Abstract vector Spaces

↳ something you can perform linear combinations on

e.g. functions $\mathbb{R} \to \mathbb{R}$

$\{f : \Omega \to \mathbb{R}\} = \mathbb{R}^{\Omega}$

subcase : $\Omega = [n] = \{1, \dots, n\}$

$\mathbb{R}^{[n]} = \mathbb{R}^n$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha(1) \\ \vdots \\ \alpha(n) \end{pmatrix}$$

$\mathbb{R}[t]$ = polynomials over $\mathbb{R}$

$\mathbb{R}^{\mathbb{N}}$ = infinite sequences of real numbers.

$(a_0, a_1, \dots)$

$(a(0), a(1), \dots)$ alternative function notation

$\mathbb{R}$ "scalars"

V vector space - elements of V are "vectors"

<u>Axioms</u>

"+" is a binary operation on V: $\underline{+ : V \times V \to V}$

① $(V, +)$ is an <u>abelian group</u>.

(a) $(\forall a, b \in V)(\exists! c \in V$ called $c = a+b)$

(addition is defined)

$\forall$ for all

$\exists$ there exists

$\forall a, b, c \in V$

(b) $(a+b)+c = a+(b+c)$

(addition is associative)

(c) $(\exists 0)(a+0 = 0+a = a)$

(additive identity exists)

(d) $(\forall a \in V)(\exists b)(a+b = b+a = 0)$

(additive inverse exists) notation: $b = -a$

(e) $(\forall a, b \in V)(a+b = b+a)$

(addition is commutative)

② Multiplication by scalars

$$\mathbb{R} \times V \to V$$

$$(\lambda, a) \to \lambda a$$

(a) $(\forall \lambda \in \mathbb{R})(\forall a \in V)(\exists!\, b \in V$ called $b = \lambda a)$

(scaler multiplication is defined)

(b) $(\forall \lambda, \mu \in \mathbb{R})(\forall a \in V)((\lambda \cdot \mu) a = \lambda (\mu a))$

(mixed associativity)

multiplication of scalars

scalar × vector

(c) $(\forall \lambda, \mu \in \mathbb{R})(\forall a \in V)((\lambda + \mu) a = \lambda a + \mu a)$

(mixed distributivity - scalars)

scaler addition

scaler × vector

vector addition

(d) $(\forall \lambda \in \mathbb{R})(\forall a, b \in V)(\lambda (a+b) = \lambda a + \lambda b)$

(distributivity - vectors)

③ $1 \cdot a = a$ (rules out mapping everything to 0)

(axiom of normalization)

<u>Cor.</u> $(\forall \lambda \in \mathbb{R})(\forall a \in V)(\lambda a = \underline{0} \Leftrightarrow \lambda = 0 \text{ or } a = \underline{0})$

$0 \in V \qquad 0 \in \mathbb{R} \qquad 0 \in V.$

<u>Proof</u> (1) WTS: $\lambda = 0 \Rightarrow \lambda a = \underline{0}$

$$0 + 0 = 0$$

$$(0+0)a = 0 \cdot a \quad \text{(Multiply by } a)$$

$$0 \cdot a + 0 \cdot a = 0 \cdot a =: f \quad \text{(Axiom 2c)}$$

$$f + f = f$$

<u>DC</u>: $f = 0$.

$$f + f + (-f) = f + (-f) \quad \text{(Axiom 1d - add } -f)$$

$$f = f + 0 = f + (f + (-f)) = (f + (-f)) = 0 \quad \text{(Axioms 1b, 1c)}$$

$$f = 0$$

DO If $a = 0$ then $\lambda a = 0$. (part 2)

(3) If $\lambda \neq 0$ and $a \neq 0$ then $\lambda a \neq 0$.

$$\frac{1}{\lambda}(\lambda a) = \left(\frac{1}{\lambda} \cdot \lambda\right) a = 1 \cdot a = a$$

normalization

If $\lambda a = 0$

then $a = \frac{1}{\lambda}(\lambda a) = \frac{1}{\lambda} \cdot 0 = 0$ by (2)

so $a = 0$ (contradiction. $\rightarrow a \neq 0$.)

($\frac{1}{\lambda}$ exists b/c $\lambda \neq 0$).

Linear combination of $a_1, \ldots, a_k \in V$:

$$\sum_{i=1}^{k} \alpha_i a_i \quad \text{where the } \alpha_i \in \mathbb{R}.$$

trivial l.c. - all $\alpha_i = 0$.

The list $a_1, \ldots, a_k$ is linearly independent if only the trivial l.c. evaluates to 0.

$S \subseteq V$ $\quad \mathrm{Span}(S) = \{$all l.c. of finite subsets of $S\}$

Subspace: V vector space

$W \subseteq V$ that is a vector space under the same operations.

↑ subset

All properties with universal quantifiers for operations in V will be inherited by any subset of the space with the same operations.

Thm. $W \subseteq V$ is a subspace $\Leftrightarrow$

(1) $0 \in W$.

DO (2) if $a, b \in W$, then $a + b \in W$.

(3) if $a \in W$, $\lambda \in \mathbb{R}$ then $\lambda a \in W$.

DO Span of any subset of V is a subspace.

Note empty set is not a subspace — vector space is nonempty.

Axiom 1c $\Rightarrow$ vector space is nonempty.

DO In particular, $0_W = 0_V$.

$\operatorname{span}(\operatorname{Span}(S)) = \operatorname{Span}(S)$

Span is an <u>idempotent</u> operator – doing it twice is the same as doing it once

(e.g. – projection for transformations.)

An <u>involution</u> is when doing it twice is the same as doing nothing (identity) $\rightarrow$ $f(f(x)) = I(x)$.

<u>Rank</u> of a list L of vectors:

$rk(L)$ = max # of lin. independent vectors in L.

if no finite max, rank $= \infty$

<u>Def.</u> $\dim V = rk(V)$.

Def. A basis of V is a list L s.t.

(1) L is lin. independent

(2) $\mathrm{Span}(L) = V$

Every linearly independent list of vectors is a basis of its span.

Thm L is a basis $\Longleftrightarrow$ L is a maximal lin independent list.

Lemma If $v_1, \dots, v_k$ are lin. indep. and (A) $v_1, \dots, v_k, v_{k+1}$ are lin. dependent, (B)

then $v_{k+1} \in \mathrm{Span}(v_1, \dots, v_k)$.

Proof (B) $\Rightarrow$ $\exists\, \alpha_1, \dots, \alpha_k, \alpha_{k+1}$ not all zero

s.t. $$\sum_{i=1}^{k+1} \alpha_i v_i = 0$$

If $\alpha_{k+1} \neq 0$ then $v_{k+1} \in \mathrm{Span}(v_1, \dots, v_k)$ (move to other sides divide by α_{k+1}).

So NTS: $\alpha_{k+1} \neq 0$

Suppose $\alpha_{k+1} = 0$.

But then $\sum_{i=1}^{k} \alpha_i v_i = 0$ and not all of

$\alpha_1, \ldots, \alpha_k = 0$ $\longrightarrow$ contradiction (as $v_1, \ldots, v_k$

are lin. indep.) $\square$

basis $\iff$ maximal lin. indep. list

Proof of Thm

(1) $\Rightarrow$ Suppose $v_1, \ldots, v_k$ basis

NTS. $(\forall w \in V)(v_1, \ldots, v_k, w$ is lin dep.)

Since $v_1, \ldots, v_k$ is basis,

$\mathrm{Span}(v_1, \ldots, v_k) = V$, so

$w \in \mathrm{Span}(v_1, \ldots, v_k)$ and

$v_1, \ldots, v_k, w$ is lin. dependent

$\therefore$ $v_1, \ldots, v_k$ maximal.

Wednesday, June 28, 2017 10:36 AM

(2) $\Leftarrow$ Suppose $v_1, \ldots, v_k$ is a maximal lin. indep. set

NTS: $\text{Span}(v_1, \ldots, v_k) \in V$

i.e. NTS: $(\forall w \in V)$, $w \in \text{Span}(v_1, \ldots, v_k)$.

By maximality, $v_1, \ldots, v_k, w$ lin. dependent,

so by lemma, $w \in \text{Span}(v_1, \ldots, v_k)$ $\square$

Thus $v_1, \ldots, v_k$ is basis.

Note: V is finite dimensional if all lin. indep. sets have bounded size, i.e.

$(\exists n_0)(\forall$ lin. indep. set $L)(|L| \leq n_0)$

Thm. In a finite-dimensional space, every linearly independent list can be extended to a basis.

Cor. In a finite-dimensional space, $\exists$ basis.

Proof: Extend the empty list

"Mathematics is about understanding the empty set".
(Fermat's Last Theorem)
Fermat's Last Tango - musical

Isomorphism of Vector Spaces:

$f: V \to W$ bijection s.t.

(1) $(\forall a, b \in V)(f(a +_V b) = f(a) +_W f(b))$

(2) $(\forall a \in V)(\forall \lambda \in \mathbb{R})(f(\lambda \cdot_V a) = \lambda \cdot_W f(a))$

DO If f is an isomorphism $V \to W$ then f^{-1} is an isomorphism $W \to V$.

V is isomorphic to W ($V \cong W$) if $\exists f: V \to W$ s.t. f is isomorphism.

<u>Thm.</u> $v_1, \dots, v_k$ is a basis of $V \Leftrightarrow$
$(\forall w \in V)(\exists! \alpha_1, \dots, \alpha_k \in \mathbb{R})(w = \sum \alpha_i v_i)$

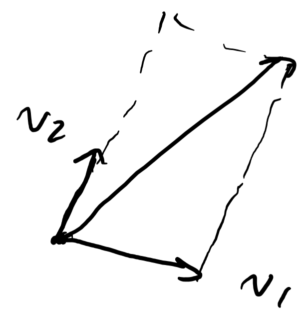
coordinates of w <u>wrt</u>. the basis $v_1, \dots v_k$.
(with respect to)

So B defines a map

$$f : V \to \mathbb{R}^k \qquad \text{coordinatization of } V$$

$$f(w) = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix} \quad \underline{[w]_B}$$

G_2 :



$$w = 1.1 v_1 + 3 v_2$$

$$[w]_B = \begin{bmatrix} 1.1 \\ 3 \end{bmatrix}$$

$B = (v_1, v_2)$

DO $w \mapsto [w]_B$ is an isomorphism.

<u>Cor.</u> If V has a basis consisting of k vectors then $V \cong \mathbb{R}^k$.

<u>First Miracle of Linear Algebra</u>

If $v_1, \dots, v_k$ are linearly independent and all $v_i \in \text{Span}(w_1, \dots, w_\ell)$ then $k \le \ell$.

"impossibility of boosting linear independence"

<u>Cor.</u> If B_1, B_2 are bases of V then

$$|B_1| = |B_2|.$$

(i.e. maximal lin. indep. set is the maximum.)

<u>Proof</u> Let B_2 be the v_i and B_1 be the w_j. By First Miracle, $|B_2| \leq |B_1|$. By symmetry, $|B_1| \leq |B_2|$ and thus

$$|B_1| = |B_2|.$$ □

Back to extending lists for a second...

<u>Thm.</u> In a finite dimensional space, every linearly independent list can be extended to a basis.

Finite-dimensional - bounded # of lin. independent vectors.

Can always add more vectors that are lin. independent if not maximal - must stop at bound ⇒ maximal ⇒ basis.

We actually don't need finite dimensionality ...

Thm. Every vector space has a basis

Proof Use Zorn's Lemma.

REWARD PROBLEM

$f : \mathbb{R} \to \mathbb{R}$ s.t.

Cauchy's functional equation is satisfied:

$$f(x+y) = f(x) + f(y)$$

(e.g. $f(x) = c \cdot x$)

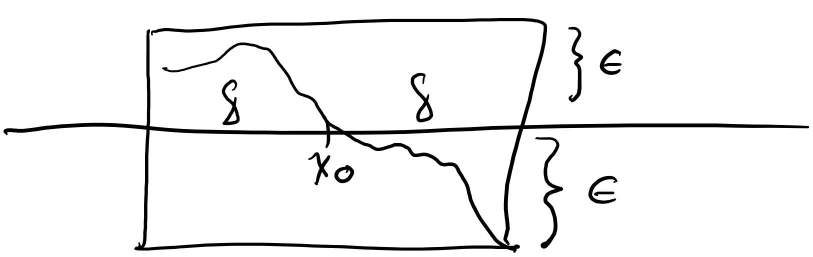
$f(x) = c \cdot x$.

(a) If f is continuous, then f is linear.

(b) If f is continuous at a point, then f is linear

(c) If f is bounded on some interval, then f is linear.

(c) $\Rightarrow$ (b) $\Rightarrow$ (a)



(d) If f is measurable then f is linear

(e) $\exists$ nonlinear solution.

$\mathbb{Q}$ can be used for coefficients.

DO Prove: $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$ (rationals).

i.e. if $\alpha, \beta, \gamma \in \mathbb{Q}$ and $\alpha(1) + \beta(\sqrt{2}) + \gamma(\sqrt{3}) = 0$,

then $\alpha = \beta = \gamma = 0$.

$\mathbb{R}$ is a vector space over $\mathbb{Q}$.

HW correction:

For 2 pts., justify why the triangle-free graph with 11 vertices and 5-fold rotational symmetry is not 3-colorable.

Be sure to check grader's comments and talk to friends $\Rightarrow$ go to OH $\Rightarrow$ speak to Prof. Babai if something doesn't seem right.

$\boxed{\text{HW}}$ From DLA:

15.1.11 (a)(b)

15.1.12

15.2.6 (a) – (ℓ) Prove only "No" answers.

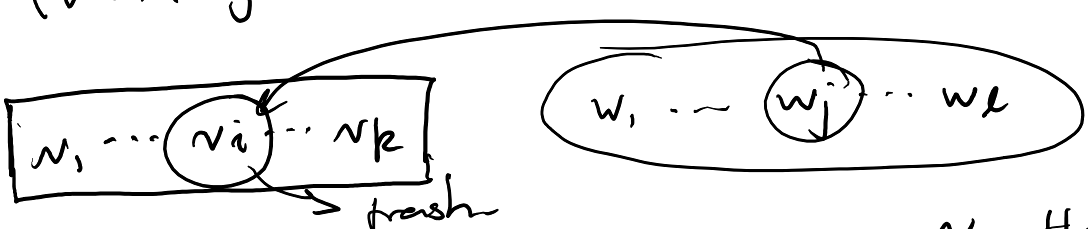
DO 15.3.11, 15.3.12, 15.3.22

First Miracle of Linear Algebra

Lemma. (Steinitz Exchange Principle)

Under conditions of First Miracle,

$(\forall i)(\exists j)(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k, w_j$ lin indep.)



(Terminology: if $S \subseteq V$ spans V then S is a set of <u>generators</u>.)

Proof. Suppose w_j doesn't work. Then $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k, w_j$ lin. <u>dep.</u>, but

$\underbrace{v_1, \ldots, v_{i-1}, v_{i+1},}_{\text{lin. indep.}}$ $\ldots, v_k$, so $w_j \in \operatorname{Span}(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k)$.

by previous lemma.

If none of the w_j work, then

$w_1, \dots, w_\ell \in \mathrm{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k)$

but $v_i \in \mathrm{Span}(w_1, \dots, w_\ell)$ and

$\mathrm{Span}(w_1, \dots, w_\ell) \subseteq \cancel{\mathrm{Span}}(\mathrm{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots v_k))$

$\therefore$ $v_i \in \mathrm{Span}(v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k)$

$\therefore$ $v_1, \dots, v_k$ lin. <u>dependent</u> - a contradiction.

Thus, at least one of w_j must work. □

<u>Proof of First Miracle</u>

copy $\quad w_1 \cdots w_{j_1} \cdots w_\ell$

$\boxed{\cancel{v_1} \cdots v_k}$

$\downarrow$

$w_{j_1}, \cancel{v_2} \cdots v_k$ $\quad$ still in $\mathrm{Span}(w_1, \dots, w_\ell)$.

$\downarrow$

$w_{j_1}, w_{j_2}, \cancel{v_3}, \cdots v_k$

$\vdots$

$w_{j_1}, w_{j_2}, w_{j_3} \cdots w_{j_k}$ $\quad$ lin independent $\rightarrow$ all w_j distinct (otherwise lin. dep. sublist)

$\Downarrow$

$\boxed{k \le \ell}$. □

<u>Cor.</u> If $\mathbb{R}^n \cong \mathbb{R}^m$ then $n = m$.

b/c $\mathbb{R}^n$ has a basis of n vectors:

"standard basis": columns of identity matrix

DO Show this is a basis.

$$\begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

DO If $f: V \to W$ isomorphism, then f maps basis to basis.

<u>Cor.</u> $\dim(\mathbb{R}^n) = n$.

Can find basis (n lin. indep.) and First Miracle guarantees no larger

<u>Def</u>. $A \in \mathbb{R}^{k \times \ell}$

column rank (A) = rank of list of columns

row rank(A) = rank of list of rows

<u>Second Miracle of Linear Algebra</u>

col rk(A) = row rk(A) =: rk(A) (rank of matrix A)

$A = [\underline{a_1}, \underline{a_2}, \ldots, \underline{a_\ell}]$ $\underline{a_i}$: columns.

The <u>column space</u> of A is $\text{Span}(\underline{a_1}, \underline{a_2}, \ldots, \underline{a_\ell})$.

$\boxed{\text{HW}}$ col $rk(A) =$ dim of space.

Proof: 1 line <u>incl.</u> key reference

$\boxed{\text{HW}}$ $A, B \in \mathbb{R}^{k \times \ell} \Rightarrow$

$$rk(A+B) \leq rk(A) + rk(B)$$

$\boxed{\text{CH}}$ Let A be matrix : $A = (a_{ij})$

$$B := (a_{ij}^2)$$

Prove: $rk(B) \leq \dfrac{rk(A)(rk(A)+1)}{2}$

Let $A \in \mathbb{R}^{k \times \ell}$.

B is a <u>right inverse</u> of A if $AB = I_k$

$B \in \mathbb{R}^{\ell \times k}$, so $AB \in \mathbb{R}^{k \times k}$.

$\boxed{\text{HW}}$ A right inverse exists $\Leftrightarrow$ $rk(A) = k$.

"A has full row rank."

Commentary :

A right inverse exists $\iff \mathrm{rk}(A) = k$

(from Second Miracle) $\iff$ rows are lin. indep.

$\iff$ columns span $\mathbb{R}^k$

DO State analogous result for left inverse.

$\boxed{\text{HW}}$ (for Monday) (submit via email)

Suppose we have

$A_1, \dots, A_m, B_1, \dots, B_m \in M_n(\mathbb{R})$

s.t. $A_i B_j = B_j A_i \iff i \neq j$.

Prove : $m \leq n^2$.

(Ask for a hint tomorrow - if you figure it out before tomorrow - email Prof. Babai)

Note: The chromatic polynomial problem is now due Mon. July 3 → check the website for a more detailed description.