Basis and dimension.

Recall that $\beta \subseteq V$ is a basis for V if $\mathrm{Span}(\beta) = V$ and β is a lin. indep. set.

We have shown (Theorem 1.8) that if $\beta = \{u_1, \dots, u_n\}$ is a basis for V, then every vector $v \in V$ can be expressed as

$v = a_1 u_1 + \dots + a_n u_n$

for a unique choice of the scalars $a_1, \dots, a_n \in F$.

- But how does one find a basis for V?

Theorem 1.9. If V is a vector space generated by a finite set S, then some subset of S is a basis for V. In particular, V has a finite basis.

Proof.

If $S = \emptyset$ or $S = \{0\}$, then $V = \mathrm{Span}(S) = \{0\}$ and $\emptyset$ is a subset of S that is a basis for V.

Otherwise, S contains a vector $u_1 \neq 0$.

By the previous example, the set $\{u_1\}$ is linearly independent.

If there is u_2 in S s.t. $\{u_1, u_2\}$ is still linearly indep., add it to $\{u_1\}$ to get $\{u_1, u_2\}$.

If there is $u_3 \in S$ $\{u_1, u_2, u_3\}$ is lin. indep., add it to obtain the set $\{u_1, u_2, u_3\}$, etc...

Since S is finite, this process must stop on some step n, and we obtain a set

$\beta = \{u_1, \dots, u_n\} \subseteq S$ s.t. β is linearly indep., but $\beta \cup \{x\}$ is lin. dependent for any $x \in S \setminus \beta$.

Claim. β is a basis for V.

- β is lin. indep. — by construction.
- Remains to show: $\mathrm{Span}(\beta) = V$.

By Theorem 1.5, need to show that $S \subseteq \mathrm{Span}(\beta)$ — as $\mathrm{Span}(\beta)$ is a subspace of V containing S, it must also contain $\mathrm{Span}(S) = V$.

Let $v \in S$ be arbitrary.

If $v \in \beta$, then $v \in \mathrm{Span}(\beta)$.

Otherwise, if $v \notin \beta$, then by construction $\beta \cup \{v\}$ is lin. dep. — so $v \in \mathrm{Span}(\beta)$ by Theorem 1.7.

Thus $S \subseteq \mathrm{Span}(\beta)$.

- Existence of a basis in V can be proved without assuming that S is finite as well, but the proof is more involved.
- Thus, any finite generating set for V can be reduced to a basis for V, by removing some vectors.

Example. The set $S = \{(2,-3,5), (1,0,-2), (7,2,0), (0,1,0)\} \subseteq \mathbb{R}^3$ generates $\mathbb{R}^3$ (check it!)

We reduce it to a basis of $\mathbb{R}^3$, as in the proof of Theorem 1.9.

$S_0 = \{(2,-3,5)\}$ — lin. indep.

$S_1 = \{(2,-3,5), (1,0,-2)\} \leftarrow$ still lin. indep. (check it!)

$S_2 = \{(2,-3,5), (1,0,-2), (7,2,0)\} \checkmark$

But $(0,1,0) \in \mathrm{Span}(S_2)$: $-\frac{7}{30}(2,-3,5) - \frac{35}{60}(1,0,-2) + \frac{3}{20}(7,2,0) = (0,1,0)$.

Hence $\beta = S_2$ is a basis for $\mathbb{R}^3$.

Now, the key technical result of this section.

Theorem 1.10 (Replacement). Let V be a v.s. generated by a set $G \subseteq V$ with $|G| = n$ (the size of G), and let $L \subseteq V$ be a lin. indep. subset of V with $|L| = m$.

Then $m \leq n$, and there exists $H \subseteq G$ with $|H| = n-m$ such that $L \cup H$ generates V.

Proof. We prove it by induction on m.

For $m = 0$, $L = \emptyset$, and so we can take $H = G$.

Now suppose the result is true for $m \geq 0$, and we prove it for $m+1$.

Let $L = \{v_1, \dots, v_{m+1}\} \subseteq V$ be lin. indep., $|L| = m+1$.

By Theorem 1.6, $\{v_1, \dots, v_m\}$ is also lin. indep. Applying the induction hypothesis, $m \leq n$ and there is a subset $\{u_1, \dots, u_{n-m}\} \subseteq G$ s.t. $\{v_1, \dots, v_m\} \cup \{u_1, \dots, u_{n-m}\}$ generates V.

So, there exist $a_1, \ldots, a_m, b_1, \ldots, b_{n-m}$ such that

$a_1 v_1 + \ldots + a_m v_m + b_1 u_1 + \ldots + b_{n-m} u_{n-m} = v_{m+1}$ $\quad (*)$

Note. Since $\{v_1, \ldots, v_m, v_{m+1}\}$ is lin. indep., we must have $n > m$ (that is, $n \geq m+1$) and some $b_i \neq 0$, say $b_1 \neq 0$.
(otherwise v_{m+1} is a lin. combination of $v_1, \ldots, v_m$).

Solving $(*)$ for u_1 gives:

$u_1 = \left(-\frac{a_1}{b_1}\right) v_1 + \ldots + \left(-\frac{a_m}{b_1}\right) v_m + \left(\frac{1}{b_1}\right) v_{m+1} + \left(-\frac{b_2}{b_1}\right) u_2 + \ldots + \left(-\frac{b_{n-m}}{b_1}\right) u_{n-m}$. $\quad (**)$

Let $H = \{u_2, \ldots, u_{n-m}\}$, so $|H| = n-(m+1)$.

Then $u_1 \in \mathrm{Span}(L \cup H)$ by $(**)$, and so $\{v_1, \ldots, v_m, u_1, \ldots, u_{n-m}\} \subseteq \mathrm{Span}(L \cup H)$.

As $\{v_1, \ldots, v_m, u_1, \ldots, u_{n-m}\}$ generates V, $\mathrm{Span}(L \cup H) = V$ (by Theorem 1.5)

Thus, the theorem is true for $m+1$.

This theorem has very important consequences.

Corollary 1. Let V be a v.s. having a finite basis. Then every basis for V contains the same number of vectors.

Proof. Suppose $\beta \subseteq V$ with $|\beta| = n$ is a basis for V, and let $\gamma \subseteq V$ be any other basis for V.
Suppose that $|\gamma| > n$, and let $S \subseteq \gamma$ have $n+1$ elements.
Since S is lin. indep. and β generates V, by replacement $n+1 \leq n$ — a contradiction.
Thus $|\gamma| = m \leq n$.
Reversing the roles of β and γ, by the same argument we get $n \leq m$. Hence $n = m$.

This fact makes possible the following important definition.

Definition. A v.s. V is finite-dimensional if it has a finite basis.
The (unique) number of vectors in a basis for V is called the dimension of V, denoted $\dim(V)$.
If there is no finite basis, then V is infinite-dimensional.

Example. In view of the previous discussion, we have:

1) $\dim(\{0\}) = 0$. $\quad$ ($\emptyset$ is the basis).
2) $\dim(F^n) = n$. $\quad$ ($\{(1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1)\}$ is a basis of size n).
3) $\dim(M_{m \times n}) = mn$. $\quad$ ($\{E^{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of size mn; recall that $E^{ij} = \begin{array}{c c} & j \\ i & \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} \end{array}$).
4) $\dim(P_n(F)) = n+1$. ($\{1, x, x^2, \ldots, x^n\}$ is a basis of size $n+1$).

Example. On the other hand, some of the familiar examples are infinite-dimensional.
By the replacement theorem, if V is finite-dimensional, then no lin. indep. set can contain more than $\dim(V)$ elements. Thus:

$P(F)$ is infinite-dimensional (as $\{1, x, x^2, x^3, \ldots\}$ is an infinite lin. indep. set).

Corollary 2. Let V be a v.s. of dimension n.
a) Any lin. indep. subset of V with n elements is a basis.
b) Every lin. indep. subset of V can be extended to a basis for V.

Proof. Let β be a basis for V, $|\beta| = n$.
a) Let $L \subseteq V$ be lin. indep. with $|L| = n$. By the Replacement theorem, $\exists H \subseteq \beta$ with $|H| = n-n = 0$ elements such that $L \cup H$ generates V. Thus $H = \emptyset$, and so L gener V — so L is a basis.
b) If $L \subseteq V$ is lin. indep. with $|L| = m$, by the Replacement theor $\exists H \subseteq \beta$ with $|H| = n-m$ such that $L \cup H$ generates V. Now $|L \cup H| \leq m + (n-m) = n$.
By Theorem 1.9 $L \cup H$ contains some subset γ which is a basis for V, and $|\gamma| = n$ by Corollary 1.
But then $\gamma = L \cup H$.

Theorem 1.11.
Let W be a subspace of a v.s. V with $\dim(V) < \infty$.
Then $\dim(W) \leq \dim(V)$.
Moreover, if $\dim(W) = \dim(V)$, then $V = W$.

Proof.

Let $\dim(V) = n$.

If $W = \{0\}$ then $\dim(W) = 0 \le n$ (by the previous example).

Otherwise $\exists\, x_1 \in W$, $x_1 \neq 0$. So $\{x_1\}$ is a lin. indep. set.

Continue choosing $x_1, \dots, x_k \in W$ s.t. $\{x_1, \dots, x_k\}$ is lin. indep.

Since no lin. indep. subset of V can contain more than n vectors (Cor 1 + Cor 2), this process must stop at a stage where:

$k \le n$, $\{x_1, \dots, x_k\}$ is lin. indep., but $\{x_1, \dots, x_k\} \cup \{v\}$ is lin. dep. for any $v \in W$.

By Theorem 1.7, this implies $\mathrm{Span}(\{x_1, \dots, x_k\}) = W$, hence $\{x_1, \dots, x_k\}$ is a basis for W.

So $\dim(W) = k \le n$.

(and by Corollary 2(a), if $k = n$ then $\{x_1, \dots, x_k\}$ is a basis for V, hence $W = V$.)

Corollary. If W is a subspace of a v.s. V with $\dim(V) < \infty$, then any basis for W can be extended to a basis for V.

Proof. If $S \subseteq W$ is a basis for W, it is a lin. indep. subset of V, so can be extended to a basis for V.

Example.

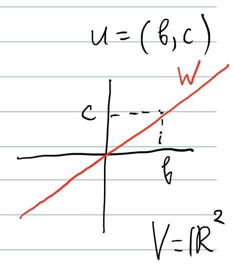
1) Let's describe all subspaces of $V = \mathbb{R}^2$.

We know $\dim(\mathbb{R}^2) = 0$ (as $\{(1,0), (0,1)\}$ is a basis).

By Theorem 1.11, for every subspace $W \le \mathbb{R}^2$ we must have $\dim(W) = 0, 1$ or 2.

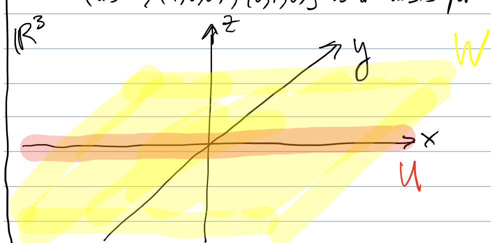
If $\dim(W) = 0$ then $W = \{0\}$ and if $\dim(W) = 2$ then $W = \mathbb{R}^2$.

And if $\dim(W) = 1$, then $W = \{a \cdot u : a \in F\}$ for some non-zero vector $u \in \mathbb{R}^2$.



2) If $V = \mathbb{R}^3$, then $\dim(V) = 3$, and for $W = \{(a, b, 0) : a, b \in \mathbb{R}\}$ we have $\dim(W) = 2$.

(as $\{(1,0,0), (0,1,0)\}$ is a basis for W) and $\dim(U) = 1$ for $U = \{(a, 0, 0) : a \in \mathbb{R}\}$.



W is the xy-plane

U is the x-axis

We can list all subspaces of $\mathbb{R}^3$:

$\dim(W) = 0$ — W is the origin point,

$\dim(W) = 1$ — W is a line through the origin,

$\dim(W) = 2$ — W is a plane through the origin,

$\dim(W) = 3$ — $W = \mathbb{R}^3$.

Linear transformations

Definition. Let V and W be v.s. (over F).

A function $T : V \to W$ is a linear transformation from V to W if, for all $x, y \in V$ and $c \in F$:

(a) $T(x+y) = T(x) + T(y)$

(b) $T(cx) = c\,T(x)$

addition and scalar mult. in V

addition and scalar mult. in W.

Basic properties of linear transformations

Let $T : V \to W$ be a lin. transformation. Then:

1) $T(0) = 0$

2) $T(cx + y) = c\,T(x) + T(y)$ for all $x, y \in V$, $c \in F$. (This holds if and only if T is linear).

3) $T(x - y) = T(x) - T(y)$

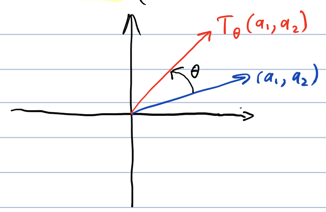
4) $T\left(\sum_{i=1}^{n} a_i x_i\right) = \sum_{i=1}^{n} a_i T(x_i)$ for all $x_i \in V$, $a_i \in F$.

Proof. Exercise.

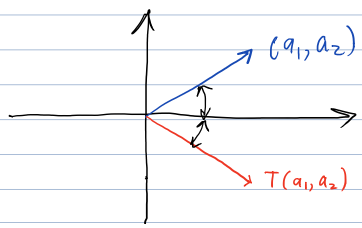
Example. Some examples of lin. transformations $T: \mathbb{R}^2 \to \mathbb{R}^2$.

1) $T(a_1, a_2) = (5a_1, 3a_2)$.
2) For any $\theta \in \mathbb{R}$, define:
   $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$
   $T_\theta(a_1, a_2) = (a_1 \cos\theta - a_2 \sin\theta,\ a_1 \sin\theta + a_2 \cos\theta)$. — check that T is linear!

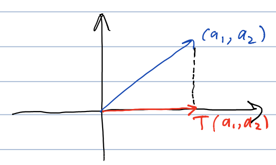
— the rotation (counter-clockwise) by the angle θ.



3) $T(a_1, a_2) = (a_1, -a_2)$ — the reflection about the x-axis.



4) $T(a_1, a_2) = (a_1, 0)$ — the projection on the x-axis.



Example. We define $T: M_{m\times n}(F) \to M_{n\times m}(F)$ by $T(A) = A^t$, where A^t is the transpose of A.
Then T is a lin. transformation.

Example. Define $T: P_n(\mathbb{R}) \to P_{n-1}(\mathbb{R})$ by $T(f(x)) = f'(x)$, where $f'(x)$ denotes the derivative of $f(x)$.
To show that T is linear, let $g(x), h(x) \in P_n(\mathbb{R})$ and $a \in \mathbb{R}$ be arbitrary. Then:
$T(ag(x) + h(x)) = (ag(x) + h(x))' = ag'(x) + h'(x) = a \cdot T(g(x)) + T(h(x))$.

Example. Let $V = C(\mathbb{R})$, the vector space of continuous real-valued functions on $\mathbb{R}$.
Let $a, b \in \mathbb{R}$, $a < b$ be fixed. We define $T: V \to \mathbb{R}$ (the v.s. $\mathbb{R}^1$) by:
$T(f) = \int_a^b f(t)\,dt$
for all functions $f \in V$.
Then T is linear (because $\int_a^b (ag(t) + h(t))\,dt = a\int_a^b g(t)\,dt + \int_a^b h(t)\,dt = a \cdot T(g) + T(h)$.

Null space and range.

Definition. Let V and W be v.s., and $T: V \to W$ be linear.
1) Let $N(T) = \{x \in V : T(x) = 0\}$ — the null space (or kernel) of T.
2) Let $R(T) = \{T(x) : x \in V\}$ — the range (or image) of T.

Example. Let V and W be v.s.
1) We define $I: V \to V$ by $I(x) = x$ for all $x \in V$ — the identity transformation.
   Then I is linear, $N(I) = \{0\}$ and $R(I) = V$.
2) We define $T_0 : V \to W$ by $T_0(x) = 0$ for all $x \in V$ — the zero transformation.
   Then T_0 is linear, $N(T_0) = V$ and $R(T_0) = \{0\}$.

Theorem 2.1. Let V, W be v.s and $T: V \to W$ linear.
Then $N(T)$ and $R(T)$ are subspaces of V and W, respectively.

Proof.

1) $N(T)$ is a subspace of V.
   (a) $0 \in N(T)$ — as $T(0) = 0$.
   b),c) Let $x, y \in N(T)$ and $c \in F$.
   Then $T(x+y) = T(x) + T(y) = 0 + 0 = 0$ and $T(cx) = c \cdot T(x) = c \cdot 0 = 0$.
   Hence $x+y \in N(T)$ and $cx \in N(T)$.
   So $N(T)$ is a subspace of V.
2) $R(T)$ is a subspace of W.
   Analogous (do it!).

Theorem 2.2 Let V, W be v.s. and $T: V \to W$ linear.
If $\beta = \{v_1, \dots, v_n\}$ is a basis for V, then
$R(T) = \mathrm{Span}(T(\beta)) = \mathrm{Span}(\{T(v_1), \dots, T(v_n)\})$.

Proof. Clearly $T(v_i) \in R(T)$ for each i.
As $R(T)$ is a subspace of W, $\mathrm{Span}(\{T(v_1), \dots, T(v_n)\}) = \mathrm{Span}(T(\beta)) \subseteq R(T)$ (by Theorem 1.5)
Suppose $w \in R(T)$, then $w = T(v)$ for some $v \in V$.
As β is a basis for V, we have
$v = \sum_{i=1}^{n} a_i v_i$ for some $a_i \in F$.
And since T is linear,
$w = T(v) = \sum_{i=1}^{n} a_i T(v_i) \in \mathrm{Span}(T(\beta))$.
Hence $R(T) \subseteq \mathrm{Span}(T(\beta))$.

Definition. Let V, W be v.s. and $T: V \to W$ linear.
If $N(T), R(T)$ are finite-dimensional, then we define
$\mathrm{nullity}(T) = \dim(N(T))$,
$\mathrm{rank}(T) = \dim(R(T))$.

- Intuitively, if $N(T)$ is "large" (that is, T sends many vectors from V to 0), then $R(T)$ should be "small" (not so many vectors in W can be obtained by T from the vectors in V). And vice versa.

Theorem 2.3 (Dimension Theorem). Let V, W be v.s. and $T: V \to W$ linear. If $\dim(V) < \infty$ then
$\mathrm{nullity}(T) + \mathrm{rank}(T) = \dim(V)$.

Proof.
Suppose that $\dim(V) = n$, $\dim(N(T)) = k$, and $\{v_1, \dots, v_k\}$ is a basis for $N(T)$.
By the Corollary to Theorem 1.11:
Can extend $\{v_1, \dots, v_k\}$ to a basis $\beta = \{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ for V.

Claim. $S = \{T(v_{k+1}), \dots, T(v_n)\}$ is a basis for $R(T)$.

- S generates $R(T)$.
  As $T(v_i) = 0$ for $1 \le i \le k$, by Theorem 2.2:
  $R(T) = \mathrm{Span}(\{T(v_1), \dots, T(v_n)\}) = \mathrm{Span}(\{T(v_{k+1}), \dots, T(v_n)\}) = \mathrm{Span}(S)$.
- S is lin. indep.:
  Suppose $\sum_{i=k+1}^{n} b_i T(v_i) = 0$ for $b_{k+1}, \dots, b_n \in F$.
  As T is linear, $T\left(\sum_{i=k+1}^{n} b_i v_i\right) = 0$.
  So $\sum_{i=k+1}^{n} b_i v_i \in N(T)$.
  Hence $\exists\, c_1, \dots, c_k \in F$ such that $\sum_{i=k+1}^{n} b_i v_i = \sum_{i=1}^{k} c_i v_i$, (as $\{v_1, \dots, v_k\}$ is a basis for $N(T)$). or $\sum_{i=1}^{k} (-c_i) v_i + \sum_{i=k+1}^{n} b_i v_i = 0$.
  Since β is a basis for V, we have $b_i = 0$ for all i.
  Hence S is lin. indep.
  So $\dim(V) = n$, $\dim(N(T)) = k$ and $\dim(R(T)) = n - k$.