The 'fundamental theorem' of (finite dimensional) vector spaces.

Throughout this note, V is a vector space over a field $\mathbf{F}$. We need the following preliminary result.

Lemma 0.1. *Suppose* $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbf{F}^m$ *is linearly independent. Then* $m \geq n$.

Proof. Suppose to the contrary that $m < n$. Observe that $x_1\mathbf{a}_1 + \ldots x_n\mathbf{a}_n = \mathbf{0}$ if and only if $(x_1, \ldots, x_n)$ solves the $m \times n$ linear system $[\mathbf{a}_1 \ldots \mathbf{a}_n \,|\mathbf{0}]$. Since there are more unknowns than equations in this system, we will necessarily find on putting things in reduced echelon form that some columns correspond to free variables. That is, each row admits at most one pivot, and since there are more columns than rows, some column will lack a pivot. Anyhow, the upshot is that the system will have infinitely many solutions, and all but one of these will be non-trivial solutions. It follows that $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ is dependent which contradicts the hypothesis of the lemma. So $m \geq n$ after all. $\square$

We remark that a similar sort of argument shows that if $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbf{F}^m$ generates $\mathbf{F}^m$, then the reverse inequality $n \geq m$ holds. The most important fact about (finite dimensional) vector spaces, and the main result of this note, is the following

Theorem 0.2. $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset V$ *is linearly independent and* $T = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\} \subset V$ *generates* V*. Then* $n \leq m$.

That is, a generating subset of V contains at least as many vectors as any linear independent set. The main thing about the theorem is that none of the vectors of S need also be contained in T.

Proof. Since T generates V, we may express each vector $\mathbf{v}_k \in S$ as a linear combination

$$\mathbf{v}_k = a_{1k}\mathbf{w}_1 + \cdots + a_{mk}\mathbf{w}_m$$

of vectors in V. We gather the coefficients of this linear combination into a vector $\mathbf{a}_k := (a_{1k}, \ldots, a_{mk}) \in \mathbf{F}^m$.

I claim that $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbf{F}^m$ is independent (and therefore $n \leq m$ by Lemma 0.1). To verify this claim, suppose we have a linear combination

$$\sum_{k=1}^{n} x_k\mathbf{a}_k = x_1\mathbf{a}_1 + \cdots + x_n\mathbf{a}_n = \mathbf{0}.$$

On the level of components this becomes, $\sum_{k=1}^{n} x_k a_{jk} = 0$ for each $j = 1, \ldots, m$. Hence

$$\sum_{k=1}^{n} x_k\mathbf{v}_k = \sum_{k=1}^{n}\sum_{j=1}^{m} x_k a_{jk}\mathbf{w}_j = \sum_{j=1}^{m}\left(\sum_{k=1}^{n} x_k a_{jk}\right)\mathbf{w}_j = \sum_{j=1}^{m} 0\mathbf{w}_j = \mathbf{0}.$$

So from independence of S, we infer $x_1 = \cdots = x_n = 0$ and conclude that $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ is independent as claimed. $\square$

The following consequence of the above theorem justifies defining the *dimension* of V to be the number of vectors in a basis (with the caveats that $\dim V = 0$ if $V = \{\mathbf{0}\}$ is the trivial vector space, and $\dim V = \infty$ if no finite set of vectors generates V.)

Corollary 0.3. *Suppose V is finite dimensional (i.e. is generate by finitely many vectors). Then V has a basis, and any two bases have the same number of vectors.*

Proof. Let S be a finite set that generates V. We showed in class that there is a basis $\mathcal{B} \subset S$ for V contained in S. If $\mathcal{C}$ is another basis for V, then $\#\mathcal{B} \leq \#\mathcal{C}$ because $\mathcal{B}$ is independent and $\mathcal{C}$ generates V. On the other hand, $\mathcal{C}$ is independent and $\mathcal{B}$ generates V, $\#\mathcal{C} \leq \#\mathcal{B}$, too. So $\mathcal{B}$ and $\mathcal{C}$ have the same number of vectors. $\square$