Linear Algebra

Definition. A **vector space (over R)** is an ordered quadruple

$$(V, \mathbf{0}, \alpha, \mu)$$

such that V is a set; $\mathbf{0} \in V$;

$$\alpha : V \times V \to V \qquad \text{and} \qquad \mu : \mathbf{R} \times V \to V;$$

and the following eight axioms hold:

(i) $\alpha(\alpha(u, v), w) = \alpha(u, \alpha(v, w)), \quad u, v, w \in V;$
(ii) $\alpha(v, \mathbf{0}) = v = \alpha(\mathbf{0}, v), \quad v \in V;$
(iii) for each $v \in V$ there is $w \in V$ such that $\alpha(v, w) = \mathbf{0} = \alpha(w, v);$
(iv) $\alpha(u, v) = \alpha(v, u), \quad u, v \in V;$
(v) $\mu(c + d, v) = \mu(c, v) + \mu(d, v), \quad c, d \in \mathbf{R}, \ v \in V;$
(vi) $\mu(c, \alpha(u, v)) = \alpha(\mu(c, u), \mu(c, v)), \quad c \in \mathbf{R}, \ u, v \in V;$
(vii) $\mu(c, \mu(d, v)) = \mu(cd, v), \quad c, d \in \mathbf{R}, \ v \in V;$
(viii) $\mu(1, v) = v, \quad v \in V.$

Axioms (i),(ii),(iii) say that $(V, \mathbf{0}, \alpha)$ is an Abelian group. Axiom (iv) says that this group is Abelian. One calls the elements of V **vectors**. From now on we write

$$u + v$$

for $\alpha(u, v)$ and call this operation **vector addition**, and we write

$$cv$$

for $\mu(c, v)$, with the latter binding more tightly than the former, and call this operation **scalar multiplication**. If $\mathbf{0}_i, \ i = 1, 2$ satisfy Axiom (ii) with $\mathbf{0}$ there replaced by $\mathbf{0}_i, \ i = 1, 2$, respectively, then

$$\mathbf{0}_1 = \mathbf{0}_1 + \mathbf{0}_2 = \mathbf{0}_2$$

so this element is unique; we call it the **zero** element of V. If $w_i, \ i = 1, 2$ satisfy Axiom (iii) for a given $v \in V$ with w there replaced by $w_i, \ i = 1, 2$, respectively, then

$$w_1 = w_1 + \mathbf{0} = w_1 + (v + w_2) = (w_1 + v) + w_2 = \mathbf{0} + w_2 = w_2$$

so the element $\mathbf{w}$ is uniquely determined; we denote it

$$-v.$$

We also write

$$u - v$$

for $u + (-v), \ u, v \in V$. For any $v \in V$ we have

$$0v = \mathbf{0} + 0v = (-0v + 0v) + 0v = -0v + (0v + 0v) = -0v + (0 + 0)v = -0v + 0v = \mathbf{0};$$

that is

$$0v = \mathbf{0}, \quad v \in V.$$

Example. Suppose S is a nonempty set. Then $\mathbf{R}^S$ is a vector space where, given $f, g \in \mathbf{R}^S$ and $c \in \mathbf{R}$, we set

$$(f+g)(s) = f(s) + g(s) \quad \text{and} \quad (cf)(s) = cf(s), \quad s \in S.$$

We call these operations **pointwise addition** and **pointwise scalar multiplication**, respectively.

Example. Since $\mathbf{R}^n = \mathbf{R}^{\{1,\ldots,n\}}$, it is a vector space by virtue of the previous Example.

Example. $\mathbf{R}$ is a vector space where vector addition is addition and where scalar multiplication is multiplication.

Example. Suppose V is a vector space and S is a nonempty set. Then V^S is a vector space where, given $f, g \in V^S$ and $c \in \mathbf{R}$, we set

$$(f+g)(s) = f(s) + g(s) \quad \text{and} \quad (cf)(s) = cf(s), \quad s \in S.$$

We call these operations **pointwise addition** and **pointwise scalar multiplication**, respectively.

Definition. Suppose V is a vector space. We say a subset U of V is a **linear subspace (of V)**
(i) if $\mathbf{0} \in U$;
(ii) $u + v \in U$ whenever $u, v \in U$;
(iii) $cu \in U$ whenever $c \in \mathbf{R}$ and $u \in U$.
Note that $(U, \mathbf{0}, \alpha|(U \times U), \mu|(\mathbf{R} \times U))$ is a vector space.

Proposition. Suppose V is a vector space and $\mathcal{U}$ is a nonempty family of linear subspaces of V. Then $\bigcap \mathcal{U}$ is a linear subspace of V.
Remark. If $\mathcal{U} = \emptyset$ then $\bigcup \mathcal{U} = \emptyset$ and $\bigcap \mathcal{U}$ is problematic.
Proof. Simple exercise for the reader. $\square$

Definition. Suppose V and W are vector spaces and $L : V \to W$. We say L is **linear** if
(i) $L(v + w) = L(v) + L(w)$ whenever $v, w \in V$;
(ii) $L(cv) = cL(v)$ whenever $c \in \mathbf{R}$ and $v \in V$.

Note that the operations on the left are with respect to V and the operations on the right are with respect to W. We say L **carries** V **isomorphically onto** W if L is univalent and $\mathbf{rng}\, L = W$.

We set

$$\mathbf{ker}\, L = \{v \in V : L(v) = \mathbf{0}\}$$

and call this subset of V the **kernel** or **null space** of L.

We let

$$\mathbf{L}(V; W)$$

be the set of linear maps from V into W. Note that $\mathbf{L}(V; W)$ is a linear subspace of W^V and is therefore a vector space with respect to the operations of pointwise addition and scalar multiplication.

Of particular importance is the case when $W = \mathbf{R}$. We set

$$V^* = \mathbf{L}(V; \mathbf{R})$$

and call this vector space the **dual space** of V.

Suppose $\omega \in V^*$ and $w \in W$. Define $\omega w : V \to W$ by setting

$$\omega w(v) = \omega(v) w, \quad v \in V.$$

Note that ωw is linear.

Proposition. Suppose V and W are vector spaces and $L : V \to W$ is linear. Then
(i) $L(\mathbf{0}) = \mathbf{0}$;

(ii) $\mathbf{ker}\, L$ is a linear subspace of V;
(iii) L is univalent if and only if $\mathbf{ker}\, L = \mathbf{0}$;
(iv) $\mathbf{rng}\, L$ is a linear subspace of W.

Proof. Simple exercise which for the reader.

Definition. Suppose V is a vector space and S is a nonempty set. For each $f \in V^S$ we set

$$\mathbf{spt}\, f = \{s \in S : f(s) \neq \mathbf{0}\}$$

and call the set the **support of** f. We let

$$(V^S)_0 = \{f \in V^S : \mathbf{spt}\, f \text{ is finite}\}.$$

Note that

$$V^\emptyset = (V^\emptyset)_0 = \emptyset.$$

Remark. Suppose V is a vector space and S is a nonempty set. Since V is an Abelian group we know that

$$(V^S)_0 = \{f \in V^S : \mathbf{spt}\, f \text{ is finite}\}$$

is a subgroup of the Abelian group V^S and that there is one and only group homomorphism

$$\sum \cdot : (V^S)_0 \to V$$

such that $\sum(s, v) = v$ whenever $(s, v) \in S \times V$. It is immediate that $(V^S)_0$ is a linear subspace of V^S. We leave as a straightforward exercise for the reader to prove by induction that $\sum \cdot$ is linear.

Definition. Suppose V is a vector space and $S \subset V$. In case $S \neq \emptyset$ we define

$$\mathbf{s} : (\mathbf{R}^S)_0 \to V$$

by setting

$$\mathbf{s}(f) = \sum_{s \in S} f(s)s, \;\; f \in (\mathbf{R}^S)_0.$$

Note that $\mathbf{s}$ is linear because it is the composition of $\sum$ with the linear map $(\mathbf{R}^S)_0 \ni f \mapsto \; (S \ni s \mapsto f(s)s \in V) \in (V^S)_0$. We let

$$\mathbf{span}\, S = \begin{cases} \{\mathbf{0}\} & \text{if } S = \emptyset, \\ \mathbf{rng}\, \mathbf{s} & \text{else} \end{cases}$$

and call this linear subspace of V the **(linear) span of** S. We say S is **independent** if either $S = \emptyset$ or $S \neq \emptyset$ and $\mathbf{s}$ is univalent. We say S is **dependent** if S is not independent. We say S is **basis for** V if S is independent and $V = \mathbf{span}\, S$. Evidently,
(i) the empty set is independent;
(ii) if $\mathbf{0} \in S$ then S is dependent;
(iii) a superset of a dependent set is dependent;
(iv) a subset of an independent set is independent.

Proposition. Suppose V is a vector space and $S \subset V$. Then

$$\mathbf{span}\, S = \bigcap \{U : U \text{ is a linear subspace of } V \text{ and } S \subset U\}.$$

Proof. If U is a linear subspace of V and $S \subset U$ then $\mathbf{span}\, S \subset U$. On the other hand, $\mathbf{span}\, S$ is a linear subspace of V and $S \subset \mathbf{span}\, S$. $\square$

Definition. Suppose V is a vector space and $\mathcal{U}$ is a family of linear subspaces of V. Let

$$\sum \mathcal{U} = \mathbf{span} \bigcup \mathcal{U}.$$

Proposition. Suppose V is a vector space and $S \subset V$. Then S is dependent if and only if there is $s_0 \in S$ such that $s_0 \in \mathbf{span}\,(S \sim \{s_0\})$.

Proof. Suppose S is dependent. Then $S \neq \emptyset$ and there is $f \in (\mathbf{R}^S)_0$ such that f in nonzero and $\sum_{s \in S} f(s)s = \mathbf{0}$. For any $s_0 \in \mathbf{spt}\, f$ we have

$$f(s_0)s_0 + \sum_{s \in S \sim \{s_0\}} f(s)s = \mathbf{0}$$

so that

$$s_0 = -\frac{1}{f(s_0)} \sum_{s \in S \sim \{s_0\}} f(s) \in \mathbf{span}\, S \sim \{s_0\}.$$

On the other hand, if $s_0 \in S$ and $s_0 \in \mathbf{span}\,(S \sim \{s_0\})$ then $s_0 = \sum_{s \in S \sim \{s_0\}} g(s)s$ for some $g \in (\mathbf{R}^{S \sim \{s_0\}})_0$. Let $f \in (\mathbf{R}^S)_0$ be such that

$$f(s) = \begin{cases} -1 & \text{if } s = s_0, \\ g(s) & \text{if } s \in S \sim \{s_0\}. \end{cases}$$

Then f is nonzero and $\sum_{s \in S} f(s)s = \mathbf{0}$ so $f \in \mathbf{ker}\, \mathbf{s}$. Thus S is dependent. $\square$

Proposition. Suppose V is a vector space S is an independent subset of V and $v \in V \sim \mathbf{span}\, S$. Then $S \cup \{v\}$ is independent.

Proof. Were $S \cup \{v\}$ dependent there would be $c \in \mathbf{R}$ and $f \in (\mathbf{R}^S)_0$ such that not both c and f are zero and

$$cv + \sum_{s \in S} f(s)s = \mathbf{0}.$$

But $c \neq 0$ since S is independent. Thus

$$v = -\frac{1}{c} \sum_{s \in S} f(s)s \in \mathbf{span}\, S$$

which is a contradiction. $\square$

Corollary. Suppose V is a vector space. Any maximal independent subset of V is a basis for V.

Proof. This is immediate. $\square$

Theorem. Suppose V is a vector space. Then V has a basis.

Proof. Suppose $\mathcal{S}$ is a nested family of independent subsets of V. Then $\bigcup \mathcal{S}$ is independent. Thus, by the Hausdorff Maximal Principle, there is a maximal independent subset of V. $\square$

Remark. Suppose $V = \mathbf{span}\, S$ where S is a finite subset of V. Then S has a maximal independent subset which, by the previous Proposition is a basis for V. Thus, in this case, we can avoid using the Hausdorff Maximal Principle to show that V has a basis.

Corollary. Suppose V is a vector space and S is an independent subset of V then S is a subset of a basis for V.

Proof. Argue as in the proof of the preceding Corollary that there is a maximal independent subset of V which contains S. $\square$

Definition. Suppose V is a nontrivial vector space and S is a basis for V. We define

$$\cdot^* : S \to V^*$$

at $s \in S$ by requiring that

$$s^*(\mathbf{s}(f)) = f(s), \quad f \in (\mathbf{R}^S)_0.$$

One easily verifies that that for any $v \in \mathbf{span}\, S$ the set $\{s \in S : s^*(v) \neq 0\}$ is finite and that

$$v = \sum_{s \in S} s^*(v)s, \quad v \in V; \tag{2}$$

simply represent v by $\mathbf{s}(f)$ for some $f \in (\mathbf{R}^S)_0$.

If the set S is indexed by the set A we will frequently write

$$s^a \quad \text{for} \quad {s_a}^* \quad \text{whenever } a \in A.$$

Theorem. Suppose V is a vector space and T is a finite independent subset of V. If $S \subset \mathbf{span}\, T$ and $\mathbf{card}\, S > \mathbf{card}\, T$ then S is dependent.

Proof. We induct on $\mathbf{card}\, T$. The Theorem holds trivially in case $\mathbf{card}\, T = 0$.

Suppose $\mathbf{card}\, T > 0$ and choose $\tilde{t} \in B$. Then

$$v = \tilde{t}^*(v)\tilde{t} + \sum_{t \in T \sim \{\tilde{t}\}} t^*(v)t, \quad v \in \mathbf{span}\, T. \tag{3}$$

In case $\tilde{t}^*(s) = 0$ for all $s \in S$ we infer from (3) that $S \subset \mathbf{span}\,(T \sim \{\tilde{t}\})$ which implies by the inductive hypothesis that S is dependent.

So suppose $\tilde{s} \in S$ and $\tilde{t}^*(\tilde{s}) \neq 0$. Define $F : S \sim \{\tilde{s}\} \to V$ by letting

$$F(s) = s - \frac{\tilde{t}^*(s)}{\tilde{t}^*(\tilde{s})}\tilde{s}, \quad s \in S \sim \{\tilde{s}\};$$

we infer from (3) and the linearity of $\tilde{t}^*$ that

$$S' \subset \mathbf{span}\,(T \sim \{\tilde{t}\}). \tag{4}$$

where we have set $S' = \mathbf{rng}\, F$.

Suppose F is not univalent. Choose $s_i \in S,\ i = 1, 2$, such that $s_1 \neq s_2$ and $F(s_1) = F(s_2)$. Then

$$s_1 - s_2 - \frac{\tilde{t}^*(s_1 - s_2)}{\tilde{t}^*(\tilde{s})}\tilde{s} = \mathbf{0}$$

which implies S is dependent.

Suppose F is univalent. Then

$$\mathbf{card}\, S' = \mathbf{card}\, S - 1 > \mathbf{card}\, T - 1 = \mathbf{card}\,(T \sim \{\tilde{t}\}).$$

By (4) and the inductive hypothesis we infer that S' is dependent. Thus there is $f \in (\mathbf{R}^{S \sim \{\tilde{s}\}})$ such that f is nonzero and

$$\sum_{s \in S \sim \{\tilde{s}\}} f(s')F(s) = \mathbf{0}.$$

But this implies that

$$\sum_{s \in S \sim \{\tilde{s}\}} f(s)s - \frac{\tilde{t}^*(\sum_{s \in S \sim \{\tilde{s}\}} f(s)s)}{\tilde{t}^*(\tilde{s})}\tilde{s} = \mathbf{0}$$

so S is dependent. □

Theorem. Suppose V is a vector space. Then any two bases have the same cardinality.

Remark. An infinite basis is not a very useful thing. At least that's my opinion.
Proof. This is a direct consequence of the previous Theorem if V has a finite basis.

More generally, Suppose A and B are bases for V and B is infinite. Let F be the set of finite subsets of B. Define $f : A \to F$ by letting

$$f(a) = \{b \in B : b^*(a) \neq 0\}, \ a \in A.$$

By the preceding Theorem we find that

$$\mathbf{card}\, \{a \in A : f(a) = F\} \leq \mathbf{card}\, F.$$

That $\mathbf{card}\, A \leq \mathbf{card}\, B$ now follows from the theory of cardinal arithmetic. $\square$

Definition. Suppose V is a vector space. We let $\mathbf{dim}\, V$ be the cardinality of a basis for V. We say V is **finite dimensional** if $\mathbf{dim}\, V$ is finite.
Remark. If S is a finite subset of V and $\mathbf{span}\, S = V$ then V is finite dimensional.

Corollary. Suppose V is a finite dimensional vector space and S is an independent subset of V. Then

$$\mathbf{card}\, S \leq \mathbf{dim}\, V$$

with equality only if S is a basis for V.
Proof. The inequality follows directly from the preceding Theorem.

Suppose $\mathbf{card}\, S \leq \mathbf{dim}\, V$. Were there $v \in V \sim \mathbf{span}\, S$ then $S \cup \{v\}$ would be an independent subset of V with cardinality exceeding $\mathbf{dim}\, V$. $\square$

Corollary. Suppose V is finite dimensional and U is a linear subspace of V. Then U is finite dimensional.
Proof. Let S be a maximal independent subset of U; such an S exists because any independent subset of V has at most $\mathbf{dim}\, V$ elements. Were there $v \in U \sim \mathbf{span}\, S$ then $S \cup \{v\}$ would be an independent subset of U with cardinality exceeding that of S. $\square$

Corollary. Suppose V and W are vector spaces and $L \in \mathbf{L}(V; W)$. Then there are $\omega \in V^*$ and $w \in W \sim \{\mathbf{0}\}$ such that $L = \omega w$ if and only if $\mathbf{dim}\, \mathbf{rng}\, L = 1$.
Proof. If there are $\omega \in V^*$ and $w \in W \sim \{\mathbf{0}\}$ such that $L = \omega w$ then $\{w\}$ is a basis for $\mathbf{rng}\, L$.

Suppose $\mathbf{dim}\, \mathbf{rng}\, L = 1$. Let $w \in W$ be such that $\{w\}$ is a basis for $\mathbf{rng}\, L$. Then, as $L(v) = w^*(L(v))w$ for $v \in V$ we can take $\omega = w^* \circ L$. $\square$

Theorem. Suppose V and W are vector spaces, $L : V \to W$ is linear and V is finite dimensional. Then $\mathbf{rng}\, L$ is finite dimensional and

$$\mathbf{dim}\, V = \mathbf{dim}\, \mathbf{ker}\, L + \mathbf{dim}\, \mathbf{rng}\, L.$$

Proof. Let A be a basis for $\mathbf{ker}\, L$. Let B be a maximal independent subset of V containing A and note that B is a basis for V. Note that $L|(B \sim A)$ is univalent and that $C = \{L(v) : v \in B \sim A\}$ is a basis for $\mathbf{rng}\, L$. The assertion to be proved follows from that fact that

$$\mathbf{card}\, B = \mathbf{card}\, A + \mathbf{card}\, C.$$

$\square$

Definition. Suppose V is a finite dimensional vector space and B is a basis for V. Then

$$B^* = \{b^* : b \in B\}$$

is a basis for V^* which we call the **dual basis (to B)**; the independence of this set is clear and the fact that it spans V^* follows from the fact that

$$\omega = \sum_{b \in B} \omega(b) b^*, \quad \omega \in V^*,$$

which follows immediately from (2). In particular, $\mathbf{dim}\, V^* = \mathbf{dim}\, V$.

Remark. The $\cdot^*$ notation is quite effective but must be used with care because of the following ambiguity. Suppose V is a finite dimensional vector space and $B_i,\ i = 1, 2$ are two different bases for V. Show that if $b \in B_1 \cap B_2$ then the v^*'s corresponding to B_1 and B_2 are different if $\mathbf{span}\, B_1 \sim \{b\} \neq \mathbf{span}\, B_2 \sim \{b\}$.

Remark. Suppose S is a nonempty set. We have linear maps

$$\mathbf{R}^S \ni g \mapsto ((\mathbf{R}^S)_0 \ni f \mapsto \sum_{s \in S} f(s)g(s)) \in {(\mathbf{R}^S)_0}^*$$

and

$${(\mathbf{R}^S)_0}^* \ni \omega \mapsto (S \ni s \mapsto \omega(\delta_s)) \in \mathbf{R}^S.$$

These maps are easily seen to be linear and inverse to each other. Thus ${(\mathbf{R}^S)_0}^*$ is isomorphic to $\mathbf{R}^S$. Now suppose S is a basis for the vector space V. Since $\mathbf{s}$ carries $(\mathbf{R}^S)_0$ isomorphically onto V we find that

$$V^* \equiv {(\mathbf{R}^S)_0}^* \equiv \mathbf{R}^S.$$

Chasing through the above isomorphisms one finds that $\{b^* : b \in B\}$ is independent but, in case S is infinite, does not span V^*. In fact, V^* is not of much use when V is not finite dimensional.

Definition. Let

$$\iota : V \to V^{**}$$

be the map

$$V \ni v \mapsto (V^* \ni \omega \mapsto \omega(v)) \in V^{**}.$$

Evidently, this map is linear and univalent.

Now suppose V is finite dimensional. Let B be a basis for V. One easily verifies that

$$\iota(b) = b^{**}, \quad b \in B.$$

Thus, since ι carries the basis B to the basis B^{**} it must be an isomorphism. It is called the **canonical isomorphism from V onto V^*∗**.

Definition. Suppose U is a linear subspace of the vector space V. We let

$$U^\perp = \{\omega \in V^* : \omega | U = 0\}$$

and note that $U^\perp$ is a linear subspace of V^*.

Theorem. Suppose U is a linear subspace of the finite dimensional vector space V. Then

$$\mathbf{dim}\, U^\perp = \mathbf{dim}\, V - \mathbf{dim}\, U.$$

Proof. Let B be a basis for U and let C be a basis for V such that $B \subset C$. Evidently, $\{b^* : b \in C \sim B\} \subset U^\perp$. Moreover, for any $\omega \in U^\perp$ we have

$$\omega = \sum_{b \in c} \omega(b) b^* = \sum_{b \in C \sim B} \omega(b) b^*.$$

□

Definition. Suppose V and W are vector spaces and $L : V \to W$ is linear. We define

$$L^* \in \mathbf{L}(W^*; V^*)$$

by letting

$$L^*(\omega) = \omega \circ L, \quad \omega \in W^*.$$

One easily verifies that $\cdot^*$ carries $\mathbf{L}(V;W)$ linearly into $\mathbf{L}(W^*;V^*)$ and that, under appropriate hypotheses,

(i) $L^{**} = L$ and

(ii) $(L \circ M)^* = M^* \circ L^*$.

The map $\cdot^*$ is called the **adjoint**. Note that this term is used in the context of inner product spaces in a similar but different way and that it occurs in the theory of determinants in a totally different way.

Theorem. Suppose V and W are finite dimensional vector spaces and $L : V \to W$ is linear. Then

$$(\mathbf{rng}\, L)^\perp = \mathbf{ker}\, L^* \quad \text{and} \quad (\mathbf{ker}\, L)^\perp = \mathbf{rng}\, L^*.$$

Remark. It is evident that the right hand side in each case is contained in the left hand side.

Proof. Let C be a basis for $\mathbf{rng}\, L$ and let D be a basis for W containing C. Let A be a subset of V such that $\{L(v) : v \in A\} = C$ and note that A is independent. Let B be the union of A with a basis for $\mathbf{ker}\, L$ and note that B is a basis for V.

Note that $\{d^* : d \in D \sim C\}$ is a basis for $(\mathbf{rng}\, L)^\perp$ and that $\{b^* : b \in A\}$ is a basis for $(\mathbf{ker}\, L)^\perp$.

For any $d \in D$ we have

$$\begin{aligned} L^*(d^*) &= \sum_{b \in B} L^*(d^*)(b) b^* \\ &= \sum_{b \in B} d^*(L(b)) b^* \\ &= \sum_{b \in B \sim A} d^*(L(b)) b^* \\ &= \begin{cases} b^* & \text{if } d = L(b) \text{ for some } b \in A, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Thus $\{b^* : b \in A\}$ is a basis for $\mathbf{rng}\, L^*$ and $\{d^*; d \in D \sim C\}$ is a basis for $\mathbf{ker}\, L^*$. $\square$

Theorem. Suppose V is a finite dimensional vector space. There is one and only one

$$\mathbf{trace} \in \mathbf{L}(V;V)^*$$

such that

$$\mathbf{trace}\,(\omega(v)) = \omega(v), \quad \omega \in V^*, \ v \in V. \tag{5}$$

Moreover, if B is a basis for V then

$$\mathbf{trace}\, L = \sum_{b \in B} b^*(L(b)). \tag{6}$$

Proof. Let B be a basis for V. Then the formula in (6) defines a member of $\mathbf{L}(V;V)$ which satisfies (5). $\square$

Theorem. Suppose U and W are subspaces of V. Then

$$\mathbf{dim}\, U + W + \mathbf{dim}\, U \cap W = \mathbf{dim}\, U + \mathbf{dim}\, W.$$

Proof. Let A be a basis for $U \cap W$. Extend A to a basis B for U and a basis C for W. Verify that $A \cup B \cup C$ is a basis for $U + W$. $\square$