A PROOF THAT EVERY VECTOR SPACE HAS A BASIS

TIM SMITS

In lecture, you saw that every vector space that can be spanned by a finite number of vectors has a basis. It turns out that more is true: *any* vector space (spanned by a finite number of elements or not) has a basis. The goal of this handout is to prove this theorem, which is one of the most important results in linear algebra.

In order to deal with infinite spanning sets, we need some set theory:

Definition 0.1. A **partial ordering** on a set S is a binary relation $\leq$ that satisfies the following conditions for all $a, b, c \in P$:

1. (Reflexivity) $a \leq a$.
2. (Anti-symmetry) If $a \leq b$ and $b \leq a$ then $a = b$.
3. (Transitivity) If $a \leq b$ and $b \leq c$ then $a \leq c$.

Definition 0.2. A **poset** is a set P with a partial ordering $\leq$. A poset is called **totally ordered** if for all pairs of elements $a, b \in P$, either $a \leq b$ or $b \leq a$. A **chain** C of a poset P is a totally ordered subset of P. For $A \subset P$, an **upper bound** of A is an element m of P such that $x \leq m$ for all $x \in A$.

Example 0.3. Let $P = \mathbb{R}$ and let $\leq$ be the usual relation of less than or equal to. Then P is a poset, and P is totally ordered.

Example 0.4. Let $P = \mathbb{N}$ and let $a \leq b \iff a \mid b$. This makes P a poset. Under this ordering, we have $3 \leq 6$, but 3 and 5 are not comparable, so P is not totally ordered. The set $P' = \{1, 2, 4, 8, 16\}$ is totally ordered, so it is a chain in P. The element 16 is an upper bound of P'.

Example 0.5. Let P a set of subsets of a vector space V, and $\leq$ be **ordering by inclusion**, i.e. $W \leq W' \iff W \subset W'$. Then P is a poset.

The proof that every vector space has a basis is one of many non-constructive existence results in mathematics that follow from *Zorn's lemma*, which is (surprisingly!) equivalent to the Axiom of Choice:

Theorem 0.6 (Zorn's lemma)**.** *Let P be a poset such that every chain in P has an upper bound in P. Then P has a maxmimal element with respect to $\leq$. That is, there is an element $m \in P$ such that $x \leq m$ for all $x \in P$.*

We are now ready to prove the theorem:

Theorem 0.7. *Every vector space has a basis.*

Proof. Let V be a vector space over some field F. The idea of the proof is as follows: use Zorn's lemma to show that V contains a maximal linearly independent subset B of V (in the sense that there is no linearly independent subset S with $B \subsetneq S$), and then show that

B must be a basis of V.

If $V = \{0\}$, then by definition $V = \text{Span}(\emptyset)$, and the empty set is linearly independent. Now suppose that $V \neq \{0\}$ and let $P = \{S \subset V : S \text{ is linearly independent}\}$ be the set of all linearly independent subset of V with an ordering on P given by inclusion. Then $P \neq \emptyset$, because there exists $v \neq 0 \in V$ so $\{v\}$ is a linearly independent subset of V. We now check the conditions of Zorn's lemma. Suppose that $C \subset P$ is a chain, and write $C = \{S_\alpha\}_{\alpha \in I}$ for some indexing set I. Set $M = \bigcup_{\alpha \in I} S_\alpha$. The claim is that M is an upper bound of C that is an element of P. The first statement is immediate by definition: for any $S_\alpha \in C$, we have $S_\alpha \subset \bigcup_{\alpha \in I} S_\alpha$, so $C \leq M$. Therefore, we only need to check that M is a linearly independent subset of V, so that $M \in P$, letting Zorn's lemma kicks in.

Suppose that M is not linearly independent, then there are vectors $s_1, \ldots, s_n$ where $s_i \in S_{\alpha_i}$ for some S_{α_i} and scalars $c_1, \ldots, c_n \in F$ not all 0 such that $c_1 s_1 + \cdots c_n s_n = 0$. As C is totally ordered, one of the sets $S_{\alpha_1}, \ldots, S_{\alpha_n}$ must contain the others, so each of the vectors s_i live in some common set, which we denote S_α. This says there is a non-trivial dependence relation among vectors in S_α, contradicting that S_α is linearly independent (because S_α lives in P!). Therefore, M is a linearly independent subset of V. By Zorn's lemma, P contains a maximal element with respect to inclusion, say B.

To finish up, we need to show that B spans V. Suppose otherwise, then there is some $v \in V$ such that $v \notin \text{Span}(B)$. This says that $B \cup \{v\}$ is a linearly independent subset of V with $B \subset B \cup \{v\}$, contradicting the maximality of B. Therefore B spans V, and we are done. □

It's important to note that the proof only shows that a basis *exists* – it gives absolutely zero indication of what one is. The proof technique of using Zorn's lemma is a rather standard one for proving existence theorems in mathematics (especially in algebra) and is worth understanding.

For vector spaces spanned by finite sets, you saw in lecture that it's not too hard to show that any two bases have the same number of elements. This allows us to define the *dimension* of a vector space. What happens if the vector space has a basis of infinitely many elements? The dimension of a vector space is still well defined, but this now becomes a fairly non-trivial result. Instead of talking about the *number* of elements in a basis, we have to talk about the *cardinality* of the basis, and if you know anything about set theory, there are many different "sizes" of infinite sets which is what causes complications. The proof is a rather technical set theoretic argument that is unenlightening, so we will take it for granted.

Proposition 1. *Let B and B' be two bases of a vector space V. Then $|B| = |B'|$.*

This gives us the following definition that works for any vector space:

Definition 0.8. Let V be a vector space. The **dimension** of V is defined as the cardinality of a basis of V. V is said to be **infinite dimensional** if it's dimension is not finite.

If you're familiar with the notion of *countability*, the following are examples of infinite vector spaces of different "sizes":

Example 0.9. The vector space $\mathbb{Q}[x]$ is infinite dimensional as a $\mathbb{Q}$-vector space, because the span of any finite set of polynomials has bounded degree. The set $\{1, x, x^2, \ldots\}$ is a basis of $\mathbb{Q}[x]$ as a $\mathbb{Q}$-vector space, and so $\mathbb{Q}[x]$ has countable dimension.

Example 0.10. $\mathbb{R}$ is infinite dimensional as a $\mathbb{Q}$-vector space, because any finite dimensional vector space over $\mathbb{Q}$ must be countable, and $\mathbb{R}$ is not countable. It turns out that $\mathbb{R}$ has uncountable dimension as a $\mathbb{Q}$-vector space (but this is much harder to show).