Lecture 4:

Properties of vector spaces
Subspaces
Linear combinations
Span

Unless otherwise stated:
Assume F is a field with more than one element (so that $0 \neq 1$).

Last time: A field F, much like $\mathbb{R}$ or $\mathbb{C}$, is a set with addition and multiplication, with lots of familiar properties (commutative, associative, and distributive properties, identity elements 0 and 1, inverses).

More examples: $\mathbb{Q}$, $\mathbb{F}_2$.

A vector space V (over a field F), much like $\mathbb{R}^n$, is a set with addition and scaling from F, with properties like distributivity, associativity of scaling, and $1 \cdot \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$. More examples: F^n, $F[x]$, $\{f \in F[x] \mid \deg(f) \leqslant n\}$, $M_{m,n}(F)$. The trivial vector space (over any field F) is $0 = \{0\}$ (with $0 + 0 = 0$ and $c \cdot 0 = 0$ for all $c \in F$).

We proved (in a specific case) that for all $\mathbf{v} \in V$, we have

$$\boxed{V = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}}$$

1. $0 \cdot \mathbf{v} = \mathbf{0}$; and

   Specific case: For any $(x, y, z) \in V$, we have
   $$0 \cdot (x, y, z) = (0 \cdot x, 0 \cdot y, 0 \cdot z) = (0, 0, 0);$$
   and $(0, 0, 0)$ is the additive identity in $\mathbb{R}^3$, and hence is the additive identity in $V \subseteq \mathbb{R}^3$.

2. $\mathbf{v} + (-1) \cdot \mathbf{v} = \mathbf{0}$.

   Specific case: For any $(x, y, z) \in V$, we have
   $$(-1) \cdot (x, y, z) = ((-1)x, (-1) \cdot y, (-1) \cdot z) = (-x, -y, -z);$$
   and $(-x, -y, -z)$ is the additive inverse of (x, y, z) in $\mathbb{R}^3$, and hence is the additive inverse of (x, y, z) in $V \subseteq \mathbb{R}^3$.

More generally, let V be a vector space over a field F. Then for any $v \in V$, we have...

1. $0 \cdot \mathbf{v} = \mathbf{0}$; and

   General proof. Let $\mathbf{v} \in V$. Since $0 + 0 = 0$ in F, we have
   $$0 \cdot \mathbf{v} = (0 + 0) \cdot \mathbf{v} = 0 \cdot \mathbf{v} + 0 \cdot \mathbf{v} \qquad (*)$$
   by the distributive property. Whatever $0 \cdot \mathbf{v}$ is, it has an additive inverse $-(0 \cdot \mathbf{v})$; adding that to both sides gives
   $$\begin{aligned} \mathbf{0} &= 0 \cdot \mathbf{v} + (-(0 \cdot \mathbf{v})) && \text{by the definition of } -(0 \cdot \mathbf{v}), \\ &= (0 \cdot \mathbf{v} + 0 \cdot \mathbf{v}) + (-(0 \cdot \mathbf{v})) && \text{by } (*), \\ &= 0 \cdot \mathbf{v} + (0 \cdot \mathbf{v} + (-(0 \cdot \mathbf{v}))) && \text{by associativity of } +, \\ &= 0 \cdot \mathbf{v}, && \text{by the definition of } -(0 \cdot \mathbf{v}). \end{aligned}$$
   Hence, $\mathbf{0} = 0 \cdot \mathbf{v}$, as desired. □

2. $\mathbf{v} + (-1) \cdot \mathbf{v} = \mathbf{0}$.

   General proof. Let $\mathbf{v} \in V$. We have
   $$\begin{aligned} \mathbf{v} + (-1) \cdot \mathbf{v} &= 1 \cdot \mathbf{v} + (-1) \cdot \mathbf{v}, && \text{since } 1 \cdot \mathbf{v} = \mathbf{v}, \\ &= (1 - 1) \cdot \mathbf{v} && \text{by the distributive property}, = 0 \cdot \mathbf{v}. \end{aligned}$$
   But $0 \cdot \mathbf{v} = \mathbf{0}$ by the previous part. And hence, $\mathbf{v} + (-1) \cdot \mathbf{v} = \mathbf{0}$, as desired. □

Lemma

Let F be a field, and let V be a vector space over F.

1. *The additive identity is unique (i.e. if $\mathbf{a} + \mathbf{v} = \mathbf{v}$ and $\mathbf{b} + \mathbf{v} = \mathbf{v}$ for all $\mathbf{v} \in V$, then $\mathbf{a} = \mathbf{b}$).*
2. *For any $\mathbf{v} \in V$,*
   (a) *the additive inverse of $\mathbf{v}$ is unique (i.e. if $\mathbf{a} + \mathbf{v} = \mathbf{0}$ and $\mathbf{b} + \mathbf{v} = \mathbf{0}$ then $\mathbf{a} = \mathbf{b}$);*
   (b) *$0 \cdot \mathbf{v} = \mathbf{0}$; and* ✓
   (c) *$-\mathbf{v} = (-1) \cdot \mathbf{v}$.* ✓
3. *For any $c \in F$, we have $c \cdot \mathbf{0} = \mathbf{0}$.*

Subspaces

Let V be a vector space (over a field F), and let $W \subseteq V$ be a nonempty subset of V. We say W is a subspace of V if it is also a vector space under the same addition and scaling as V.
Necessary conditions:

- $\mathbf{0} \in W$
- W is closed under addition and scaling: for all $\mathbf{u}, \mathbf{w} \in W$ and $c \in F$, we have

$$\mathbf{u} + \mathbf{w} \in W \qquad \text{and} \qquad c \cdot \mathbf{u} \in W.$$

For any $\mathbf{u}_1, \dots, \mathbf{u}_n \in W$ and $a_1, \dots, a_n \in F$, we call

$$a_1 \cdot \mathbf{u}_1 + \cdots + a_n \cdot \mathbf{u}_n$$

a linear combination of $u_1, \dots, u_n \in W$.
[Think: the sorts of expressions you'll get via iteratively applying scalars and sums.]

Prop. A subset $W \subseteq V$ is a subspace if and only if (1) it's non-empty, and (2) W is closed under linear combinations of any pair of elements (and hence under linear combinations in general).

Proof.
($\Rightarrow$) Assume W is a subspace...
($\Leftarrow$) Assume $W \neq \varnothing$ and is closed under linear combinations... □

Cor. (Subspace critreon) A subset $W \subseteq V$ is a subspace if and only if
(1) it's non-empty, and
(2) for all $\mathbf{u}, \mathbf{w} \in W$ and $c \in F$ we have $\mathbf{u} + c \cdot \mathbf{w} \in W$.

You try

Let $V = \mathbb{R}^2$, and let $a, b, c \in \mathbb{R}$. Consider $W = \{(x, y) \in \mathbb{R}^2 \mid ax + by = c\}$.

(a) Under what circumstances could W be empty?

(b) Under what circumstances could $\mathbf{0} \in W$?

(c) Under what circumstances could W be closed under addition?
[*Hint:* Assume $(x_1, y_1), (x_2, y_2) \in W$, so that $ax_1 + by_1 = c$ and $ax_2 + by_2 = c$. Now, take $(x, y) = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and plug it into $ax + yb$ and compute.]

(d) Under what circumstances would W be closed under scaling?

A linear equation

$$a_1x_1 + \cdots + a_nx_n = b$$

is homogeneous if $b = 0$. (We say terms like a_ix_i have degree 1 since $x_i = x_i^1$, and $b = bx_i^0$ has degree 0. So ever non-zero term in a linear equation has the same degree exactly when $b = 0$.)

Lemma. Consider a linear equation in n variables with coefficients in F. The solution set to that system is a subspace of F^n if and only if that equation is homogeneous. [Otherwise it's a "shift" of a v.s.]

Proof. Consider the equation $a_1x_1 + \cdots + a_nx_n = b$ $(*)$. First, $\mathbf{0}$ is a solution exactly when $b = 0$. Next, if $\mathbf{y} = (y_1, \ldots, y_n)$ and $\mathbf{z} = (z_1, \ldots, z_n)$ are both solutions, that means

$$a_1y_1 + \cdots + a_ny_n = b \quad \text{and} \quad a_1z_1 + \cdots + a_nz_n = b.$$

So

$$\begin{aligned} a_1(y_1 + z_1) + \cdots + a_n(y_n + z_n) &= (a_1y_1 + a_1z_1) + \cdots + (a_ny_n + a_nz_n) \\ &= (a_1y_1 + \cdots + a_ny_n) + (a_1z_1 + \cdots + a_nz_n) \\ &= b + b = 2b. \end{aligned}$$

So $\mathbf{y} + \mathbf{z}$ is a solution to $(*)$ if and only if $2b = b$, i.e. $b = 0$.
Similarly, for $c \in F$,

$$a_1(cy_1) + \cdots + a_n(cy_n) = c(a_1y_1 + \cdots + a_ny_n) = cb.$$

So $c \cdot \mathbf{y}$ is a solution to $(*)$ if and only if $cb = b$; so my solution set is closed under scaling by *any* $c \in F$ if and only if $b = 0$. □

Lemma. Consider a linear equation in n variables with coefficients in F. The solution set to that system is a subspace of F^n if and only if that equation is homogeneous. [Otherwise it's a "shift" of a v.s.]

Lemma. Let U and W be subspaces of a vector space V (over a field F). Then $U \cap W$ is also a subspace of V. [See practice exercises.]

Proposition. Consider a system of linear equations with coefficients in F:

$$(*) \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1, \\ \qquad\qquad \vdots \qquad\quad \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m. \end{cases}$$

Then the set of solutions W is a subspace of F^n if and only if $b_1 = \cdots = b_m = 0$ (all of the equations are homogeneous).

($\Rightarrow$: $\mathbf{0} \in W$ implies $b_i = 0$ for all i.)

Note: From the reading, we saw that the solutions to $(*)$ in general look like

{ (fixed particular solution) + (any solution to associated homogeneous) }

$$= \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} + \text{(vector space of solutions to associated homogeneous)}$$

Let V be a vector space (over F), and let $S \subseteq V$ be a subset of V. The closure of S (under linear combinations) is the set

$$[S] = \{a_1 s_1 + \cdots + a_n s_n \mid n \in \mathbb{Z}_{\geqslant 0}, a_i \in F, s_i \in S\}.$$

We also call $[S]$ the span of S, which is also denoted FS or $\mathrm{span}_F(S)$.

Convention: If $S = \varnothing$, we set $[S] = \{0\}$, then empty linear combination.

Example: Let $\mathbf{v} \in \mathbb{R}^3 - \mathbf{0}$ and let $S = \{\mathbf{v}\}$. Then

$$\mathbb{R}S = \mathbb{R}\mathbf{v} = \{t\mathbf{v} \mid t \in \mathbb{R}\}.$$

Geometrically: $[S]$ is a line through $\mathbf{0}$ in the direction of $\mathbf{v}$.

Example: Let $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3 - \mathbf{0}$ (not parallel) and let $S = \{\mathbf{u}, \mathbf{v}\}$. Then

$$\mathbb{R}S = \mathbb{R}\{\mathbf{u}, \mathbf{v}\} = \{s\mathbf{u} + t\mathbf{v} \mid s, t \in \mathbb{R}\}.$$

Geometrically: $\mathbb{R}S$ is a plane through $\mathbf{0}$ with direction vectors $\mathbf{u}$ and $\mathbf{v}$.

Lemma. (Two.I.2.15)
Let V be a vector space over F, and let $S \subseteq V$.
Then FS is a subspace of V.
Proof. Use the subspace critereon.

Remark. The span FS is also the smallest vector space in V that contains S. (Uniqueness!)

Let V be a v.s. over F, and let $S \subseteq V$.

Question: For a given $\mathbf{v} \in V$, how do we know if $\mathbf{v} \in FS$?

Example: Let $V = \mathbb{R}[x]$, $F = \mathbb{R}$, and $S = \{p, q\}$, where

$$p = x^2 + 3x - 2 \text{ and } q = 2x^2 + 5x - 3.$$

Is $f = -x^2 - 4x + 1$ in $\mathbb{R}S$?

Namely, do there exist $a, b \in \mathbb{R}$ such that $f = ap + bq$? i.e.

$$\begin{aligned} -x^2 - 4x + 1 &= a(x^2 + 3x - 2) + b(2x^2 + 5x - 3) \\ &= (a + 2b)x^2 + (3a + 5b)x + (-2a - 3b)? \end{aligned}$$

Two polynomials are equal exactly when the coefficients match; so comparing coefficients produces the three equations

$$\begin{cases} a + 2b = -1 \\ 3a + 5b = -4 \\ -2a - 3b = 1 \end{cases} \quad \text{which encodes as} \quad \left(\begin{array}{cc|c} 1 & 2 & -1 \\ 3 & 5 & -4 \\ -2 & -3 & 1 \end{array}\right)$$

To finish up: Put into reduced echelon form. If there are solutions, then yes, $f \in FS$. If not, then no, $f \notin FS$.