ is a basis for V, / $\mathrm{span}(S) = V$, so if $v \in V$ is an arbitrary vector in V, then there exist $c_1, \dots, c_n \in F$ such that $v = \sum_{i=1}^{n} c_i v_i$.

If $a_1, \dots, a_n \in F$ are other scalars such that $v = \sum_{i=1}^{n} a_i v_i$ as well,

then $\sum_{i=1}^{n} c_i v_i = \sum_{i=1}^{n} a_i v_i$

so by cancellation Thus we get

$$\sum_{i=1}^{n} c_i v_i - \sum_{i=1}^{n} a_i v_i = 0$$

which using assoc. & commutativity of addition + distributivity of scalar multiplication gives

$$(*) \quad (c_1 - a_1)v_1 + (c_2 - a_2)v_2 + \cdots + (c_n - a_n)v_n = 0$$

But since $S = \{v_1, \ldots, v_n\}$ is a basis, the vectors $v_1, \ldots, v_n$ are lin. independent, so this implies all coefficients $c_i - a_i$ in $(*)$ must be equal to 0, thus

$$c_1 = a_1, \quad c_2 = a_2, \ldots, c_n = a_n$$

So we showed v can be expressed in only one way as a linear combination of $v_1, \ldots, v_n$.

"$\Leftarrow$" if any $v \in V$ can be expressed in a unique way as lin. comb. of $S = \{v_1, \dots, v_m\}$, then in particular $\mathrm{span}(S) = V$.

If we would have

$$c_1 v_1 + c_2 v_2 + \dots + c_m v_m = 0$$

for some $c_1, \dots, c_m \in \mathbb{F}$, then by uniqueness, since we also have

$$0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 v_m = 0$$

it follows that $c_1 = 0, c_2 = 0, \dots, c_m = 0$

Thus $\{v_1, \dots, v_m\}$ lin. indep.

so S is a basis

8.6. Theorem Let S be a finite subset of the vector space V. If $\mathrm{span}(S) = V$ (i.e. if S generates V) then there exists a subset $S' \subset S$ such that S' is a basis for V.

$\boxed{\text{Proof}}$. If $S = \{0\}$ then $\mathrm{span}(S) = \{0\}$

so " $\{0\}$ and S is a basis for V.

if S contains at least one non-zero element, say $u_1 \neq 0$, then $\{u_1\}$ is linearly independent (see 7.6)

We then continue to choose (if possible!) $u_2, \dots, u_k$ in S so that $u_1, \dots, u_k$ are linearly independent, until this is no longer possible (Note that this must be the case, because S is finite!)

This happens if either we have exhausted all S, i.e. if

(a) $\{u_1, \dots, u_k\} = S$, or if

(b) any $u \in S$ that's not among $u_1, \dots, u_k$ is so that $u_1, \dots, u_k, u$ is linearly dependent.

In case we have (a), it means $S = \{u_1, \dots, u_k\}$ is lin. indep. and since we also have $\text{span}(S) = V$, it follows that S itself is a basis for V and we are done.

in case we have (b), it means there exist scalars $c_1, c_2, \dots, c_k, c$, not all equal to 0, such that

(*) $c_1 u_1 + c_2 u_2 + \dots + c_k u_k + c u = 0$

if $c = 0$, then it would follow that $c_1 u_1 + \dots + c_k u_k = 0$ with $c_1, c_2, \dots, c_k$ not all equal to 0, contradicting the fact that $\{u_1, \dots, u_k\}$ is lin. indep. Thus, $c \neq 0$, and then from (*) we deduce

$$u = -\frac{c_1}{c} u_1 - \frac{c_2}{c} u_2 - \dots - \frac{c_k}{c} u_k$$

showing that $u \in \mathrm{span}(\{u_1, \dots, u_k\})$

Thus, in case (b), we showed that the set $S' = \{u_1, \dots, u_k\} \subset S$ is lin. independent and any

$u \in S \setminus \{u_1, \dots, u_k\}$ is in $\operatorname{span}(S')$. So $\operatorname{span}(S')$ contains $u_1, \dots, u_k$ and all $S \setminus \{u_1, \dots, u_k\}$, so $S \subset \operatorname{span}(S')$.

Since $\operatorname{span}(S) = V$, by (Thm 6.6 or Thm 7.8), it follows that $\operatorname{span}(S')$ contains all $\operatorname{span}(S)$

Thus $\operatorname{span}(S') = V$ (because $\operatorname{span} S = V$)

So S' is lin. indep. & $\operatorname{span}(S') = V$

so $S' \subset S$ is a basis for V ☒

8.7. Corollary If V contains a finite subset $S \subset V$ that generates V, i.e. $\operatorname{span}(S) = V$, then V has a finite basis

$\boxed{8.8. \text{ Example}}$ Here is a concrete example showing how the method of finding a basis S' as a subset of a generating set $S \subset V$ works:

Let $S = \{(1,-1), (-1,1), (0,2), (3,0)\} \subset \mathbb{R}^2$. Show that there exists $S' \subset S$ such that S' is a basis for $\mathbb{R}^2$.

$\boxed{\text{Solution}}$. Since S contains non-zero vectors we can start by choosing $u_1 = (1,-1) \in S$. Then we look at the 2'nd vector $(-1,1)$ in S. We see that

$(-1,1) = -1 \cdot (1,-1)$, i.e. $(-1,1) = -u_1$

so $(-1,1)$ is not lin. indep of u_1

We then take the 3'rd vector in S, $(0,2)$. If $\underbrace{a(1,-1) + b(0,2)}_{= (a+b\cdot 0, -a+2b)} = 0$

then $(a, -a+2b) = (0,0)$ so $a = 0$ and $-0+2b = 0$ so $b = 0$ as well

Thus $u_2 = (0,2) \in S$ is lin. indep. of u_1

so we can ~~take~~ add u_2 to our lin ind. subset S' of S

So by now we have $u_1 = (1,-1)$, $u_2 = (0,2) \in S'$. We see that in fact $\text{span}\{u_1, u_2\} = \mathbb{R}^2$ so we have $(3,0) \in \text{span}\{u_1, u_2\}$ and we can stop and conclude that $S' = \{u_1, u_2\} = \{(1,-1),(0,2)\} \subset S$ is a basis for $\mathbb{R}^2$.

8.9. Theorem (The so-called "Replacement Theorem")

Let V be a vector space. Assume $G \subset V$ is a subset with n vectors that generates V, i.e. $\text{span}(G) = V$. If $L \subset V$ is a linearly independent subset of V with m vectors, then $m \leq n$ and there exists a subset $H \subset G$ containing $n-m$ vectors such that $L \cup H$ generates V.

$\boxed{\text{Proof}}$. We prove this by induction over m (i.e. over the # of elements in the lin. ind. set L).

If $m = 0$, this means L has 0 many elements, i.e. $L = \emptyset$ and we can just take $H = G$, which satisfies the required conditions.

Suppose now that the statement holds true for some $m \geq 0$. We then want to show that the statement holds true for $m+1$ as well.

So let $L = \{v_1, \ldots, v_{m+1}\}$ be linear ind. subset of V. By Thm 7.7 any subset of L is lin. indep., so $\{v_1, \ldots, v_m\}$ is lin. indep. By induction, since we have that the statement of thm is true for m, it follows that $m \leq n$ and that there exist $\{u_1, \ldots, u_{n-m}\} \subset G$

such that $\{v_1, \dots, v_m\} \cup \{u_1, \dots, u_{n-m}\}$ spans V. So in particular, v_{m+1} can be expressed as a linear combination

$$(*) \quad \left\{ v_{m+1} = a_1 v_1 + \dots + a_m v_m + \underbrace{b_1 u_1} + \dots + b_{n-m} u_{n-m} \right.$$

Now notice that in fact we must have $n - m \geq 1$, or else we would have

$$v_{m+1} = a_1 v_1 + \dots + a_m v_m + 0$$

which contradicts the fact that $L = \{v_1, \dots, v_{m+1}\}$ is lin. indep.

In other words, we must have $n \geq m+1$.

Also, in $(*)$ we must have that some b_i are non-zero. Say $b_1 \neq 0$, which allows us to solve in $(*)$ for u_1:

$$(**) \quad \left\{ \begin{aligned} u_1 = \left(-\frac{a_1}{b_1}\right) v_1 + \left(-\frac{a_2}{b_1}\right) v_2 + \dots + \left(-\frac{a_m}{b_1}\right) v_m + \frac{1}{b_1} v_{m+1} \\ + \left(-\frac{b_2}{b_1}\right) u_2 + \dots + \left(-\frac{b_{n-m}}{b_1}\right) u_{n-m} \end{aligned} \right.$$

Thus, if we take $H = \{u_2, \dots, u_{n-m}\}$ then $u_1 \in \operatorname{span}(L \cup H)$ by $(**)$

and since $v_1, \dots, v_m, u_2, \dots, u_{n-m}$

are obviously in $\operatorname{span}(L \cup H)$,

we actually have that

$$\{v_1, \dots, v_m, u_1, \dots, u_{n-m}\} \subset \operatorname{span}(L \cup H)$$

Since $\{v_1, \dots, v_m, u_1, u_2, \dots, u_{n-m}\}$ generates V, it follows (see Thm 6.10) that $\operatorname{span}(L \cup H) = V$ with $H \subset G$ being a subset that contains $(n-m)-1 = n-(m+1)$ elements, showing that statement of Thm holds true for $m+1$.