Recap

Fields : Sets where we can do arithmetic, $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ $\qquad \cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

Vector Spaces : Sets where we can add and scale

$+ : V \times V \longrightarrow V$, $\cdot : \mathbb{F} \times V \longrightarrow V$

e.g. $\mathbb{R}^d$, Polynomials $\mathbb{R}[x]$, $\mathbb{R}$ over $\mathbb{Q}$,

continuous functions $C([0,1], \mathbb{R})$

Basis : Linearly independent set B s.t. $\mathrm{Span}(B) = V$

Lagrange interpolation : For distinct $a_1, \ldots, a_n \in \mathbb{F}$

$$f_i = \prod_{j \neq i} (x - a_j) \quad \forall i \in [n] \quad \text{basis for } \mathbb{F}^{\leq n-1}[x]$$

Unknown f with $f(a_1) = b_1, \ldots \ldots f(a_n) = b_n$

can be found as $\displaystyle f(x) = \sum \frac{b_i}{f_i(a_i)} \cdot f_i(x)$

Application: Secret Sharing [Shamir 79]

Share secret $s \in [0, M]$ with n people s.t.

- If any d get together, they learn s
- Fewer than d do not get any information

Scheme

- Choose $\mathbb{F}_p$ with $p > \max\{n, M\}$
- Choose (random) $c_1, \ldots, c_{d-1} \in \mathbb{F}_p$ and take

$$Q(x) = s + c_1 \cdot x + \cdots + c_{d-1} \cdot x^{d-1}$$

- Person i gets $(i, Q(i))$ for $i = 1, \ldots, n$

Any d people can find s

- Say people $a_1, \ldots, a_d$ get together
- Let $b_1 = Q(a_1), \ldots, b_d = Q(a_d)$
- Use Lagrange interpolation to find unique f s.t. $f(a_1) = b_1, \ldots, f(a_d) = b_d$. Must have $f \equiv Q$.
- Output $s = f(0)$

Fewer than d people learn nothing

- For any $(a_1, Q(a_1)), \ldots, (a_{d-1}, Q(a_{d-1}))$ and any $s' \in \mathbb{F}_p$, $\exists f$ s.t. $f(a_i) = Q(a_i)$ and $f(0) = s'$.

Research Question: Anonymous Secret Sharing [Con 25]

Back to Bases

LI set B s.t. $\text{Span}(B) = V$. } How do we check this?

- B is a basis $\iff$ B is a maximal LI set
  $B \cup \{v\}$ is LD for any $v \notin B$.

Proof: ($\Leftarrow$)

$$\text{Span}(B) = V$$

Pick any $v \in V$, say $v \notin B$ (easy otherwise)

$B \cup \{v\}$ is LD

$$c_0 v + \sum c_i \cdot v_i = 0 \qquad v_i \in B, \quad c_0 \neq 0$$

$$v = -c_0^{-1} \sum c_i \cdot v_i = \sum (-c_0^{-1} \cdot c_i) \cdot v_i \in \text{Span}(B)$$

Building a basis: Steinitz Exchange Principle

- Let $\{v_1, \ldots, v_k\}$ be LI and $\{v_1, \ldots, v_k\} \subseteq \text{Span}\{w_1, \ldots, w_n\}$

  Then $\forall i \in [k]\ \exists j \in [n]$ s.t.

  - $(\{v_1 \ldots v_k\} \setminus \{v_i\}) \cup \{w_j\}$ is LI
  - $w_j \notin \{v_1, \ldots, v_k\} \setminus \{v_i\}$

__Proof__: Suppose not. Then $\exists i\ \forall j\ w_j \in \text{Span}(\{v_1 \ldots v_k\} \setminus \{v_i\})$

$\Rightarrow$ $\text{Span}(\{w_1, \ldots, w_n\}) \subseteq \text{Span}(\{v_1 \ldots v_k\} \setminus \{v_i\})$

But $v_i \in \text{Span}(\{w_1, \ldots, w_n\})$

$\therefore$ $v_i \in \text{Span}(\{v_1 \ldots v_k\} \setminus \{v_i\}) \rightarrow$ contradiction!

All (finite) bases have equal sizes

- Let $B_1 = \{v_1 \ldots v_k\}$ and $B_2 = \{w_1 \ldots w_n\}$ be two bases for V. Then $k = n$.

<u>Proof:</u> Repeatedly remove a v, add a w

$\{v_1, \ldots, v_k\}$ LI, $\{v_1 \ldots v_k\} \subseteq \mathrm{Span}(\{w_1 \ldots w_n\})$

$\therefore k \leq n$

$\{w_1 \ldots w_n\}$ LI, $\{w_1 \ldots w_n\} \subseteq \mathrm{Span}(\{v_1 \ldots v_k\})$

$\therefore n \leq k$

Finitely generated vector spaces

(Defn) : V is called finitely generated if $\exists\, T \subseteq V$ s.t.

T is finite and $\mathrm{Span}(T) = V$.

Ex: Any finitely generated space V has a basis

(which is a subset of the generating set T)

- Finitely generated spaces have at least one basis.

- Sizes of any two bases B_1, B_2 are equal.

Called dimension of $V \equiv \dim(V)$

Ex: Let S be any LI set with $|S| = \dim(V)$.
Then S is a basis

(Claim) Let $S \subseteq V$ be any LI set, for finitely gen. V.

Then S can be extended to a basis.

($\exists$ basis B s.t. $S \subseteq B$)

Say $S = \{v_1, \ldots, v_k\}$

While $\exists\, v \in V$ s.t. $v \notin \text{Span}(S)$

$S \leftarrow S \cup \{v\}$

If T is a generating set, there is a basis of size $\leq |T|$

$\therefore$ Above loop cannot go on for more than $|T|$ steps.

What if V is not finitely generated?

Examples: - Polynomials $\mathbb{R}[x]$ over $\mathbb{R}$
- $\mathbb{R}$ over the field $\mathbb{Q}$

Can still find basis B s.t. $V = \text{Span}(B) = \left\{ \sum_{i=1}^{n} c_i \cdot v_i \;\middle|\; \begin{array}{l} v_1 \dots v_n \in B \\ c_1 \dots c_n \in \mathbb{F} \\ n \in \mathbb{N} \end{array} \right\}$

Need axiom of choice (Zorn's lemma) to show the existence of such a basis (Hamel basis). See notes.

Every vector space has a basis!

Linear Transformations

(Defn) V and W vector spaces over same $\mathbb{F}$.

$\varphi : V \longrightarrow W$ is called a linear transformation if

- $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \quad v_1, v_2 \in V$
- $\varphi(c \cdot v_1) = c \cdot \varphi(v) \quad c \in \mathbb{F}, v \in V$

Ex: Show that for any linear $\varphi : V \longrightarrow W$, $\varphi(0_V) = 0_W$.

E.g. $A \in \mathbb{R}^{m \times n}$ defines $\varphi_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$

$$\varphi_A(v) = Av$$

Examples (or not)?

- $\varphi : C([0,1], \mathbb{R}) \longrightarrow C([0,2], \mathbb{R})$. $\varphi(f)(x) = f(x/2)$

$\varphi(f_1+f_2)(x) = (f_1+f_2)(x/2) = f_1(x/2) + f_2(x/2) = \varphi(f_1)(x) + \varphi(f_2)(x)$

- $\varphi : C([0,1], \mathbb{R}) \longrightarrow C([0,1], \mathbb{R})$. $\varphi(f)(x) = f(x^2)$

$\varphi(f_1+f_2)(x) = (f_1+f_2)(x^2) = f_1(x^2) + f_2(x^2) = \varphi(f_1)(x) + \varphi(f_2)(x)$

- $\varphi : \text{Fib} \longrightarrow \text{Fib}$ defined as $\varphi(f)(n) = f(n+1)$

$\varphi(f_1+f_2)(n) = (f_1+f_2)(n+1) = f_1(n+1) + f_2(n+1) = \varphi(f_1)(n) + \varphi(f_2)(n)$

- derivative $\frac{d}{dx} : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$