Basis and Dimension

Let V be a vector space over a field F. If $v_1, v_2, \ldots, v_n V$ is a sequence of vectors in V then by a linear combination of these vectors we mean a vector of V of the form

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n,$$

with $a_1, a_2, \ldots, a_n \in F$. If $n = 0$, this is an empty sum which, by convention, is the zero vector. The set of all linear combinations of elements the vectors $v_1, v_2, \ldots, v_n$ is denoted by $\operatorname{span}(v_1, v_2, \ldots, v_n)$ and is called the linear span of $v_1, v_2, \ldots, v_n$. Note that $\operatorname{span}(\emptyset) = \{0\}$. More generally, if S is a subset of V then

$$\operatorname{span}(S) = \{v \in V \mid (\exists n \geq 0, a_1, \ldots, a_n \in F, v_1, \ldots v_n \in S) v = a_1 v_1 + a_2 v_2 + \ldots a_n v_n\}$$

is the set of all linear combinations of elements of S.

Theorem 1. If S is a subset of the vector space V then $\operatorname{span}(S)$ is a subspace of V. It is the smallest subspace of V which contains S; if W is a subspace of V containing S then $\operatorname{span}(S) \subseteq W$.

Generating Set. If the vector space $V = \operatorname{span}(S)$ then the vector space V is said to be spanned or generated by S. The set S is then called a spanning or generating set. If $V = \operatorname{span}(S)$ with S finite then V is said to be finitely generated.

Linearly Independent Set. A subset S of a vector space V is said to be linearly independent if $v \notin \operatorname{span}(S - \{v\})$ for all $v \in S$. This is equivalent to the statement that for any distinct vectors $v_1, v_2, \ldots, v_n$ the relation

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0$$

implies that the scalars $a_1, a_2, \ldots, a_n$ are all zero. Note that the empty set is a linearly independent set. If S is not a linearly dependent set then there are distinct vectors $v_1, v_2, \ldots, v_n$ and scalars $a_1, a_2, \ldots, a_n$ not all zero such that

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0.$$

In this case, S is said to be a linearly dependent set. If $a_i \neq 0$ then $v_i \in \operatorname{span}(S - \{v_i\}) = \operatorname{span}(S)$. Note that any set S containing the zero vector is linearly dependent.

Dependence Relations. If $v_1, v_2, \ldots, v_n$ are vectors in V then by any relation of the form

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0$$

is said to be a dependence relation for the sequence $(v_1, v_2, \ldots, v_n)$. The dependence relation is said to be trivial if $n \geq 1$ and $a_1 = a_2 = \cdots = a_n = 0$. If the only dependence relation is the trivial one then the vectors $v_1, v_2, \ldots, v_n$ are distinct and $S = \{v_1, v_2, \ldots, v_n\}$ is a linearly independent set. In this case, we also say that the sequence $(v_1, v_2, \ldots, v_n)$ is linearly independent. If there are on trivial dependence relations for the sequence $(v_1, v_2, \ldots, v_n)$ then we say that the sequence is linearly dependent. Note that the sequence $(v_1, v_2, \ldots, v_n)$ can be linearly dependent while the set $\{v_1, v_2, \ldots, v_n\}$ is linearly independent. This can only happen if $v_i = v_j$ for some $i \neq j$. For example, if v is any non-zero vector, then (v, v) is linearly dependent while $\{v, v\} = \{v\}$ is linearly independent.

Basis. A basis for a vector space is a linearly independent generating set.

Theorem 2. Let S be a subset of a vector space V. Then the following are equivalent:

(a) The set S is maximal linearly independent subset of V;

(b) The set S is a maximal generating subset of V;

(c) The set S is a basis for V.

Proof. (a) $\implies$ (c). If S is a maximal linearly independent subset of V and $V \neq \operatorname{span}(S)$ then there is a vector $v \in V$ such that $v \notin \operatorname{span}(S)$. But then the following Lemma shows that $S \cup \{v\}$ is a linearly independent subset of V larger than S which is impossible.

Lemma. If S is a linearly independent subset of a vector space V and $v \in V$, $v \notin \operatorname{span}(S)$ then $S \cup \{v\}$ is a linearly independent subset of V.

Proof of Lemma. If $S \cup \{v\}$ is linearly dependent then there are distinct vectors $v_1, v_2, \ldots, v_n$ in S and scalars $a_1, a_2, \ldots, a_n, a$, not all zero, with

$$a_1v_1 + a_2v_2 + \ldots + a_nv_n + av = 0.$$

We must have $a = 0$ since $v \notin \operatorname{span}(S)$. But then $a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0$ is a non-trivial dependence relation for the vectors $v_1, v_2, \ldots, v_n$ contradicting the linear independence of the set S.

(c) $\implies$ (b). If S is a basis for V then S is a generating set for V. The set S is a minimal generating set since the linear independence of S implies $v \notin \operatorname{span}(S - \{v\})$ for any $v \in V$.

(b) $\implies$ (c). If S is a minimal generating subset of V then, for any $v \in V$, we have $\operatorname{span}(S - \{v\}) \neq V = \operatorname{span}(S)$ which implies that $v \notin \operatorname{span}(S - \{v\})$ since $v \in \operatorname{span}(S - \{v\})$ implies $S \subseteq \operatorname{span}(S - \{v\})$ and hence that $V = \operatorname{span}(S) \subseteq \operatorname{span}(S - \{v\})$ which is not the case.

(c) $\implies$ (a). If S is a basis for V then $v \in \operatorname{span}(S)$ for all $v \in V$. If $v \in V - S$ then $T = S \cup \{v\}$ is linearly dependent since $S = T - \{v\}$. **QED**

Replacement Theorem. Let $V = \operatorname{span}(S)$ be a vector space over a field F and let T be a linearly independent subset of V. Then there is an injective mapping f of T into S such that

$$\operatorname{span}(S) = \operatorname{span}((S - f(T)) \cup T).$$

Proof. We give the proof for the case S, T are finite. The proof can be adapted to prove the general case.

Choose an ordering of $S \cup T$ so that the elements of T come before the elements of $S - T$ and the elements of $T_0 = S \cap T$ come before the elements of $T - T_0$. Define $f_0 : T_0 \to S$ by $f_0(v) = v$ for $v \in T_0$. Then f_0 is injective and

$$\operatorname{span}(S) = \operatorname{span}((S - f_0(T_0)) \cup T_0)$$

since $S = (S - f_0(T_0)) \cup T_0$. Let f be an extension of f_0 to an injective mapping with range a subset of S and domain $D_f \subseteq T$ largest possible with the following two properties:

(a) $u \in D_f$ and $v < u \implies v \in D_f$;

(b) $\operatorname{span}(S) = \operatorname{span}((S - f(D_f)) \cup D_f)$.

Suppose that $D_f \neq T$ and let v be the smallest element of $T - D_f$. Then

$$v = a_1u_1 + a_2u_2 + \cdots a_nu_n$$

with $u_i \in (S - f(D_f)) \cup D_f$, $u_1 < u_2 \cdots < u_n$ and $a_1, a_2, \ldots, a_n \neq 0$. In this case, $u_n \notin f(D_f)$. Otherwise, we have $u_n \in D_f$ which implies that $u_i \in D_f$ for all i by property (a) and hence that $v \in \mathrm{Span(D_f)}$ which is impossible since $\{v\} \cup D_f$ is an independent set. Let $u = u_n$. Then

$$u \in \operatorname{span}(u_1, u_2, \ldots, u_{n-1}, v) = \operatorname{span}(u_1, u_2, \ldots, u_{n-1}, v)$$

so that, setting $S_f = (S - f(D_f)) \cup D_f$, we have $\operatorname{span}(S_f) = \operatorname{span}((S_f - \{u\}) \cup \{v\})$. We now define an extension g of f with domain $D_f \cup \{v\}$ by setting $g(v) = u$. Then g is injective since $u \notin f(D_f)$. We also have that $u \in D_g$ and $v < u \implies v \in D_g$. In addition, since

$$(S - g(D_g)) \cup D_g = (S_f - \{u\}) \cup \{v\},$$

we have $\mathrm{span}(S) = \mathrm{span}((S - g(D_g)) \cup D_g)$ which which is impossible since D_g is bigger than D_f. Hence $D_f = T$. **QED**

Theorem 3. If V is a vector space then V has a basis and any two bases of V have the same number of elements.

Proof. We prove this in he case V is finitely generated. The proof can be adapted to prove the general case.

Let $V = \mathrm{span}(S)$ with $|S| =$ cardinality of S finite. Since the number of elements of a linearly independent subset of V is at most the number of elements of S, there is a maximal linearly independent subset of V. By Theorem 2, this set is a basis for V. If T_1, T_2 are two bases of V then, by the Replacement Theorem, $|T_1| \leq |T_2|$ and $|T_2| \leq |T_1|$ so that $|T_1| = |T_2|$. **QED**

Dimension. The dimension of a vector space V is the number of elements in a basis for V. The dimension of V is denoted by $\dim(V)$. Two vector spaces are isomorphic if and only if they have the same dimension.

Corollary. Let V be a finite dimensional vector space. If W is a subspace of V then

$$\dim(W) \leq \dim(V)$$

with equality if and only if $W = V$.

Remark. The proofs of of the Replacement Lemma and Theorem 3 in the general case require the use of Zorn's Lemma and the Well Ordering Principle, both of which are equivalent to the Axiom of Choice.

(Updated March 25, 2004)