Week 6

Vector spaces (Section 4.1)

Question	Answer (by example)
What is a vector?	An element of some $\mathbb{R}^m$
What is a mammal?	A cat

Answers (by definition):

> A *mammal* [...] is a vertebrate animal of the class **Mammalia**. Mammals are characterized by the presence of milk-producing mammary glands [...][1]

> A vector is an element of a **vector space**. Vector spaces are characterized by the presence of two operations on their elements: vector addition and scalar multiplication.

Definition 4.1: A *vector space* is a triple $(V, +, \cdot)$ where V is a set (the vectors), and

$$\begin{array}{lll} + & : & V \times V \to V \quad \text{is a function (vector addition),} \\ \cdot & : & \mathbb{R} \times V \to V \quad \text{is a function (scalar multiplication),} \end{array}$$

satisfying the following *axioms* (rules) for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and all $\lambda, \mu \in \mathbb{R}$.

1.	$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$	commutativity
2.	$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$	associativity
3.	There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$	zero vector
4.	There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$	negative vector
5.	$1 \cdot \mathbf{v} = \mathbf{v}$	identity element
6.	$(\lambda \cdot \mu)\mathbf{v} = \lambda \cdot (\mu \cdot \mathbf{v})$	compatibility of $\cdot$ and $\cdot$ in $\mathbb{R}$
7.	$\lambda(\mathbf{v} + \mathbf{w}) = \lambda\mathbf{v} + \lambda\mathbf{w}$	distributivity over $+$
8.	$(\lambda + \mu)\mathbf{v} = \lambda\mathbf{v} + \mu\mathbf{v}$	distributivity over $+$ in $\mathbb{R}$

Observation 4.2: $(\mathbb{R}^m, +, \cdot)$, with "$+$" as in Definition 1.1 and "$\cdot$" as in Definition 1.3, is a vector space.

Definition 4.3: A polynomial $\mathbf{p}$ is a sum of the form

$$\mathbf{p} = \sum_{i=0}^{m} p_i x^i,$$

for some $m \in \mathbb{N}$. x: a variable; $p_0, p_1, \ldots, p_m \in \mathbb{R}$ the *coefficients*. Largest i such that $p_i \neq 0$: *degree* of $\mathbf{p}$. If all p_i are 0: *zero polynomial* (degree -1).

[1] `https://en.wikipedia.org/wiki/Mammal`

Examples:

$$\begin{aligned}
\mathbf{p} &= 2x^2 + x + 1 &&: \text{degree } 2 \\
\mathbf{q} &= 5x - 2 &&: \text{degree } 1 \\
\mathbf{p} + \mathbf{q} &= 2x^2 + 6x - 1 &&: \text{“}+\text{”} \\
5\mathbf{p} &= 10x^2 + 5x + 5 &&: \text{“}\cdot\text{”}
\end{aligned}$$

Lemma 4.4: Let $\mathbb{R}[x]$ be the set of polynomials in one variable x. Then $(\mathbb{R}[x], +, \cdot)$ is a vector space.

Proof. Check the obvious! □

Lemma 4.5: Let $\mathbb{R}^{m\times n}$ be the set of $m \times n$ matrices, with $A+B$ and λA defined in the usual way (Definition 2.2). Then $(\mathbb{R}^{m\times n}, +, \cdot)$ is a vector space.

Proving the obvious: vector spaces behave as expected (from $\mathbb{R}^m$). Example:

Fact 4.6: Let $(V, +, \cdot)$ be a vector space. V contains exactly one zero vector (a vector satisfying axiom 3).

Proof. Take two zero vectors $\mathbf{0}$ and $\mathbf{0}'$. Then

$$\begin{aligned}
\mathbf{0}' &= \mathbf{0}' + \mathbf{0} && \text{(axiom 3: } \mathbf{0} \text{ is a zero vector)} \\
&= \mathbf{0} + \mathbf{0}' && \text{(axiom 1: commutativity)} \\
&= \mathbf{0} && \text{(axiom 3: } \mathbf{0}' \text{ is a zero vector)}
\end{aligned}$$

□

Abuse of notation: $(V, +, \cdot) \to V$

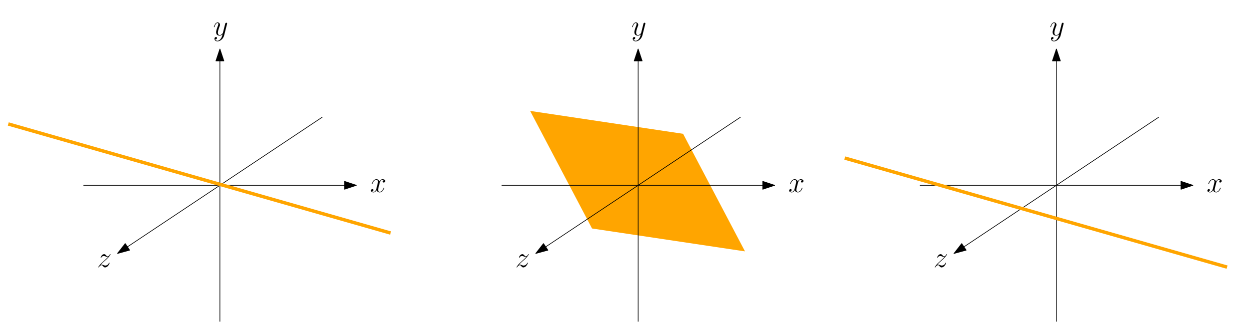
Subspaces:

Definition 4.8: Let V be a vector space. A nonempty subset $U \subseteq V$ is a *subspace* of V if the following two axioms hold for all $\mathbf{v}, \mathbf{w} \in U$ and all $\lambda \in \mathbb{R}$.

(i) $\mathbf{v} + \mathbf{w} \in U$;

(ii) $\lambda \mathbf{v} \in U$.

We always have $\mathbf{0} \in U$: take any $\mathbf{u} \in U$, then $0\mathbf{u} = \mathbf{0} \in U$ by (ii). Needs “obvious” Fact 4.10.



subspaces of R^3: a line   a plane   not a subspace (misses $\mathbf{0}$)

Lemma 4.11: Let A be an $m \times n$ matrix. Then $\mathbf{C}(A)$ is a subspace of $\mathbb{R}^m$.

Proof. Let $\mathbf{v}, \mathbf{w} \in \mathbf{C}(A)$: there exist $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ such that $\mathbf{v} = A\mathbf{x}, \mathbf{w} = A\mathbf{y}$.

$$A(\underbrace{\mathbf{x} + \mathbf{y}}_{\in \mathbb{R}^n}) = A\mathbf{x} + A\mathbf{y} = \mathbf{v} + \mathbf{w} \quad \Rightarrow \quad \mathbf{v} + \mathbf{w} \in \mathbf{C}(A)$$

$\Rightarrow$ subspace axiom (i).
For $\lambda \in \mathbb{R}$,

$$A(\underbrace{\lambda\mathbf{x}}_{\in \mathbb{R}^n}) = \lambda A\mathbf{x} = \lambda\mathbf{v} \quad \Rightarrow \quad \lambda\mathbf{v} \in \mathbf{C}(A)$$

$\Rightarrow$ subspace axiom (ii). □

Lemma 4.12: Let V be a vector space and U a subspace. Then U is also a vector space (with the same "$+$" and "$\cdot$" as V).

Proof. Check the (almost) obvious! □

Subspaces of...
... $\mathbb{R}[x]$:
The polynomials *without constant term*:

$$\mathbf{p} = \sum_{i=0}^{m} p_i x^i \text{ where } p_0 = 0$$

The *quadratic polynomials*: lookalike of (*isomorphic* to) $\mathbb{R}^3$

$$\mathbf{p} = p_0 + p_1 x + p_2 x^2$$

$\mathbb{R}[x]$ "contains" $\mathbb{R}^1, \mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^4, \ldots$ (constant, linear, quadratic, cubic,... polynomials)!

... $\mathbb{R}^{2\times 2}$: isomorphic to $\mathbb{R}^4$
The symmetric matrices: $\begin{bmatrix} a & b \\ b & d \end{bmatrix}$
The matrices of *trace* 0: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a + d = 0$

Bases and dimension (Section 4.2)

Basis of V: linearly independent vectors whose span is V.
Formal definition uses *set* of vectors, not sequence (more practical; handles infinite case).
Definition 4.13: Let V be a vector space, $G \subseteq V$ a (possibly infinite) subset of vectors. A *linear combination* of G is a sum of the form

$$\sum_{\mathbf{v} \in F} \lambda_{\mathbf{v}} \mathbf{v},$$

where $F \subseteq G$ is a finite subset of G and $\lambda_{\mathbf{v}} \in \mathbb{R}$ for all $\mathbf{v} \in F$.

Lemma 4.14: Let V be a vector space, $G \subseteq V$. Every linear combination of $G \subseteq V$ is again in V.

Proof. Linear combination (of finite $F \subseteq G$, in some order): $\sum_{j=1}^{n} \lambda_j \mathbf{v}_j$.

- $\mathbf{w}_j := \lambda_j \mathbf{v}_j \in V$ for all j (function $\cdot : \mathbb{R} \times V \to V$)
- $\mathbf{w}_1 + \mathbf{w}_2 \in V$ (function $+ : V \times V \to V$)
- Repeat: $\underbrace{(\mathbf{w}_1 + \mathbf{w}_2)}_{\in V} + \mathbf{w}_3 \in V$, and so on, until $\mathbf{w}_1 + \mathbf{w}_2 + \cdots + \mathbf{w}_n \in V$

□

Why not infinite linear combinations? Previous lemma may fail (example: polynomials)!

G: the *unit monomials*: $1, x^2, x^3, \ldots$; $\sum_{\mathbf{p} \in G} 1\mathbf{p} = \sum_{i=0}^{\infty} x^i$ is *not* a polynomial.

Definition 4.15:
Let V be a vector space, $G \subseteq V$ a subset of vectors.
$\mathbf{Span}(G)$: set of all linear combinations of G.
G is *linearly independent* if no vector $\mathbf{v} \in G$ is a linear combination of $G \setminus \{\mathbf{v}\}$.

Definition 4.16: Let V be a vector space. $B \subseteq V$ is a *basis* of V if B is linearly independent and $\mathbf{Span}(B) = V$.

Examples: (For linear independence, use *private nonzero* argument!)

vector space V	basis B
$\mathbb{R}^m$	$\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m\}$
$\mathbf{C}(A)$ (subspace of $\mathbb{R}^m$)	independent columns of A
2×2 symmetric matrices (subspace of $R^{2\times 2}$)	$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$
$\mathbb{R}[x]$ (polynomials)	$\{x^i : i = 0, 1, \ldots\}$ (infinite set)
$\{\mathbf{0}\}$ (smallest vector space)	(empty set)

There can be many bases:
Observation 4.18: Every set $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ of m linearly independent vectors is a basis of $\mathbb{R}^m$.

Proof. Still need $\mathbf{Span}(B) = \mathbb{R}^m$ (every $\mathbf{v} \in \mathbb{R}^m$ is a linear combination of B).
A: $m \times m$ matrix with columns $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$. Theorem 3.11: $A\mathbf{x} = \mathbf{v}$ has a unique solution

$$\Rightarrow \quad \mathbf{v} = \underbrace{\sum_{j=1}^{m} x_j \mathbf{v}_j}_{A\mathbf{x}}$$

□

Steinitz exchange lemma:
Lemma 4.19: Let V be a vector space, $F \subseteq V$ finite and linearly independent, $G \subseteq V$ finite with $\mathbf{Span}(G) = V$. Then

(i) $|F| \leq |G|$.

(ii) There exists a subset $E \subseteq G$ of size $|G| - |F|$ such that $\mathbf{Span}(F \cup E) = V$.

Remark: $|F \cup E| \leq |G|$ (E is allowed to contain elements of F).

Proof. Induction on $f = |F|$.
$f = 0$ ($F = \emptyset$): (i) clear, for (ii), take $E = G$.
$f > 0$: choose $\mathbf{u} \in F$, $F' = F \setminus \{\mathbf{u}\}$, $g = |G|$. F' is also linearly independent.
Induction hypothesis:

(i) $g \geq f - 1$.

(ii) There exists a subset $E' \subseteq G$ of size $g - (f-1)$ with $\mathbf{Span}(F' \cup E') = V$.

$$\begin{array}{ll} \mathbf{u} \in V = \mathbf{Span}(F' \cup E'), & \mathbf{u} \notin \mathbf{Span}(F') \text{ (F linearly independent!)} \\ \Downarrow & \Downarrow \\ \mathbf{u} = \displaystyle\sum_{\mathbf{v} \in F' \cup E'} \lambda_{\mathbf{v}} \mathbf{v}, & \lambda_{\mathbf{w}} \neq 0 \text{ for some } \mathbf{w} \in E' \end{array} \qquad (\star)$$

$\Rightarrow |E'| = g - (f-1) \geq 1 \Leftrightarrow g \geq f \Rightarrow$ (i) for size f.
(ii) for size f: $E = E' \setminus \{w\}$; solve $(\star)$ for $\mathbf{w}$:

$$\mathbf{w} = \frac{1}{\mu_{\mathbf{w}}} \left(\mathbf{u} - \sum_{\mathbf{v} \in F' \cup E} \lambda_{\mathbf{v}} \mathbf{v} \right)$$

$$\begin{array}{llcll} & & & \text{Lemma 1.23:} & \\ \Rightarrow & \mathbf{w} \text{ is linear combination of } \overbrace{\{u\} \cup F' \cup E}^{F \cup E}: & \mathbf{Span}(F \cup E) & = & \mathbf{Span}(\overbrace{F \cup E \cup \{\mathbf{w}\}}^{F \cup E'}) \\ & & \| & & \| \\ (\star): & \mathbf{u} \text{ is linear combination of } F' \cup E': & \underbrace{\mathbf{Span}(F' \cup E')}_{V} & = & \mathbf{Span}(\underbrace{F' \cup E' \cup \{\mathbf{u}\}}_{F \cup E'}) \end{array}$$

□

Theorem 4.20: Let V be a vector space; $B, B' \subseteq V$ two finite bases of V. Then $|B| = |B'|$.

Proof. As bases, B and B' are linearly independent, and $\mathbf{Span}(B) = \mathbf{Span}(B') = V$. Apply Steinitz exchange lemma (i):

- $F = B, G = B' \Rightarrow |B| \leq |B'|$

- $F = B', G = B \Rightarrow |B'| \leq |B|$.

□

Also works without "finite" (case of polynomials). For infinite sets, $|B| = |B'|$ means "the same kind of infinity".

Does every vector space have a basis? Yes! Here: the "finite" case.

Definition 4.21: A vector space V is called *finitely generated* if there exists a finite subset $G \subseteq V$ with $\mathbf{Span}(G) = V$.

$\mathbb{R}^m$: finitely generated ($G = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m\}$)

$\mathbb{R}[x]$: not finitely generated

Theorem 4.22: Let V be a finitely generated vector space, $G \subseteq V$ a finite subset with $\mathbf{Span}(G) = V$. Then V has a basis $B \subseteq G$.

Proof. If G is linearly independent, $B = G$ is a basis by Definition 4.16. "line 1"

Otherwise, some $\mathbf{v} \in G$ is a linear combination of the other vectors $\Rightarrow$
$\mathbf{Span}(G \setminus \{\mathbf{v}\}) = \mathbf{Span}(G) = V$ (Lemma 1.23).

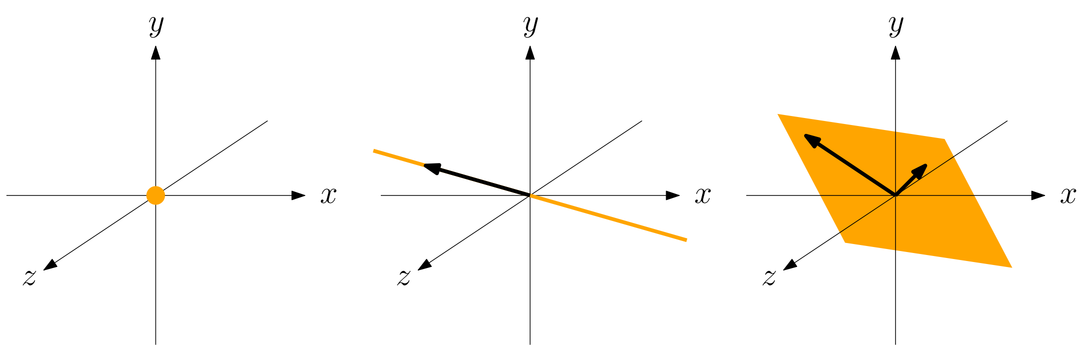
Replace G with $G \setminus \{\mathbf{v}\}$ (still spans V) and go to line 1.

G gets smaller in every step: this finally stops with $B = G$. □

Dimension:

Definition 4.23: Let V be a finitely generated vector space. Then $\dim(V)$, the dimension of V, is the size of any basis B of V.

$\dim(\mathbb{R}^m) = m$ (no surprise)



dim = 0 dim = 1 dim = 2

Simplified basis criterion:

Lemma 4.24: Let V be a vector space with $\dim(V) = d$.

(i) Let $F \subseteq V$ be a set of d linearly independent vectors. Then F is a basis of V.

(ii) Let $G \subseteq V$ be a set of d vectors with $\mathbf{Span}(G) = V$. Then G is a basis of V.

Proof.
(i): Let G be a basis of V. Steinitz exchange Lemma 4.19 (ii) applies with F and G.
$|F| = |G| = d \Rightarrow E = \emptyset$. $\mathbf{Span}(F) = \mathbf{Span}(F \cup E) = V \Rightarrow F$ is a basis.

(ii) We find a basis $B \subseteq G$ of size d (Theorem 4.22). $|B| = |G| \Rightarrow B = G \Rightarrow G$ is a basis. $\square$