Lecture 6: Bases Dimension

Unless otherwise stated:

Assume F is a field with more than one element (so that $0 \neq 1$). Let V be a vector space over F.

Last time

Let V be a vector space (over F), and let $S \subseteq V$ be a subset of V. There are two main ways we think about the span of S:

- Bottom-up: FS is the vector space that you can build out of S. Focus on S and see where you can get.
- Top-down: S is enough to build FS. Focus on the vector space FS and find a way to build it.

A set $S \subseteq V$ is *linearly independent* if

 $c_1\mathbf{s}_1 + \cdots + c_n\mathbf{s}_n = \mathbf{0}$ implies $c_1 = \cdots = c_n = 0$ for any $\mathbf{s}_1, \ldots, \mathbf{s}_n \in S$. Otherwise, if there exist c_1, \ldots, c_n with at least some $c_\ell \neq 0$ such that $c_1\mathbf{s}_1 + \cdots + c_n\mathbf{s}_n = \mathbf{0}$, we say S is *linearly dependent*. Other characterizations of linear (in)dependence:

• *S* is *independent* if and only if

 $c_1\mathbf{s}_1 + \cdots + c_n\mathbf{s}_n = d_1\mathbf{s}_1 + \cdots + d_n\mathbf{s}_n$ implies $c_i = d_i$ for $i = 1, \ldots, n$; i.e. each element in FS has a *unique* expression as a linear combination of elements of S.

• S is dependent if and only if

there exists $\mathbf{v} \in S$ such that $\mathbf{v} \in F(S - {\mathbf{v}})$; i.e. there's redundancy in S as a set of building blocks for FS. Bases

Still: Let V be a vector space over F.

A spanning set for V is a subset $S \subseteq V$ such that FS = V. *Think:* S is "enough" to build/generate V.

A basis for V is a linearly independent spanning set. *Think:* S is *minimal* in being "enough" to build/generate V.

Example: We showed last time that $\left\{ \begin{pmatrix} 2\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\3\\1 \end{pmatrix} \right\}$ is a basis of \mathbb{R}^3 .

Example: Another basis of \mathbb{R}^3 is the natural or standard basis

$$\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$$
 where $\mathbf{e}_1 = \begin{pmatrix} 1\\0\\0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0\\1\\0 \end{pmatrix}$, and $\mathbf{e}_3 = \begin{pmatrix} 0\\0\\1 \end{pmatrix}$.

Reflection questions (from last time):

- 1. We have lots of examples of vector spaces now. Can you come up with a basis for each of them? For example, can you find a basis for... (next slide)
 - $V = \mathcal{P}_n(\mathbb{R}) = \{ f \in \mathbb{R}[x] \mid \deg(f) \leq n \} \text{ over } F = \mathbb{R};$
 - $V = M_{2,2}(\mathbb{R}) = \{ 2 \times 2 \text{ matrices w} / \text{ coefs in } \mathbb{R} \}$, over $F = \mathbb{R}$;
 - $V = 0 = \{0\}$, the trivial vector space over a field F;
- 2. Many vector spaces have more than one basis. Under what circumstances will a basis of V be unique?
- 3. Does every vector space even *have* a basis? (How could you prove or disprove?)

Standard bases

There are usually lots of bases of a given vector space, and there will be very concrete examples where "non-standard" bases are important. But generally, we start to think about most of our favorite vector spaces in terms of natural choices of bases already.

The standard basis for... • $V = F^n$ (over F) is

$$\mathcal{E}\{\mathbf{e}_1,\ldots,\mathbf{e}_n\} \quad \text{where} \quad \mathbf{e}_i = (0,\ldots,0,1,0,\ldots,0);$$

• $V = M_{a,b}(F)$ (over F) is $\mathcal{E} = \{E_{i,j} \mid i = 1, \dots, a, j = 1, \dots, b\}$ where

$$E_{i,j} = \begin{pmatrix} 0 & \cdots & 0 & & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$
 ith row in the ith row and jth col);

•
$$V = F[x]$$
 (over F) is $\mathcal{E} = \{1, x, x^2, \dots\} = \{x^{\ell} \mid \ell \in \mathbb{Z}_{\geq 0}\};$
and $V = \mathcal{P}_n(F)$ (over F) is $\mathcal{E} = \{1, x, x^2, \dots, x^n\}$

Putting together what we learned about span, together with the fact that a basis generates all of V we know...

Prop. Let V be a vector space over F, and let B be a basis of V. Then every element $\mathbf{v} \in V$ has a *unique* expression in the form $\mathbf{v} = \sum_{\mathbf{b} \in B} c_{\mathbf{b}} \mathbf{b}$;

i.e. there is a unique way to express \mathbf{v} as a linear combination of elements of B (being smart about order and 0's).

[For example,

$$2\begin{pmatrix}1\\0\\0\end{pmatrix}+5\begin{pmatrix}0\\1\\0\end{pmatrix}, \quad 5\begin{pmatrix}0\\1\\0\end{pmatrix}+2\begin{pmatrix}1\\0\\0\end{pmatrix}, \quad \text{and} \quad 5\begin{pmatrix}0\\1\\0\end{pmatrix}+0\begin{pmatrix}0\\0\\1\end{pmatrix}+2\begin{pmatrix}1\\0\\0\end{pmatrix}$$

all count as the "same" linear combination.]

An ordered basis B is a basis together with a fixed order on its elements.

Note: This is what the book just calls a "basis"; this *not* standard. We'll write

$$B = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$$

to mean the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ considered in *that order*.

Aside: There is no standard notation for ordered bases—the literature uses (), [], etc. *Most* people just use { }, even though technically sets don't have order, but it can be helpful to have separate notation while we're first learning, so we'll use special notation for now.

An ordered basis B is a basis together with a fixed order on its elements). We'll write

 $B = \langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$

to mean the set $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ considered in *that order*.

For now, let's focus on cases where V has a *finite* basis.

yes: F^n , $M_{a,b}(F)$, $\mathcal{P}_n(F) = \{p \in F[x] \mid \deg(p) \leq n\}$ no: F[x]

Examples:

 $\begin{array}{l} \left< \mathbf{e}_1, \dots, \mathbf{e}_n \right> & \text{is the standard ordered basis of } F^n; \\ \left< E_{1,1}, E_{1,2}, \dots, E_{1,b}, \\ E_{2,1} \dots, E_{2,b}, \\ \dots, E_{a,b} \right> & \text{is the standard ordered basis of } M_{a,b}(F); \\ \left< 1, x, x^2, \dots, x^n \right> & \text{is the standard ordered basis of } \mathcal{P}_n(F). \end{array}$

Example:

 $\langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle$, $\langle \mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_2 \rangle$, and $\langle \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_1 \rangle$ are all different ordered bases of \mathbb{R}^3 (corresponding to the same underlying basis). Example. Let's consider the three ordered bases in \mathbb{C}^3 given by

$$\mathcal{E} = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle \qquad \text{with } \mathbf{e}_1 = \begin{pmatrix} 1\\0\\0 \end{pmatrix}, \ \mathbf{e}_2 = \begin{pmatrix} 0\\1\\0 \end{pmatrix}, \ \mathbf{e}_3 = \begin{pmatrix} 0\\0\\1 \end{pmatrix};$$
$$A = \langle \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3 \rangle \qquad \text{with } \mathbf{a}_1 = \begin{pmatrix} 0\\1\\0 \end{pmatrix}, \ \mathbf{a}_2 = \begin{pmatrix} 0\\0\\1 \end{pmatrix}, \ \mathbf{a}_3 = \begin{pmatrix} 1\\0\\0 \end{pmatrix}; \text{ and}$$
$$B = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \rangle \qquad \text{with } \mathbf{b}_1 = \begin{pmatrix} 1\\0\\0 \end{pmatrix}, \ \mathbf{b}_2 = \begin{pmatrix} 1\\1\\0 \end{pmatrix}, \ \mathbf{b}_3 = \begin{pmatrix} 1\\1\\1 \end{pmatrix}.$$

[How do I know they're bases? One can check that these are each independent sets using the techniques of last time, and the following confirms that they're spanning sets as well.] We can solve relevant systems of linear equations (e.g. $\mathbf{x} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + c_3\mathbf{v}_3$) to find

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = x \mathbf{e}_1 + y \mathbf{e}_2 + z \mathbf{e}_3,$$

= $y \mathbf{a}_1 + z \mathbf{a}_2 + x \mathbf{a}_3,$ and
= $(x - y) \mathbf{b}_3 + (y - z) \mathbf{b}_2 + z \mathbf{b}_3.$

Encoding V using an ordered basis

Let $B = \langle \mathbf{b}_1, \dots, \mathbf{b}_n \rangle$ be an ordered basis of a vector space V (over the field F). For each $\mathbf{v} \in V$, we again note that the expression

$$\mathbf{v} = c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n$$

is unique, meaning that there is a bijection

$$\begin{array}{cccc} F^n & \longrightarrow & V \\ (c_1, \dots, c_n) & \longmapsto & c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n. \end{array}$$
(*)

Recall: A map $f: X \to Y$ is well-defined if for all $x \in X$ we have (1) f(x) is uniquely identified and (2) $f(x) \in Y$.

A bijection, or bijective function, is a function $f : X \to Y$ that is both injective, meaning

 $f(x_1) = f(x_2)$ implies $x_1 = x_2$,

and surjective, meaning

for all
$$y \in Y$$
, there is some $x \in X$ such that $f(x) = y$.

The function in (*) is *well-defined* because *B* is ordered;

it is surjective because B is a spanning set; and

it is *injective* because B is independent.

In other words, the definition of ordered basis is *exactly* what's needed for (*) to be well-defined and bijective.

Encoding V using an ordered basis

Let $B = \langle \mathbf{b}_1, \dots, \mathbf{b}_n \rangle$ be an ordered basis of a vector space V (over F). Recall that a function is bijective if and only if it's invertible; so take (*) from the last and turn it around (invert it) to get the bijection

$$\operatorname{Rep}_B: \begin{array}{ccc} V & \longrightarrow & F^n \\ c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n & \longmapsto & (c_1, \dots, c_n). \end{array}$$

We call c_1, \ldots, c_n the coordinates of

$$\mathbf{v} = c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n$$

with respect to B, and

$$\operatorname{Rep}_{B}(\mathbf{v}) = \begin{pmatrix} c_{1} \\ c_{2} \\ \vdots \\ c_{n} \end{pmatrix}$$

is the representation of \mathbf{v} with respect to B.

Example: Using the ordered bases \mathcal{E} , A, and B of $V = \mathbb{C}$ from before, we have

$$\operatorname{Rep}_{\mathcal{E}}\left(\begin{pmatrix}x\\y\\z\end{pmatrix}\right) = \begin{pmatrix}x\\y\\z\end{pmatrix}, \quad \operatorname{Rep}_{A}\left(\begin{pmatrix}x\\y\\z\end{pmatrix}\right) = \begin{pmatrix}y\\z\\x\end{pmatrix}, \quad \text{and} \quad \operatorname{Rep}_{B}\left(\begin{pmatrix}x\\y\\z\end{pmatrix}\right) = \begin{pmatrix}x-y\\y-z\\z\end{pmatrix}.$$

You try.

1. Consider the ordered basis $B = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \rangle$ of \mathbb{Q}^3 , where

$$\mathbf{b}_1 = \begin{pmatrix} 1\\1\\0 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 1\\0\\-1 \end{pmatrix}, \quad \text{and} \quad \mathbf{b}_3 = \begin{pmatrix} 0\\-2\\1 \end{pmatrix}.$$

(You *could* verify that *B* is independent by solving

$$c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3 = \mathbf{0} \text{ for } c_1, c_2, c_3 \in \mathbb{Q}.$$

Compute $\operatorname{Rep}_B(\mathbf{u})$ for

(i)
$$\mathbf{u} = \begin{pmatrix} 5\\0\\1 \end{pmatrix}$$
 and (ii) $\mathbf{u} = \begin{pmatrix} x\\y\\z \end{pmatrix}$ (where $x, y, z \in \mathbb{Q}$).

[*Hint.* Start by solving $\mathbf{u} = c_1\mathbf{b}_1 + c_2\mathbf{b}_2 + c_3\mathbf{b}_3$ for c_1, c_2, c_3 .]

2. Let V be a vector space with ordered basis $B = \langle \mathbf{b}_1, \dots, \mathbf{b}_n \rangle$, so that $\operatorname{Rep}_B(\mathbf{u}) = (c_1, \dots, c_n)$ means $\mathbf{u} = c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n$.

Verify that, for any $\mathbf{u}, \mathbf{v} \in V$ and $\alpha \in F$, we have

$$\operatorname{Rep}_B(\mathbf{u} + \mathbf{v}) = \operatorname{Rep}_B(\mathbf{u}) + \operatorname{Rep}_B(\mathbf{v})$$
 and $\operatorname{Rep}_B(\alpha \mathbf{u}) = \alpha \operatorname{Rep}_B(\mathbf{u}).$

[*Hint*. Start the first identity by writing $\mathbf{v} = d_1\mathbf{b}_1 + \cdots + d_n\mathbf{b}_n$ and computing (I) $\operatorname{Rep}_B(\mathbf{u})$ and $\operatorname{Rep}_B(\mathbf{v})$, so to compute $\operatorname{Rep}_B(\mathbf{u}) + \operatorname{Rep}_B(\mathbf{v})$ using vector addition in F^n ; and (II) $\mathbf{u} + \mathbf{v}$ (collecting like terms) and using *that* to compute $\operatorname{Rep}_B(\mathbf{u} + \mathbf{v})$.]

Dimension

Theorem

If V has bases B and C, then |B| = |C|.

(Proof in the finite case in a moment...)

In particular, if V has a basis B, then |B| is a statistic for V, not just B.

[Aside: This is a statement about vector spaces with infinite bases as well, where |B| = |C| means that there exists a bijection $B \rightarrow C$.]

Definition. We call the size of a basis B of V the dimension of V, denoted $\dim(V) = |B|.$

If we need to emphasize what field we're working with, we can write $\dim_F(V)$.

Examples.

- $\dim(F^n) = n$ because $|\{\mathbf{e}_1, \dots, \mathbf{e}_n\}| = n;$
- $\dim(M_{a,b}(F)) = ab$ because $|\{E_{i,j} \mid i = 1, \dots, a, j = 1, \dots, b\}| = ab;$
- $\dim(\mathcal{P}_n(F)) = n+1$ because $|\{1, x, \dots, x^n\}| = n+1;$
- $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ because $\{1, i\}$ is a basis for \mathbb{C} over \mathbb{R} .

Thm. (Finite case) If V has finite bases B and C, then |B| = |C|.

Lemma. (Exchange Lemma)

Let $B = {\mathbf{b}_1, \dots, \mathbf{b}_n}$ be a (finite^{*}) basis of V and let $\mathbf{v} \in V - {\mathbf{0}}$. Then there exists an element $\mathbf{b} \in B$ such that $B' = (B - {\mathbf{b}}) \cup {\mathbf{v}}$ is also a basis of V. (* also true in infinite case.)

Proof. Fix $\mathbf{v} \in V - \{\mathbf{0}\}$. Since B is a basis of V and $\mathbf{v} \neq 0$, we can write

$$\mathbf{v} = c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n$$

for some $c_i \in F$ not all 0. Take ℓ such that $c_{\ell} \neq 0$ and solve for \mathbf{b}_{ℓ} :

$$\mathbf{b}_{\ell} = \frac{1}{c_{\ell}} \mathbf{v} + \sum_{\substack{i=1,\dots,n\\i\neq\ell}} \left(\frac{-c_i}{c_{\ell}}\right) \mathbf{b}_i \in FB', \text{ where } B' = (B - \{\mathbf{b}_{\ell}\}) \cup \{\mathbf{v}\}. \quad (\diamond)$$

To see that B' spans V, we see that for any $\mathbf{u} \in V$, we have

$$\begin{split} \mathbf{u} &= d_1 \mathbf{b}_1 + \dots + d_n \mathbf{b}_n = d_\ell \mathbf{b}_\ell + \sum_{\substack{i=1,\dots,n\\i \neq \ell}} d_i \mathbf{b}_i & \text{for some } d_i \in F, \\ &= d_\ell \bigg(\frac{1}{c_\ell} \mathbf{v} + \sum_{\substack{i=1,\dots,n\\i \neq \ell}} \bigg(\frac{-c_i}{c_\ell} \bigg) \mathbf{b}_i \bigg) + \sum_{\substack{i=1,\dots,n\\i \neq \ell}} d_i \mathbf{b}_i & \text{by } (\diamond) \\ &= \frac{d_\ell}{c_\ell} \mathbf{v} + \sum_{\substack{i=1,\dots,n\\i \neq \ell}} \bigg(\frac{-d_\ell c_i}{c_\ell} + d_i \bigg) \mathbf{b}_i \in FB'. & \frac{\left| \begin{array}{c} \mathsf{So} \ FB' = V. \\ \mathsf{FB'} \subseteq V \ \mathsf{already } \mathsf{by } \mathsf{closure} \right|}{\mathsf{FB'} \subseteq V \ \mathsf{already } \mathsf{by } \mathsf{closure}} \end{split}$$

Lemma. (Exchange Lemma)

Let $B = {\mathbf{b}_1, \dots, \mathbf{b}_n}$ be a (finite) basis of V and let $\mathbf{v} \in V - {\mathbf{0}}$. Then there exists an element $\mathbf{b} \in B$ such that $B' = (B - {\mathbf{b}}) \cup {\mathbf{v}}$ is also a basis of V.

Proof (continued). We fixed $\mathbf{v} \in V - \{\mathbf{0}\}$, wrote $\mathbf{v} = c_1 \mathbf{b}_1 + \cdots + c_n \mathbf{b}_n$, and took ℓ such that $c_{\ell} \neq 0$. Then we defined $B' = (B - \{\mathbf{b}_{\ell}\}) \cup \{\mathbf{v}\}$ and showed FB' = V. It remains to show that B' is independent. To that end, suppose (for some $\alpha, \alpha_i \in F$) we have

$$\mathbf{0} = \alpha \mathbf{v} + \sum_{\substack{i=1,\dots,n\\i\neq\ell}} \alpha_i \mathbf{b}_i$$
 (how we always start
to test for dependence)
$$= \alpha \left(c_1 \mathbf{b}_1 + \dots + c_n \mathbf{b}_n\right) + \sum_{\substack{i=1,\dots,n\\i\neq\ell}} \alpha_i \mathbf{b}_i,$$
 using our formula for \mathbf{v} ,
$$= \alpha c_\ell \mathbf{b}_\ell + \sum_{\substack{i=1,\dots,n\\i\neq\ell}} (\alpha c_i + \alpha_i) \mathbf{b}_i,$$
 combining like terms.

But B is a basis (and therefore is independent), so this implies that

 $\alpha c_{\ell} = 0$ and $\alpha c_i + \alpha_i = 0$ for all $i \neq \ell$. We assumed $c_{\ell} \neq 0$, and hence $\alpha = 0$; and this further implies that $\alpha_i = 0$ for all $i \neq \ell$ (as desired).

So B' is independent, and is therefore a basis. \Box

Lemma. (Exchange Lemma) Let $B = {\mathbf{b}_1, \ldots, \mathbf{b}_n}$ be a (finite^{*}) basis of V and let $\mathbf{v} \in V - {\mathbf{0}}$. Then there exists an element $\mathbf{b} \in B$ such that $B' = (B - {\mathbf{b}}) \cup {\mathbf{v}}$ is also a basis of V.

Note: Our proof more specifically showed... Let $B = {\mathbf{b}_1, ..., \mathbf{b}_n}$ be a (finite) basis of V and let $\mathbf{v} = c_1 \mathbf{b}_1 + \cdots + c_n \mathbf{b}_n \in V - {\mathbf{0}}$. Then for any ℓ such that $c_{\ell} \neq 0$, we have that $B' = (B - {\mathbf{b}_{\ell}}) \cup {\mathbf{v}}$ is also a basis of V. (We cooked up a specific recipe for finding *what* to replace with \mathbf{v} .)

Theorem (Ch Two, §III, Thm. 2.4) If V has finite bases B and C, then |B| = |C|. Namely, dimension is well-defined.

Proof (sketch). [See book for full deatails] Inductively move from $B \to C$, replacing one term at a time. Step 0: Let $B_1 = B$. Step i: If $C \subseteq B_i$, you're done. Otherwise... • Take some element $\mathbf{v}_i \in C - B$, and find $\mathbf{u}_i \in B_0 - C$ such that the coefficient of \mathbf{u}_i in $\operatorname{Rep}_{B_i}(\mathbf{v}_i)$ is not 0. • Let $B_{i+1} = (B_i - {\mathbf{u}_i}) \cup {\mathbf{v}_i}$. (Recurse step *i* until $C \subseteq B_i$.)

Homework: Show that if $C \subseteq B_i$ with C spanning V and B_i being independent, then $C = B_i$.

Epilog: Some tips for translating between lecture and the book.

- The book defines a basis as an ordered set (that spans and is independent)—i.e. what we're calling an ordered basis. This isn't standard, so we'll differentiate between the two.
- The book notationally distinguishes between a linearly independent spanning set $B = \{\vec{\beta}_1, \vec{\beta}_2, \dots, \vec{\beta}_n\}; \quad \text{(set)}$

and an ordered linearly independent spanning set (the thing they call basis)

$$B = \langle \beta_1, \beta_2, \dots, \beta_n \rangle. \quad \text{(ordered set)}$$

In $\[Mathebbe]$, those angle brackets *aren't* just < and >; the angle bracket symbols are more shallow (e.g. < versus \langle). They're coded as \langle and \rangle ("left angle" and "right angle"). You also have the shortcuts \< and \> coded in our preambles for those two commands, respectively.

Note: There is no standard convention for what to use for notation in the second case. If you're looking at other resources, keep an eye out for () (thinking of an ordered basis as a sequence) or []. But mostly, folks just use $\{$ $\}$, even though technically sets don't have order, and use words to specify that they've fixed an order.