

10 Learning to do proofs

PF1HS132. Prove the following theorem.

Theorem 10.1. (Exchange Theorem) Let V be an $\mathbb{F}$ -vector space. Let $B = \{v_1, \dots, v_k\}$ be a basis of V and let $D = \{d_1, \dots, d_\ell\}$ be another basis of V . Then there exists $d_{i_1} \in D$ such that

$$\{d_{i_1}, b_2, b_3, \dots, b_k\} \text{ is a basis of } V.$$

Solution. Proof of the Exchange Theorem.

Assume

$$\begin{aligned} B = \{b_1, \dots, b_k\} & \text{ is a basis of } V \text{ and} \\ D = \{d_1, \dots, d_\ell\} & \text{ is another basis of } V. \end{aligned}$$

If $d_1, \dots, d_\ell \in \text{span}(B - \{b_1\})$ then

$$V = \text{span}(d_1, \dots, d_\ell) \subseteq \text{span}(B - \{b_1\}) \subseteq V$$

giving $V = \text{span}(B - \{b_1\})$.

But since B is a minimal spanning set then $V \neq \text{span}(B - \{b_1\})$ and so

there exists $d_{i_1} \in D$ such that $d_{i_1} \notin \text{span}(B - \{b_1\})$.

$$d_{i_1} = c_1 b_1 + c_2 b_2 + \dots + c_k b_k, \quad \text{with } c_1 \neq 0.$$

To show: $B_1 = \{d_{i_1}, b_2, \dots, b_k\}$ is a basis of V .

To show: (1) $\text{span}\{d_{i_1}, b_2, \dots, b_k\} = V$.

(2) $\{d_{i_1}, b_2, \dots, b_k\}$ is linearly independent.

(1) Since

$$b_1 = c_1^{-1}(-d_{i_1} + c_2 b_2 + \dots + c_k b_k)$$

then $b_1, b_2, \dots, b_k \in \text{span}\{d_{i_1}, b_2, \dots, b_k\}$. So $V = \text{span}\{b_1, \dots, b_k\} \subseteq \text{span}\{d_{i_1}, b_2, \dots, b_k\} \subseteq V$. So

$$V = \text{span}(d_{i_1}, b_2, \dots, b_k).$$

(2) If $a_1 d_{i_1} + a_2 b_2 + \dots + a_k b_k = 0$ then

$$a_1(c_1 b_1 + c_2 b_2 + \dots + c_k b_k) + a_2 b_2 + \dots + a_k b_k = 0.$$

Since B is linearly independent then $a_1 c_1 = 0$.

Since $c_1 \neq 0$ then $a_1 = 0$ and $a_2 b_2 + \dots + a_k b_k = 0$.

Since B is linearly independent then $a_2 = 0, \dots, a_k = 0$.

So $\{d_{i_1}, b_2, \dots, b_k\}$ is linearly independent.

So $\{d_{i_1}, b_2, \dots, b_k\}$ is a basis of V . □

PF2HS134. Prove the following theorem.

Theorem 10.2. (Dimension Theorem) Let V be an $\mathbb{F}$ -vector space. Any two bases of V have the same number of elements.

Solution. Proof of the Dimension Theorem.

Assume

$$\begin{aligned} B = \{b_1, \dots, b_k\} & \text{ is a basis of } V \text{ and} \\ D = \{d_1, \dots, d_\ell\} & \text{ is another basis of } V. \end{aligned}$$

Using the Exchange theorem, there exists $d_{i_1} \in D$ such that $d_{i_1} \notin \text{span}(B - b_1)$. Then

$$B_1 = \{d_{i_1}, b_2, b_3, b_4, \dots, b_k\} \text{ is a basis of } V.$$

Using the Exchange theorem, there exists $d_{i_2} \in D$ such that $d_{i_2} \notin \text{span}(B_1 - b_2)$. Then

$$B_2 = \{d_{i_1}, d_{i_2}, b_3, b_4, \dots, b_k\} \text{ is a basis of } V.$$

Continue this replacement process to obtain

$$B' = \{d_{i_1}, \dots, d_{i_k}\} \subseteq D, \text{ such that } B' \text{ is a basis of } V.$$

By the Minimax Theorem D is a minimal spanning set.

So $B' = D$ and $k = \ell$.

So B and D have the same number of elements. □

The following provides an example of a spanning set that is not minimal, and another spanning set for the same subspace that is minimal.

PF3Example V14. Let S be the subset of $\mathbb{R}^3$ given by

$$S = \{(1, 1, 1), (2, 2, 2), (3, 3, 3)\}. \quad \text{Determine } \mathbb{R}\text{-span}(S).$$

In this case

$$\begin{aligned} \mathbb{R}\text{-span}(S) &= \{c_1 |1, 1, 1\rangle + c_2 |2, 2, 2\rangle + c_3 |3, 3, 3\rangle \mid c_1, c_2, c_3 \in \mathbb{R}\} \\ &= \{c_1 |1, 1, 1\rangle + 2c_2 |1, 1, 1\rangle + 3c_3 |1, 1, 1\rangle \mid c_1, c_2, c_3 \in \mathbb{R}\} \\ &= \{(c_1 + 2c_2 + 3c_3) |1, 1, 1\rangle \mid c_1, c_2, c_3 \in \mathbb{R}\} \\ &= \{t |1, 1, 1\rangle \mid t \in \mathbb{R}\} = \mathbb{R}\text{-span}\{|1, 1, 1\rangle\} \\ &= \{t |t, t, t\rangle \mid t \in \mathbb{R}\}. \end{aligned}$$

Here $\{|1, 1, 1\rangle\}$ is a basis of $\mathbb{R}\text{-span}(S)$ and

$$\dim(\mathbb{R}\text{-span}(S)) = 1 \quad (\text{even though } S \text{ has 3 elements}).$$

□

PF4 Prove the following proposition.

Proposition 10.3. (*Span is a subspace*) Let V be a $\mathbb{R}$ -vector space. Let $B = \{b_1, \dots, b_k\}$ be a subset of V . Then $\mathbb{R}\text{-span}(B)$ is a subspace of V .

Solution. Proof.

To show: (1) $0 \in \text{span}(B)$.

(2) If $v_1, v_2 \in \text{span}(B)$ then $v_1 + v_2 \in \text{span}(B)$.

(3) If $v \in \text{span}(B)$ and $c \in \mathbb{R}$ then $cv \in \text{span}(B)$.

(1) Since $0 = 0b_1 + \cdots + 0b_k$ then $0 \in \text{span}\{b_1, \dots, b_k\} = \text{span}(B)$.

(2) Assume $v_1, v_2 \in \mathbb{R}\text{-span}(B)$. To show $v_1 + v_2 \in \text{span}(B)$.

Since $v_1, v_2 \in \mathbb{R}\text{-span}(B)$ then there exist $a_1, \dots, a_k, c_1, \dots, c_k \in \mathbb{R}$ such that

$$v_1 = a_1b_1 + \cdots + a_kb_k \quad \text{and} \quad v_2 = c_1b_1 + \cdots + c_kb_k.$$

Then

$$\begin{aligned} v_1 + v_2 &= (a_1b_1 + \cdots + a_kb_k) + (c_1b_1 + \cdots + c_kb_k) \\ &= (a_1 + c_1)b_1 + \cdots + (a_k + c_k)b_k. \end{aligned}$$

So $v_1 + v_2 \in \text{span}\{b_1, \dots, b_k\} = \text{span}(B)$.

(3) Assume $v \in \mathbb{R}\text{-span}(B)$ and $c \in \mathbb{R}$.

To show $cv \in \mathbb{R}\text{-span}(B)$.

Since $v \in \mathbb{R}\text{-span}(B)$ then there exist $a_1, \dots, a_k \in \mathbb{R}$ such that

$$v = a_1b_1 + \cdots + a_kb_k.$$

Then

$$cv = c(a_1b_1 + \cdots + a_kb_k) = (ca_1)b_1 + \cdots + (ca_k)b_k.$$

So $cv \in \mathbb{R}\text{-span}\{b_1, \dots, b_k\}$. So $cv \in \mathbb{R}\text{-span}(B)$. □

PF5HS134. Prove the following proposition.

Proposition 10.4. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{R})$.

If $\ker(A) = 0$ then the columns of A are linearly independent.

Solution. *Proof.* Let $a_1, \dots, a_s$ be the columns of A .

Assume $\ker(A) = 0$.

To show: $a_1, \dots, a_s$ are linearly independent.

To show: If $c_1, \dots, c_s \in \mathbb{R}$ and $c_1a_1 + \cdots + c_sa_s = 0$

$$\text{then } c_1 = 0, c_2 = 0, \dots, c_s = 0.$$

Assume $c_1, \dots, c_s \in \mathbb{R}$ and $c_1a_1 + \cdots + c_sa_s = 0$.

Then

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = 0. \quad \text{So } \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \in \ker(A). \quad \text{So } \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

So $c_1 = 0, c_2 = 0, \dots, c_s = 0$.

So $\{a_1, \dots, a_s\}$ is linearly independent. □

PF6HS134. Prove the following proposition.

Proposition 10.5. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{R})$. Then

$$\text{im}(A) = \mathbb{R}\text{-span}\{\text{columns of } A\}.$$

Solution. *Proof.* Let $a_1, \dots, a_s$ be the columns of A . Then

$$\begin{aligned} \text{im}(A) &= \left\{ A \begin{pmatrix} c_1 \\ \vdots \\ c_s \end{pmatrix} \mid c_1, \dots, c_s \in \mathbb{R} \right\} \\ &= \{c_1 a_1 + \dots + c_s a_s \mid c_1, \dots, c_s \in \mathbb{R}\} \\ &= \text{span}\{a_1, \dots, a_s\} \\ &= \text{span}\{\text{columns of } A\}. \end{aligned}$$

□

PF7HS133. Prove the following proposition.

Proposition 10.6. *Let $A \in M_{t \times s}(\mathbb{Q})$. Then $\ker(A)$ is a subspace of $\mathbb{Q}^s$.*

Solution. *Proof.* (a) Since $A0 = 0$ then $0 \in \ker(A)$.

(b) Assume $w_1, w_2 \in \ker(A)$. Then $Aw_1 = 0$ and $Aw_2 = 0$. So

$$A(w_1 + w_2) = Aw_1 + Aw_2 = 0 + 0 = 0. \quad \text{So } w_1 + w_2 \in \ker(A).$$

(c) Assume $w \in \ker(A)$ and $c \in \mathbb{Q}$. Then $Aw = 0$ and

$$A(cw) = cAw = c0 = 0. \quad \text{So } cw \in \ker(A).$$

So $\ker(A)$ is a subspace of $\mathbb{Q}^s$.

□

PF8HS133. Prove the following proposition.

Proposition 10.7. *Let $A \in M_{t \times s}(\mathbb{Q})$. Then $\text{im}(A)$ is a subspace of $\mathbb{Q}^t$.*

Solution. *Proof.* (a) Since $0 = A0$ then $0 \in \text{im}(A)$.

(b) Assume $y_1, y_2 \in \text{im}(A)$. Then there exist $x_1, x_2 \in \mathbb{Q}^s$ such that $y_1 = Ax_1$ and $y_2 = Ax_2$. Then

$$y_1 + y_2 = Ax_1 + Ax_2 = A(x_1 + x_2). \quad \text{So } y_1 + y_2 \in \text{im}(A).$$

(c) Assume $y \in \text{im}(A)$ and $c \in \mathbb{Q}$. Then there exists $x \in \mathbb{Q}^s$ such that $y = Ax$. Then

$$cy = cAx = A(cx). \quad \text{So } cy \in \text{im}(A).$$

So $\text{im}(A)$ is a subspace of $\mathbb{Q}^t$.

□

PF9Example A5. Let $T: V \rightarrow W$ be an $\mathbb{R}$ -linear transformation.

Show that $\ker(T) = \{v \in V \mid T(v) = 0\}$ is a subspace of V .

Solution. *Proof.* Let $v_1, v_2 \in \ker(T)$. Then

$$T(v_1 + v_2) = T(v_1) + T(v_2) = 0 + 0 = 0. \quad \text{So } v_1 + v_2 \in \ker(T).$$

Subtracting $T(0)$ from each side of the equation $T(0) = T(0 + 0) = T(0) + T(0)$ gives

$$0 = T(0), \quad \text{and so } 0 \in \ker(T).$$

Let $v \in \ker(T)$ and let $c \in \mathbb{R}$. Then

$$T(cv) = cT(v) = c \cdot 0 = 0 \quad \text{and so} \quad cv \in \ker(T).$$

So $\ker(T)$ is a subspace of V . □

PF10Example A6. Let $T: V \rightarrow W$ be an $\mathbb{R}$ -linear transformation. Show that $\text{im}(T) = \{T(v) \mid v \in V\}$ is a subspace of W .

Solution. Subtracting $T(0)$ from each side of the equation $T(0) = T(0 + 0) = T(0) + T(0)$ gives

$$0 = T(0), \quad \text{and so} \quad 0 \in \text{im}(T).$$

Let $w_1, w_2 \in W$. Then there exist $v_1, v_2 \in V$ such that

$$T(v_1) = w_1 \quad \text{and} \quad T(v_2) = w_2.$$

Then $w_1 + w_2 = T(v_1) + T(v_2) = T(v_1 + v_2)$,

$$\text{and so} \quad w_1 + w_2 \in \text{im}(T).$$

Let $w \in W$ and let $c \in \mathbb{R}$. Then there exists $v \in V$ such that

$$T(v) = w.$$

Then $cw = cT(v) = T(cv)$

$$\text{and so} \quad cw \in \text{im}(T).$$

So $\text{im}(T)$ is a subspace of W . □

PF11HS133. Prove the following theorem.

Theorem 10.8. (Basis Minimax Theorem) Let V be an $\mathbb{F}$ -vector space and let B be a subset of V . The following are equivalent:

- (a) B is a basis of V .
- (b) B is a minimal spanning set of V .
- (c) B is a maximal linearly independent set of V .

Solution. Proof of the Minimax Basis Theorem

(a) $\Rightarrow$ (b): Assume $B = \{b_1, \dots, b_k\}$ is a basis of B .

To show: B is a minimal spanning set of V .

To show: (1) B is a spanning set.

(2) If $i \in \{1, \dots, k\}$ then $B - \{b_i\}$ is not a spanning set.

(1) Since B is a basis then B is a spanning set.

(2) To show: If $i \in \{1, \dots, k\}$ and $B - \{b_i\}$ is a spanning set then B is not a basis.

Assume $i \in \{1, \dots, k\}$ and $B - \{b_i\}$ is a spanning set.

Then there exist $c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_k \in \mathbb{R}$ such that

$$b_i = c_1 b_1 + \dots + c_{i-1} b_{i-1} + c_{i+1} b_{i+1} + \dots + c_k b_k.$$

Then

$$0 = c_1b_1 + \cdots + c_{i-1}b_{i-1} - b_i + c_{i+1}b_{i+1} + \cdots + c_kb_k.$$

So $\{b_1, \dots, b_k\}$ is not linearly independent.

So B is not a basis.

So if $i \in \{1, \dots, k\}$ then $B - \{b_i\}$ is not a spanning set.

(b) $\Rightarrow$ (c): Assume B is a minimal spanning set.

To show: B is a maximal linearly independent set in V .

To show: (1) B is a linearly independent set in V .

(2) If $v \in V$ then $B \cup \{v\}$ is not linearly independent.

(1) To show: If B is a spanning set and B is not linearly independent then B is not a minimal spanning set.

Assume B is a spanning set and B is not linearly independent.

Then there exist $c_1, \dots, c_k \in \mathbb{R}$ and $i \in \{1, \dots, k\}$ such that

$$c_1b_1 + \cdots + c_kb_k = 0 \quad \text{and} \quad c_i \neq 0.$$

Then $b_i = -c_i^{-1}(c_1b_1 + \cdots + c_{i-1}b_{i-1} + c_{i+1}b_{i+1} + \cdots + c_kb_k)$.

So $\text{span}(B - \{b_i\}) \supseteq \text{span}(b_1, \dots, b_k) = V$.

So $\text{span}(B - \{b_i\}) = V$ and B is not a minimal spanning set of B .

So if B is a minimal spanning set then B is linearly independent.

(2) To show: If $v \in V$ then $B \cup \{v\}$ is not linearly independent.

Assume $v \in V$. To show: $B \cup \{v\}$ is not linearly independent.

Since $\text{span}(B) = V$ then there exist $c_1, \dots, c_k \in \mathbb{R}$ such that

$$v = c_1b_1 + \cdots + c_kb_k.$$

So $0 = c_1b_1 + \cdots + c_kb_k - v$.

So $B \cup \{v\} = \{b_1, \dots, b_k, v\}$ is not linearly independent.

(c) $\Rightarrow$ (a): Assume B is a maximal linearly independent set.

To show: B is a basis.

To show: $\text{span}(B) = V$.

Assume $v \in V$. To show $v \in \text{span}(B)$.

Since B is a maximal linearly independent set then $B \cup \{v\}$ is not linearly independent.

So there exist $c_1, \dots, c_k, c_{k+1} \in \mathbb{R}$ and $i \in \{1, \dots, k+1\}$ such that

$$c_1b_1 + \cdots + c_kb_k + c_{k+1}v = 0 \quad \text{and} \quad c_i \neq 0.$$

The case $c_{k+1} = 0$ cannot occur since B is linearly independent.

So $c_{k+1} \neq 0$ and $v = -c_{k+1}^{-1}(c_1b_1 + \cdots + c_kb_k)$.

So $v \in \text{span}\{b_1, \dots, b_k\} = \text{span}(B)$.

So $V = \text{span}(B)$. So B is a basis of V . □

PF12HS134. Prove the following proposition.

Proposition 10.9. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{R})$. Let $a_1, \dots, a_s$ be the columns of A . Then

$$\text{im}(A) = \text{span}\{a_1, \dots, a_s\}.$$

Solution. *Proof.*

$$\begin{aligned} \text{im}(A) &= \{Ax \mid x \in \mathbb{R}^s\} = \left\{ \left(\begin{pmatrix} | & & | \\ a_1 & \cdots & a_s \\ | & & | \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_s \end{pmatrix} \mid x_1, \dots, x_s \in \mathbb{R} \right\} \\ &= \left\{ x_1 \begin{pmatrix} | \\ a_1 \\ | \end{pmatrix} + \cdots + x_s \begin{pmatrix} | \\ a_s \\ | \end{pmatrix} \mid x_1, \dots, x_s \in \mathbb{R} \right\} \\ &= \mathbb{R}\text{-span}\{\text{columns of } A\}. \end{aligned}$$

So $\text{im}(A)$ is the set of linear combinations of the columns of A . □

Pf13HS137. Prove the following theorem.

Theorem 10.10. (Invertible matrices are square) Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{R})$. Suppose there exists

$$P \in M_{s \times t}(\mathbb{R}) \quad \text{be such that} \quad PA = 1.$$

Suppose there exists

$$Q \in M_{s \times t}(\mathbb{R}) \quad \text{be such that} \quad AQ = 1.$$

Then

- (a) $\ker(A) = 0$.
- (b) $\text{im}(A) = \mathbb{R}^t$.
- (c) The set of columns of A is a basis of $\mathbb{Q}^t$.
- (d) $s = t$.
- (e) $P = Q$.

Solution. *Proof.* (a) To show: $\ker(A) = \{0\}$.

To show: (aa) $\{0\} \subseteq \ker(A)$.

(ab) $\ker(A) \subseteq \{0\}$.

(aa) Since $A \cdot 0 = 0$ then $0 \in \ker(A)$.

So $\{0\} \subseteq \ker(A)$.

(ab) To show: If $x \in \ker(A)$ then $x \in \{0\}$.

Assume $x \in \ker(A)$. To show: $x = 0$.

Since $x \in \ker(A)$ then

$$Ax = 0. \quad \text{So } PAx = P0 = 0.$$

So $x = 1x = PAx = 0$. So $\ker(A) \subseteq \{0\}$.

So $\ker(A) = \{0\}$.

(b) To show: $\text{im}(A) = \mathbb{R}^t$.

To show: (ba) $\text{im}(A) \subseteq \mathbb{R}^t$.

(bb) $\mathbb{R}^t \subseteq \text{im}(A)$.

(ba) By definition of $\text{im}(A) = \{Ax \mid x \in \mathbb{R}^s\}$.

Since A is a $t \times s$ matrix then $\text{im}(A) \subseteq \mathbb{R}^t$.

(bb) To show: If $v \in \mathbb{R}^t$ then $v \in \text{im}(A)$.

Assume $v \in \mathbb{R}^t$. To show: $v \in \text{im}(A)$.

$$v = 1v = AQv \in \{Ax \mid x \in \mathbb{R}^t\} = \text{im}(A).$$

So $v \in \text{im}(A)$. So $\mathbb{R}^t \subseteq \text{im}(A)$.

So $\mathbb{R}^t = \text{im}(A)$.

(c) Since $\ker(A) = 0$ then

the columns of A are linearly independent.

Since $\text{im}(A) = \text{span}\{\text{columns of } A\}$ and $\mathbb{R}^t = \text{im}(A)$ then

$$\mathbb{R}^t = \text{span}\{\text{columns of } A\}.$$

So $\{\text{columns of } A\}$ is a basis of $\mathbb{R}^t$.

(d) Let $a_1, \dots, a_s$ be the columns of A . By part (c),

$$\{a_1, \dots, a_s\} \text{ is a basis of } \mathbb{R}^t.$$

Let e_i be the $t \times 1$ matrix with 1 in the i th entry and 0 elsewhere. Then

$$\{e_1, \dots, e_t\} \text{ is a basis of } \mathbb{R}^t.$$

By the Dimension Theorem, any two bases of $\mathbb{R}^t$ have the same number of elements.

So $s = t$.

(e) To show: $P = Q$.

$$P = P \cdot 1 = P(AQ) = (PA)Q = 1 \cdot Q = Q. \quad \square$$