1 Vector Space

We continue our discussion about **vector spaces**.

1.1 Basis

Definition 1.1: Basis

Let V be a vector space over a field F. A subset B of V is called a **basis** for V if B is linearly independent and every element of V is a linear combination of elements of B (i.e. B spans V).

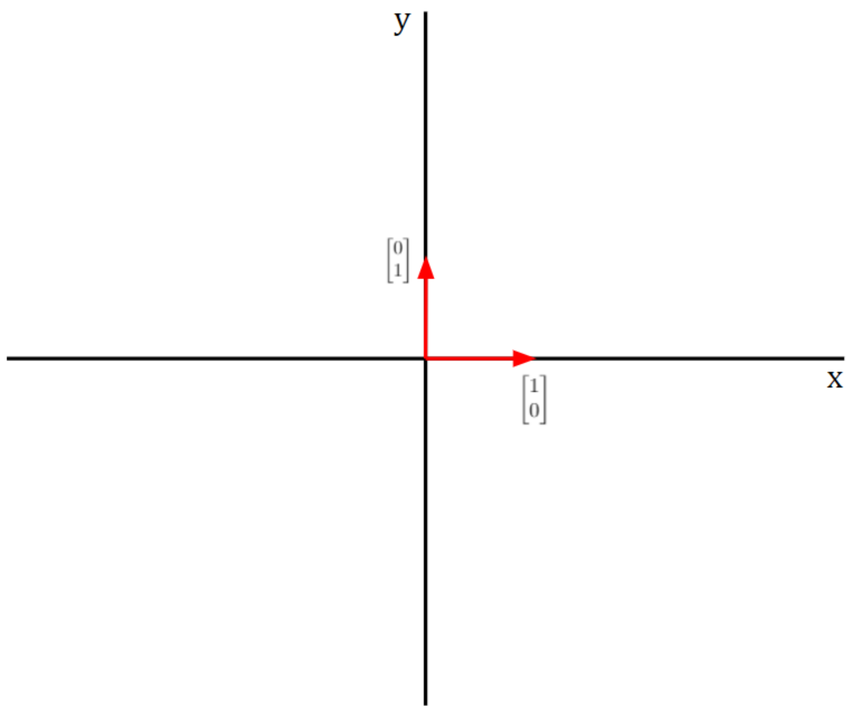
Fact: Every $v \in V$ is a unique linear combination of basis vectors.

1.1.1 Example 1: Standard Basis Vector

Consider the standard basis vector of $\mathbb{R}^n$:

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}$$

A classic example is $\mathbb{R}^2$, which has basis $\left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$. Here, we can visualize this by looking at a graph.



Here, the idea is that we can reach any point in this graph uniquely by multiplying $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ by the appropriate scalar constants.

1.1.2 Example 2: Vector Space over Rational Numbers

We claim that $\mathbb{Q}[x]/I$, where $I = \langle x^3 + x + 1\rangle$, is a vector space over $\mathbb{Q}$. To see this, we note the following:

- This is a ring, and in fact is a field since $x^3 + x + 1$ is irreducible. Therefore, addition is implied, and since this is a field, it is abelian.
- Consider the set of all cosets
$$\left\{ax^2 + bx + c + I \mid a, b, c \in \mathbb{Q}\right\}$$
If $r \in \mathbb{Q}$, then $r(ax^2 + bx + c + I) = rax^2 + rbx + rc + \langle x^2 + x + 1\rangle$. So, scalar multiplication is satisfied.
- The set $\{1 + I, x + I, x^2 + I\}$ is a basis for this vector space. Once again, to see this, we show that the properties of a basis are satisfied.
  - The linear combinations of these vectors clearly span the entire set. That is,
  $$a_0(1 + I) + a_1(x + I) + a_2(x^2 + I) = a_0 + a_1x + a_2x^2 + I$$
  - To see linear independence, we note that
  $$a_0(1 + I) + a_1(x + I) + a_2(x^2 + I) = 0 + I$$
  But we see that
  $$a_0 + a_1x + a_2x^2 + I = 0 + I$$
  However, this implies that
  $$a_0 + a_1x + a_2x^2 \in I$$
  This further implies that
  $$a_0 + a_1x + a_2x^2 = (x^3 + x + 1)g(x)$$
  But note that if $g(x)$ is not zero, then $(x^3 + x + 1)g(x)$ will have degree 3 or larger, but the left-hand side will never have this. This means that
  $$g(x) = 0$$
  This implies that $a_0 = a_1 = a_2 = 0$.

1.2 Invariance of Basis Size

Theorem 1.1

If $\{u_1, u_2, \ldots, u_m\}$ and $\{w_1, w_2, \ldots, w_n\}$ are bases of V, then $m = n$.

Facts: Let V be a finite dimensional vector space.

- Every spanning set contains a basis.
- If $\dim V = n$, a spanning set has size $\geq n$ with equality if and only if it is a basis.
- Every linearly independent set is contained in a basis.
- If $\dim V = n$, a linearly independent set has size $\leq n$ with equality if and only if it is a basis.

Proof. Suppose towards a contradiction that $m \neq n$, WLOG $m < n$. The u's span V. So, we write $w_1 = a_1u_1 + \cdots + a_mu_m$. Here, we're starting the process of expressing one basis in terms of another basis. We claim that $w_1 \neq 0$. Then, $a_i \neq 0$ for some i. WLOG let $a_1 \neq 0$. Then, we can solve for u_1. In particular, since the scalars are from a field, we can use inverses like so

$$u_1 = a_1^{-1}w_1 - a_1^{-1}a_2u_2 - \cdots - a_1^{-1}a_mu_m.$$

This implies that

$$u_1 \in \text{Span}\{w_1, u_2, \ldots, u_m\}.$$

We now do the same thing for w_2. So

$$w_2 = b_1 w_1 + b_2 u_2 + \cdots + b_m u_m$$

Evidently, we end up with

$$u_2 \in \operatorname{Span}\{w_1, w_2, u_3, \ldots, u_m\}.$$

and $u_1 \in \operatorname{Span}\{w_1, w_2, u_3, \ldots, u_m\}$. By repeating this process, repeating m times, we get

$$u_1, \ldots, u_m \in \operatorname{Span}\{w_1, \ldots, w_m\}.$$

We note that there is at least one more w to account for. So

$$w_{m+1} = c_1 u_1 + \cdots + c_m u_m \in \operatorname{Span}\{w_1, w_2, \ldots, w_m\}.$$

This is a contradiction as we have a dependent relationship. □

1.3 Dimension of a Vector Space

Definition 1.2: Dimension

A vector space V has dimension n, written $\dim V = n$, if V has a basis with n vectors.

Remarks:

- Sometimes, we write $\dim_F V = n$, where F is the field used.
- For completion, $\dim\{0\} = 0$.
- $\dim_F F[x]/\langle f(x)\rangle = \deg f(x)$.
- $|\mathbb{F}_p[x]/\langle f(x)\rangle| = p^n$ where $\deg f(x) = n$.
- If V is an n-dimensional vector space over $\mathbb{F}_p$, then $|V| = p^n$.

1.3.1 Example 1: Dimension

What is $\dim \mathbb{Q}[x]/\langle x^3 + x + 1\rangle$?

This has dimension 3 because the basis, $\{1 + I, x + I, x^2 + I\}$, has length 3.

1.3.2 Example 2: Dimension

What is $\dim \mathbb{R}[x]/\langle x^2 + 1\rangle$?

This has dimension 2.