Announcements

1) Error in HW #2,
Question 4 should read
"linearly dependent"

2) Colloquium, 3-4
Wednesday CB 2070
Speaker: Alan Wiggins
"Sofic groups and entropy"

Definition (basis)

A **basis** for a vector space V over a field $\mathbb{F}$ is a maximal linearly independent subset of V.

Maximal = not contained in any larger linearly independent set.

Proposition A linearly independent subset S of a vector space V is a basis if and only if S is spanning for V.

proof: $\Rightarrow$) Suppose S is a basis for V. Assume, by way of contradiction, that S is not spanning for V.

Choose $y \in V \setminus \operatorname{span}(S)$.

Then y is linearly independent from S, and S is strictly contained in $S \cup \{y\}$, which contradicts the maximality of S

Therefore, S is spanning for V.

$\Leftarrow$ Suppose S is spanning for V. Choose $y \notin S$. Then

$\exists$ $n \in \mathbb{N}$, scalars $\alpha_1, \dots, \alpha_n$ and $y_{i_1}, y_{i_2}, \dots, y_{i_n} \in S$

with

$$y = \sum_{j=1}^{n} \alpha_j y_{i_j},$$ i.e.,

y is not linearly independent from S.

This shows that $S \cup \{y\}$ is linearly dependent $\forall\ y \in V \setminus S$,

so S is maximal linearly independent. $\square$

Example 1: If V is $\mathbb{R}^n$, considered as a vector space over $\mathbb{R}$, then $\{e_i\}_{i=1}^n$ is a basis for $\mathbb{R}^n$.

We've already shown that $S = \{e_i\}_{i=1}^n$ is a linearly independent set.

To show spanning,

write $v = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n$.

Then

$$v = \sum_{i=1}^{n} \alpha_i e_i ,$$

So $\{e_i\}_{i=1}^{n}$ is spanning

for $\mathbb{R}^n$.

More or less the same proof shows that $\{e_{i,j}\}_{i,j=1}^{n}$ is a basis for $M_n(\mathbb{R})$ over $\mathbb{R}$.

Example 2: Over $\mathbb{C}$,

$\mathbb{C}$ has a basis consisting of $\{1\}$, since if $\alpha \in \mathbb{C}$, we can write $\alpha = \alpha \cdot 1$ (scalar multiplication as a complex vector space).

Over $\mathbb{R}$, $\mathbb{C}$ has a basis consisting of $\{1, i\}$, since now we can only scalar multiply by real numbers.

If $z \in \mathbb{C}$, write

$$z = x + iy = x \cdot 1 + y \cdot i$$

for $x, y \in \mathbb{R}$. This shows $\{1, i\}$ is spanning for $\mathbb{C}$ over $\mathbb{R}$.

Why is $\{1, i\}$ a linearly independent set (over $\mathbb{R}$)?

This is because i is not a real number! $i^2 = -1$, but $x^2 \geq 0$ for all x in $\mathbb{R}$.

Therefore $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

Moral: Be sure you know what field you're working over when calculating a basis.

Example 3: (polynomials)

For the vector space V of polynomials with real coefficients over $\mathbb{R}$, a basis is given by

$$\{x^n\}_{n=0}^{\infty},$$

so not finite.

We've already checked linear independence, and spanning is from definition! if p is a polynomial, then $\exists\ n \in \mathbb{N} \cup \{0\}$ and real numbers $\alpha_0, \alpha_1, \cdots, \alpha_n$ with

$$p(x) = \sum_{i=0}^{n} \alpha_i x^i .$$

Existence of bases and the Hausdorff Maximality Principle

Q: Why need a vector space have a basis?

Definition: (partial order)

A **partial order** is a relation "$\leq$" on a set S satisfying

1) $x \leq x \ \forall x \in S$.

2) If $x \leq y$ and $y \leq x$, then $x = y$. $(x, y \in S)$

3) If $x \leq y$ and $y \leq z$, then $x \leq z$ $(x, y, z \in S)$

Example 4:

On $S = \mathbb{R}$, let "$\leq$" be the usual notion of "less than or equal to".

Then $\mathbb{R}$ is partially ordered by "$\leq$".

Check conditions:

1) trivial.

2) trivial.

3) Immediate from definition

Now let S be any (nonempty) set and let "$\subseteq$" be set inclusion on the subsets of S ($\mathcal{P}(S)$, the power set of S).

Then $\mathcal{P}(S)$ is partially ordered by set inclusion.

1) trivial

2) If $S_0, S_1 \subseteq S$,

$S_0 \subseteq S_1$ and $S_1 \subseteq S_0$.

Then this means "if $x \in S_0$, $x \in S_1$" and "if $y \in S_1$, $y \in S_0$" so S_0 has the same elements as S_1, which implies

$S_0 = S_1$.

3) Suppose $S_0, S_1, S_2 \subseteq S$,

$S_0 \leq S_1$, $S_1 \leq S_2$.

Then since every element of S_0 is then an element of S_1, whose elements are in turn all elements of S_2, then

$S_0 \leq S_2$.

Definition: (total order)

A **total order** on a set S is a partial order "$\leq$" satisfying the additional property

- if $x, y \in S$, either

$$\boxed{x \leq y \quad \text{or} \quad y \leq x}$$

For example, "less than or equal to" is a total order on $\mathbb{R}$, but subset inclusion is not a total order on $\mathcal{P}(S)$ provided $|S| > 1$.

Consider $x \in S$. Then $\{x\}$ and $S \setminus \{x\}$ are are not contained one in the other if $|S| > 1$.

The Hausdorff Maximality Principle

Given a set S and a partial ordering "$\leq$" on S, if T is any collection of subsets of S that is totally ordered, then $\exists$ a maximal totally ordered collection M containing T:

Maximal totally ordered Collection:

If Ψ is a collection of subsets of S and $X \in M$

$\Rightarrow X \in \Psi$ then either

$\Psi = M$ or Ψ is not totally ordered.