9. Basis and dimension

Definition 9.1. *Let V be a vector space over a field F.*

A ***basis*** $\mathfrak{B}$ *of V is a finite set of vectors $v_1, v_2, \dots, v_n$ which span V and are independent. If V has a basis then we say that V is finite dimensional, and the* ***dimension*** *of V, denoted $\dim V$, is the cardinality of $\mathfrak{B}$.*

One way to think of a basis is that every vector $v \in V$ may be uniquely expressed as

$$v = r_1 v_1 + r_2 v_2 + \cdots + r_n v_n.$$

The existence of such a decomposition is given by the fact the vectors $v_1, v_2, \dots, v_n$ span V. If there were two ways to write v as a sum,

$$s_1 v_1 + s_2 v_2 + \cdots + s_n v_n = v = r_1 v_1 + r_2 v_2 + \cdots + r_n v_n,$$

then we would have a way to write 0 as a linear combination of $v_1, v_2, \dots, v_n$,

$$(s_1 - r_1)v_1 + (s_2 - r_2)v_2 + \cdots + (s_n - r_n)v_n = 0.$$

By independence $s_1 - r_1 = s_2 - r_2 = \cdots = s_n - r_n = 0$. But then $r_1 = s_1, r_2 = s_2, \cdots, r_n = s_n$ and so the decomposition is unique.

F^n has dimension n. A basis is given by $e_1, e_2, \dots, e_n$, where e_i is the vector with a 1 in the ith row and zero everywhere else.

$M_{m,n}(F)$ has dimension mn. A basis is given by the matrices $A_{i,j}$, which have a 1 in the (i, j) entry and zero everywhere else.

$P_n(F)$ has dimension $n + 1$. A basis is given by the polynomials $1, x, x^2, \cdots, x^n$.

There is one problem with all of this. We have not checked that the size of a basis is independent of the basis. For example why couldn't a vector space have dimension three and five at the same time (that is why could there not be a basis with three elements and another with five)? If the vector space is F^n we can appeal to the fact that a basis $\mathfrak{B}$ cannot have more than n elements, since then the vectors are dependent. On the other hand, it cannot have less than n elements since then they cannot span.

In fact

Theorem 9.2. *Let $v_1, v_2, \dots, v_m$ be m vectors in F^n. Let A be the matrix whose columns are the vectors $v_1, v_2, \dots, v_m$.*

The set $\mathfrak{B} = \{v_1, v_2, \dots, v_m\}$ is a basis for if and only if the equation $Ax = b$ always has a unique solution. In particular $m = n$.

Proof. This simply puts together two statements. The fact that $\mathfrak{B}$ spans means that the equation $Ax = b$ always has a solution. The fact that $Ax = 0$ has a unique solution means that the vectors $v_1, v_2, \dots, v_n$ are independent. $\square$

In an arbitrary vector space there is another way to proceed.

Lemma 9.3. *Let $v_1, v_2, \dots, v_n$ be a finite collection of vectors in a vector space V.*

(1) *If v_n is a linear combination of $v_1, v_2, \dots, v_{n-1}$ then*
$$\operatorname{span}\{v_1, v_2, \dots, v_{n-1}\} = \operatorname{span}\{v_1, v_2, \dots, v_n\}.$$
(2) *If $v_1, v_2, \dots, v_{n-1}$ are independent and v_n is not a linear combination of $v_1, v_2, \dots, v_{n-1}$ then $v_1, v_2, \dots, v_n$ are independent.*

Proof. Both of these results are easy to prove and are left as exercises. $\square$

(1) and (2) of (9.3) give two useful ways to construct bases:

Algorithm 9.4. *Let V be a vector space. Suppose that $v_1, v_2, \dots, v_n$ span V.*

(1) *If $v_1, v_2, \dots, v_n$ are independent then **STOP**.*
(2) *Otherwise we may write v_i as a linear combination of the other vectors. Throw away v_i and return to (1).*

Algorithm 9.5. *Let V be a vector space. Suppose that $v_1, v_2, \dots, v_n$ are independent.*

(1) *If $v_1, v_2, \dots, v_n$ span V then **STOP**.*
(2) *Otherwise pick v_{n+1} not in the span of $v_1, v_2, \dots, v_n$. Then $v_1, v_2, \dots, v_{n+1}$ are independent. Replace $v_1, v_2, \dots, v_n$ by $v_1, v_2, \dots, v_{n+1}$ and return to (1).*

In other words, we can either start with a set that spans and throw away vectors to get a basis or start with a set which is independent (e.g the empty set) and add vectors until we get a basis. Note that the first algorithm always terminates; the second one only terminates if V is finite dimensional.

Theorem 9.6. *Let V be a finite dimensional vector space.*

Then any two bases have the same cardinality.

Proof. Suppose that $\mathfrak{B} = \{v_1, v_2, \dots, v_m\}$ and $\mathfrak{C} = \{w_1, w_2, \dots, w_n\}$ are two bases of V. We want to show that $m = n$. We may assume that $m, n > 0$.

Consider the set $\mathfrak{B} \cup \{w_n\}$. $w_n \in V$ belongs to the span of $v_1, v_2, \dots, v_m$. Therefore we may find $r_1, r_2, \dots, r_m$ such that
$$w_n = r_1 v_1 + r_2 v_2 + \cdots r_m v_m.$$

$w_n \neq 0$ and so at least one of $r_1, r_2, \ldots, r_m$ is non-zero. We may assume that $r_m \neq 0$. In this case

$$v_m = w_n - (r_1 v_1 + r_2 v_2 + \cdots r_{m-1} v_{m-1})/r_m,$$

and so v_m is a linear combination of $v_1, v_2, \ldots, v_{m-1}$ and w_n. (1) of (9.3) implies that $\mathfrak{B} - \{v_m\} \cup \{w_n\}$ also spans V.

So now consider $v_1, v_2, \ldots, v_{m-1}$, w_{n-1} and w_n. As $v_1, v_2, \ldots, v_{m-1}$ and w_n span V it follows that w_{n-1} is a linear combination of $v_1, v_2, \ldots, v_{m-1}$ and w_n,

$$w_{n-1} = r_1 v_1 + r_2 v_2 + \cdots + r_{m-1} v_{m-1} + s_n w_n.$$

Suppose that every $r_i = 0$. Then w_{n-1} and w_n are dependent, which contradicts the fact that $\mathfrak{C}$ is a basis. Thus $r_i \neq 0$ some i. Relabelling we may suppose that $r_{m-1} \neq 0$. As before this implies that v_{m-1} is a linear combination of $v_1, v_2, \ldots, v_{m-2}$, w_{n-1} and w_n. But then (1) of (9.3) implies that $v_1, v_2, \ldots, v_{m-2}$, w_{n-1} and w_n span V.

We can repeat this process for every vector in $\mathfrak{C}$. It follows that $m \leq m$. By symmetry $n \leq m$. But then $m = n$. $\square$

A careful analysis of the proof yields that every set of vectors which spans is always bigger than any set of independent vectors. In particular (9.5) always terminates in a finite dimensional vector space (in fact in exactly $\dim V - n$ steps).