ECE 269- Tuesday Jan 14th

- Vector space over a field
  - basic properties
  - subspace
  - spanning set / independent set
  - and basis

$\mathbb{Z}_2 = \{0,1\}$

$\mathbb{Z}_2^4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ = set of all binary vectors of length 4

Lists of length n: tuples of length n

Notation: $-a :=$ additive inverse of a

in this class: for a vector space $(V, +, \cdot)$ over $\mathbb{F}$ we denote $\underline{0} :=$ identity vector of $+$

Review: Field is $(\mathbb{F}, +, \cdot)$ satisfying:

- $(\mathbb{F}, +)$ is an Abelian group
- $(\mathbb{F}^*, \cdot)$ is an Abelian group
- $+$ and $\cdot$ are distributive: $a \cdot (b + c) = a \cdot b + a \cdot c$

Vector space over $\mathbb{F}$: $(V, +, \cdot)$

$V \times V \to V$ $\quad$ $\mathbb{F} \times V \to V$

(i) $(V, +)$ is an Abelian group

(ii) $\cdot$ satisfies:

(a) $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ $\quad$ $\forall \alpha, \beta \in \mathbb{F}$ and $v \in V$

(b) $\alpha \cdot (v + u) = \alpha \cdot v + \alpha \cdot u$

(c) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ $\quad$ & $1 \cdot v = v$

Examples: (I) $\mathbb{F} = (\mathbb{R}, +, \cdot)$, $(\mathbb{R}^k, +, \cdot)$ is a vector space over $\mathbb{R}$

where

$$(v_1, \dots, v_k) + (u_1, \dots, u_k) := (v_1 + u_1, \dots, v_k + u_k)$$

$$\alpha \cdot (v_1, \dots, v_k) := (\alpha v_1, \dots, \alpha v_k)$$

(II): $F = (\mathbb{C}, +, \cdot)$, $(\mathbb{C}^k, +, \cdot)$

(III): $(\mathbb{F}, +, \cdot)$ any field, $(\mathbb{F}^k, +, \cdot)$:

$$(v_1, \dots, v_k) + (u_1, \dots, u_k) := (v_1 + u_1, \dots, v_k + u_k)$$

$$\alpha \cdot (v_1, \dots, v_k) = (\alpha v_1, \dots, \alpha v_k)$$

Example: $\mathbb{Z}_2^4 = \{(0,\dots,0), (1,0,0,0), \dots, (1,1,1,1)\}$ is

a vector space over $\mathbb{Z}_2$.

Set of $\underbrace{\text{functions}}_{\text{real-valued}}$ from $\underbrace{I}_{\text{interval}} \to \mathbb{R}$: $\underbrace{\mathbb{R}^I}_{\text{denoted by}}$ is

a vector space over $\mathbb{R}$:

$$(f+g)(x) := f(x)+g(x)$$

$$(\alpha . f)(x) := \alpha . (f(x)).$$

Set of sequences $\overbrace{\{(\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots) \mid \alpha_i \in \mathbb{R}\}}^{\{\alpha_k\}_{k\geq 1}}$

is a vector space over $\mathbb{R}$ given by:

- $(\{\alpha_k\}_{k\geq 1} + \{\beta_k\}_{k\geq 1})(t) := \alpha_t + \beta_t$
- $(\gamma \cdot \{\alpha_k\}_{k\geq 1})(t) := \gamma \alpha_t$

Note that identity element is $\underset{\rightarrow}{0} = (0, 0, 0, \ldots)$

We refer to this vector space as $\mathbb{R}^{\mathbb{N}} = \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} \times \cdots}_{\mathbb{N}}$

Some basic properties of vector spaces V over $\mathbb{F}$:

✓ (a) $0 \cdot v = \underline{0} \quad \forall v \in V$

(b) $-v = (-1) \cdot v$ and in general $\underbrace{-(a \cdot v) = (-a) \cdot v}_{b'}$

(c) $a \cdot v = \underline{0} \Rightarrow$ either $a = 0$ or $v = \underline{0}$

Pf of b': $\underset{\substack{\parallel \\ 0}}{\underline{0}} = 0 \cdot v = (a - a) \cdot v = \underbrace{a \cdot v} + \underbrace{(-a) \cdot v}$

$$\Rightarrow -(a \cdot v) = (-a) \cdot v$$

Pf of (c): if $a \cdot v = \underline{0}$ and $a \neq 0 \Rightarrow \underset{\substack{\parallel \\ v = 1 \cdot v}}{a^{-1} \cdot (a \cdot v)} = a^{-1} \cdot \underline{0} = \underline{0}$

If V is a vector space over $\mathbb{F} = \mathbb{R}$, V is called a real vector space

and if it is over $\mathbb{F} = \mathbb{C}$, V is called a complex vector space.

(Linear) Subspace: We say that $\emptyset \neq U \subseteq V$ is a subspace (of V) if

(i) $u+v \in U \quad \forall u,v \in U$

(ii) $\alpha u \in U \quad \forall u \in U$ and $\alpha \in \mathbb{F}$

By induction, we can show that $U \subseteq V$ is a subspace iff $k \geq 1$; $\forall v_1, \dots, v_k \in U$ and $\alpha_1, \dots, \alpha_k \in \mathbb{F}$

$$\alpha_1 v_1 + \dots + \alpha_k v_k \in U$$

Such a combination is called a linear combination of vectors in V. IMPORTANT: k is FINITE!

Def: We say that $S \subseteq V$ is an independent set

if $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \underline{0} \Rightarrow \alpha_1 = \cdots = \alpha_n = 0$

$\forall\, v_1, \ldots, v_n \in S.$

Remark: if $\alpha_1 v_1 + \cdots + \alpha_n v_n = \underline{0}$ and $\alpha_1 \neq 0$

$$\Rightarrow v_1 + \alpha_1^{-1}\alpha_2 v_2 + \cdots + \alpha_1^{-1}\alpha_n v_n = 0$$

$$\parallel$$

$$v_1 = -(\alpha_1^{-1}\alpha_2 v_2 + \cdots + \alpha_1^{-1}\alpha_n v_n)$$

$\Rightarrow$ $S \subseteq V$ is independent iff none of elements in S can be written as a linear combination of other elements in S.

Def: For a subset $T \subseteq V$, we define

$$\text{span}(T) := \{ \text{all linear combination of vectors in } T \}$$

Example: $V = \mathbb{R}^3$ (over $\mathbb{R}$). Let $S = \{ \overset{v_1}{(1,0,1)}, \overset{v_2}{(1,1,0)} \}$.

Then if $(0,0,0) = \alpha_1 v_1 + \alpha_2 v_2$

$$= (\alpha_1 + \alpha_2, \alpha_2, \alpha_1) \iff \alpha_1 = \alpha_2 = 0$$

$\Rightarrow$ S is an independent set.

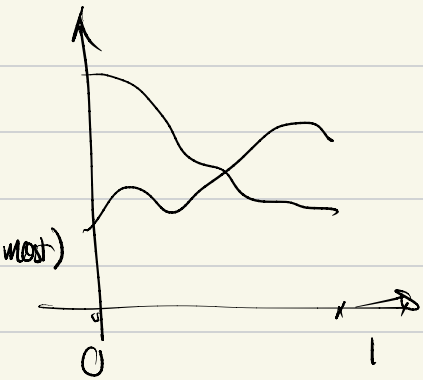
$$\mathrm{Span}(S) = \left\{ \alpha_1 v_1 + \alpha_2 v_2 \;\middle|\; \alpha_1, \alpha_2 \in \mathbb{R} \right\}$$

$$= \left\{ (\alpha_1 + \alpha_2, \alpha_2, \alpha_1) \;\middle|\; \alpha_1, \alpha_2 \in \mathbb{R} \right\}$$

$I = (0,1)$, $\quad \mathbb{R}^I = \mathbb{R}^{(0,1)} := \{ f : I \to \mathbb{R} \}$

$C^0(I) := \{ f : I \to \mathbb{R} \mid f \text{ is conti's} \}$

$\Rightarrow C^0(I)$ is a subspace of $\mathbb{R}^{(0,1)}$

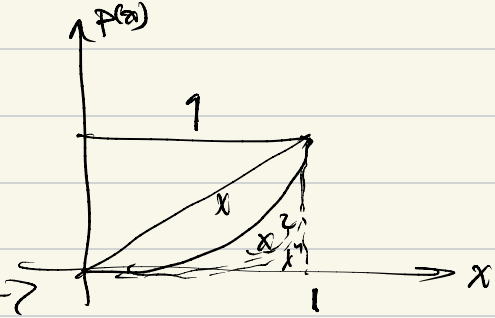


$P^n(I) := \{$ set of polynomials of degree (at most) $n \}$

$= \{ \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \mid \alpha_1, \ldots, \alpha_n \in \mathbb{R} \}$

In fact $P^n(I)$ is subspace of $C^0(I)$ which is a subspace of $\mathbb{R}^I$.

Let $S = \{ \overset{v_0}{1}, \overset{v_1}{x}, \overset{v_2}{x^2}, \dots, \overset{v_n}{x^n} \} \subseteq P^n(I)$



Q: Is S an independent set?

Let $\alpha_0 v_0 + \alpha_1 v_1 + \dots + \alpha_n v_n = \underline{0}$.

$$\| $$

$$p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n$$

Note that if $\alpha_i \neq 0$ for $0 \leq i \leq n$, then $p(x)$ is a polynomial of degree at least i and at most n, which has at most n roots $\Rightarrow p(x) \neq \underline{0} \Rightarrow p(x) = \underline{0} \Rightarrow \alpha_0 = \dots = \alpha_n = 0$.

证 2: if $p(x) = \underline{0} \Rightarrow p(0) = 0 = \alpha_0$

$$p(x) = \underline{0} \Rightarrow p'(x) = \underline{0} \Rightarrow \alpha_1 = 0$$

$$\vdots$$

$$\frac{d^n}{dx^n} p(x) = \underline{0} \Rightarrow \cdots \Rightarrow \alpha_n = 0$$

In fact: $S = \{1, x, x^2, \ldots, x^k, \ldots\}$ is an independent set.