3-18-1994

Bases.

I want to define the dimension of a vector space as the cardinality of a basis for the vector space. In order for this to make sense, I have to show that bases for a given vector space have the same cardinality.

I'll do the finite case first.

Lemma. Let V be an F-vector space. If V is spanned by $\{v_1, \ldots, v_n\}$, then any independent subset of V contains $\leq n$ elements.

Proof. Let $\{w_i\}$ be an independent subset of V. Since $w_1 \in V = \langle v_1, \ldots, v_n \rangle$, I may write it as a linear combination of the v_i's:

$$w_1 = a_1 v_1 + \cdots + a_n v_n.$$

If $a_i = 0$ for all i, then $w_1 = 0$, which contradicts independence of $\{w_i\}$. Therefore, at least one of the a's is nonzero; assume without loss of generality that it's a_1. Write

$$v_1 = \frac{1}{a_1}\left(w_1 - a_2 v_2 - \cdots - a_n v_n\right).$$

It follows that $\{w_1, v_2, \ldots, v_n\}$ still spans V (since I can use this set to build v_1, and then I have all the v_i's, which span V).

Repeat this procedure with w_2 in place of w_1. Keep going. Eventually, I'll run out of w's or I'll run out of v's.

If I run out of v's, I wind up with $\{w_1, \ldots, w_n\}$ spanning V. If there are any w's not in this spanning set, I can write them as linear combinations of $\{w_1, \ldots, w_n\}$. This contradicts independence of the original set $\{w_i\}$. Hence, this is all the w's, and there are n of them.

On the other hand, if I run out of w's first, the number of w's is obviously less than or equal to the number of v's.

In either case, I've shown that $\{w_i\}$ contains no more than n elements. $\square$

Corollary. Let V be a vector space, and let $\{v_1, \ldots, v_n\}$ be a basis. Then every basis for V contains n elements.

Proof. Let $\mathcal{B}$ be another basis for V. Since $\{v_1, \ldots, v_n\}$ spans and $\mathcal{B}$ is independent, the lemma shows that $|\mathcal{B}| \leq n$.

On the other hand, $\mathcal{B}$ spans and $\{v_1, \ldots, v_n\}$ is independent, so the lemma shows that $n \leq |\mathcal{B}|$. Therefore, $|\mathcal{B}| = n$. $\square$

The proof in the infinite case requires a little set theory. I'll do most of the set-theoretic stuff, though I'll take for granted a couple of simple facts about infinite cardinals. The proof revolves around the following innocuous sounding result — innocuous, but far from trivial!

Theorem. (Cantor-Schröder-Bernstein) Let X and Y be sets. Suppose there are injective functions $f : X \to Y$ and $g : Y \to X$. Then $|X| = |Y|$.

Proof. Let $x \in X$. Either x is in the image of g or it is not. In the former case, there is a $y \in Y$ such that $g(y) = x$. Such a y is unique, since g is 1-1.

Likewise, if $y \in Y$, either y is not in the image of f, or there is a unique $x \in X$ such that $f(x) = y$.

It follows that starting in X or Y, I can trace an element back along f and g. Pictorially, it looks like this:

$$\cdots \xrightarrow{g} x_n \xrightarrow{f} y_n \xrightarrow{g} x_{n+1} \xrightarrow{f} \cdots$$

The x's or y's preceding an element in such a sequence are called the element's **ancestors**. With this terminology, it's clear that an element's ancestry can extend backward forever, or terminate with an element with no ancestors.

Therefore, X and Y are each partitioned into three subsets:

$$\begin{aligned} X_1 &= \{x \in X \mid x'\text{s ancestry terminates in } X\}, \\ X_2 &= \{x \in X \mid x'\text{s ancestry terminates in } Y\}, \\ X_3 &= \{x \in X \mid x'\text{s ancestry doesn't terminate}\}, \\ Y_1 &= \{y \in Y \mid y'\text{s ancestry terminates in } X\}, \\ Y_2 &= \{y \in Y \mid y'\text{s ancestry terminates in } Y\}, \\ Y_3 &= \{y \in Y \mid y'\text{s ancestry doesn't terminate}\}. \end{aligned}$$

It's clear from the discussion above and the definitions that these really are partititions.

I'll use these sets to construct a bijection $\phi : X \to Y$.

Claim 1: f maps X_1 bijectively onto Y_1.

Since f is injective, I only need to show it maps X_1 onto Y_1. I'll show that $f(X_1) \subset Y_1$ and $Y_1 \subset f(X_1)$.

If $x \in X_1$, then x's ancestry terminates in X. Hence, $f(x)$ is an element of Y whose ancestry terminates in X. Therefore, $f(x) \in Y_1$, and $f(X_1) \subset Y_1$.

If $y \in Y_1$, then y's ancestry terminates in X. Hence, there is a sequence

$$x_1 \xrightarrow{f} y_1 \xrightarrow{g} \cdots \xrightarrow{g} x_n \xrightarrow{f} y_n = y$$

with $x_i \in X$ and $y_i \in Y$.

x_n is an element of X whose ancestry terminates in X, so $x_n \in X_1$. Then $y = f(x_n) \in f(X_1)$. Therefore, $Y_1 \subset f(X_1)$, and hence $Y_1 = f(X_1)$.

Claim 2: g maps Y_2 bijectively onto X_2.

The proof is essentially the same as the proof of Claim 1.

Claim 3: f maps X_3 bijectively onto Y_3.

If $x \in X_3$, x's ancestry doesn't terminate. Then $f(x)$ is an element of Y whose ancestry doesn't terminate, so $f(x) \in Y_3$. Therefore, $f(X_3) \subset Y_3$.

If $y \in Y_3$, y's ancestry doesn't terminuate. In particular, there exists $x \in X$ such that $f(x) = y$ (or else y's ancestry terminates with itself). Now x and y share the same ancestry, so x's ancestry doesn't terminate. Therefore, $x \in X_3$, and $y = f(x) \in f(X_3)$. Hence, $Y_3 \subset f(X_3)$, so $Y_3 = f(X_3)$.

Now define $\phi : X \to Y$ by

$$\phi(x) = \begin{cases} f(x) & \text{if } x \in X_1 \cup X_3 \\ g^{-1}(x) & \text{if } x \in X_2 \end{cases}.$$

ϕ is a bijection, since each piece is a bijection. Therefore, $|X| = |Y|$. □

Lemma. Let V be a vector space over F, and let $\mathcal{B}$ be a basis for V. Every $v \in V$ can be *uniquely* written as

$$v = a_1 v_1 + \cdots a_n v_n, \quad \text{where} \quad a_i \in F, v_i \in \mathcal{B}.$$

Proof. Since $\mathcal{B}$ spans, the only thing at issue is uniqueness. Suppose then that

$$a_1 v_1 + \cdots a_n v_n = v = b_1 v_1 + \cdots b_n v_n, \quad a_i, b_i \in F, v_i \in \mathcal{B}.$$

(I may assume the same v_i's occur on both sides by padding the expressions with terms with zero coefficients if necessary.)

Now

$$(a_1 - b_1)v_1 + \cdots + (a_n - b_n)v_n = 0.$$

By independence, $a_i - b_i = 0$ for all i, so $a_i = b_i$ for all i. This proves the the two linear combinations are actually the same. □

Theorem. Two bases $\mathcal{B}$ and $\mathcal{B}'$ for an F-vector space V have the same cardinality.

Proof. I proved the finite case earlier. Assume then that $\mathcal{B}$ is infinite.

First, I claim that $\mathcal{B}'$ must be infinite as well. Suppose not. Write

$$\mathcal{B}' = \{v_1, \ldots, v_n\}.$$

Since $\mathcal{B}'$ is a spanning set, the independent set $\mathcal{B}$ must contain no more than n elements. This contradicts the assumption that $\mathcal{B}$ is infinite.

Next, I'll show that $|\mathcal{B}| = |\mathcal{B}'|$. By symmetry, it's enough to show that $|\mathcal{B}| \leq |\mathcal{B}'|$. (Then I can apply Cantor-Schröder-Bernstein.)

Each $u \in \mathcal{B}$ can be written as a finite linear combination of elements of $\mathcal{B}'$. By the preceding lemma, such a representation is unique:

$$u = a_1 v_1 + \cdots a_n v_n.$$

Define $\phi : \mathcal{B} \to \mathcal{T} =$ (finite subsets of $\mathcal{B}'$) by

$$\phi(u) = \{v_1, \ldots, v_n\}.$$

The argument above shows that $\operatorname{im} \phi$ is infinite. (If not, I could build all the elements of $\mathcal{B}$ out of finitely many elements of $\mathcal{B}'$.)

Next, I claim that if $T \in \mathcal{T}$, then $\phi^{-1}(T)$ is finite.

First,

$$\phi^{-1}(T) \subset \langle T \rangle.$$

Since T is finite, each element of T may be written as a finite linear combination of elements of $\mathcal{B}$. Collect all such elements of $\mathcal{B}$ into a subset $\mathcal{S} \subset \mathcal{B}$. By construction,

$$\phi^{-1}(T) \subset \langle T \rangle \subset \langle S \rangle.$$

In particular, each $v \in \phi^{-1}(T)$ can be written as finite linear combination of elements of $\mathcal{S}$. But $\{v\} \cup \mathcal{S} \subset \mathcal{B}$, an independent set. This is a contradiction unless $v \in \mathcal{S}$. Therefore, $\phi^{-1}(T) \subset \mathcal{S}$, and the latter is a finite set.

Observe that $\{\phi^{-1}(T)\}$ is a partition of $\mathcal{B}$. If $u \in \phi^{-1}(T_1) \cap \phi^{-1}(T_2)$, then u can be written as linear combinations of elements of T_1 and T_2. These are both subsets of $\mathcal{B}'$, and contradicts unique representation for the basis. On the other hand, $\mathcal{B}'$ spans, so everything in $\mathcal{B}$ can be written as a linear combination of elements of $\mathcal{B}'$.

Therefore,

$$|\mathcal{B}| \leq |\operatorname{im} \phi||(\text{countable})| = |\operatorname{im} \phi| \leq |\mathcal{T}| = |\mathcal{B}'|.$$

(I've used some facts about cardinals here.) This completes the proof. $\square$

Definition. The **dimension** of a vector space is the cardinality of a basis for the vector space.

