Linear Algebra Done Right

Jiuru Lyu

May 30, 2023

Contents

1 Vector Spaces

1.1 $\mathbb{R}^n$ and $\mathbb{C}^n$

Definition 1.1.1 (Complex Number). A *complex number* is an ordered pair (a, b), where $a, b \in \mathbb{R}$, but we write it as $a + b\mathrm{i}$.

Notation 1.1 $\mathbb{C} \coloneqq \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\}$

Definition 1.1.2 (Addition & Multiplication).

$$(a + b\mathrm{i}) + (c + d\mathrm{i}) = (a + c) + (b + d)]\mathrm{i}$$

$$(a + b\mathrm{i})(c + d\mathrm{i}) = (ac - bd) + (ad + bc)\mathrm{i}$$

Theorem 1.1.1 Properties of Complex Arithmetic

1. commutativity: $\alpha + \beta = \beta + \alpha; \quad \alpha\beta = \beta\alpha, \quad \forall \alpha, \beta \in \mathbb{C}$.
2. associativity: $(\alpha + \beta) + \lambda = \alpha + (\beta + \lambda); \quad (\alpha\beta)\lambda = \alpha(\beta\lambda), \quad \forall \alpha, \beta, \lambda \in \mathbb{C}$.
3. identities: $\lambda + 0 = \lambda; \quad \lambda \cdot 1 = \lambda, \forall \lambda \in \mathbb{C}$.
4. additive inverse: $\forall \alpha \in \mathbb{C}, \exists$ unique $\beta \in \mathbb{C}$ *s.t.* $\alpha + \beta = 0$.
5. multiplicative inverse: $\forall \alpha \in \mathbb{C}, \alpha \neq 0, \exists$ unique $\beta \in \mathbb{C}$ *s.t.* $\alpha\beta = 1$.
6. distributivity: $\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta, \quad \forall \lambda, \alpha, \beta \in \mathbb{C}$.

Definition 1.1.3 (Subtraction). If $-\alpha$ is the additive inverse of α, *subtraction* on $\mathbb{C}$ is defined by

$$\beta - \alpha = \beta + (-\alpha).$$

Definition 1.1.4 (Division). For $\alpha \neq 0$, let $\dfrac{1}{\alpha}$ denote the multiplicative inverse of α. Then, *division* on $\mathbb{C}$ is defined by

$$\frac{\beta}{\alpha} = \beta \cdot \left(\frac{1}{\alpha}\right)$$

Notation 1.2 $\mathbb{F}$ *is either* $\mathbb{R}$ *or* $\mathbb{C}$.

Definition 1.1.5 (List/Tuple). Suppose n is a non-negative integer. A list of length n is an ordered collection of n elements separated by commas and surrounded by parentheses: $(x_1, x_2, x_3, \cdots, x_n)$. Two lists are equal if and only if they have the same length and the same elements in the same order.

Remark *Lists must have a FINITE length.*

Definition 1.1.6 ($\mathbb{F}^n$ and Coordinate). $\mathbb{F}^n$ is the set of all lists of length n of elements of $\mathbb{F}$:

$$\mathbb{F}^n \coloneqq \{(x_1, \cdots, x_n) \mid x_i \in \mathbb{R} \forall i = 1, \cdots, n\},$$

where x_i is the i^{th} *coordinate* of $(x_1, \cdots, x_n)$.
Example 1.1.1 $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ and $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$.
Definition 1.1.7 (Addition on $\mathbb{F}^n$). *Addition* on $\mathbb{F}^n$ is defined by adding corresponding coordinates:

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n).$$

Theorem 1.1.2 Commutativity of Addition on $\mathbb{F}^n$
If $x, y \in \mathbb{F}^n$, then $x + y = y + x$.

Proof 1. Suppose $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. Then

$$\begin{aligned} x + y &= (x_1 + y_1, \cdots, x_n + y_n) \\ &= (y_1 + x_1, \cdots, y_n + x_n) = y + x. \end{aligned}$$

■

Definition 1.1.8 (Zero). Let 0 denote the list of length n whose coordinates are all 0: $0 \coloneqq (0, \cdots, 0)$.
Definition 1.1.9 (Additive Inverse on $\mathbb{F}^n$). For $x \in \mathbb{F}^n$, the additive inverse of x, denoted $-x$, is the vector $-x \in \mathbb{F}^n$ *s.t.* $x + (-x) = 0$.
Definition 1.1.10 (Scalar Multiplication in $\mathbb{F}^n$). The product of a number $\lambda \in \mathbb{F}$ and a vector $x \in \mathbb{F}^n$ is computed by multiplying each coordinate of the vector by λ :

$$\lambda x = \lambda(x_1, \cdots, x_n) = (\lambda x_1, \cdots, \lambda x_n),$$

where $x = (x_1, \cdots, x_n) \in \mathbb{F}^n$.

Theorem 1.1.3 Properties of Arithmetic Operations on $\mathbb{F}^n$

1. $(x + y) + z = x + (y + z) \quad \forall x, y, z \in \mathbb{F}^n$
2. $(ab)x = a(bx) \quad \forall x \in \mathbb{F}^n$ and $\forall a, b \in \mathbb{F}$.
3. $1 \cdot x = x \quad \forall x \in \mathbb{F}^n$ and $1 \in \mathbb{F}$.
4. $\lambda(x + y) = \lambda x + \lambda y \quad \forall \lambda \in \mathbb{R}$ and $\forall x, y \in \mathbb{F}^n$.
5. $(a + b)x = ax + bx \quad \forall a, b \in \mathbb{F}$ and $\forall x \in \mathbb{F}^n$.

1.2 Definition of Vector Space

Definition 1.2.1 (Addition on V). An *addition* on V is a function $(u, v) \mapsto u + v$ for all $u, v \in V$.
Definition 1.2.2 (Scalar Multiplication on V). A *scalar multiplication* on V is a function $(\lambda, v) \mapsto \lambda v$ for all $\lambda \in \mathbb{F}$ and $v \in V$.
Definition 1.2.3 (Vector Space). A *vector space* is a set V along with an addition on V and a scalar multiplication *s.t.* the following properties hold:

1. commutativity: $u + v = v + u \quad \forall u, v \in V$
2. associativity: $(u + v) + w = u + (v + w)$ and $(ab)v = a(bv) \quad \forall u, v, w \in V$ and $\forall a, b \in \mathbb{F}$.
3. additive identity: $\exists 0 \in V$ *s.t.* $v + 0 = v \quad \forall v \in V$.
4. additive inverse: $\exists w \in V$ *s.t.* $v + w = 0 \quad \forall v \in V$.
5. multiplicative identity: $\exists 1 \in V$ *s.t.* $1 \cdot v = v \quad \forall v \in V$.
6. distributive properties: $a(u + v) = au + av$ and $(a + b)v = av + bv \quad \forall u, v \in V$ and $a, b \in \mathbb{F}$.

Definition 1.2.4 (Vector). Elements of a vector space are called *vectors* or points.

Notation 1.3 *V is a vector space over $\mathbb{F}$.*

Definition 1.2.5 (Real and Complex Vector Space). A vector space over $\mathbb{R}$ is called a *real vector space*, and a vector space over $\mathbb{C}$ is called a *complex vector space*.

Theorem 1.2.1 Unique Additive Identity of Vector Spaces
A vector space has a unique additive identity.

Proof 1. Suppose 0 and $0'$ are both additive identities for some vector space V. So,

$$\begin{aligned} 0' &= 0' + 0 && \textit{Since } 0 \textit{ is an additive identity} \\ &= 0 + 0' && \textit{commutativity} \\ &= 0. && \textit{Since } 0' \textit{ is an additive identity} \end{aligned}$$

Then, $0' = 0$. ■

Theorem 1.2.2 Unique Additive Inverse of Vector Spaces
A vector in a vector space has a unique additive inverse.

Proof 2. Let V be a vector space. Suppose w and w' are additive inverses of v for some $v \in V$. Note that

$$\begin{aligned} w &= w + 0 \\ &= w + (v + w') \\ &= (w + v) + w \\ &= 0 + w' = w'. \end{aligned}$$

■

Notation 1.4 *Let $v, w \in V$. Then, $-v$ denotes the additive inverse of v.*

Definition 1.2.6 (Subtraction). $w - v$ is defined to be $w + (-v)$.

Theorem 1.2.3
$0 \cdot v = 0 \quad \forall v \in V.$

Proof 3. Since $v \in V$, we know

$$\begin{aligned} 0 \cdot v &= (0+0)v = 0 \cdot v + 0 \cdot v \\ 0 \cdot v + (-0 \cdot v) &= 0 \cdot +0 \cdot +(-0 \cdot v) \\ 0 &= 0 \cdot v \end{aligned}$$

■

Theorem 1.2.4
$a \cdot 0 = 0 \quad \forall a \in \mathbb{F}.$

Proof 4. For $a \in \mathbb{F}$, we have

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0) = a \cdot 0 + a \cdot 0 \\ a \cdot 0 + (-a \cdot 0) &= a \cdot 0 + a \cdot 0 + (-a \cdot 0) \\ 0 &= a \cdot 0. \end{aligned}$$

■

Theorem 1.2.5
$(-1)v = -v \quad \forall v \in V.$

Proof 5. For $v \in V$, we have

$$v + (-1)v = 1 \cdot v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0.$$

Therefore, by definition, $(-1)v = -v$. ■

Notation 1.5 $\mathbb{F}^S$

1. *If S is a set, then $\mathbb{F}^S$ denotes the set of functions from S to $\mathbb{F}$.*
2. *For $f, g \in \mathbb{F}^S$, the sum $f + g \in \mathbb{F}^S$ is the function defined by $(f+g)(x) = f(x) + g(x) \quad \forall x \in S$.*
3. *For $\lambda \in \mathbb{F}$ and $f \in \mathbb{F}^S$, the product $\lambda f \in \mathbb{F}^S$ is the function defined by $(\lambda f)(x) = \lambda f(x) \quad \forall x \in S$.*

Theorem 1.2.6
$\mathbb{F}^S$ is a vector space.

1.3 Subspace

Definition 1.3.1 (Subspace). A subset U of V is called a *subspace* of V if U is also a vector space using the same addition and scalar multiplication as on V.

Theorem 1.3.1 Conditions for a Subspace

A subset U of V is a subspace of V if and only if U satisfies the following conditions:

1. additive identity: $0 \in U$;
2. closed under addition: $u, w \in U \implies u + w \in U$;
3. closed under scalar multiplication: $a \in \mathbb{F}$ and $u \in U \implies au \in U$.

Proof 1.

($\Rightarrow$) Suppose U is a subspace of V. By definition, U is then a vector space, and so those conditions are automatically satisfied. $\square$

($\Leftarrow$) Suppose U satisfies the three conditions. Since U is a subset of V, U automatically has *associativity, commutativity, multiplicative identity,* and *distributivity.* So, we want to check U has additive inverse and additive identities.

For additive identity, we know $0 \in U$, by assumption.

For additive inverse, by condition #3, we know $-u = (-1)u \in U$.

Then, U is a vector space. $\blacksquare$

Example 1.3.1 If $b \in \mathbb{F}$, then $\left\{(x_1, x_2, x_3, x_4) \in \mathbb{F}^4 \mid x_3 = 5x_4 + b\right\}$ is a subspace of $\mathbb{F}^4$ if and only if $b = 0$.

Proof 2.

($\Rightarrow$) Suppose $U = \left\{(x_1, x_2, x_3, x_4) \in \mathbb{F}^4 \mid x_3 = 5x_4 + b\right\}$ is a subspace of $\mathbb{F}^4$. Then, $0 = (0, 0, 0, 0) \in U$. So, $0 = 5 \cdot 0 + b$, or $b = 0$. $\square$

($\Leftarrow$) Suppose $b = 0$. Then, $x_3 = 5x_4$. So, $U = \left\{(x_1, x_2, 5x_4, x_4) \in \mathbb{F}^4\right\}$

① $0 = (0, 0, 0, 0) \in U$

② Note that

$$(x_1, x_2, 5x_4, x_4) + (y_1, y_2, 5y_4, y_4) = (x_1 + y_1, x_2 + y_2, 5(x_4 + y_4), x_4 + y_4) \in U$$

So, addition is closed under U.

③ $\forall a \in \mathbb{F}$, we have

$$a(x_1, x_2, 5x_4, x_4) = (ax_1, ax_2, 5(ax_4), ax_4) \in U$$

Then, U is a subspace of $\mathbb{F}^4$.

$\blacksquare$

Example 1.3.2 The set of continuous real-valued functions on interval $[0, 1]$ is a subspace of $\mathbb{R}^{[0,1]}$.

Proof 3.

1. 0 (zero mapping)$\in U$
2. Set f and $g \in \mathcal{C}[0, 1]$, the set of continuous functions on interval $[0, 1]$. Then, $f + g \in \mathcal{C}[0, 1]$.

3. From Calculus, we know that $\forall a \in \mathbb{F}, \quad af \in \mathcal{C}[0,1]$.

■

Definition 1.3.2 (Sum of Subspaces). Suppose $U_1, \cdots, U_m$ are subspaces of V. The *sum* of $U_1, \cdots, U_m$, denoted as $U_1 + \cdots + U_m$, is the set of all possible sums of elements of $U_1, \cdots, U_m$:

$$U_1 + \cdots + U_m = \{u_1 + \cdots + u_m \mid u_i \in U_i \quad \forall i = 1, \cdots, m\}.$$

Example 1.3.3 Suppose $U = \{(x,0,0) \in \mathbb{F}^3 \mid x \in \mathbb{F}\}$ and $W = \{(0,y,0) \in \mathbb{F}^3 \mid y \in \mathbb{F}\}$, then

$$U + W = \{(x,y,0) \in \mathbb{F}^3 \mid x, y \in \mathbb{F}\}.$$

Theorem 1.3.2
Suppose $U_1, \cdots, U_m$ are subspaces of V. Then, $U_1 + \cdots + U_m$ is the *smallest subspace* of V containing $U_1, \cdots, U_m$.

Proof 4. Suppose $U_1, \cdots, U_m$ are subspaces of U. Let $U_1 + \cdots + U_m = \{u_1 + \cdots + u_m \mid u_j \in U_j, j = 1, \cdots m\}$. Suppose $w_j \in U_j$, then $w_1 + \cdots + w_m \in U_1 + \cdots + U_m$.

1. $U_1 + \cdots + U_m$ is a subspace of V.
   (a) Note that
   $$(u_1 + \cdots + u_m) + (w_1 + \cdots + w_m) = (u_1 + w_1) + \cdots + (u_m + w_m) \in U_1 + \cdots + U_m,$$
   so $U_1 + \cdots + U_m$ is closed under addition.
   (b) Similarly, $U_1 + \cdots + U_m$ is closed under scalar multiplication.
   (c) Note that U_j is a subspace, so $0 \in U_j$. Hence, $(0, \cdots, 0) = 0 \in U_1 + \cdots + U_m$

   Therefore, we've proven $U_1 + \cdots + U_m$ is a subspace of V. □

2. Now, we want to show this subspace is the smallest subspace containing $U_1, \cdots, U_m$. That is, we want to show $\forall\, W \supseteq U_1 \cup \cdots \cup U_m$, we have $W \supseteq U_1 + \cdots + U_m$.

   Note that $U_j \subseteq U_1 + \cdots + U_m$, so we have $(U_1 \cup U_2 \cup \cdots \cup U_m) \subseteq U_1 + \cdots + U_m$. This means $U_1 + \cdots + U_m$ must contain $U_1, \cdots, U_m$. Let W be some subspace containing $U_1, \cdots, U_m$. Then, for $j = 1, \cdots, m$, we have $u_j \in U_j$, which indicates $u_j \in W$. Therefore, $u_1 + \cdots + u_m \in V$ and thus $U_1 + \cdots + U_m \subseteq W$.

   Since W was arbitrary, we've shown $\forall\, W$ that contains $U_1, \cdots, U_m$, $U_1 + \cdots + U_m \subseteq W$. Therefore, $U_1 + \cdots + U_m$ is the smallest.

■

Definition 1.3.3 (Direct Sum). Suppose $U_1, \cdots, U_m$ are subspaces of V. $U_1 + \cdots + U_m$ is called a *direct sum* if each element of $U_1 + \cdots + U_m$ can be written in only one way as a sum $u_1 + \cdots + u_m$, where $u_j \in U_j$.

Notation 1.6 *If $U_1 + \cdots + U_m$ is a direct sum, then we use $U_1 \oplus \cdots \oplus U_m$ to denote it.*

Example 1.3.4 Let $U = \{(x, y, 0) \in \mathbb{F}^3 \mid x, y \in \mathbb{F}\}$ and $W = \{(0, 0, z) \in \mathbb{F}^3 \mid z \in \mathbb{F}\}$. Then, $\mathbb{F}^3 = U \oplus W$.
Proof 5. Note that $U + W = \{(x, y, z) \mid x, y, z \in \mathbb{F}\} = \mathbb{F}^3$. Suppose ①: $(x, y, z) = (x, y, 0) + (0, 0, z)$, for some $x, y, z \in \mathbb{F}$ and ②: $(x, y, z) = (x', y', 0) + (0, 0, z')$ for some $x', y', z' \in \mathbb{F}$. Then, ①−②:

$$(0, 0, 0) = (x - x', y - y', 0) + (0, 0, z - z') = (x - x', y - y', z - z').$$

Then, $x - x' = y - y' = z - z' = 0$, which indicates $x = x',\ y = y',\ z = z'$. So, by definition $U + W$ is a direct sum, or $\mathbb{F}^3 = U \oplus W$. ∎

Example 1.3.5 Suppose U_j is the subspace of $\mathbb{F}^n$ *s.t.*

$$\begin{aligned} U_1 &= \{x, 0, 0, \cdots, 0 \mid x \in \mathbb{F}\} \\ U_2 &= \{0, x, 0, \cdots, 0 \mid x \in \mathbb{F}\} \\ &\vdots \\ U_n &= \{0, 0, 0, \cdots, x \mid x \in \mathbb{F}\} \end{aligned}$$

Then, $\mathbb{F}^n = U_1 \oplus U_2 \oplus \cdots \oplus U_n$.
Proof 6. Note that $\mathbb{F}^n = U_1 + U_2 + \cdots + U_n$ is evident. Now, we'll prove that $U_1 + U_2 + \cdots + U_n$ is a direct sum. Consider $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}^n$. Assume that

$$\begin{aligned} & x = (x_1, 0, \cdots, 0) + \cdots + (0, \cdots, 0, x_n) && ① \\ \text{and} \quad & x = (x_1', 0, \cdots, 0) + \cdots + (0, \cdots, 0, x_n') && ② \end{aligned}$$

Then, from ①-②, we know that

$$0 = (x_1 - x_1', \cdots, x_n - x_n') = (0, 0, \cdots, 0).$$

Then, $\forall i = 1, \cdots, n$ we have $x_i - x_i' = 0$, or $x_i = x_i'$. Therefore, by definition, we know $U_1 + \cdots + U_n$ is a direct sum. ∎

Example 1.3.6 Let

$$\begin{aligned} U_1 &= \{(x, y, 0) \mid x, y \in \mathbb{F}\} \\ U_2 &= \{(0, 0, z) \mid z \in \mathbb{F}\} \\ U_3 &= \{(0, y, y) \mid y \in \mathbb{F}\} \end{aligned}$$

Show that $U_1 + U_2 + U_3$ is not a direct sum.
Proof 7. Consider $(0, 0, 0) \in \mathbb{F}^3$. Note that

$$(0, 0, 0) = (0, 0, 0) + (0, 0, 0) + (0, 0, 0)$$

and

$$(0, 0, 0) = (0, 1, 0) + (0, 0, 1) + (0, -1, -1).$$

Then, $U_1 + U_2 + U_3$ is not a direct sum by definition. ∎

Theorem 1.3.3
Suppose $U_1, \cdots, U_m$ are subspaces of V. Then,$U_1 + \cdots + U_m$ is a direct sum if and only if the only way to write 0 as a sum $u_1 + \cdots + u_m$ is by taking each $u_j = 0$.

Proof 8.

($\Rightarrow$) Since $U_1 + \cdots + U_m$ is a direct sum, by definition, the only way to write $0 \in \mathbb{F}^n$ is to write it as

$$0 = 0 + \cdots + 0 \qquad \text{where } 0 \in U_i \forall i = 1, \cdots, m. \qquad \square$$

($\Leftarrow$) Suppose the only way to write 0 as a sum $u_1 + \cdots + u_m$ is by taking each $u_j = 0$. Assume that for some $v \in V$, we have

$$\begin{aligned} v &= u_1 + \cdots + u_m, \quad u_j \in U_j \qquad ① \\ \text{and} \quad v &= u_1' + \cdots + u_m', \quad u_j' \in U_j \qquad ②. \end{aligned}$$

Then, by ①-②, and according to the conclusion from Example 1.3.6, we have

$$0 = (u_1 - u_1') + \cdots + (u_m - u_m') = 0 + \cdots + 0.$$

So, $\forall i \in 1, \cdots, m$, we have $u_i - u_i' = 0$. that is, $u_i = u_i'$. So, $\forall v \in V$, there is only one way to write v as a sum of $u_1 + \cdots_u + m$. Therefore, by definition, $U_1 + \cdots + U_m$ is a direct sum. ■

Theorem 1.3.4

Suppose U amd W are subspaces of V. Then, $U + W$ is a direct sum if and only if $U \cap W = \{0\}$.

Proof 9.

($\Rightarrow$) Suppose $U + W$ is a direct sum. Assume $v \in U \cap W$. Then, $v \in U$ and $v \in W$. By definition of subspace, we know $-v \in W$ as well. Note that

$$0 = v + (-v) \in U \cap W.$$

Then, by Theorem 1.3.4, we know that the only representation of $0 \in U \cap W$ is $0 = 0 + 0$ since $U \cap W$ is a direct sum. Hence, it must be that $v = -v = 0$, and thus $U \cap W = \{0\}$. $\square$

($\Leftarrow$) Suppose $U \cap W = \{0\}$. Let $u \in U$ and $w \in W$ *s.t.* $u + w = 0$. Then, we have $u = -w$. Since $-w \in W$, we know $u = -w \in W$. By $u \in U$ and $u \in W$, we know that $u \in U \cap W = \{0\}$. Therefore, $0 = 0 + 0$ is the only to represent $0 \in U + W$. By Theorem 1.3.4, we know $U + W$ is a direct sum. ■

Remark *When extending Theorem 1.3.4 to 3 subspaces $U_1, U+2, U+3$, we cannot conclude $U_1 \oplus U_2 \oplus U_3$ if we have $U_1 \cap U_2 = U_1 \cap U_3 = U_2 \cap U_3 = \{0\}$. See Example 1.3.6 as a counter example.*

2 Finite-Dimensional Vector Spaces

2.1 Span and Linear Independence

Notation 2.1 *We usually write list of vectors without using parentheses.*

Example 2.1.1 $(4,1,6),(9,5,7)$ is a list of vectors of length 2 in $\mathbb{R}^3$.
Definition 2.1.1 (Linear Combination). A *linear combination* of a list $v_1,\cdots,v_m$ of vectors in V is a vector of the form

$$a_1v_1+\cdots+a_mv_m,$$

where $a_1,\cdots,a_m\in\mathbb{F}$.
Example 2.1.2 Since $(17,-4,2)=6(2,1,-3)+5(1,-2,4)$, we say $(17,-4,2)$ is a linear combination of $(2,1,-3),(1,-2,4)$.
Definition 2.1.2 (Span).

$$\operatorname{span}(v_1,\cdots,v_m)=\{a_1v_1+\cdots+a_mv_m \mid a_1\cdots a_m\in\mathbb{F}\}.$$

Example 2.1.3 Consider $\operatorname{span}(e_1,e_2,e_3)$:

$$\begin{aligned}\operatorname{span}(e_1,e_2,e_3)&=\{a_1e_1+a_2e_2+a_3e_3 \mid a_1,a_2,a_3\in\mathbb{F}\}\\&=\{(a_1,a_2,a_3)\mid a_1,a_2,a_3\in\mathbb{F}\}=\mathbb{R}^3.\end{aligned}$$

Theorem 2.1.1
The span of a list of vectors in V is the smallest subspace of V containing all the vectors in the list.

Proof 1. To prove this theorem, we will prove two parts: span is a subspace and span is the smallest subspace.

1. Span is a subspace of V.

   (a) By definition of span, we know $\operatorname{span}(v_1,\cdots,v_m)=\{a_1v_1+\cdots+a_mv_m \mid a_1,\cdots,a_m\in\mathbb{F}\}$. If we set $a_1,\cdots,a_m=0$, then we have $0=0v_1+\cdots+0v_m$. So, $0\in\operatorname{span}v_1,\cdots,v_m$.

   (b) Let $a_1v_1+\cdots+a_mv_m\in\operatorname{span}(v_1,\cdots,v_m)$ and $b_1v_1+\cdots+b_mv_m\in\operatorname{span}(v_1,\cdots,v_m)$. Then,

   $$(a_1v_1+\cdots+a_mv_m)+(b_1v_1+\cdots+b_mv_m)=(a_1+b_1)v_1+\cdots+(a_m+b_m)v_m.$$

   Since $(a_1+b_1),\cdots,(a_m+b_m)\in\mathbb{F}$, we know $(a_1+b_1)v_1+\cdots+(a_m+b_m)v_m\in\operatorname{span}(v_1,\cdots,v_m)$.

   (c) Let $\lambda\in\mathbb{F}$ and $a_1v_1+\cdots+a_mv_m\in\operatorname{span}(v_1,\cdots,v_m)$. Then,

   $$\lambda(a_1v_1+\cdots+a_mv_m)=\lambda a_1v_1+\cdots+\lambda a_mv_m.$$

   Since $\lambda a_1,\cdots,\lambda a_m\in\mathbb{F}$, we know that $\lambda(a_1v_1+\cdots+a_mv_m)\in\operatorname{span}(v_1,\cdots,v_m)$.

   Therefore, we have proven that span is a subspace of V. $\square$

2. Now, we want to show that span is the smallest subspace.

Let U be a subspace of V containing $v_1, \cdots, v_m$. If we can show that $\operatorname{span}(v_1, \cdots, v_m) \subseteq U$, we then know span is the smallest subspace containing $v_1, \cdots, v_m$. Since U is a subspace containing $v_1, \cdots, v_m$, it is closed under addition and scalar multiplication. So, $a_1v_1 + \cdots + a_mv_m \in \operatorname{span}(v_1, \cdots, v_m)$. Therefore, $\operatorname{span}(v_1, \cdots, v_m) \subseteq U$.

■

Definition 2.1.3 (Span as a Verb). If $\operatorname{span}(v_1, \cdots, v_m) = V$, we say $v_1, \cdots, v_m$ *spans* V.
Definition 2.1.4 (Finite-Dimensional Vector Space). A vector space V is called *finite-dimensional* if $\exists$ a list of vectors, say $v_1, \cdots, v_m$ *s.t.* $\operatorname{span}(v_1, \cdots, v_m) = V$. In the following of this notes, we will use $\mathrm{F.D.}$ as a shortcut for saying "finite-dimensional."
Definition 2.1.5 (Infinte-Dimensional Vector Space). A vector space V is infinite-dimensional if it is not $\mathrm{F.D.}$. This is equivalent to say that $\forall$ lists of vectors in V, they do not span V.
Definition 2.1.6 (Polynomial Functions). A function $p : \mathbb{F} \to \mathbb{F}$ is called a *polynomial* with coefficients in $\mathbb{F}$ if $\exists\, a_0, \cdots, a_m \in \mathbb{F}$ *s.t.* $p(z) = a_0 + a_1z + a_2z^2 + \cdots + a_mz^m \quad \forall z \in \mathbb{F}$.

Notation 2.2 *We use $\mathcal{P}(\mathbb{F})$ to denote the set of all polynomial with coefficients in $\mathbb{F}$.*

Theorem 2.1.2
$\mathcal{P}(\mathbb{F})$ is a vector space over $\mathbb{F}$.

Proof 2. Recall the definition of $\mathbb{F}^{\mathbb{F}}$. We will show $\mathcal{P}(\mathbb{F})$ is a subspace of $\mathbb{F}^{\mathbb{F}}$.

1. $0 = 0 + 0z + \cdots + 0z^m \in \mathcal{P}(\mathbb{F})$.
2. Suppose $p(z) = a_mz^m + \cdots + a_1z + a_0$ and $q(z) = b_nz^n + \cdots + b_1z + b_0 \in \mathcal{P}(\mathbb{F})$. WLOG, suppose $m > n$, then we have $p(z) + q(z) = a_mz^m + \cdots + (a_n + b_n)z^n + \cdots + (a_0 + b_0) \in \mathcal{P}(\mathbb{F})$.
3. Suppose $\lambda \in \mathbb{F}$. Then, $\lambda p(z) = \lambda(a_mz^m + \cdots + a_1z + a_0) = \lambda a_mz^m + \cdots + \lambda a_0 \in \mathcal{P}(\mathbb{F})$.

Hence, we've shown $\mathcal{P}(\mathbb{F})$ is a subspace over $\mathbb{F}$. ■
Definition 2.1.7 (Degree of a Polynomial). A polynomial $p \in \mathcal{P}(\mathbb{F})$ is said to have *degree* m if $\exists$ scalars $a_0, \cdots, a_m \in \mathbb{F}$ with $a_m \neq 0$ *s.t.* $p(z) = a_mz^m + \cdots + a_1z + a_0 \quad \forall z \in \mathbb{F}$. We write $\deg p = m$. Specially, $\deg 0 \coloneqq -\infty$ and $\deg a_0 \coloneqq 0$ when $a_0 \neq 0$.

2.2 Bases

2.3 Dimension