A vector space $V$ over a field $F$ is defined to be a set $V$ with an operation $+$ taking two elements $v, w \in V$ to $v + w \in V$ and an operation taking $r \in F$ and $v \in V$ to $rv \in V$. The operation $+$ is associative and commutative, there is an element $\vec{0} \in V$ with $v + \vec{0} = v$, and for each $v \in V$ there is an element $-v \in V$ such that $v + (-v) = \vec{0}$. The multiplicative operation satisfies the distributive properties $(r + s)v = rv + sv$ and $r(v + w) = rv + rw$ for $r,s \in F$ and $v,w \in V$.

The most familiar example of a vector space is the plane $\mathbb{R}^2$ consisting of pairs $(x,y)$ of real numbers with

$$(a,b) + (x,y) = (a + x, b + y)$$

and

$$r(x,y) = (rx, ry).$$

Let $V$ be a vector space over the field $F$. We say a subset $U \subset V$ is closed (under addition of vectors and multiplication of vectors by scalars), if

$$v,w \in U \Rightarrow v + w \in U \quad \text{and} \quad v \in U, a \in F \Rightarrow av \in U.$$ 

Under this condition the addition and scalar multiplication of $V$ define operations on $U$ making $U$ a vector space over $F$. $U$ is called a subspace of $V$. There are some things to check, for example, if $v \in U$ then $-v \in U$.

If $S$ is a set of vectors in $V$ a linear combination of vectors in $S$ is a finite sum, $\sum a_i v_i$, where the vectors $v_i \in S$ and scalars $a_i \in F$. The set $L(S)$ of all linear combinations of vectors in $S$ is closed under vector addition and multiplication by scalars and therefore is a subspace of $V$. A set $S$ of vectors in $V$ is a generating set for $V$ if $L(S) = V$.

**Lemma 1.** If $S \subset U$ for some subspace $U$ of $V$, then $L(S) \subset U$.

**Proof.** Since $U$ is closed under vector addition and scalar multiplication, the elements of $L(S)$ all lie in $U$.

The lemma says that $L(S)$ is the smallest vector subspace of $V$ containing $S$.

**Lemma 2.** If $V = L(S)$, $U$ is a subspace of $V$, and $U \neq V$, then there is a vector $v \in S$ with $v \notin U$.

**Proof.** Otherwise $S \subset U$ and, by lemma 1, $V = L(S) \subset U$ which would imply $V = U$.

The vectors $v_1, \ldots, v_n$ are linearly dependent if there is a sum

$$\sum_{i=1}^{n} a_i v_i = \vec{0} \quad \text{where not all } a_i = 0.$$
In this case, if \( a_j \neq 0 \), then \( v_j \) is a linear combination of the other vectors. The vectors \( v_1, \ldots, v_n \) are \textit{linearly independent} if they are not linearly dependent, so if

\[
\sum_{i=1}^{n} a_i v_i = \vec{0} \Rightarrow \text{all } a_i = 0.
\]

A set \( S \) of vectors in \( V \) is \textit{independent} if every finite subset of \( S \) is linearly independent.

**Lemma 3.** If \( I \subset V \) is an independent set of vectors and if \( v \in V \) with \( v \notin L(I) \), then \( I \cup \{ v \} \) is independent.

**Proof.** If there were a dependence relation, then \( av + \sum a_i v_i = \vec{0} \) for a finite set of vectors \( v_i \in I \) where not all the \( a \)'s are 0. Since \( I \) is independent, we must have \( a \neq 0 \). Then \( v = -\sum a^{-1} a_i v_i \in L(I) \), a contradiction.

**Bases.**

A \textit{basis} for \( V \) is a generating set \( B \) of vectors in \( V \) which are also linearly independent. This means that

1. every vector \( v \in V \) can be written as a finite sum:

\[
v = \sum a_i v_i \text{ where each } v_i \in B \text{ and only a finite number of } a_i \neq 0,
\]

2. the expression for \( v \) is unique because, if also \( v = \sum b_i v_i \), then \( \sum (a_i - b_i) v_i = \vec{0} \), so \( a_i = b_i \) for each \( i \).

The set \( \{ \vec{0} \} \) is dependent because \( 1\vec{0} = \vec{0} \) and \( 1 \neq 0 \). On the other hand, the empty set is independent since there is no dependence relation. The set \( V = \{ \vec{0} \} \) is a vector space and the empty set is a basis for it using the convention that the empty sum of vectors is \( \vec{0} \).

If a vector space \( V \) is generated by a finite subset \( S \subset V \), we say \( V \) is \textit{finitely generated}.

**Proposition 1.** If a finite set of vectors, \( S = \{ v_1, \ldots, v_n \} \), generate a vector space \( V \), then a subset of these vectors is a basis for \( V \).

**Proof.** We construct a basis \( B \) which is a subset of \( S \). Start by letting \( B \) be the empty set. If \( V = \{ \vec{0} \} \), then \( B \) is a basis for \( V \). If \( V \neq \{ \vec{0} \} \) then, by lemma 2, there is a vector in \( S \) which is not in \( L(B) = \{ \vec{0} \} \). Renumber the vectors so that \( v_1 \neq \vec{0} \) and set \( B = \{ v_1 \} \). \( B \) is a linearly independent set.

Suppose inductively that \( B = \{ v_1, \ldots, v_k \} \) is independent. If \( L(B) = V \) we are done. If \( L(B) \neq V \), then by lemma 2 there is a vector in \( S \) which is not in \( L(B) \). Renumber so that the vector \( v_{k+1} \notin L(B) \). Then \( B \cup \{ v_{k+1} \} \) is independent by lemma 3. Now set \( B = \{ v_1, \ldots, v_{k+1} \} \). After \( m \) steps where \( m \leq n \) we have \( L(B) = V \) where \( B = \{ v_1, \ldots, v_m \} \) is independent. This \( B \) is a basis for \( V \).
Proposition 2. Let $V$ be a vector space and assume:

$I = \{u_1, \ldots, u_m\}$ are independent vectors in $V$,

$S = \{v_1, \ldots, v_n\}$ generate $V$.

Then $m \leq n$.

**Proof.** We construct a sequence of generating sets in which the $u$’s replace the $v$’s. Since $S$ is a generating set, $u_1 = \sum a_i v_i$. Since $u_1 \neq \vec{0}$, some $a_j \neq 0$, renumber to assume $a_1 \neq 0$. Then

$v_1 = a_1^{-1} u_1 - \sum_{i=2}^{n} a_1^{-1} a_i v_i \in L(u_1, v_2, \ldots, v_n)$.

Then $V = L(v_1, \ldots, v_n) \subset L(u_1, v_2, \ldots, v_n)$ so $L(u_1, v_2, \ldots, v_n) = V$.

Now assume $L(u_1, \ldots, u_k, v_{k+1}, \ldots, v_n) = V$ for some $k < m$. Then

$u_{k+1} = \sum_{i=1}^{k} a_i u_i + \sum_{i=k+1}^{n} a_i v_i$.

If $a_i = 0$ for all $i \geq k + 1$, then this is a dependence relation on $u_1, \ldots, u_{k+1}$, but these vectors are independent. So there must be $a_i \neq 0$ for some $i \geq k + 1$ Reumber so that $a_{k+1} \neq 0$. Then $v_{k+1} \in L(u_1, \ldots, u_{k+1}, v_{k+2}, \ldots, v_n)$ and therefore $L(u_1, \ldots, u_{k+1}, v_{k+2}, \ldots, v_n) = V$.

This can be repeated to show $L(u_1, \ldots, u_m, v_{n+1}, \ldots, v_n) = V$. It follows that $m \leq n$.

Theorem. If $V$ is finitely generated, then $V$ has a basis and any two bases have the same number of vectors.

**Proof.** The existence of a basis is proposition 1. Let $B_1$ and $B_2$ be two bases with $m$ and $n$ vectors respectively. Since $B_1$ is independent and $B_2$ generates, proposition 2 shows $m \leq n$. Also $B_2$ is independent and $B_1$ generates, so $n \leq m$. Hence $m = n$.

The dimension of a vector space $V$, $\dim V$, is the number of vectors in a basis. A vector space with a finite set of generators is said to be finitely generated and by the theorem has finite dimension.

If $F$ is a field, a basis for the vector space $F^n = \{(f_1, \ldots, f_n) : f_i \in F\}$ is given by the vectors:

$e_1 = (1, 0, 0, \ldots, 0)$

$e_2 = (0, 1, 0, \ldots, 0)$

$\vdots$

$e_n = (0, 0, \ldots, 0, 1)$.

Proposition 3. If $V$ is finite dimensional over $F$ and $\dim F = n$, then $V$ is isomorphic to $F^n$. 
Proof. Let \( v_1, \ldots, v_n \) be a basis for \( V \). The map \( \phi : V \rightarrow F^n \) defined on the basis by \( \phi(v_i) = e_i \) and extended to \( V \) by \( \phi(\sum a_i v_i) = \sum a_i e_i \) is one-to-one and onto and preserves the vector operations:

\[
\phi(v + w) = \phi(v) + \phi(w) \\
\phi(fv) = f\phi(v).
\]

The proof of Proposition 2 gives a useful result that was not stated in the proposition:

**Proposition 2.1** Any independent set of vectors in a finitely generated vector space is contained in a basis.

By contrast, Proposition 1 states that any finite set of generators contains a basis. There is a stronger version of Proposition 1 that requires a new proof.

**Proposition 1.1** If \( U \) is a subspace of a finitely generated vector space \( V \), then \( U \) has a basis and \( \text{dim} U \leq \text{dim} V \).

**Proof.** If \( U = \{ \vec{0} \} \), the empty set is a basis. If \( U \neq \{ \vec{0} \} \), choose a nonzero vector \( u_1 \in U \) and set \( B = \{ u_1 \} \). \( B \) is a linearly independent set.

Suppose, inductively, that \( B = \{ u_1, \ldots, u_k \} \subset U \) is a linearly independent set. If \( L(B) = U \), then \( B \) is a basis for \( U \). If \( L(B) \neq U \), choose \( u_{k+1} \in U \) with \( u_{k+1} \notin L(B) \). By Lemma 3, \( B \cup \{ u_{k+1} \} \) is an independent set. Redefine \( B = \{ u_1, \ldots, u_{k+1} \} \).

Since the independent set \( B \) is a subset of \( V \), by Proposition 2.1 \( B \) is contained in a basis \( B' \) for \( V \). Hence the number of vectors in \( B \), \( \#(B) \leq \text{dim} V \) and, if \( \#(B) = \text{dim} V \), then by Lemma 3 \( L(B) = V \) so \( U = V \). Thus after \( m \leq \text{dim} V \) steps we find a basis \( B = \{ u_1, \ldots, u_m \} \) for \( U \).

**Linear maps.** Let \( V \) and \( W \) be vector spaces over a field \( F \). A function \( \phi \) with domain \( V \) and range \( W \) which satisfies the conditions

\[
\phi(u + v) = \phi(u) + \phi(v) \quad \text{and} \quad \phi(av) = a\phi(v) \quad \text{for} \ u, v \in V \quad \text{and} \ a \in F
\]

is called a **linear map** and written \( \phi : V \rightarrow W \).

The set of vectors in \( V \) which the map \( \phi \) takes to \( \vec{0} \in W \) is called the **kernel** of \( \phi \),

\[
\ker \phi = \{ v \in V : \phi(v) = \vec{0} \} \subset V.
\]

The **image** of \( \phi \) is the set

\[
\text{im} \phi = \{ \phi(v) : v \in V \} \subset W.
\]

**Proposition 3.** If \( \phi : V \rightarrow W \) is a linear map, then

- \( \ker \phi \) is a subspace of \( V \),
- \( \text{im} \phi \) is a subspace of \( W \).