4/3/25

Logistics

- introduction: Matt, email, office hours, research
- note: I am <u>not</u> the HW grader.
- heads up: I will be gone for 3 discussions b/c of a conference in France. There will be a sub.
  (for 115ah, you may have an extra lecture for one)
- today: proofs, stop me if I miss details

Proof introductions

a series of logical statements that show a statement is true/false based on definitions and theorems.

informally, convince your reader.

<u>Always</u> use sentences and <u>always</u> set up your problem.

General process

1. set up problem
2. unravel definitions
3. identify conclusion
4. ??? be creative, try to connect setup to conclusion.

<u>def</u>: an integer n is even if $\exists$ an integer k s.t. $n = 2k$

(we assume basic knowledge of $\mathbb{R}$ (closure, $+, -, \leq, \geq$, etc)

<u>if-then statements</u>

<u>thm</u>: if n is even, then $n+2$ is even

<u>proof</u>: Suppose n is even. Then $\exists$ k s.t. $n = 2k$.

Then $n+2 = 2k+2 = 2(k+1)$. Therefore $n+2$ is even

because $k+1 \in \mathbb{Z}$. (Direct proof) $\square$

<u>thm</u>: if n^2 is even, then n is even.

<u>proof</u>: it suffices to show that (contrapositive)

if n is not even (odd), then n^2 is not even (odd).

suppose that n is odd. Then $\exists$ $k \in \mathbb{Z}$ s.t. $n = 2k+1$.

Then $n^2 = (2k+1)^2 = 2(2k^2 + k) + 1$ is odd and hence

not even. (contrapositive) $\square$

<u>thm</u>: 1 is not even

<u>proof</u>: Suppose for the sake of contradiction that 1 is even.

Then $\exists$ $k \in \mathbb{Z}$ s.t. $1 = 2k$. Then $k = 1/2$.

But $1/2 \notin \mathbb{Z}$ so we have a contradiction $\divideontimes$

Therefore 1 is not even. (contradiction) $\square$

<u>thm</u>: $\forall\ a \in \mathbb{Z}$, $\exists$ an even $b \in \mathbb{Z}$ s.t. $a \leq b$.

<u>proof</u>: Let $\exists\ a \in \mathbb{Z}$ (a here is arbitrary).

If $a \geq 0$, then $2a \geq a$ and $2a$ is even.

If $a < 0$ then $-2a \geq a$ and $-2a = 2(-a)$ is even. $\square$

determine if the following are true/false.

<u>claim</u>: $\exists$ an even $b \in \mathbb{Z}$ s.t. $\forall\ a \in \mathbb{Z}$, $a \leq b$. FALSE.

negation: $\forall$ even $b \in \mathbb{Z}$, $\exists\ a \in \mathbb{Z}$ s.t. $a > b$

proof: Let $\exists\ b \in \mathbb{Z}$ even. Then $b+1 > b$ and $b+1 \in \mathbb{Z}$. $\square$

<u>claim</u>: if $a+b$ is even then a and b are even. FALSE

Q: what does it mean for this to be false?

A: $\exists\ a, b \in \mathbb{Z}$ s.t. a or b is not even and $a+b$ is even.

<u>proof</u>: (counter-example) 1 is not even, but $1+1 = 2$ is even.

<u>always</u> provide an explicit counter-example to disprove something (specifically if-then statements)

<u>claim</u>: if a is even then $\exists\ k \in \mathbb{Z}$ s.t. $a = 4k$. FALSE

<u>proof</u>: (counter-example) 2 is even.

Suppose that $2 = 4k$ for some $k \in \mathbb{Z}$. Then $k = 2/4 = 1/2$.

However $1/2 \notin \mathbb{Z}$. Therefore $2 \neq 4k$. $\square$

Negation

a lot of our proof techniques rely on finding the "negation" of a statement, i.e. the logical opposite.

intuitively, what makes the original statement false?

examples

not (P and Q) $\iff$ (not P) or (not Q)

not (P or Q) $\iff$ (not P) and (not Q)

not ($\forall x$, P(x)) $\iff$ $\exists x$ s.t. (not P(x))

not ($\exists x$ s.t. P(x)) $\iff$ $\forall x$, not P(x)

not (if P then Q) $\iff$ P and (not Q)

counter-example!

these rules stack. Consider

$\forall x$, if (P(x) and Q(x)) then (R(x) or S(x))

negation: $\exists x$ s.t. P(x) and Q(x) and (not R(x))

and (not S(x))

extra

<u>def</u>: an integer m is odd if $m = 2k+1$ for some integer k.

<u>thm</u>: if n is even then n is not odd

<u>proof</u>: (contradiction). Suppose on the contrary that n is even and odd. Then $\exists\ j,k \in \mathbb{Z}$ s.t.

$n = 2j+1 = 2k$. Rearranging, we find

$$1 = 2(k-j)$$

For ease of notation, let $a = k-j \in \mathbb{Z}$. Then $1 = 2a$.

<u>case 1: $a<0$</u>

if $a<0$ then $1 = 2a < 0$ which is a contradiction.

<u>case 2: $a=0$</u>

if $a=0$ then $1 = 2a = 0$ which is a contradiction.

<u>case 3: $a \geq 1$</u>. Then $1 = 2a \geq 2$ which is a contradiction. $\square$

Review: fields

<u>def (field)</u>: set F w/ $+ : F \times F \to F$, $\cdot : F \times F \to F$ s.t.

0 closure: $\forall\, a, b \in F$, $a+b,\ ab \in F$ note, implied above

1 commutativity: $\forall\, a, b \in F$, $a+b = b+a$, $ab = ba$

2 associativity: $\forall\, a, b, c \in F$, $a+(b+c) = (a+b)+c$

$a(bc) = (ab)c$.

3 identities: $\exists\, 0 \in F$ s.t. $a+0 = a$ $\forall\, a \in F$

$\exists\, 1 \neq 0 \in F$ s.t. $1a = a$ $\forall\, a \in F$

4 inverses $\forall\, a \neq 0$, $\exists\, -a, a^{-1} \in F$ s.t. $a + (-a) = 0$

$aa^{-1} = 1$

5 distributive $\forall\, a, b, c \in F$, $a(b+c) = ab + ac$.

exercise: are the following fields? If so, prove it. If not, identify some properties that fail.

- $\mathbb{R}^2 = \{(x,y) : x,y \in \mathbb{R}^2\}$ w/ $+$ and $\cdot$ defined component-wise.

  i.e. $(a,b)+(c,d) = (a+c, b+d)$, $(a,b)\cdot(c,d) = (ac, bd)$.

  proof: not a field. $(1,1)$ is the (unique) multiplicative identity. $(1,0)\cdot(a,b) = (a,0)$ $\forall$ $(a,b) \in \mathbb{R}^2$ therefore $(1,0)$ does not have a multiplicative inverse. $\square$

- challenge: given a field F, define $F[x]$ to be polynomials

  $F[x] = \{a_0 + a_1 x + \dots + a_n x^n : n \geq 0, a_i \in F\}$

  Define $+$ and $\cdot$ in the usual way.

  proof: not a field. $p(x) = 1$ is the multiplicative identity sps for the sake of contradiction that $\exists$ $q(x)$ s.t. $xq(x) = 1$. Evaluating at $x=0$, we find that $0=1$. This contradicts the fact that F is a field. $\square$

<u>exercise</u> suppose that F is a field w/ finitely many elements.

① prove that $\exists$ $p>0$ s.t.

$$\underbrace{1+1+\cdots+1}_{p\text{-times}} = 0$$

In particular, $\exists$ a smallest $p>0$ s.t. $1+1+\cdots+1=0$.

proof: pigeonhole $\Rightarrow$ $\exists$ $j>k$ s.t.

$$1+\cdots+1 \ (j \text{ times}) = 1+\cdots+1 \ (k \text{ times}$$

then $1+\cdots+1 \ (j-k \text{ times}) = 0$

② prove that p is prime

proof: suppose on the contrary that $p = ab$ for $a,b \neq 1. >0$

then $1+\cdots+1 \ (ab \text{ times})$

$$= \left(1+\cdots+1 \ (a \text{ times})\right) \cdot \left(1+\cdots+1 \ (b \text{ times})\right)$$

$$= 0$$

Then without loss of generality, $1+\cdots+1 \ (a \text{ times}) = 0$.

B/c $b \neq 1$, $a < p$ which contradicts the minimality of p. $\square$

4/10/25 Added (joint) OH Tues 12-1 in MS3975.

Logistics: Still focusing on proof writing/structure.

Vector Spaces:

technically, $V = \{\vec{u} : u \in (0,\infty)\}$

<u>exercise</u>: Let $V = (0,\infty)$ and $\mathbb{F} = \mathbb{R}$ (w/ usual structure).

Define $\oplus : V \times V \to V$ by $\vec{u} \oplus \vec{v} = \overrightarrow{uv}$

e.g. $\vec{2} \oplus \vec{3} = \vec{6}$

Define $\odot : \mathbb{F} \times V \to V$ by $a \odot \vec{u} = \overrightarrow{u^a}$

e.g. $2 \odot \vec{3} = \vec{9}$

Prove that V is a vector space over $\mathbb{F}$.

<u>proof</u>: We show all of the vector space axioms.

<u>V0 (closure)</u>

Let $\exists\ \vec{u}, \vec{v} \in V$. Bk $u, v \in (0,\infty)$, $uv \in (0,\infty)$.

Then $\vec{u} \oplus \vec{v} = \overrightarrow{uv} \in V$.

Let $\exists\ a \in \mathbb{F}$, $\vec{u} \in V$. Bk $u \in (0,\infty)$, $a \in \mathbb{R}$, $u^a \in (0,\infty)$.

Then $a \odot \vec{u} = \overrightarrow{u^a} \in V$.

<u>V1 (commutativity of $\oplus$)</u>

Let $\exists\ \vec{u}, \vec{v} \in V$. By commutativity of mult in $\mathbb{R}$,

$\vec{u} \oplus \vec{v} = \overrightarrow{uv} = \overrightarrow{vu} = \vec{v} \oplus \vec{u}$.

V2 (associativity of $\oplus$)

Let $\exists\ \vec{u}, \vec{v}, \vec{w} \in V$. By associativity of multiplication in $\mathbb{R}$,

$$(\vec{u} \oplus \vec{v}) \oplus \vec{w} = \overrightarrow{uv} \oplus \vec{w} = \overrightarrow{(uv)w} = \overrightarrow{u(vw)} = \vec{u} \oplus (\vec{v} \oplus \vec{w}).$$

V3 (additive identity)

We claim that the additive identity of V is $\vec{1}$.

Let $\exists\ \vec{u} \in V$. Then $\vec{1} \oplus \vec{u} = \overrightarrow{1u} = \vec{u}$.

As this holds for all $\vec{u} \in V$, $\vec{1}$ is the additive identity of V.

V4 (additive inverses)

We claim that $\forall\ \vec{u} \in V$, $-\vec{u} = \overrightarrow{1/u}$.

Let $\exists\ \vec{u} \in V$. Then $\vec{u} \oplus \overrightarrow{1/u} = \overrightarrow{u/u} = \vec{1}$, which is the additive identity in V. Therefore $\forall\ \vec{u} \in V$, $\exists\ -\vec{u} = \overrightarrow{1/u}$ s.t. $\vec{u} \oplus -\vec{u} = \vec{1}$.

V5 (multiplicative identity)

Let $\exists\ \vec{u} \in V$. Then $1 \odot \vec{u} = \vec{u^1} = \vec{u}$ as desired.

V6 (assoc. of $\odot$)

Let $\exists\ a, b \in \mathbb{F}$, $\vec{u} \in V$. Then by definition,

$$a \odot (b \odot \vec{u}) = a \odot \overrightarrow{u^b} = \overrightarrow{(u^b)^a} = \overrightarrow{u^{(ab)}} = (ab) \odot \vec{u}$$

as desired.

V7 (distributivity)

- Let $\exists\, a \in \mathbb{F}$, $\vec{u}, \vec{v} \in V$. Then by definition

$$a \odot (\vec{u} \oplus \vec{v}) = a \odot \overrightarrow{uv} = \overrightarrow{(uv)^a} = \overrightarrow{u^a v^a}$$

$$= \overrightarrow{u^a} \oplus \overrightarrow{v^a} = (a \odot \vec{u}) \oplus (a \odot \vec{v})$$

as desired.

- Let $\exists\, a, b \in \mathbb{F}$, $\vec{u} \in V$. Then by definition

$$(a+b) \odot \vec{u} = \overrightarrow{u^{(a+b)}} = \overrightarrow{u^a u^b}$$

$$= \overrightarrow{u^a} \oplus \overrightarrow{u^b} = (a \odot \vec{u}) \oplus (b \odot \vec{u})$$

as desired.

This completes our proof that V is a vector space over $\mathbb{F}$. $\square$

Linear Transformations

NOTE: $ax+b$ is <u>not</u> linear.

intuition: $T: V \to W$ is linear if it preserves the linear structure of V, W:

formal: $T(u+w) = Tu + Tw$ and $T(av) = aTv$.

<u>exercise</u>: given $V = (0, \infty)$ w/ the structure from earlier, define $T: V \to \mathbb{R}$ by $T\vec{u} = \log(u)$.

Prove that T is linear.

<u>proof</u>: Let $\exists\ \vec{u}, \vec{v} \in V$. Then by standard properties of the logarithm,

$$T(\vec{u} \oplus \vec{v}) = T(\overrightarrow{uv}) = \log(uv) = \log u + \log v$$
$$= T\vec{u} + T\vec{v}.$$

Let $\exists\ a \in \mathbb{R}, \vec{u} \in V$. Then by prop of log,

$$T(a \odot \vec{u}) = T\vec{u}^a = \log(u^a) = a \log u = a \cdot T\vec{u}. \qquad \square$$

def: isomorphism – $T: V \to W$ s.t. T is bijective (surjective and injective; invertible).

<u>exercise</u> T above is an isomorphism

<u>proof</u>: Define $T^{-1}: \mathbb{R} \to V$ by

$T^{-1}(w) = \overrightarrow{e^w}$. Then

$$\forall\ w \in \mathbb{R}, \quad TT^{-1}(w) = T\overrightarrow{e^w} = \log e^w = w$$
$$\forall\ u \in V, \quad T^{-1}T(\vec{u}) = T^{-1}\log u = \overrightarrow{e^{\log u}} = \vec{u}. \qquad \square$$

Q. In the definition of invertible, we require both

$TT^{-1} = 1_V$ and $T^{-1}T = 1_W$.

Are these both necessary?

A: We want T, T^{-1} s.t. $TT^{-1} = 1_V$ but $T^{-1}T \neq 1_W$

idea: lose information w/ T

$T: \mathbb{R}^2 \to \mathbb{R}: \begin{pmatrix} a \\ b \end{pmatrix} \to a$

$T^{-1}: \mathbb{R} \to \mathbb{R}^2: a \to \begin{pmatrix} a \\ 0 \end{pmatrix}$

Then $TT^{-1}(a) = T\begin{pmatrix} a \\ 0 \end{pmatrix} = a$

but $T^{-1}T\begin{pmatrix} a \\ b \end{pmatrix} = T^{-1}a = \begin{pmatrix} a \\ 0 \end{pmatrix}$.

<u>Prove/disprove the following:</u>

$T: U \to V \quad S: V \to W$

- if $ST: U \to W$ is surjective then S is surjective

<u>proof</u>: Let $\exists\, w \in W$. B/c ST is surjective, $\exists\, u \in U$ s.t. $STu = w$. Then $S(Tu) = w$.

B/c $Tu \in V$, this implies that $\forall\, w \in W\ \exists\, v \in V$ s.t. $Sv = w$ and so S is surjective. $\square$

- if $ST: U \to W$ is surjective then T is surjective

<u>counter-example</u>: Let $U, W = \{0\}$, $V = \mathbb{R}$ w/

$T0 = 0$ and $S(v) = 0\ \forall\, v \in V$. Then $ST0 = 0$, so

ST is surjective but $\forall\, u \in U$, $Tu = 0 \neq 1$ so T is not $\square$

Subspaces

<u>intuition</u>: a subspace is a vector space inside another vector space w/ the same structure $(+, \cdot, \vec{0}, \mathbb{F})$.

<u>exercise</u>: (dis)prove whether the following are subspaces

- Define $$W = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : \begin{array}{l} x+y=0 \\ x+y+z=0 \end{array} \right\} \subset \mathbb{R}^3$$

Yes, this is a subspace.

<u>proof</u>: It suffices to show the following.

<u>W is non-empty</u>: B/c $0+0=0$ and $0+0+0=0$, $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in W$. Then W is non-empty.

<u>closure under vector addition</u>

Let $\exists$ $(x,y,z)^T, (a,b,c)^T \in W$.

Then $x+y = x+y+z = a+b = a+b+c = 0$.

This implies $(x+a)+(y+b) = (x+a)+(y+b)+(z+c) = 0$

and so $(x,y,z)^T + (a,b,c)^T \in W$.

<u>closure under scalar multiplication</u>

Let $\exists$ $a \in \mathbb{R}$, $v = (x,y,z)^T \in W$.

Then $a(x+y) = a(x+y+z) = 0$

and so $ax+ay = ax+ay+az = 0$. Therefore

$av = (ax, ay, az)^T \in W$ as desired. $\square$

- $W = \left\{ \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} : x, y \in \mathbb{R} \right\} \subset \mathbb{R}^3$

<u>proof</u>: Not a subspace. $\vec{0} \notin W$.

Q: can you make W into a vector space w/ alternative operations?

A: yes. Define $+$ and $\cdot$ to only act on the first 2 entries.

Q: Given subspaces $U, V \subset W$, is $U \cup V$ a subspace? Prove or find a counter-example.

Can you find a condition on U, V which ensures that $U \cup V$ is a subspace?

A: No. Consider $U = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} : a \in \mathbb{R} \right\} \subset \mathbb{R}^2$

$V = \left\{ \begin{pmatrix} 0 \\ a \end{pmatrix} : a \in \mathbb{R} \right\} \subset \mathbb{R}^2$

$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \notin U \cup V$ but $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in U \cup V$.

This is true iff $U \subset V$ or $V \subset U$.

4/15/25

- 115A: briefly explain linear independence
- advertise proof-writing workshop.
- 115AH: Zorn's lemma on Th.

4/16/25

Logistics: I recommend heavily that you collaborate on homework, start as early as possible, and ask lots of questions. The professor/instructor and I can provide a lot of help.

- midterm 1 is next week.

115AH only: Zorn's Lemma not relevant to your midterm.

<u>def</u> (partial order) on a set S is a relationship $\leq$ between <u>some</u> elements s.t. hence partial

① <u>reflexive</u>: $\forall s \in S$, $s \leq s$

② <u>antisymmetry</u>: if $a \leq b$ and $b \leq a$ then $a = b$.

③ <u>transitivity</u>: if $a \leq b$ and $b \leq c$ then $a \leq c$

this is called a poset

<u>examples</u>: $\mathbb{R}$ w/ usual ordering $\leq$

- given a set S, the power set 2^S is

$$2^S = \{A : A \subset S\} \text{ (all subsets of } S\text{)}$$

we define a partial order on 2^S w/

$$A \leq B \text{ if } A \subset B.$$

<u>note</u>: we can't compare all subsets in 2^S.

for instance, $\{0\} \not\leq \{1\}$ and $\{1\} \not\leq \{0\}$ in $2^{\mathbb{Z}}$

- on $\mathbb{N} = \{1, 2, 3, \ldots\}$, define $a \leq b$ if $a \mid b$ "a divides b"

ie. $3 \mid 6$, $2 \mid 8$, etc but $3 \nmid 5$ and $5 \nmid 3$.

- reverse divisibility: $a \leq b$ if $b \mid a$

ie. $3 \geq 6$, $2 \geq 8$, etc...

- $\mathcal{F}(\mathbb{R} \to \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$. Define $f \leq g$ if $f(x) \leq g(x)$ $\forall x$.

ie. $\sin x \leq 2$ but $\sin x$ and $\cos x$ aren't comparable

<u>def</u>: (totally ordered) we say that $(S, \leq)$ is totally ordered if $\forall\, a, b \in S$, $a \leq b$ or $b \leq a$.

Everything is comparable.

<u>examples</u>

- $\mathbb{R}$ w/ $\leq$ is totally ordered
- in $2^{\mathbb{Z}}$ w/ $\subset$ ordering, $\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\}$ is totally ordered, though $2^{\mathbb{Z}}$ is not.

  this is a totally ordered subset

<u>def</u> (upper bound): S poset, $T \subset S$.

s is an upper bound of T if $\forall\, t \in T$, $t \leq s$.

<u>examples</u>

- in $2^{\mathbb{Z}}$, $\mathbb{N} = \{1, 2, \ldots\}$ is an upper bound of $\{\{0\}, \{0,1\}, \{0,1,2\}, \ldots\}$
- in $\mathbb{N}$ w/ reverse divisibility, 2 is an upper bound of $\{2, 4, 6, 8, \ldots\}$ but not of $\{2, 3, 4, \ldots\}$.
- in $\mathcal{F}(\mathbb{R} \to \mathbb{R})$, $P(\mathbb{R})$ has no upper bound.

<u>def</u> (maximal element) poset $(S, \leq)$

m is a maximal element of S if

$s \geq m \Rightarrow s = m$ ← does <u>not</u> require that all $s \in S$ is comparable to m.

equivalently, $\nexists\, s \neq m$ s.t. $m \leq s$.

<u>examples</u>

- in $(2^S, \subset)$, S is a maximal element

  (silly example b/c S is comparable to everything)

- in $\{2, 3, \ldots\}$ w/ reverse divisibility,

  the primes are all maximal elements

- in $\mathcal{F}(\mathbb{R} \to \mathbb{R})$, there is no maximal element

<u>Zorn's Lemma</u>:

given a poset S, if every totally ordered $T \subset S$ has an upper bound, then S has a maximal element.

<u>trivial example</u>: $\mathbb{Z}_{>1} = \{2, 3, \ldots\}$ w/ reverse divisibility.

sps $T \subset \mathbb{Z}_{>2}$ is totally ordered. Let s be the smallest (normal sense) element of T. B/c T is totally ordered, $\forall\, t \in T$, $s \mid t$ or $t \mid s$. B/c $s \leq t$, if $t \mid s$ then $t = s$. Therefore s is an upper bound of T.

By Zorn's lemma, $\mathbb{Z}_{>1}$ has a maximal element.

Linear (In)dependence

a set of vectors S is linearly dependent if

$\exists$ $a_1, \dots, a_n$, not all zero, and $v_1, \dots, v_n \in S$ distinct s.t.

$$a_1 v_1 + \dots + a_n v_n = 0$$

i.e. $\exists$ a non-trivial linear combination which equals 0

a set of vectors S is linearly independent if

$$a_1 v_1 + \dots + a_n v_n = 0 \implies a_1 = \dots = a_n = 0$$

<u>examples</u>

- prove that $\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}, \begin{pmatrix}2\\1\\1\end{pmatrix}$ are linearly independent in $\mathbb{R}^3$

  <u>proof</u>: Suppose $\exists$ a, b, c s.t.

  $$a\begin{pmatrix}1\\1\\1\end{pmatrix} + b\begin{pmatrix}1\\1\\2\end{pmatrix} + c\begin{pmatrix}2\\1\\1\end{pmatrix} = 0$$

  Then $a+b+2c=0$, $a+b+c=0$, $a+2b+c=0$

  Therefore $c=0$, $b=0$, $a=0$. $\square$

- prove that x^2+1, $2x^2+x-1$, $4x^2-2x+10$ are linearly dependent in $P(\mathbb{R})$

  <u>proof</u>: We find that

  $$-8(x^2+1) + 2(2x^2+x-1) + 1(4x^2-2x+10)$$
  $$= 0$$

  Therefore the polynomials are linearly dependent.

Span

<u>115AH</u>: $\operatorname{span}(S) = \bigcap_{\text{subspaces } W \supset S} W$

span(S) is the smallest subspace containing S

<u>115A</u>: $\operatorname{span}(S) = \{a_1 v_1 + \cdots + a_n v_n : n \geq 1, v_i \in S, a_i \in \mathbb{F}\}$

w/ $\operatorname{span}(\emptyset) = \{0\}$ ← in which vector space?

<u>examples</u>

- $\operatorname{span}\underbrace{\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right)}_{S} = \mathbb{R}^3$

  <u>proof</u>: By closure, $\operatorname{span}(S) \subset \mathbb{R}^3$. It then suffices to show $\mathbb{R}^3 \subset \operatorname{span}(S)$.

  Let $\exists \begin{pmatrix}a\\b\\c\end{pmatrix} \in \mathbb{R}^3$. Then

  $$\begin{pmatrix}a\\b\\c\end{pmatrix} = (a-b)\begin{pmatrix}1\\0\\0\end{pmatrix} + (b-c)\begin{pmatrix}1\\1\\0\end{pmatrix} + c\begin{pmatrix}1\\1\\1\end{pmatrix}$$

  and so $\begin{pmatrix}a\\b\\c\end{pmatrix} \in \operatorname{span}(S)$. Therefore $\operatorname{span}(S) \supset \mathbb{R}^3$. $\square$

- $\operatorname{span}\left(\begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}\right) = \operatorname{Sym}(\mathbb{R}, 2\times 2)$

  symmetric real 2×2 matrices

  $$\begin{pmatrix}a&c\\c&b\end{pmatrix} = c\begin{pmatrix}0&1\\1&0\end{pmatrix} + \frac{a+b}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} + \frac{a-b}{2}\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

<u>exercise</u>: Sps $x \in \text{span}(S)$. Then $\text{span}(S \cup \{x\}) = \text{span}(S)$.

<u>proof</u>: By definition, $\text{span}(S)$ is a subspace containing S and x. Therefore, $\text{span}(S \cup \{x\}) \subset \text{span}(S)$.

Also by definition, $\text{span}(S \cup \{x\})$ is a subspace containing S. Therefore $\text{span}(S) \subset \text{span}(S \cup \{x\})$.

This completes the proof. $\square$

<u>exercise</u>: let V be a vector space over $\mathbb{R}$.

Then v, w are linearly independent iff $v+w$, $v-w$ are linearly independent.

<u>proof</u>: this is on the homework for 115A. Oops.

Q: does this hold over any field $\mathbb{F}$?

A: no. Consider $\mathbb{F}_2^2$. Then $\binom{1}{0}, \binom{1}{1}$ are lin. ind but $\binom{0}{1}, \binom{0}{-1} = \binom{0}{1}$ are not.

Q: if S is linearly ind. and T is linearly ind. is $S \cup T$ linearly ind?

A: No. Consider $S = \{\vec{v}\}$ and $T = \{2\vec{v}\}$

Q: Let $S \subset V$. Suppose that $\forall\ T \subsetneq S$, T is linearly independent. Is S necessarily lin ind?

A: No. Consider $S = \{ \binom{1}{0}, \binom{1}{1}, \binom{0}{1} \}$.

Each pair is lin. ind. but S is not.

lesson: you need to treat <u>all</u> vectors at once.

Q: $\text{span}(S \cup T) = \text{span}(S) \cup \text{span}(T)$?

A: no. Consider $S = \{ \binom{1}{0} \}$, $T = \{ \binom{0}{1} \}$.

Then $\text{span}(S \cup T) = \mathbb{R}^2$ but $\text{span}(S) \cup \text{span}(T)$ is only the axes.

4/24/25

Logistics

- (115AH) midterm tomorrow
  - DO THE PRACTICE MIDTERMS under a time pressure

<u>exercise</u>: suppose $T: V \to W$ is linear

a) Suppose S spans V. Does $T(S) = \{Tv : v \in S\}$ span W?

If not, what is a necessary + sufficient condition on T to ensure this?

<u>answer</u>: No. Consider $V = \{\vec{0}\}$, $W = \mathbb{R}$. Then $\emptyset$ spans V but $T(\emptyset) = \emptyset$ does not span $\mathbb{R}$.

T is surjective is necessary/sufficient.

<u>proof</u>: We prove $T(S)$ spans W iff T is surjective.

Suppose $T(S)$ spans W. Then $\forall\, w \in W\ \exists\, a_1, \ldots, a_n \in \mathbb{F}$ and $Tv_1, \ldots, Tv_n \in T(S)$ s.t. $w = a_1 Tv_1 + \ldots + a_n Tv_n$.

Then $T(a_1 v_1 + \ldots + a_n v_n) = w$. Thus T is surjective.

this is on the practice midterm

Now suppose T is surjective. Let $\exists\, w \in W$.

Then $\exists\, v \in V$ s.t. $Tv = w$. B/c $\operatorname{span}(S) = V$,

$\exists\, a_1, \ldots, a_n \in \mathbb{F}$ and $v_1, \ldots, v_n \in S$ s.t. $v = a_1 v_1 + \ldots + a_n v_n$.

Then $w = a_1 Tv_1 + \ldots + a_n Tv_n \in \operatorname{span}(T(S))$.

Since $\operatorname{span}(T(S)) \subset W$, this proves $\operatorname{span}(T(S)) = W$. $\square$

<u>note</u>: I excluded the case $S = \emptyset$ from the above proof for convenience. Briefly verify this.

b) Suppose R spans W. Does $T^{-1}(R) = \{v : Tv \in R\}$ span V?

If not, what is a sufficient + necessary condition on T?

answer: No. Consider $V = \mathbb{R}$, $W = \mathbb{R}$, $R = \{1\}$, $T = 0$.

Then $T^{-1}(R) = \emptyset$ and $\text{span}(\emptyset) \neq \mathbb{R}$.

Again, T being surjective is necessary and sufficient.

Proof is similar to previous proof.

<u>exercise</u>: Let $M_n(\mathbb{R}) = \{\text{real } n \times n \text{ matrices}\}$ w/ the usual addition and scalar multiplication.

Let $S = \{A \in M_n : A^T = A\}$, $K = \{A \in M_n : A^T = -A\}$.

Prove that $M_n = S \oplus K$.

hint: recall the trick used for even/odd functions

<u>proof</u>: We see $0 \in S \cap K$. If $A \in S \cap K$ then $A = A^T = -A$ and so $2A = 0$. B/c A consists of real entries, this implies $A = 0$. Then $S \cap K = \{0\}$.

To show $M_n = S + K$, note that $\forall A \in M_n$,

$$\tfrac{1}{2}(A + A^T) \in S \quad \text{and} \quad \tfrac{1}{2}(A - A^T) \in K.$$

The details are left to you. $\square$

<u>example</u>: Let $\exists$ vector spaces V, W. Let $T, S \in \mathcal{L}(V, W)$ w/ $T, S \neq 0$ and $\operatorname{im} T \cap \operatorname{im} S = \{0\}$. Prove $\{T, S\}$ is linearly independent in $\mathcal{L}(V, W)$.

<u>sketch</u>: There are many different methods for this problem. Suppose on the contrary that S, T are lin. dep. Then wLOG, $\exists$ c s.t. $S = cT$. B/c $T \neq 0$, $\exists$ $v \neq 0$ s.t. $Tv \neq 0$. Then $Sv = cTv$. B/c $S \neq 0$, $c \neq 0$. Then $Sv \neq 0$ and $Sv \in \operatorname{im} T \cap \operatorname{im} S$ $\#$

<u>example</u>: Define $T : P_n(\mathbb{R}) \to P_n(\mathbb{R})$ by $p \mapsto xp' + p$. Prove that T is an isomorphism.

<u>hint</u>: The product rule will help.

<u>sketch</u>: Linearity is straightforward. Should note that T is well-defined (that it doesn't increase degree.)

To prove isomorphism, you can construct the inverse

$$T^{-1} p = \frac{\int_0^x p(y)\,dy}{x}$$

need to verify this is well-defined.

Alternatively, show injective and surjective.

This is straightforward using $Tp = (xp)'$.

<u>example</u> Sps $x \in \text{span}(S)$. Then $\text{span}(S \cup \{x\}) = \text{span}(S)$.

<u>proof</u>: By definition, $\text{span}(S)$ is a subspace containing S and x. Therefore, $\text{span}(S \cup \{x\}) \subset \text{span}(S)$.

Also by definition, $\text{span}(S \cup \{x\})$ is a subspace containing S. Therefore $\text{span}(S) \subset \text{span}(S \cup \{x\})$.

This completes the proof. $\square$

<u>example</u>: Prove the following statements or find a counter-example.

- Parwise linear independence implies linear independence.

  (if $\{v, w\}$ is linearly independent $\forall\ v \neq w \in L$, then L is linearly independent.)

  <u>counter-example</u>: $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^2$

- $S: V \to W$, $T: U \to V$
  - if $ST: U \to W$ is injective then T is injective
  - if $ST: U \to W$ is surjective then T is surjective
- $S: V \to W$, $T: W \to V$. If $ST = id_W$, then $TS = id_W$.

  <u>counter-example</u>: $S: \mathbb{R} \to \{0\}$, $T: \{0\} \to \mathbb{R}$

extra interesting/challenging problems

1) Does there exist a vector space V w/ subspace $W \subsetneq V$ s.t. $V \cong W$?

Yes, $V = \mathbb{R}^\infty = \{(a_1, a_2, \dots) \mid a_i \in \mathbb{R}\}$, $W = \{(a_1, 0, a_2, 0, \dots)\}$.

2) How about V w/ $U, W \subset V$, $V = U \oplus W$ and $V \cong U \cong W$?

Yes, same as above w/ $U = \{(0, a_2, 0, \dots)\}$.

3) Consider $P(\mathbb{F})$ ($\mathbb{F}[x]$) w/ the usual operations.

If we allow polynomial multiplication, can $P(\mathbb{F})$ be a field?

No. Sps $xp(x) = 1$. Then $0 = 1$. $\divideontimes$

5/1/25

Logistics

- midterms are almost graded. Expect them within a day.

Coordinate representation

this topic is largely computational. This is a good consistent source of points on exams. So we will do some practice.

given a basis $v_1, \dots, v_n$ of V, we know that

$$\forall\ v \in V \quad \exists!\ x_1, \dots, x_n \quad \text{s.t.} \quad v = x_1 v_1 + \dots + x_n v_n$$

w/ this, when $v_1, \dots, v_n$ are fixed, all information about $v \in V$ is encoded in the coefficients $x_1, \dots, x_n$.

Given a basis $B = (v_1, \dots, v_n)$, we define the coordinate representation $[v]_B$ of $v \in V$ as

$$[v]_B = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

<u>theorem</u>: $[\cdot]_B : V \to \mathbb{F}^n$ is an isomorphism

example

$\mathcal{B} = (1,\ 1+x,\ x+x^2,\ x^2+x^3)$ is a basis of $P_3(\mathbb{R})$.

find $[\,2+x+3x^3\,]_{\mathcal{B}}$

$$[\,2+x+3x^3\,]_{\mathcal{B}} = \begin{bmatrix} -2 \\ 4 \\ -3 \\ 3 \end{bmatrix}$$

compute $[p(x)]_{\mathcal{B}}$ in general

$$[a+bx+cx^2+dx^3]_{\mathcal{B}} = \begin{bmatrix} a-b+c-d \\ b-c+d \\ c-d \\ d \end{bmatrix}$$

based on your above formula, prove that $[\cdot]_{\mathcal{B}}$ is an isomorphism

<u>proof</u>: As $\dim P_3 = \dim \mathbb{R}^4 = 4 < \infty$, it suffices to show that $[\cdot]_{\mathcal{B}}$ is injective. Suppose $\exists$

$$p_1 = a_1+b_1x+c_1x^2+d_1x^3,\quad p_2 = a_2+b_2x+c_2x^2+d_2x^3 \in P_3(\mathbb{R})$$

s.t. $[p_1]_{\mathcal{B}} = [p_2]_{\mathcal{B}}$. Then

$$d_1=d_2,\ c_1-d_1=c_2-d_2,\ b_1-c_1+d_1=b_2-c_2+d_2,\ a_1-b_1+c_1-d_1=a_2-b_2+c_2-d_2$$

Solving this, we find $p_1 = p_2$. $\square$

example

Consider $B = \left(\overbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}^{\text{note the order}} \right)$ as a basis for $M_2(\mathbb{R})$. Compute

$$\left[\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} \right]_B = \begin{bmatrix} 3 \\ 2 \\ 5 \\ 4 \end{bmatrix}$$

Consider $B = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right)$ as a basis for $M_2(\mathbb{R})$. Compute

$$\left[\begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} \right]_B = \begin{bmatrix} 7/2 \\ -3/2 \\ 7/2 \\ -1/2 \end{bmatrix}$$

Matrix Representation

Suppose we have V w/ basis $B = (v_1, \dots, v_n)$

and W w/ basis $\Gamma = (w_1, \dots, w_m)$.

Given (linear) $T: V \to W$, we can represent T w/ a matrix as

output

$$[T]_B^\Gamma = \begin{bmatrix} | & & | \\ [Tv_1]_\Gamma & \cdots & [Tv_n]_\Gamma \\ | & & | \end{bmatrix}$$

input

As we will see, everything works as expected w/ these matrices.

<u>examples</u>

define $\partial_x : P_3(\mathbb{R}) \to P_3(\mathbb{R})$. Compute the matrix representation w/ respect to the usual bases $B = (1, x, x^2, x^3)$

$$[\partial_x]_B^B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

note that this is evaluation

define $E: P_3(\mathbb{R}) \to \mathbb{R}^3$ by $p(x) \longmapsto \begin{bmatrix} p(0) \\ p(1) \\ p(2) \end{bmatrix}$.

Compute the matrix representation w/ respect to the usual bases

$B = (1, x, x^2, x^3)$, $\Gamma = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right)$

$$[E]_B^\Gamma = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \end{bmatrix}$$

Consider $T: P_2(\mathbb{R}) \to M_2(\mathbb{R}): p(x) \longmapsto \begin{bmatrix} p(0) & p'(1) \\ 0 & p''(2) \end{bmatrix}$

Let $\mathcal{B} = (1, x, x^2)$, $\Gamma = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$.

Compute $[T]_{\mathcal{B}}^{\Gamma} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}$

5/7/25

Logistics: midterms have been returned. I'm impressed!

Honors Only - Quotient Spaces

recall: given a set X and an <u>equivalence relation</u> $\sim$

satisfies reflexivity: $x \sim x \quad \forall \; x \in X$

symmetry: $x \sim y$ iff $y \sim x$

transitivity: if $x \sim y$ and $y \sim z$ then $x \sim z$

we define the <u>equivalence class</u> of $x \in X$ as

<u>not</u> unique

$$\bar{x} = \{ y : y \sim x \}$$

and the <u>quotient space</u> $X/\sim$ as

$$X/\sim \; = \{ \bar{x} \mid x \in X \}.$$

Today we discuss defining functions on $X/\sim$ and quotient vector spaces. (11.3 and 11.4 in Will's notes)

11.3 - defining functions on a quotient space

<u>recall</u>: a function $f: A \to B$ assigns one element $b \in B$ to each $a \in A$. So, $\forall a \in A \ \exists! \ f(a) \in B$.

Let's see how to do this on $X/\sim$.

<u>example</u>: On $\mathbb{R}$, define $x \sim y$ if $\lfloor x \rfloor = \lfloor y \rfloor$.

- what is $\bar{3}$? What is $\bar{e}$? How about $\bar{x}$ in general?

  $\bar{3} = [3,4)$, $\bar{e} = [2,3)$, $\bar{x} = [\lfloor x \rfloor, \lfloor x \rfloor + 1)$

- "Define" $f: \mathbb{R}/\sim \to \mathbb{Z}$ by $f(\bar{x}) = \lfloor x + 1.5 \rfloor$

  Is this a function?

  No, $0, 1/2 \in \bar{0}$ so $f(\bar{0}) = f(\overline{1/2})$.

  But $f(\bar{0}) = 1$ and $f(\overline{1/2}) = 2$.

<u>definition</u>: we say that $f: X/\sim \to Y$ is well-defined if it is actually a function. That is, if $\bar{a} = \bar{b}$ then $f(\bar{a}) = f(\bar{b})$.

So the "representative element" of $\bar{a}$ does not matter to f.

Given a function $f: X \to Y$, it is natural to ask if $\exists$ an associated function $\bar{f}: X/\sim \to Y$ where $\bar{f}(\bar{a}) = f(a)$.

We can do this, so long as f respects the structure $\sim$ as above.

That is, if f satisfies

$$\forall\ a \sim b, \quad f(a) = f(b)$$

then $\bar{f} : X/\sim \to Y$ defined by $\bar{f}(\bar{x}) = f(x)$ is well-defined.

We say that f <u>induces</u> $\bar{f}$ or that f <u>factors through</u> the quotient $X/\sim$.

theorem: (First isomorphism theorem for sets)

Let $f : X \to Y$ be surjective. Define an equivalence relation $\sim$ on X by $x \sim y$ if $f(x) = f(y)$.

Define $\bar{f} : X/\sim \to Y$ by $\bar{f}(\bar{x}) = f(x)$. Then $\bar{f}$ is a (set) isomorphism (bijection).

<u>proof</u>: $\bar{f}$ is well-defined b/c $x \sim y \Rightarrow f(x) = f(y)$.

B/c f is surjective, $\forall\ y \in Y\ \exists\ x \in X$ s.t. $f(x) = y$.

Then $\bar{f}(\bar{x}) = y$ and $\bar{f}$ is surjective.

Suppose that $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. Then $f(x) = f(y) \Rightarrow x \sim y \Rightarrow \bar{x} = \bar{y}$. $\square$

<u>intuition</u>: $\bar{f}$ is already surjective. Then quotienting "crushes" all issues w/ injectivity.

11.4 - The quotient of a vector space by a subspace

Let $W \subset V$ be a subspace. We define an equivalence relation $\equiv_W$ on V by

$$x \equiv_W y \quad \text{if} \quad x - y \in W$$

$$\iff \text{if } \exists\, w \in W \text{ s.t. } y = x + w$$

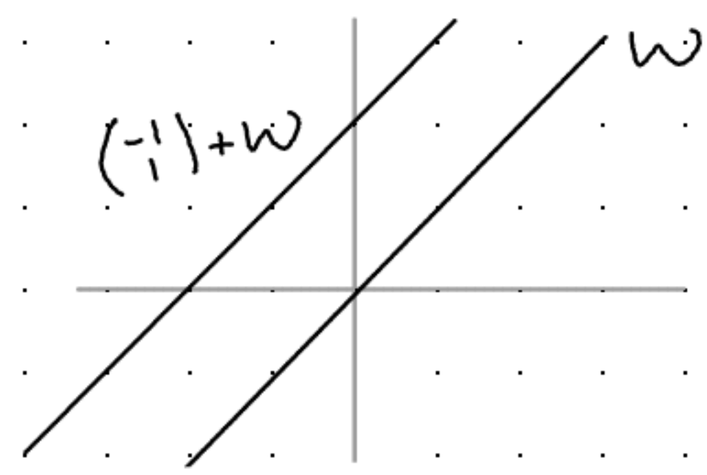
<u>notation</u>: often written/said $x = y \pmod{W}$

What is the equivalence class of some $\vec{x} \in V$?

<u>example</u>: $V = \mathbb{R}^2$, $W = \{ \binom{x}{y} : x = y \}$. $\vec{x} = \binom{-1}{1}$.

Then $\binom{x}{y} = \binom{-1}{1} \bmod W$ if $x + 1 = y - 1 \iff y = x + 2$

Equivalently, if $\binom{x}{y} \in \binom{-1}{1} + W$



<u>definition</u> (coset)

$$\vec{x} + W = \{ \vec{x} + \vec{w} \mid \vec{w} \in W \}$$

<u>theorem</u>: The equivalence class of $\vec{x}$ in V/W is the coset $\vec{x} + W$.

We can now investigate the structure of V/W as a vector space.

<u>theorem</u> let $W \subset V$ over a field F. Define

$$+ : V/W \times V/W \to V/W \quad \text{by} \quad (x+W)+(y+W) = (x+y)+W.$$

Define $\cdot : F \times V/W \to V/W$ by $a(x+W) = ax+W$.

Then $+, \cdot$ are well-defined and V/W is a vector space.

<u>proof</u>: We only show that $+$ is well-defined.

By symmetry, it suffices to consider the first entry.

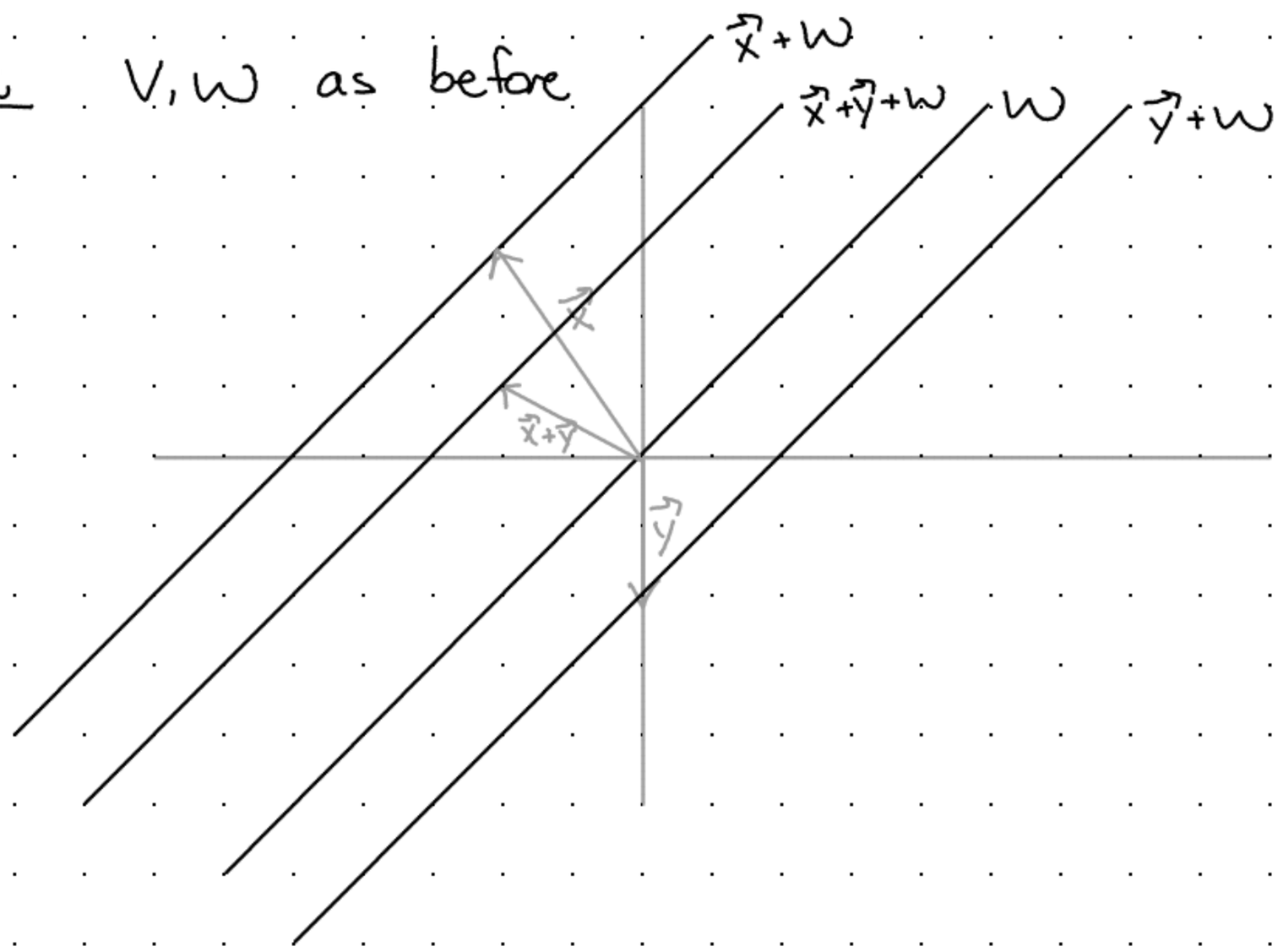
Let $\exists\ \vec{x}, \vec{y}, \vec{z} \in V$ w/ $\vec{x} = \vec{z} \bmod W$. Then $\exists\ \vec{w} \in W$ s.t. $\vec{x} = \vec{z} + \vec{w}$. Then

$$\begin{aligned}
(\vec{x}+W)+(\vec{y}+W) &= (\vec{x}+\vec{y})+W \\
&= (\vec{z}+\vec{y}+\vec{w})+W \\
&= (\vec{z}+\vec{y})+W \\
&= (\vec{z}+W)+(\vec{y}+W)
\end{aligned}$$

requires argument.

$\square$

<u>example</u> V, W as before



<u>theorem</u> let $T: V \to Z$ be linear and $W \subset V$. Then $\overline{T}: V/W \to Z$ defined by $\overline{T}(\vec{x}+W) = T\vec{x}+W$ is well-defined and linear iff $W \subset \ker T$.

<u>proof</u>: Suppose $W \subset \ker T$. Let $\vec{x} = \vec{y} \bmod W$.

Then $\exists\ \vec{w} \in W \subset \ker T$ s.t. $\vec{x} = \vec{y} + \vec{w}$.

Then $T\vec{x} = T(\vec{y}+\vec{w}) = T\vec{y} + \vec{0} = T\vec{y}$.

Suppose $\overline{T}$ is well-defined. Then $\forall\ \vec{w} \in W$,

$\vec{w} = \vec{0} \bmod W \Rightarrow T\vec{w} = T\vec{0} = \vec{0}$.

We exclude the proof of linearity. $\square$

<u>theorem</u> (first isomorphism theorem for vector spaces)

Let $T: V \to Z$ be surjective. Then $\overline{T}: V/\ker T \to W$ is an isomorphism.

<u>proof</u>: Same as the one for sets.

Non-Honors Students

Review: coordinate representations

given $B = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right)$ basis for $\mathbb{R}^2$, compute

$$\left[\begin{pmatrix} 4 \\ 5 \end{pmatrix} \right]_B = \begin{bmatrix} -1/2 \\ 3/2 \end{bmatrix}$$

given $B = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right)$ basis for M_2.

find $\left[\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right]_B$

$$\left[\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right]_B = \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix}$$

given $B = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$,

$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $L_A : M_2 \to M_2$ defined by $M \mapsto AM$

compute $[L_A]_B^B$ (output: B; input: B) $= \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & 4 \end{bmatrix}$

everything works how we want it to!

$$[Tv]_B = [T]_\Gamma^B [v]_\Gamma, \quad [T \circ S]_B^C = [T]_\Gamma^C [S]_B^\Gamma, \quad \text{etc}$$

abstract example

Let V, W be finite dimensional vector spaces w/ $\dim V = \dim W$

For $T: V \to W$, prove $\exists$ bases $\mathcal{B}, \mathcal{C}$ of V, W s.t. $[T]_{\mathcal{B}}^{\mathcal{C}}$ is diagonal.

idea: for $\mathcal{B} = (v_1, \dots, v_n)$ and $\mathcal{C} = (w_1, \dots, w_n)$,

$[T]_{\mathcal{B}}^{\mathcal{C}}$ is diagonal iff $Tv_i = a_i w_i$

another idea: if T is bijective then this is easy

b/c $T(v_1), \dots, T(v_n)$ is a basis of W

final idea: need to deal w/ $Tv_i = 0$. Do that first.

proof: Let $v_1, \dots, v_k$ be a basis of $\ker T$.

Complete this to a basis $v_1, \dots, v_n$ of V. why?

Then $Tv_{k+1}, \dots, Tv_n$ is a basis of $\operatorname{im} T$. needs reasoning

Complete this to a basis $w_1, \dots, w_k, Tv_{k+1}, \dots, Tv_n$

of W. Then let $\mathcal{B} = (v_1, \dots, v_n)$, $\mathcal{C} = (w_1, \dots, Tv_n)$.

Then $[T]_{\mathcal{B}}^{\mathcal{C}} = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix}$ is diagonal $\square$

NOTE: THIS IS NOT DIAGONALIZABILITY.

<u>true/false</u> if $\exists$ B, C bases of V s.t. $[T]_B^C = I_n$,

then $T = id_V$

False.

<u>Counter-example:</u> $V = \mathbb{R}^2$, $Tv = 2v$, $B = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$

and $B = \left(\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\right)$. Then $[T]_B^C = I_n$

<u>follow-up</u> what if $[T]_B^B = I_n$?

true

<u>proof:</u> $\forall\ v \in V$, $[Tv]_B = [T]_B^B [v]_B = [v]_B$

so $Tv = v$ $\forall\ v$ b/c $v \mapsto [v]_B$ is injective.

then $T = id_V$.

<u>follow-follow-up</u> what if $[T]_B^C = I_n$ and $[T]_C^B = I_n$?

false

<u>counter-example:</u> $V = \mathbb{R}^2$, $Tv = -v$, $B = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$, $C = \left(\begin{pmatrix}-1\\0\end{pmatrix}, \begin{pmatrix}0\\-1\end{pmatrix}\right)$.

Then $[T]_B^C = I_2 = [T]_C^B$. $\square$

<u>extra time:</u> extending by linearity theorem

first, give concrete example

then, abstract

5/15/25

Logistics

honors - midterm on Monday

non-honors - midterm on Wednesday

interest in extra OH?

Eigen-stuff

fix $T: V \to V$

λ is an eigenvalue if $\exists\ \vec{x} \neq \vec{0}$ s.t. $T\vec{x} = \lambda\vec{x}$,

then $\vec{x}$ is an eigenvector ← we do not count $\vec{0}$

the eigenspace $E_\lambda(T) = \{\vec{x} : T\vec{x} = \lambda\vec{x}\} = \ker(\lambda\, \mathrm{id}_V - T)$

<u>thm</u>: if $\dim V < \infty$, the eigenvalues of T are precisely the zeros of the characteristic polynomial $\chi_T(\lambda) = \det(\lambda\, \mathrm{id}_V - T)$

<u>reminder</u>: we can compute $\det(L)$ in any basis. why?

<u>A</u>: $\det [L]_B^B = \det([I]_B^C)^{-1} [L]_C^C [I]_B^C$

$= \cancel{\det([I]_B^C)^{-1} [I_B^C]}^{\,1} \cdot \det [L]_C^C$

examples true/false, $\dim V > 0$

- if $T: V \to V$ is invertible, then T has an eigenvalue

  false: $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} : \mathbb{R}^2 \to \mathbb{R}^2$, $T\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \lambda a \\ \lambda b \end{pmatrix} \Rightarrow \begin{matrix} b = \lambda a \\ -a = \lambda b \end{matrix} \Rightarrow b = -\lambda^2 b$, all 0

- if $T: V \to V$ is <u>not</u> invertible, then T has an eigenvalue

  $\dim V < \infty$: true. T not injective $\Rightarrow \exists\ \vec{x} \neq \vec{0}$ s.t. $T\vec{x} = 0\vec{x}$.

  $\dim V = \infty$: not necessarily. $S: \mathbb{R}^\infty \to \mathbb{R}^\infty : (a_1, \dots) \mapsto (0, a_1, \dots)$

  then S not surjective, hence not invertible

  if $Sa = \lambda a$ then $a_1 = \lambda 0 \Rightarrow a_1 = 0 \Rightarrow a_2 = 0 \Rightarrow \dots$

- if $T \circ T = T$, $T \neq 0$ then T has an eigenvalue

  true: $T(T(\vec{v})) = T\vec{v} \Rightarrow$ eigenvalue 1

- if λ is an eigenvalue of $T+S$, then λ is an eigenvalue of both T and S

  false: sps $T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} : \mathbb{R}^2 \to \mathbb{R}^2$ and consider $T + (-T)$.

<u>honors only</u> let $\lambda_1, \dots, \lambda_n$ be distinct eigenvalues of T w/ eigenvectors $\vec{x}_1, \dots, \vec{x}_n$. Prove that $x_1, \dots, x_n$ are lin. ind.

<u>hint</u>: Usual setup and then apply $(T-\lambda_i I)$.

<u>proof</u>: Sps $a_1 x_1 + \dots + a_n x_n = 0$.

Applying $T-\lambda_1 I$, we find

$$(\lambda_2-\lambda_1) a_2 x_2 + \dots + (\lambda_n-\lambda_1) a_n x_n = 0$$

applying $T-\lambda_2 I, \dots, T-\lambda_{n-1} I$, we then find

$$a_n \prod_{j<n} (\lambda_n - \lambda_j) v_n = 0 \implies a_n = 0.$$

Repeating, we find $a_1 = \dots = a_n = 0$. $\square$

Diagonalizability

we say $T: V \to V$ is diagonalizable if $\exists$ a basis B s.t.

$$[T]_B^B = {}_B[T]_B \quad \text{is diagonal.}$$

<u>non-honors only</u>: Let $\dim V < \infty$. Sps $\exists$ $T, S: V \to V$ that are simultaneously diagonalizable. That is, $\exists$ B s.t. $[T]_B^B$ and $[S]_B^B$ are diagonal. Prove that $TS = ST$.

<u>proof</u>: B/c $\mathcal{L}(V) \to M_n : \cdot \mapsto [\cdot]_B^B$ is an isomorphism, it suffices to show $[TS]_B^B = [ST]_B^B$.

Because diagonal matrices commute, we then see

$$[TS]_B^B = [T]_B^B [S]_B^B = [S]_B^B [T]_B^B = [ST]_B^B$$

as desired. $\square$

what if $\dim V = \infty$? Can't use $[*]_B^B$.

<u>proof</u>: Let B denote the eigenbasis. $\forall\, v \in V$, $\exists!$ $v = \alpha_1 b_1 + \dots + \alpha_n b_n$. Then

$$STv = S(\alpha_1 \lambda_1 b_1 + \dots + \alpha_n \lambda_n b_n) = \sum_i \alpha_i \mu_i \lambda_i b_i$$

$$TSv = T(\alpha_1 \mu_1 b_1 + \dots + \alpha_n \mu_n b_n) = \sum_i \alpha_i \mu_i \lambda_i b_i$$

where μ_i, λ_i are eigenvalues of S, T. Then $ST\vec{v} = TS\vec{v}$ $\forall v$ and so $ST = TS$. $\square$

<u>example</u>: for each of the following, find a basis which diagonalizes T

- $T: P_2 \to P_2$, $T(A) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot A$

  2 options: compute $[T]_B^B$ or find eigenvalues by inspection.

  Past here, it is all computation.

- follow up, compute $\det(T)$

Quotient Spaces

interior direct sum

<u>example</u>: Prove that $W \cong \frac{U \oplus W}{U}$

remark: if $\dim < \infty$, then this is immediate. $\dim = \infty$ requires work.

<u>proof</u>: let $\{w_i\}$ be a basis of W.

We claim $\{w_i + U\}$ is a basis of $U \oplus W / U$

<u>linear independence</u>: Immediate from linear independence of $\{w_i\}$.

<u>spanning</u>: Let $\exists\ \vec{v} \in \frac{U \oplus W}{U}$. Unraveling definitions,

$\exists\ u \in U,\ w \in W$ s.t. $\vec{v} = u + w + U$

Then $v = w + U$. Bc $\{w_i\}$ spans W, $\exists\ x_1, \dots, x_n$

and $w_1, \dots, w_n$ (abuse of notation) s.t. $v = x_1(w_1 + U) + \dots$

Then $\{w_i + U\}$ is a basis of $U \oplus W / U$.

Define $T : W \to \frac{U \oplus W}{U}$ by $w_i \longmapsto w_i + U$ and

extending by linearity. Then T is an isomorphism. $\square$

extra problems

- V is a real vector space w/ $T, S \in \mathcal{L}(V)$. Sps T has eigenvalues $0, 1, 2$ and S is invertible. Prove that

$$\{S, T, T^2\} \text{ is linearly independent.}$$

proof: $aS + bT + cT^2 = 0$. Choosing $v \neq 0$ s.t. $Tv = 0$ gives $a = 0$.

Choosing $Tu = u$ and $Tw = 2w$ gives $b + c = 0$, $b + 2c = 0$

which concludes $a = b = c = 0$. $\square$

- give an example of $T, S \in \mathcal{L}(V)$ s.t. T is diagonalizable but $S \circ T$ is not.

- sps $\dim V = 4$ and $T \in \mathcal{L}(V)$ satisfies $\dim E_\lambda(T) = 4$ for some λ. Compute $[T]_B^B$ for <u>any</u> B.

5/22/24

Logistics: expect midterm grading to take ~1 week

Eigenvectors/vals

<u>example</u> Binet's formula

Using diagonalizability, we'll prove an explicit formula for the Fibonacci numbers. Namely, w/ $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$,

$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - (1-\varphi)^n\right) \quad \text{w/} \quad \varphi = \frac{1+\sqrt{5}}{2}$$

proof: Let $v_0 = \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Then $v_n = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = A^n v_0$.

We calculate A has eigenvalues φ, $1-\varphi$ w/ eigenvectors $\begin{pmatrix} 1 \\ \varphi \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1-\varphi \end{pmatrix}$. So

$$A = \begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix} \begin{pmatrix} \varphi & 0 \\ 0 & 1-\varphi \end{pmatrix} \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi - 1 & 1 \\ 1-\varphi & -1 \end{pmatrix}$$

So $A^n = P \begin{pmatrix} \varphi^n & 0 \\ 0 & (1-\varphi)^n \end{pmatrix} P^{-1}$

$$v_n = A^n v_0 = P \begin{pmatrix} \varphi^n & 0 \\ 0 & (1-\varphi)^n \end{pmatrix} \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$= \frac{1}{\sqrt{5}} P \begin{pmatrix} \varphi^n \\ -(1-\varphi)^n \end{pmatrix}$$

$$\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \varphi^n - (1-\varphi)^n \\ \sim \end{pmatrix} \Rightarrow F_n = (\varphi^n - (1-\varphi)^n)/\sqrt{5}.$$

$\square$

computation

check the following for diagonalizability (over $\mathbb{R}$) and diagonalize if possible

- $$A = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ -1 & -1 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & -1 & -1 \\ 0 & 1 & -2 \\ 1 & 0 & 1 \end{pmatrix}}_{P} \begin{pmatrix} 2 & & \\ & 2 & \\ & & 4 \end{pmatrix} P^{-1}$$

- $$\begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} -4 & 1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} -2 & \\ & 5 \end{pmatrix} P^{-1}$$

- $$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$$ char poly $= (\lambda^2+1)(\lambda-1)$ which doesn't split over $\mathbb{R}$

examples

- nilpotent matrices

  sps $A^n = 0$ for some $n > 0$ and $A \neq 0$. Prove that A is not diagonalizable. ($A^n = 0$ is "nilpotent".)

  proof: If $A = PDP^{-1}$ then $A^n = PD^nP^{-1} = 0 \Rightarrow D = 0$

  $\Rightarrow A = 0$ ※.

- challenge sps $\dim V = d$. If $A^n = 0$ for some $n = 0$. Then $A^d = 0$.

  hint (honors only): use Cayley-Hamilton

  proof: if $n < d$ then done.

  if $n > d$, the CH $\Rightarrow$ minimal poly w/ deg $\leq d$ and minimal poly divides $A^n \Rightarrow A^m$ for $m \leq d$ $\square$

- V is a real vector space w/ $T, S \in \mathcal{L}(V)$. Sps T has eigenvalues $0, 1, 2$ and S is invertible. Prove that

  $$\{S, T, T^2\} \text{ is linearly independent.}$$

  proof: $aS + bT + cT^2 = 0$. Choosing $v \neq 0$ s.t. $Tv = 0$ gives $a = 0$.

  Choosing $Tu = u$ and $Tw = 2w$ gives $b + c = 0$, $b + 2c = 0$ which concludes $a = b = c = 0$. $\square$

examples

- Fix $A \in \mathcal{L}(V)$ and define $\phi_A : \mathcal{L}(V) \to \mathcal{L}(V)$ by

$$\phi_A(T) = A \circ T.$$

If λ is an eigenvalue of A, then λ is an eigenvalue of ϕ_A.

proof: By def, $E_\lambda(A) \neq \{\vec{0}\}$. Let P be a projection onto $E_\lambda(A)$. Then $P \neq 0$ and $\forall\, v \in V$,

$Pv \in E_\lambda \Rightarrow A(Pv) = \lambda Pv$.

Then $\phi_A P = \lambda P$. $\square$

- challenge: sps $\dim V = n < \infty$

if A is diagonalizable, then ϕ_A is diagonalizable.

proof: Let $\{v_i\}$ be an eigenbasis of V w.r.t. A.

Define P_i^j s.t. $P_i^j(\dots + \alpha_i v_i + \dots) = \alpha_i v_j$

We claim P_i^j is an eigenbasis of $\mathcal{L}(V)$.

- eigenvector: $\forall\, v$, $AP_i^j v = \lambda_j P_i^j v \Rightarrow \phi_A P_i^j = \lambda_j P_i^j$
- spanning: follows b/c $\{v_i\}$ is a basis of V.
- basis: $\dim \mathcal{L}(V) = n^2$ and $\#\{P_i^j\} = n^2$. $\square$

- open Q (to me)

Does this hold for $\dim V = \infty$?

Cayley-Hamilton (honors only)

<u>example</u> prove that if A is invertible then A^{-1} can be written as a polynomial $p(A)$.

<u>proof</u> $A^n + \dots + a_1 A + a_0 I = 0$

Rewrite as $A^k(A^{n-k} + \dots + a_k I) = 0$

for maximal k. Then $a_k \neq 0$ and

$-a_k^{-1} A(A^{n-k-1} + \dots + a_{k+1}) = I$

so $A^{-1} = -a_k^{-1}(A^{n-k-1} + \dots + a_{k+1})$.

use this to find A^{-1} for $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

$\chi_A = (\lambda - 1)\lambda - 1 = \lambda^2 - \lambda - 1$

so $A^2 - A = I \Rightarrow A(A-I) = I \Rightarrow A^{-1} = A - I$.

5/28/25

Honors only

22.1 - Orthonormal

Recall: the inner product gives us a notion of geometry in a vector space. Specifically, it defines

- length (norm): $\|\vec{v}\|^2 = \langle v, v \rangle$
- angle (in $\mathbb{R}^n$): $\langle u, v \rangle = \|u\| \|v\| \cos\theta$

definition

- vectors u, v are orthogonal ($u \perp v$) if $\langle u, v \rangle = 0$.
- unit vectors satisfy $\|u\| = 1$

this generalizes naturally to sets of vectors

definition: we say a set $S \subset V$ is

- orthogonal if $\forall\, u \neq v \in S$, $u \perp v$
- orthonormal if S is orthogonal and $\|u\| = 1$ $\forall\, u \in S$.

notation: we use $\langle x, y \rangle = \delta_{x,y}$ as shorthand for this.

$\delta_{x,y} = 1$ if $x = y$ and 0 if $x \neq y$.

<u>technique</u>: Given a linear combination of orthogonal vectors

$$\alpha_1 v_1 + \dots + \alpha_n v_n$$

we can take the inner product w/ v_i to isolate α_i.

Namely, $\langle \alpha_1 v_1 + \dots + \alpha_n v_n, v_i \rangle = \alpha_1 \langle v_1, v_i \rangle + \dots + \alpha_n \langle v_n, v_i \rangle$

$$= \alpha_i \langle v_i, v_i \rangle$$

This is very useful in the following two theorems.

<u>theorem</u> (orthogonal => linearly independent)

Suppose V is an inner product space and $S \subset V$ is an orthogonal set of nonzero vectors. Then S is linearly ind.

<u>proof</u>: Suppose $\alpha_1 s_1 + \dots + \alpha_n s_n = 0$ for $s_1, \dots, s_n \in S$.

Taking the inner product w/ s_i and noting $\langle s_j, s_i \rangle = \delta_{ji}$

$$\alpha_1 \langle s_1, s_i \rangle + \dots + \alpha_n \langle s_n, s_i \rangle = 0$$

$$\alpha_i \langle s_i, s_i \rangle = 0$$

B/c $s_i \neq 0$, $\langle s_i, s_i \rangle \neq 0 \Rightarrow \alpha_i = 0 \ \forall i$. $\square$

<u>theorem</u> Let $S \subset V$ be an orthogonal set of nonzero vectors.

If $\vec{v} \in \text{span}(S)$ then $\vec{v} = \sum_{s \in S} \frac{\langle v, s \rangle}{\|s\|^2} s$.

<u>note</u>: this sum is always finite b/c

if $v = a_1 s_1 + \dots + a_n s_n$ then $a_i = \frac{\langle v, s_i \rangle}{\|s_i\|^2}$.

<u>proof</u>: Immediate from above technique. $\square$

<u>corollary</u> If $B = \{x_1, \dots, x_n\}$ is an orthonormal basis of V, then $\forall\, v \in V$, ${}_B[v] = \begin{bmatrix} \langle v, x_1 \rangle \\ \vdots \\ \langle v, x_n \rangle \end{bmatrix}$.

Similarly, if $T \in \mathcal{L}(V)$,

$$\left({}_B[T]_B\right)_{ij} = \langle T(x_j), x_i \rangle.$$

This corollary implies that orthonormal bases are incredibly nice to work w/ computationally. A natural question is whether orthonormal bases exist. w/ the following theorem, we can construct them.

<u>theorem</u> (Gram-Schmidt)

Let $\{v_1, v_2, \dots\}$ be linearly independent. Define

$$x_1 = v_1$$

$$x_2 = v_2 - \frac{\langle v_2, x_1 \rangle}{\|x_1\|^2} x_1$$

$$\vdots$$

$$x_k = v_k - \sum_{j=1}^{k-1} \frac{\langle v_k, x_j \rangle}{\|x_j\|^2} x_j$$

Then $\{x_1, x_2, \dots\}$ is linearly independent and orthogonal.

Moreover, $\operatorname{span}\{x_1, \dots, x_k\} = \operatorname{span}\{v_1, \dots, v_k\}$ $\forall\, k$.

<u>note</u>: only finite k for the span.

<u>corollary</u>: any finite dimensional vector space has an orthonormal basis. <u>Not</u> true for infinite dimensions.

<u>proof</u>: WLOG, sps $k > l$. To show orthogonality, we calculate

$$\langle x_k, x_l \rangle = \langle v_k, x_l \rangle - \sum_{j=1}^{k-1} \frac{\langle v_k, x_j \rangle}{\|x_j\|^2} \langle x_j, x_l \rangle$$

$$= \langle v_k, x_l \rangle - \frac{\langle v_k, x_l \rangle}{\|x_l\|^2} \langle x_l, x_l \rangle$$

$$= 0.$$

To show the span claim, we proceed by induction.

<u>Base case $(n=1)$:</u> $\{x_1\} = \{v_1\} \Rightarrow \operatorname{span}\{x_1\} = \operatorname{span}\{v_1\}$.

<u>Inductive step:</u> Sps $\operatorname{span}\{x_1, \dots, x_k\} = \operatorname{span}\{v_1, \dots, v_k\}$.

By construction, $x_{k+1} \in \operatorname{span}\{x_1, \dots, x_k, v_{k+1}\}$

and $\operatorname{span}\{x_1, \dots, x_k, v_{k+1}\} = \operatorname{span}\{x_1, \dots, x_k\} + \operatorname{span}\{v_k\}$

$$= \operatorname{span}\{v_1, \dots, v_{k+1}\}$$

Therefore, because

$$\operatorname{span}\{x_1, \dots, x_k\} = \operatorname{span}\{v_1, \dots, v_k\} \subset \operatorname{span}\{v_1, \dots, v_{k+1}\}$$

and $x_{k+1} \in \operatorname{span}\{v_1, \dots, v_{k+1}\}$, it follows that

$\operatorname{span}\{x_1, \dots, x_{k+1}\} \subset \operatorname{span}\{v_1, \dots, v_{k+1}\}$.

Rearranging the formula for x_{k+1}, we find $v_{k+1} \in \operatorname{span}\{x_1, \dots, x_{k+1}\}$.

B/c $v_1, \dots, v_k \in \operatorname{span}\{x_1, \dots, x_k\} \subset \operatorname{span}\{x_1, \dots, x_{k+1}\}$,

this concludes $\operatorname{span}\{x_1, \dots, x_{k+1}\} = \operatorname{span}\{v_1, \dots, v_{k+1}\}$.

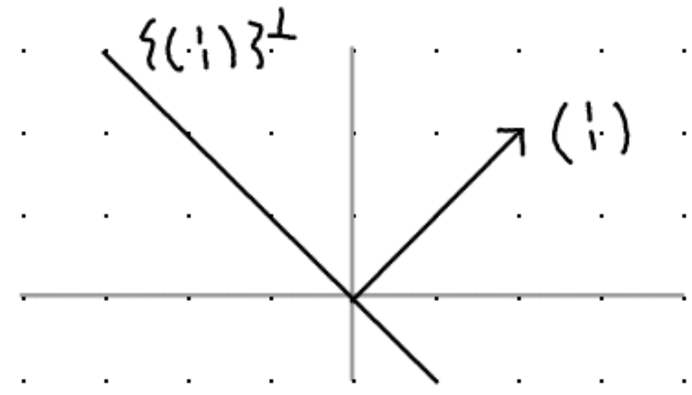
$\square$

22.2 - Orthogonal Complement

<u>definition</u>: given a set $S \subset V$, the orthogonal complement of S is $S^\perp = \{ x \in V : \langle x, y \rangle = 0 \ \forall y \in S \}$.

<u>example</u> Consider $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2$. Its orthogonal complement is

$$\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}^\perp = \left\{ \begin{pmatrix} a \\ -a \end{pmatrix} : a \in \mathbb{R} \right\}$$



<u>theorem</u>: Let V be an inner product space.

① $\forall S \subset V$, $S^\perp$ is an inner product space

② $\forall S_1 \subset S_2 \subset V$, $S_1^\perp \supset S_2^\perp$

③ $V^\perp = \{0\}$

④ $\{0\}^\perp = V$

<u>proof</u> ① follows by checking the subspace axioms

②: Sps $x \in S_2^\perp$. Then $\forall s \in S_1 \subset S_2$, $\langle s, x \rangle = 0$.

Hence $x \in S_1^\perp$. Therefore $S_2^\perp \subset S_1^\perp$

③: By linearity, $\langle 0, x \rangle = 0 \ \forall x \in V$. Then $\{0\} \subset V^\perp$

Sps $x \in V^\perp$. Then $x \in V$ and so $\langle x, x \rangle = 0$.

Therefore $x = 0$ and so $V^\perp \subset \{0\}$.

④ By def, $\{0\}^\perp \subset V$. By linearity, $\langle 0, x \rangle = 0 \ \forall x \in V$.

Therefore $V \subset \{0\}^\perp$. $\square$

<u>theorem</u> Let $W \subset V$ be a subspace.

① $W \cap W^\perp = \{0\}$

② If $\dim W < \infty$ then $V = W \oplus W^\perp$

③ $W \subset (W^\perp)^\perp$

④ If $\dim W < \infty$ then $W = (W^\perp)^\perp$

<u>proof</u>:

① By def of a subspace, $0 \in W \cap W^\perp$.

Consider $x \in W \cap W^\perp$. Then $\langle x, x \rangle = 0 \Rightarrow x = 0$.

② Let $v_1, \ldots, v_k$ be an orthonormal basis of W.

Let $\exists$ $x \in V$ and define $w = \langle x, v_1 \rangle v_1 + \cdots + \langle x, v_k \rangle v_k$.

Then $w \in W$ and $\forall$ $y \in W$,

$$\begin{aligned} \langle x, y \rangle &= \sum_i \langle x, \langle y, v_i \rangle v_i \rangle \\ &= \sum_i \langle v_i, y \rangle \langle x, v_i \rangle \\ &= \langle \sum_i \langle x, v_i \rangle v_i, y \rangle \\ &= \langle w, y \rangle. \end{aligned}$$

So $\langle x - w, y \rangle = 0$ $\forall$ $y \in W$. Hence $x - w \in W^\perp$.

As $x = w + (x - w)$, this concludes $W + W^\perp$.

③ Consider $w \in W$. Then $\forall\ x \in W^\perp$, $\langle w, x \rangle = 0$.

Then $w \in (W^\perp)^\perp$ and so $W \subset (W^\perp)^\perp$.

④ Sps $x \in (W^\perp)^\perp$. From ②, $\exists\ w \in W$ and $v \in W^\perp$

s.t. $x = w + v$. Then $x - w = v \in W^\perp$.

By ③, $w \in (W^\perp)^\perp$, so $x - w \in (W^\perp)^\perp$. Then

$v \in W^\perp \cap (W^\perp)^\perp$. By ①, $v = \vec{0}$. Therefore $x = w \in W$.

So $(W^\perp)^\perp \subset W$. $\square$

taking inspiration from the preceding theorem, we define...

<u>definition</u>: Let $W \subset V$ be a subspace. For any

$v \in W + W^\perp$, $\exists!\ \text{proj}_W(v) \in W$ called the orthogonal

projection of v onto W s.t. $v - \text{proj}_W(v) \in W^\perp$.

<u>note</u>: $W + W^\perp$ is not necessarily all of V.

So $\text{proj}_W(v)$ may be undefined.

non-Honors course

inner products

recall, an inner product $\langle \cdot, \cdot \rangle : V \times V \to F$ satisfies

① $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$

② $\langle ax, y \rangle = a \langle x, y \rangle$

④ for $x \neq 0$, $\langle x, x \rangle \in \mathbb{R}$ and $\langle x, x \rangle > 0$

③ $\langle x, y \rangle = \overline{\langle y, x \rangle}$

why complex conjugate for #3? Otherwise #4 is not possible.

Sps #3 was just $\langle x, y \rangle = \langle y, x \rangle$ w/ $F = \mathbb{C}$.

Take any $x \neq 0$. Then $ix \neq 0$. But

$$\langle ix, ix \rangle = i \langle x, ix \rangle = - \langle x, x \rangle$$

so either $\langle ix, ix \rangle < 0$ or $\langle x, x \rangle < 0$, contradicting #4.

basic example

consider $\mathbb{C}^3$ w/ $\left\langle \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} d \\ e \\ f \end{pmatrix} \right\rangle = a\bar{d} + b\bar{e} + c\bar{f}$

compute $\langle (1, 1+i, -i)^T, (3, -i, -4-i)^T \rangle$

recall, $\bar{\cdot}$ just flips all i's to $-i$'s

$$\overline{x+iy} = x - iy \text{ for } x, y \in \mathbb{R}$$

abstract examples

- on $C^\infty([0,2\pi] \to \mathbb{C})$, prove that

$$\langle f,g \rangle = \int_0^{2\pi} f(x)\overline{g(x)}\,dx$$

is an inner product

  - non-example: is $\langle f,g \rangle = \int_0^{\pi} f(x)\overline{g(x)}\,dx$ an inner product on $C^\infty([0,2\pi] \to \mathbb{C})$?

- Let $(V, \langle \cdot,\cdot \rangle)$ be an inner product space. Prove that $\langle \cdot,\cdot \rangle_T$ defined by $\langle \cdot,\cdot \rangle_T = \langle T\cdot, T\cdot \rangle$ is an inner product iff T is injective.

proof: linearity and conjugate symmetry are immediate. positivity iff injective follows from $\ker T = \{\vec{0}\}$ iff injective. $\square$

<u>theorem</u>: let V be a complex finite-dimensional inner product space. Let $v_1, \dots, v_n$ be an orthonormal basis.

Then $\langle x,y \rangle = \sum_i \langle x, v_i \rangle \langle v_i, y \rangle = \sum_i \langle x, v_i \rangle \cdot \overline{\langle y, v_i \rangle}$

i.e. $\langle x,y \rangle = \langle [x]_B, [y]_B \rangle_{std}$

note: this implies that the inner product space $(V, \langle \cdot,\cdot \rangle)$ is equivalent to $(\mathbb{C}^n, \langle \cdot,\cdot \rangle_{std})$

- <u>challenge</u>: Suppose that V is an inner product space w/ $\dim V = 3$.

  Sps $\exists\ v_0, w_0 \in V$ s.t. $\langle v_0, w_0 \rangle = 4$.

  Define $T: V \to V : v \mapsto \langle v, v_0 \rangle w_0$.

  a) compute $\operatorname{rank}(T)$ and $\operatorname{nullity}(T)$

  $w_0 \neq 0$ and $\operatorname{im} T = \operatorname{span}\{w_0\}$. So $\operatorname{rank} T = 1$, $\operatorname{nullity}(T) = 2$.

  b) prove T is diagonalizable. Find its diagonal form.

  $T w_0 = 4 w_0$ and $\dim \ker T = 2$. So

  $$[T]_B^B = \begin{pmatrix} 4 & & \\ & 0 & \\ & & 0 \end{pmatrix}.$$

6/5/25

Logistics: prepare @ the same time as your final

115AH: 8am

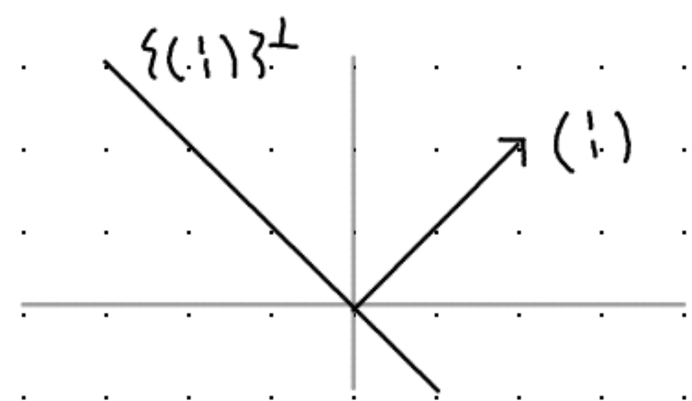
115A: 11:30am

non-honors

<u>definition</u>: given a set $S \subset V$, the orthogonal complement of S is $S^\perp = \{ x \in V : \langle x, y \rangle = 0 \ \forall y \in S \}$.

<u>example</u> Consider $\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2$. Its orthogonal complement is

$$\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}^\perp = \left\{ \begin{pmatrix} a \\ -a \end{pmatrix} : a \in \mathbb{R} \right\}$$



<u>example</u>: calculate $\{x\}^\perp$ in P_2 w/

$$\langle f, g \rangle = \int_{-1}^{1} fg \, dx$$

$$0 = \langle a + bx + cx^2, x \rangle = b \langle x, x \rangle \Rightarrow b = 0$$

$\{x\}^\perp = \{a + cx^2\}$ even polynomials.

non-honors

<u>theorem 5</u>: Let V be an inner product space w/ subspace W.

1) $W \cap W^\perp = \{0\}$

2) if $\dim W < \infty$ then $W + W^\perp = V$

3) $W \subset (W^\perp)^\perp$

4) if $\dim W < \infty$ then $W = (W^\perp)^\perp$

<u>proof</u>:

① By def of a subspace, $0 \in W \cap W^\perp$.

Consider $x \in W \cap W^\perp$. Then $\langle x, x \rangle = 0 \Rightarrow x = 0$.

② Let $v_1, \ldots, v_k$ be an orthonormal basis of W.

Let $\exists$ $x \in V$ and define $w = \langle x, v_1 \rangle v_1 + \cdots + \langle x, v_k \rangle v_k$.

Then $w \in W$ and $\forall$ $y \in W$,

$$\begin{aligned} \langle x, y \rangle &= \sum_i \langle x, \langle y, v_i \rangle v_i \rangle \\ &= \sum_i \langle v_i, y \rangle \langle x, v_i \rangle \\ &= \langle \sum_i \langle x, v_i \rangle v_i, y \rangle \\ &= \langle w, y \rangle. \end{aligned}$$

So $\langle x - w, y \rangle = 0$ $\forall$ $y \in W$. Hence $x - w \in W^\perp$.

As $x = w + (x - w)$, this concludes $W + W^\perp$.

③ Consider $w \in W$. Then $\forall\ x \in W^\perp$, $\langle w, x \rangle = 0$.

Then $w \in (W^\perp)^\perp$ and so $W \subset (W^\perp)^\perp$.

④ Sps $x \in (W^\perp)^\perp$. From ②, $\exists\ w \in W$ and $v \in W^\perp$

s.t. $x = w + v$. Then $x - w = v \in W^\perp$.

By ③, $w \in (W^\perp)^\perp$, so $x - w \in (W^\perp)^\perp$. Then

$v \in W^\perp \cap (W^\perp)^\perp$. By ①, $v = \vec{0}$. Therefore $x = w \in W$.

So $(W^\perp)^\perp \subset W$. $\square$

<u>example</u> Let V be finite dimensional w/ subspaces W_1, W_2.

Then $(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$

$\subseteq$: sps $\exists\ v \in (W_1 + W_2)^\perp$. Then $\forall\ w_1 \in W_1$,

$w_1 \in W_1 + W_2 \Rightarrow \langle v, w_1 \rangle = 0$. Then $v \in W_1^\perp$.

Similarly, $v \in W_2^\perp$ so $v \in W_1^\perp \cap W_2^\perp$.

$\supseteq$: Sps $\exists\ u \in W_1^\perp \cap W_2^\perp$. Consider $w_1 + w_2 \in W_1 + W_2$.

Then $\langle u, w_1 + w_2 \rangle = \langle u, w_1 \rangle + \langle u, w_2 \rangle = 0$.

Therefore $u \in (W_1 + W_2)^\perp$. $\square$

inner product examples

- <u>challenge</u>: Suppose that V is an inner product space w/ $\dim V = 3$.

  Sps $\exists\ v_0, w_0 \in V$ s.t. $\langle v_0, w_0 \rangle = 4$.

  Define $T: V \to V : v \mapsto \langle v, v_0 \rangle w_0$.

  a) compute $\operatorname{rank}(T)$ and $\operatorname{nullity}(T)$

  $w_0 \neq 0$ and $\operatorname{im} T = \operatorname{span}\{w_0\}$. So $\operatorname{rank} T = 1$, $\operatorname{nullity}(T) = 2$.

  b) prove T is diagonalizable. Find its diagonal form.

  $T w_0 = 4 w_0$ and $\dim \ker T = 2$. So

  $$[T]_B^B = \begin{pmatrix} 4 & & \\ & 0 & \\ & & 0 \end{pmatrix}.$$

Honors

recall: for $T: V \to W$, T^* is the <u>unique</u> map s.t.

$$\langle Tx, y\rangle_W = \langle x, T^* y\rangle$$

<u>theorem 23.7</u>: Let V, W be inner product spaces over F.

Let $T: V \to W$ have an adjoint.

(a) $\langle x, Ty\rangle_W = \langle T^* x, y\rangle$

$\langle x, Ty\rangle_W = \overline{\langle Ty, x\rangle_W} = \overline{\langle y, T^* x\rangle_V} = \langle T^* x, y\rangle_V$

(b) T^* has an adjoint: $T^{**} = T$

immediate from (a)

(c) sps $S: V \to W$ has an adjoint. Then $(S+T)^* = S^* + T^*$

$\langle (S+T)x, y\rangle_W = \langle Sx, y\rangle_W + \langle Tx, y\rangle_W = \langle x, S^* y\rangle_V + \langle x, T^* y\rangle_V$

$= \langle x, (S^* + T^*) y\rangle_V$

(d) $(aT)^* = \bar{a} T^*$

$\langle aTx, y\rangle_W = a\langle x, T^* y\rangle_V = \langle x, \bar{a} T^* y\rangle$

(e) sps $S: W \to Z$ has an adjoint. Then $(ST)^* = T^* S^*$

$\langle STx, y\rangle_Z = \langle Tx, S^* y\rangle_W = \langle x, T^* S^* y\rangle_V$

(f) $id_V^* = id_V$: $\langle id_V x, y\rangle = \langle x, id_V y\rangle$

(g) if T^{-1} exists and has an adjoint, then $(T^{-1})^* = (T^*)^{-1}$

combine (e), (f): $(T^{-1})^* T^* = (TT^{-1})^* = id_V = (T^{-1}T)^* = T^* (T^{-1})^*$

<u>theorem 24.4</u>: Let V be an inner product space w/ subspace W. Let $T: V \to V$ have an inner product.

(a) if W is T-invariant then $W^\perp$ is T^* invariant

Let $\exists\ v \in W^\perp$. Then $\forall\ x \in W$, $Tx \in W$ and so

$$\langle T^* v, x \rangle = \langle v, Tx \rangle = 0$$

Hence $T^* v \in W^\perp$. Therefore $W^\perp$ is T^*-invariant.

(b) Sps W is T-invariant and T^*-invariant.

Then T_W has an adjoint $(T_W)^* = (T^*)_W$.

Moreover, if T is normal, then T_W is normal.

recall: T is normal if $TT^* = T^*T$

By definition, T_W and $(T^*)_W$ are well-defined $W \to W$.

Consider $w_1, w_2 \in W$. Then

$$\langle T_W w_1, w_2 \rangle = \langle T w_1, w_2 \rangle = \langle w_1, T^* w_2 \rangle = \langle w_1, (T^*)_W w_2 \rangle$$

Therefore $(T_W)^* = (T^*)_W$.

Consider $x \in W$. Then

$$\begin{aligned} T_W (T_W)^* x &= T_W (T^*)_W x = T_W T^* x \\ &= T T^* x = T^* T x \\ &= (T^*)_W T_W x = (T_W)^* T_W x \end{aligned}$$

so T_W is normal.

Adjoints

(non)-examples

- consider $C^1([0,1]\to\mathbb{R})$ w/ L^2 inner product. Then

  ∂_x does not have an adjoint

  intuition: $\langle \partial_x f, g\rangle = \int_0^1 \partial_x f\, g = f(1)g(1) - f(0)g(0) - \int_0^1 f\,\partial_x g$

  if boundary terms are 0, then yes

  restrict attention to $W = \{f \mid f(0) = f(1) = 0\} \subset C^1([0,1]\to\mathbb{R})$.

  then $\partial_x^* = -\partial_x$

  or restrict attention to finite dimensions, $P_1(\mathbb{R}) \subset C^1$

  $\langle \partial_x(a_0 + a_1 x), \; b_0 + b_1 x\rangle$

  $$= \int_0^1 a_1(b_1 x + b_0)$$

  $$= \frac{a_1 b_1}{2} + b_0 a_1$$

  $$= \int_0^1 (a_1 x + a_0)(c_1 x + c_0)$$

  $$= \frac{a_1 c_1}{3} + \frac{a_0 c_1 + a_1 c_0}{2} + a_0 c_0$$

  $$= a_1\left(\frac{c_1}{3} + \frac{c_0}{2}\right) + a_0\left(\frac{c_1}{2} + c_0\right) \qquad 2c_0 = -c_1$$

  $$\frac{c_1}{12} = \frac{b_1}{2} + b_0$$

  $$c_1 = 6b_1 + 12b_0 \rightsquigarrow c_0 = -3b_1 - 6b_0$$

  $$= \int_0^1 (a_1 x + a_0)\left((6b_1 + 12b_0)x - 3b_1 - 6b_0\right)$$

  $$\partial_x^* : (b_0 + b_1 x) \longmapsto -3b_1 - 6b_0 + (6b_1 + 12b_0)x$$

helpful trick: if $\langle x, y\rangle = 0 \ \forall y$, then $x = 0$.

example

- $(\mathrm{im}(T^*))^\perp = \ker T$, $T: V \to V$

  $\subseteq$: $x \in \mathrm{im}(T^*)^\perp$. Then $\forall y \in V$,

  $$0 = \langle x, T^* y\rangle = \langle Tx, y\rangle$$

  In particular, $\langle Tx, Tx\rangle = 0 \Rightarrow Tx = 0$.

  $\supseteq$: $x \in \ker T$. Then $\forall T^* y$,

  $$\langle T^* y, x\rangle = \langle y, Tx\rangle = 0$$

- $\ker(T^* T) = \ker(T)$

  $\supseteq$: see midterm 2

  $\subseteq$: sps $T^* T u = 0$. Then

  $$0 = \langle T^* T u, u\rangle = \langle Tu, Tu\rangle \Rightarrow Tu = 0.$$

Cayley-Hamilton (honors only)

<u>example</u> prove that if A is invertible then A^{-1} can be written as a polynomial $p(A)$.

<u>proof</u> $A^n + \dots + a_1 A + a_0 I = 0$

Rewrite as $A^k(A^{n-k} + \dots + a_k I) = 0$

for maximal k. Then $a_k \neq 0$ and

$-a_k^{-1} A(A^{n-k-1} + \dots + a_{k+1}) = I$

so $A^{-1} = -a_k^{-1}(A^{n-k-1} + \dots + a_{k+1})$.

use this to find A^{-1} for $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

$\chi_A = (\lambda - 1)\lambda - 1 = \lambda^2 - \lambda - 1$

so $A^2 - A = I \Rightarrow A(A-I) = I \Rightarrow A^{-1} = A - I$

non-reflexivity of orthogonal complements

<u>example</u>: $V = C[-1,1]$ w/ standard inner product.

$W = \{f : f(0) = 0\}$ is a subspace but $W^\perp = \{0\}$

$\Rightarrow (W^\perp)^\perp = V \neq W$.

extra time

theorem: let V be a complex finite-dimensional inner product space. Let $v_1, \dots, v_n$ be an orthonormal basis.

Then $\langle x, y \rangle = \sum_i \langle x, v_i \rangle \langle v_i, y \rangle = \sum_i \langle x, v_i \rangle, \overline{\langle y, v_i \rangle}$

i.e. $\langle x, y \rangle = \langle [x]_B, [y]_B \rangle_{std}$

note: this implies that the inner product space $(V, \langle \cdot, \cdot \rangle)$ is equivalent to $(\mathbb{C}^n, \langle \cdot, \cdot \rangle_{std})$

example Let V be finite dimensional w/ subspaces W_1, W_2.

Then $(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$

$\subseteq$: sps $\exists$ $v \in (W_1 + W_2)^\perp$. Then $\forall$ $w_1 \in W_1$, $w_1 \in W_1 + W_2 \Rightarrow \langle v, w_1 \rangle = 0$. Then $v \in W_1^\perp$.

Similarly, $v \in W_2^\perp$ so $v \in W_1^\perp \cap W_2^\perp$.

$\supseteq$: Sps $\exists$ $u \in W_1^\perp \cap W_2^\perp$. Consider $w_1 + w_2 \in W_1 + W_2$.

Then $\langle u, w_1 + w_2 \rangle = \langle u, w_1 \rangle + \langle u, w_2 \rangle = 0$.

Therefore $u \in (W_1 + W_2)^\perp$. $\square$