MATH405: Linear Algebra

Michael Li

Contents

1 Vector Space

Goals of this course is to discuss

- Vector spaces
- Linear transformations between vector spaces
- Other operations on vector spaces

1.1 Definitions

Definition - Field: A set of numbers containing $0, 1$ that can be added, subtracted, multiplied, and divided (except cannot divide by 0) that satisfy the following **Field Axioms**

1. $a, b \in K \implies a + b, ab \in K$
2. $+, \times$ are commutative so $a + b = b + a$ and $ab = ba$
3. $+, \times$ are associative so $(a + b) + c = a + (b + c)$ and $a(bc) = (ab)c$
4. Distributive Law: $a(b + c) = ab + ac$
5. Additive Identity: $a + 0 = 0 + a = a$
6. Multiplicative Identity: $a \cdot 1 = 1 \cdot a = a$
7. Additive Inverse: $\forall a \in K, \exists b$ such that $a + b = 0$, namely $b = -a$ which is unique
8. Multiplicative Inverse: $\forall a \in K, \exists b$ such that $ab = 1$, name $b = 1/a$ which is unique

- **Example**: R, Q are fields. Z is not a field since there is no multiplicative inverse of 2

Example: $C = \{a + bi \mid a, b \in R\}$, where $i = \sqrt{-1}$ is a field under

- $+ : (a + bi) + (c + di) = (a + c) + (b + d)i$
- $\times : (a + bi)(c + di) = (ac - bd) + (ad + bc)i$

Example: $F_2 = \{0, 1\}$ is a field under

- $+$: where

  $0 + 0 = 0$

  $0 + 1 = 1 + 0 = 1$

  $1 + 1 = 0$

- $\times$: where

  $0 \cdot 0 = 0$

  $0 \cdot 1 = 1 \cdot 0 = 0$

  $1 \cdot 1 = 1$

Example: For a prime p, let $F_p = \{0, \ldots, p - 1\}$. Then F_p is a field under

- $+ : a + b \pmod{p}$
- $\times : ab \pmod{p}$

Definition - Vector Space: For an arbitrary field K, a K-vector space is a set V with a distinguished element O such that any 2 elements in V can be added and scalar multiplied by $c \in K$

- $u, v \in V \implies u + v \in V$
- $c \in K, u \in V \implies cu \in V$

Satisfying the following properties

1. Commutative Addition: $u + v = v + u$
2. Associative Addition: $(u + v) + w = u + (v + w)$
3. Additive Identity: $u + O = u$

4. Additive Inverse: $\forall u \in V, \exists v \in V$ such that $u + v = O$, namely $v = -u$ which is unique
5. Distributive Laws: $\forall a, b \in K, a(u + v) = au + av$ and $(a + b)u = au + bu$
6. Commutative Scalar Multiplication: $(ab)u = a(bu)$
7. Multiplicative Identity: $1 \cdot u = u$

Example: R^3 is an R-vector space defined by the operations

$$R^3 = \{(x, y, z) \mid x, y, z \in R\}$$

- $+$: add componentwise so $(a, b, c) + (d, e, f) = (a + d, b + e, c + f)$
- Scalar $\times$: for $r \in R$, $r(a, b, c) = (ra, rb, rc)$
- Additive Identity is $O = (0, 0, 0)$

Example: For any field K, K^2 is a K-vector space defined by the oepartions

$$K^2 = \{(x, y) \mid x, y \in K\}$$

- $+$: add componentwise so $(a, b) + (c, d) = (a + c, b + d)$
- Scalar $\times$: for $k \in K$, $k(a, b) = (ka, kb)$
- Additive Identity is $O = (0, 0)$

Example: R is an R-vector space since clearly the properties hold

Example R is a Q-vector space since clearly the properties hold

- Notably, for $q \in Q$ and $r \in R$, we have $qr \in R$. Thus scalar multiplication is closed

Example: For any field K, the set $\{O\}$ is a K-vector space

Example: Let X be any non-empty set and let $\mathcal{F}(X)$ be the set of all functions $f : X \to R$. Then $\mathcal{F}$ is an R-vector space under the operations

- $+$: for $f, g \in \mathcal{F}(X)$, define $f + g := (f + g)(x)$
- Scalar $\times$: let $r \in R$, then define $rf := r(f(x))$
- Additive Identity is $O = f(x) = 0$, the function that takes any x to 0

Example: Take $X = N$ and let $F(X) = \{$ all functions $f : N \to R\}$ is a vector space

- **Note**: $f : N \to R$ is a sequence $(a_0, \ldots, a_n)$ where $a_n = f(n)$

Lemma 1 - Cancellation: For $u, v, w \in V$ and if $u + v = w + v$, then $u = w$

Proof: $v \in V$ has an additive inverse, namely $-v$. Thus we have

$$u + v - v = w + v - v \implies u = w$$

Lemma 2 - Unique Additive Inverse: For all $v \in V$, there is a unique additive inverse, namely $-v$

Proof: Suppose u, w are both additive inverses of v. Then we have

$$v + u = v + w \implies u = w$$

Lemma 3 - 0 Times a Vector: For all $v \in V$, $0v = O$

Proof: $v = 1v = (0+1)v = 0v + 1v = 0v + v \implies 0v = O$

Lemma 4 - (-1)v is the Additive Inverse: For all $v \in v, (-1)v$ is the unique additive inverse of v

Proof: $(-1)v + v = (-1+1)v = 0v = O$. Thus $(-1)v$ is the additive inverse of v, which is unique by Lemma 2

Definition - Subspace: For a K-vector space V and a non-empty subset $W \subseteq V$, W is a **subspace** if it satisfies

- $w_1, w_2, \in W \implies w_1 + w_2 \in W$
- $\forall a \in K, w \in W \implies aw \in W$

Theorem 1: Every subspace of a K-vector space is a K-vector space

Proof: We need to show that $W \subseteq V$ satisfies all the necessary properties of a vector space

1. Verify $O \in W$

   Since W is non-empty and closed under scalar multiplication, take $0w = O \in W$ by Lemma 3
2. $u, v \in W \implies u + v \in W$ and $a \in K, v \in W \implies aw \in W$ by definition of subspace
3. Every $w \in W$ has an additive inverse, namely $-w$

   Since W is closed under scalar multiplication, $(-1)w = -w \in W$ by Lemma 4
4. Other conditions (e.g. associative addition, commutative addition, etc.) hold because $u, v, w \in V \implies u, v, w \in W$

   For example, choose $u, v \in V$, then $u + v = v + u$, which also holds under W. Thus commutative addtion is satisfied

Example: Take $(5, 3, 2) \in R^3$. Then let $W = \{r(5, 3, 2) \mid r \in R\}$

Then W is an R-vector space. We prove this by showing that W is a subspace of R^3

- $+$: Choose 2 arbitrary elements of W, $r(5, 3, 2)$ and $s(5, 3, 2)$ for $r, s \in R$

  Then $r(5, 3, 2) + s(5, 3, 2) = (r + s)(5, 3, 2) \in W$
- $\times$: Choose $r(5, 3, 2) \in W$ and take $s \in R$

  Then $s(r(5, 3, 2)) = (sr)(5, 3, 2) \in W$

Example: Let $U = \{(x, y, z) \in R^3 \mid 2x + 3y = 0\}$. We show that U is a vector space by showing it's a subspace of R^3

- $+$: Take (x_1, y_1, z_1) and $(x_2, y_2, z_2) \in U \implies 2x_1 + 3y_1 = 0$ and $2x_2 + 3y_2 = 0$

  Then $2(x_1 + x_2) + 3(y_1 + y_2) = 0$

  Thus $(x_1 + x_2, y_1 + y_2, z_1 + z_2) \in U$
- $\times$: Let $(x, y, z) \in U$ and $r \in R$

  Then $2x + 3y = 0 \implies r(2x + 3y) 2rx + 3ry = 0$

  Thus $r(x, y, z) \in U$

Example: Consider $\sin(x), \cos(x) \in \mathcal{F}(R)$ and let $W = \{a \sin(x) + b \cos(x) \mid a, b \in R\}$. Then W is a subspace of $\mathcal{F}(R)$

- $+$: Take $a_1 \sin(x) + b_1 \cos(x)$ and $a_2 \sin(x) + b_2 \cos(x) \in W$. Then $(a_1 + a_2) \sin(x) + (b_1 + b_2) \cos(x) \in W$
- $\times$: Take $r \in R$. Then $r(a \sin(x) + b \cos(x)) = (ra) \sin(x) + (rb) \cos(x) \in W$

1.2 Basis

Definition - Linear Combination: For vectors $\{v_1, \ldots, v_n\} \subseteq V$, a **linear combination** of $\{v_1, \ldots, v_n\}$ is any vector of the form

$$a_1 v_1 + \cdots + a_n v_n \qquad a_i \in K$$

Definition - Span: $\text{span}(\{v_1, \ldots, v_n\}) = \{$ all linear combinations of $\{v_1, \ldots, v_n\}\}$

Proposition 1: $W = \text{span}(\{v_1, \ldots, v_n\})$ is a subspace of V and thus is itself a K-Vector Space

Proof: We show that W satisfies the necessary criteria to be a subspace of V

- $+$: Let $a = a_1 v_1 + \cdots + a_n v_n \in W$ and $b = b_1 v_1 + \cdots + b_n v_n \in W$

  Then $a + b = (a_1 + b_1)v_1 + \cdots + (a_n + b_n) \in W$

  Thus W is closed under addition
- Scalar $\times$: Let $a = a_1 v_1 + \cdots + a_n v_n \in W$ and let $c \in K$

  Then $ca = (ca_1)v_1 + \cdots + (ca_n) \in W$

  Thus W is closed under scalar multiplication

Example: Take $(5, 3, 1)$ and $(4, 0, -2) \in R^3$

$\text{span}(\{(5, 3, 1), (4, 0, -2)\})$ is a plane in R^3 passing through $(0, 0, 0)$

Example: Take $(5, 3, 1)$ and $(10, 6, 2) \in R^3$

$\text{span}(\{(5, 3, 1), (10, 6, 2)\})$ is a line in R^3 passing through $(0, 0, 0)$

- **Note**: $(10, 6, 2) = 2(5, 3, 1)$. Thus $\text{span}(\{(5, 3, 1), (10, 6, 2)\}) = a_1(5, 3, 1) + a_2(10, 6, 2) = (a_1 + 2a_2)(5, 3, 1)$

Definition - Linearly Independent: $\{v_1, \cdots, v_n\}$ is **linearly independent** if whenever $a_1 v_1 + \cdots + a_n v_n = 0$, then $a_1 = \cdots = a_n = 0$

- Otherwise $\{v_1, \ldots, v_n\}$ is **linearly dependent**

Proposition 2: $\{v_1, \ldots, v_n\}$ is linearly independent if and only if no v_i is a linearly combination of the other $n - 1$ vectors

Proof: $\implies$ Assume $\{v_1, \ldots, v_n\}$ is linearly independent

BWOC, assume some $v_i = a_1 v_1 + \cdots + a_n v_n$ for some $v_i \notin \{v_1, \ldots, v_n\}$

Then we have

$$O = a_1 v_1 + \cdots + a_n v_n + (-1)v_i$$

Since v_i is a linear combination of $\{v_1, \ldots, v_n\}$, the above equation shows that $\{v_1, \ldots, v_n\}$ is linearly dependent. Contradiction

Thus v_i cannot be written as a linear combination of the other vectors

$\impliedby$ Assume by way of contraposition that $\{v_1, \ldots, v_n\}$ is not linearly independent

Thus choose $a_1, \ldots, a_n \in K$, not all 0 such that

$$a_1 v_1 + \cdots + a_n v_n = O$$

WLOG, assume $a_1 \neq 0$. Then $v_2 a_2 + \cdots + a_n v_n = a_1 v_n$

Since $a_1 \neq 0$ and K is a field, we have

$$v_1 = \frac{a_2}{-a_1} v_2 + \cdots + \frac{a_n}{-a_1} v_n$$

Thus we have shown that v_1 is a linear combination of the other $n-1$ vectors

Corollary 3: $\{v_1, \ldots, v_n\}$ is linearly independent if and only if for each i, $v_i \notin \text{span}(\{v_1, \ldots, v_n\} \setminus \{v_i\})$

Proof: This follows from the previous proposition

Definition - Spans: Let W be a K-Vector Space and $\{v_1, \ldots, v_n\} \subseteq W$. If $\text{span}(\{v_1, \ldots, v_n\})$, then $\{v_1, \ldots, v_n\}$ **spans** W, so every $w \in W$ is a linear combination of $\{v_1, \ldots, v_n\}$

Definition - Basis: $\{v_1, \ldots, v_n\}$ is a **basis** of W if it spans W and is linearly independent

Example: $\{(5,3,1),(4,0,-2)\}$ is a basis for $\text{span}(\{(5,3,1),(4,0,-2)\})$

Example: $\{(5,3,1),(10,6,2)\}$ is not a basis for $\text{span}(\{(5,3,1),(10,6,2)\})$ since it is not linearly independent

Proposition 4: Let $\{v_1, \ldots, v_n\}$ be a basis for W and let $w \in W$ be arbitrary. Then w can be written uniquely as

$$w = a_1 v_1 + \cdots + a_n v_n \qquad a_i \in K$$

Proof: Since $\{v_1, \ldots, v_n\}$ spans W, every $w \in W$ is a linear combination of $\{v_1, \ldots, v_n\}$

For uniqueness, suppose

$$w = a_1 v_1 + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n$$

Then we have

$$O = (b_1 - a_1)v_1 + \cdots (b_n - a_n)$$

Since $\{v_1, \ldots, v_n\}$ is linearly independent, we must have $b_i - a_i = 0$, and thus $b_i = a_i$ for each i

Thus each $w \in W$ can be written uniquely as a linear combination of $\{v_1, \ldots, v_n\}$

Example: Let $W = \text{span}(\{\sin(x), \cos(x)\} = \{$ all functions of the form $a\sin(x) + b\cos(x) \mid a, b \in R\}$

We know that W is an R-Vector Space

$\{\sin(x), \cos(x)\}$ is linearly independent. Otherwise $\sin(x) = r\cos(x)$ for all $x \in X$ and some $r \in R$. However, this cannot hold for when $x = \pi/2$ since $\sin(\pi/2) = 1 \neq r\cos(\pi/2) = r0$

Let $\{v_1, \ldots, v_n\} \subseteq V$ and let $W = \text{span}(\{v_1, \ldots, v_n\})$

Now let $X = \{w_1, \ldots, w_m\} \subseteq W$. Then there are 2 desirable properties of X

- **X is Big**: X spans W if $\text{span}(X) = W$, i.e. all $w \in W$ is a linear combination of vectors from X
- **X is Small**: X is linearly independent, i.e. no element in X is a linear combination of the remaining elements

Note: the empty set $\emptyset$ is linearly independent since no element in $\emptyset$ is a linear combination of the others. More notably, $\emptyset$ is a basis for $\{O\}$

Shrinking Lemma: Let $X = \{w_1, \ldots, w_m\} \subseteq W$ and spans W but X is not linearly independent. Then $X \setminus \{w_i\}$ still spans W for some $w_i \in X$

Proof: Since X is not linearly independent, we know that some w_i is a linear combination of elements in $X \setminus \{w_i\}$. Suppose

$$w_i = a_1 w_1 + \cdots + a_m w_m \qquad \text{without } w_i \text{ occurring}$$

Then take arbitrary $u \in W$ where

$$u = b_1 w_1 + \cdots + b_m w_m$$

Replacing w_i above with the previous equation, we see that u is a linear combination of $X \setminus \{w_i\}$

Thus $X \setminus \{w_i\} = \text{span}(W)$

Shrinking Theorem: Let $X = \{w_1, \ldots, w_m\}$ span W. Then for some subset $Y \subseteq X$ is a basis of W

Proof:

Case 0: If X is linearly independent, then X is a basis by definition

Otherwise, apply the shrinking lemma to get $X_1 = X \setminus \{w_i\}$, which spans W

Case 1: If X_1 is linearly independent, then X_1 is a basis

...

Since X is finite (it has m elements), we will stop eventually. Either

- Some X_i is linearly independent and we are done
- Otherwise if we hit case m: $X_m = \emptyset$, which is linearly independent and thus X_m spans $W = \{O\}$

Corollary: If $W = \text{span}(\{v_1, \ldots, v_n\})$, then some subset of $\{v_1, \ldots, v_n\}$ is a basis

- **Note**: In particular, W has to have a basis

Enlarging Lemma: Suppose $X = \{w_1, \ldots, w_m\} \subseteq W$ and is linearly independent but doesn't span W. Then for any $w \in W \setminus \text{span}(X)$, $X \cup \{w\}$ is still linearly independent

Proof: Suppose $a_1 w_1 + \cdots + a_m w_m + bw = O$. We show that $a_1 = \cdots = a_m = b = 0$

Suppose BWOC, $b \neq 0$, then we can solve for w

$$w = \frac{-a_1}{b} w_1 + \cdots + \frac{-a_m}{b} w_m$$

Which means that w is a linear combination of $X \implies w \in \text{span}(X)$. Contradiction

Thus $b = 0$. This gives

$$a_1 w_1 + \cdots + a_m w_m + 0w = O$$

Since $X = \{w_1, \ldots, w_m\}$ is linearly independent, we also have $a_1 = \cdots = a_m = 0$

Thus $X \cup \{w\}$ is linearly independent

Main question: does the enlarging process above terminate? After some number of steps, do we get a set $\{w_1, \ldots, w_m\}$ that spans W?

Exchanging Lemma: Let $X = \{v_1, \ldots, v_n\}$ be any basis for W. Choose any $w \in W$ but $w \notin \text{span}(\{v_k, \ldots, v_n\})$. Then $\exists v_i, i < k$, such that $Y = (X \setminus \{v_i\}) \cup \{w\}$ is still a basis

- **Note**: If $k > n$, then $\{v_k, \ldots, v_n\} = \emptyset$

Proof: First we show that $\text{span}(Y) = W$. Since X spans W, we can write

$$w = a_1 v_1 + \cdots + a_n v_n \implies v_1 = \frac{1}{a_1} w + \frac{-a_2}{a_1} v_2 + \cdots + \frac{-a_m}{a_1} v_m$$

Since $w \notin \text{span}(\{v_k, \ldots, v_n\})$, we must have $a_i \neq 0$ for some $i < k$

WLOG, let $a_1 \neq 0$. We show that Y spans W

Since X spans W, for arbitrary $u \in W$, we have

$$u = d_1 v_1 + \cdots + d_n v_n$$

Replacing v_1 above with the previous equation, we see that u is a linear combination of elements of Y and thus $u \in \text{span}(Y)$

Next we show that Y is linearly independent

Suppose we have

$$cw + b_2v_2 + b_nv_n = O$$

We show that $c = b_2 = \cdots = b_n = 0$

- If $c = 0 \implies b_2 = \cdots = b_n = 0$ since $\{b_2, \ldots, b_n\}$ is linearly independent
- Otherwise suppose $c \neq 0$, then we can solve for w

$$w = \frac{-b_2}{c}v_2 + \cdots + \frac{-b_n}{c}v_n \implies v_1 = \frac{1}{a_1}(\frac{-b_2}{c}v_2 + \cdots + \frac{-b_n}{c}v_n) + \frac{-a_1}{a_1}v_2 + \cdots + \frac{-a_m}{a_1v_m}$$

Thus v_1 is a linear combination of $\{v_2, \ldots, v_n\}$, which is a contradiction since we said X was linearly independent. Thus $c = 0$

Theorem: Let $X = \{v_1, \ldots, v_n\}$ be a basis for W, and let $\{w_1, \ldots, w_m\} \subseteq W$ be linearly independent. Then $m \leq n$

Proof: If $m < n$, we are done

Now assume $m \geq n$, we show that $m = n$

Since $\{w_1, \ldots, w_m\}$ is linearly independent, we have that $w_1 \neq O = \text{span}(\emptyset)$

Now apply the Exchanging Lemma to the basis X, with $k > n$ and w_1 Then $\exists v_i$ such that $X_1 = (X \setminus \{v_i\}) \cup \{w_1\}$ is a basis

After reindexing, we see that X_1 has $n - 1$ vectors from X and 1 vector from w_1

Now take $k = n$. Since $\{w_1, \ldots, w_m\}$ is linearly independent, $w_2 \notin \text{span}(\{w_1\})$

Thus applying the Exchanging Lemma again, there exists $j < k = n$ such that $X_2 = (X_1 \setminus \{v_j\}) \cup \{w_2\}$ is a basis

Reindexing again, we get that $X_2 = \{v_1, \ldots, v_{n-2}, w_1, w_2\}$ is a basis

After n steps, X_n has no elements from X and $X_n = \{w_1, \ldots, w_n\}$ is a basis

Furthermore, we see that $w_m \in \text{span}(\{w_1, \ldots, w_n\})$, contradicting that $\{w_1, \ldots, w_m\}$ is linearly independent

Thus $m = n$

Corollary: If W is any K-vector space and some basis of W has n elements, then every basis of W has n elements

Definition - Finite Dimensional: Let W be a K-vector space. Then W is **finite dimensional** if some basis for W is finite

Definition - Dimension: Number of elements in any basis for a vector space W

Corollary: Suppose $\dim(W) = n$ and $X = \{w_1, \ldots, w_n\}$ are any n-vectors

1. If X spans W, then X is a basis for W
2. If X is linearly independent, then X is a basis for W

Proof:

1. By Shrinking Theorem, there exists a basis $Y \subseteq X$

   However, $|Y| < n$ contradicts that $\dim(W) = n$

   Thus $Y = X$, i.e. X is a basis
2. By Expansion Theorem, we can expand X to a basis Y

   However, $|Y| > n$ contradicts that $\dim(W) = n$

   Thus $Y = X$, i.e. X is a basis