

B Linear algebra

Vector spaces over the real numbers are familiar creatures. But the definition of a real vector space makes perfect sense when you replace the real numbers \mathbb{R} by an arbitrary field F . The crucial thing is that given a non-zero $x \in F$ there is a $y \in F$ such that $xy = 1$.

Definition B.0.9 A vector space V over a field F is an abelian group $(V, +)$ with neutral element 0 and a (scalar) multiplication $F \times V \rightarrow V$ denoted $(a, v) \mapsto av$ such that

- (i) $(ab)v = a(bv)$
- (ii) $1v = v$
- (iii) $(a + b)v = av + bv$
- (iv) $a(v + w) = av + aw$

for every $a, b \in F$ and every $v, w \in V$.

A subspace of V is a subgroup $W \subseteq V$ such that $av \in W$ if $a \in F$ and $v \in W$. A group homomorphism $\varphi : V \rightarrow W$ between vector spaces V and W over a field F is called a linear map if $\varphi(av) = a\varphi(v)$ where $a \in F$ and $v \in V$.

Let $\varphi : V \rightarrow W$ be a linear map. The subset $\text{Ker}(\varphi) = \{v \in V \mid \varphi(v) = 0\} \subseteq V$ is called the kernel of φ and $\text{Im}(\varphi) = \{\varphi(v) \mid v \in V\} \subseteq W$ is called the image of φ . Both are subspaces. Let $V' \subseteq V$ be a subspace; then the quotient group $V/V' = \{v + V' \mid v \in V\}$ is a vector space through the (well defined) scalar multiplication given by $a(v + V') = av + V'$. By Theorem 2.5.1 we have a group isomorphism

$$\tilde{\varphi} : V/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi),$$

where $\varphi : V \rightarrow W$ is a linear map. This group isomorphism is also a linear map.

A vector space V over a field F is called finitely generated if there exists a finite set of vectors $v_1, \dots, v_n \in V$ such that every $v \in V$ can be written as a linear combination $v = a_1 v_1 + \dots + a_n v_n$ for suitable $a_1, \dots, a_n \in F$. Such a set of vectors is called a (finite) generating set for V . We will assume that vector spaces are finitely generated.

Example B.0.10 Let F be a field. Then

$$V = F^n = F \times \dots \times F$$

is a vector space resembling \mathbb{R}^n . The multiplication $F \times V \rightarrow V$ is given by

$$a(v_1, \dots, v_n) = (av_1, \dots, av_n),$$

where $a \in F$ and $(v_1, \dots, v_n) \in V$. The vectors $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, \dots , $e_n = (0, 0, \dots, 1) \in V$ form a generating set for V .

B.1 Linear independence

Definition B.1.1 Let V be a vector space over a field F . A set of vectors v_1, \dots, v_n is called *linearly independent* if

$$a_1 v_1 + \dots + a_n v_n = 0,$$

where $a_1, \dots, a_n \in F$ implies that $a_1 = \dots = a_n = 0$.

We now prove what is known as the *Steinitz exchange lemma*.

Lemma B.1.2 Let V be a vector space over a field F , w_1, \dots, w_m a linearly independent set of vectors and v_1, \dots, v_n a generating set for V . Then $m \leq n$ and $w_1, \dots, w_m, v'_{m+1}, \dots, v'_n$ gives a generating set for V , where $v'_{m+1}, \dots, v'_n \in \{v_1, \dots, v_n\}$.

Proof. We may assume by rearranging v_1, \dots, v_n that $w_1 = a_1 v_1 + \dots + a_n v_n$, with $a_1 \neq 0$. This gives that v_1 can be written as a linear combination of w_1, v_2, \dots, v_n . Therefore w_1, v_2, \dots, v_n is a generating set for V . We continue this procedure with w_2 . Write $w_2 = a_1 w_1 + a_2 v_2 + \dots + a_n v_n$. Here we must have $a_i \neq 0$ for some $i > 1$, otherwise w_1 and w_2 would not be linearly independent. Assume that $a_2 \neq 0$. In the same way as before $w_1, w_2, v_3, \dots, v_n$ is a generating set. Proceeding like this we cannot exceed the n th vector v_n ; This would contradict that w_1, \dots, w_m is a linearly independent set of vectors. Thus $m \leq n$ and in the process we have also shown that $w_1, \dots, w_m, v'_{m+1}, \dots, v'_n$ is a generating set for V , where $v'_{m+1}, \dots, v'_n \in \{v_1, \dots, v_n\}$. \square

Definition B.1.3 A basis for a vector space V is a linearly independent generating set for V .

Proposition B.1.4 *A (finitely generated) vector space V over a field F has a basis. More precisely, a minimal generating set for V is linearly independent.*

Proof. Let $v_1, \dots, v_n \in V$ be a minimal generating set for V . This means that if we exclude any of v_1, \dots, v_n we are left with a set of vectors that is not a generating set. We wish to prove that v_1, \dots, v_n is a linearly independent set. If not, we would have $a_1, \dots, a_n \in F$, not all zero, such that

$$a_1 v_1 + \dots + a_n v_n = 0.$$

We may assume that $a_1 \neq 0$. This means that

$$v_1 = -a_1^{-1} a_2 v_2 - \dots - a_1^{-1} a_n v_n.$$

Therefore v_2, \dots, v_n is a generating set, contradicting that v_1, \dots, v_n is a minimal generating set. \square

Proposition B.1.5 *If v_1, \dots, v_m and w_1, \dots, w_n are two bases of a vector space then $m = n$.*

Proof. This follows from Lemma B.1.2. \square

B.2 Dimension

Definition B.2.1 Let V be a vector space over a field F . The *dimension* $\dim_F V$ of V over F is the number of elements in a basis of V .

Proposition B.2.2 *Let V be a vector space over a field F and $W \subseteq V$ a subspace of V . If $\dim_F W = \dim_F V$ then $W = V$.*

Proof. Let $n = \dim_F W = \dim_F V$. Suppose that w_1, \dots, w_n is a basis for W and v_1, \dots, v_n a basis for V . Then we may use Lemma B.1.2 to conclude that w_1, \dots, w_n is also a basis for V . Thus $W = V$. \square

Proposition B.2.3 *Let V be a vector space over a field F and $W \subseteq V$ a subspace of V . Then*

- (i) $\dim_F V/W = \dim_F V - \dim_F W$,
- (ii) $\dim_F V + W = \dim_F V + \dim_F W - \dim_F V \cap W$,
- (iii) $\dim_F \text{Ker}(\varphi) + \dim_F \text{Im}(\varphi) = \dim_F V$ where $\varphi : V \rightarrow W$ is a linear map.

Proof. If w_1, \dots, w_r is a basis for W and v_1, \dots, v_n a basis for V then we may assume that $w_1, \dots, w_r, v_{r+1}, \dots, v_n$ is a basis for V by Lemma B.1.2. It is easy to verify that $v_{r+1} + W, \dots, v_n + W$ is a basis for V/W . This proves the first formula. To prove the second formula recall that $V + W$ is the subspace

defined as $\{v + w \mid v \in V, w \in W\}$ and that V and W are subspaces of $V + W$. The composed map

$$\psi : V \rightarrow V + W \rightarrow V + W/W$$

is given by $\psi(v) = v + W$. It is linear and surjective and $\text{Ker}(\psi) = V \cap W$, since $\psi(v) = v + W = W$ if and only if $v \in W$. Therefore

$$V/V \cap W \cong V + W/W.$$

This shows that $\dim_F V/V \cap W = \dim_F V + W/W$, and (ii) follows from (i). Use the isomorphism

$$V/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$$

to deduce the formula in (iii). \square

If $\varphi : V \rightarrow W$ is a linear map, v_1, \dots, v_m a basis of V and w_1, \dots, w_n a basis of W then

$$\varphi(v_1) = a_{11}w_1 + \dots + a_{n1}w_n.$$

$$\vdots$$

$$\varphi(v_m) = a_{1m}w_1 + \dots + a_{nm}w_n,$$

If $v = x_1v_1 + \dots + x_mv_m \in V$, where $x_1, \dots, x_m \in F$, we see that

$$\varphi(v) = x_1\varphi(v_1) + \dots + x_m\varphi(v_m).$$

Thus

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix},$$

where $\varphi(v) = y_1w_1 + \dots + y_nw_n$.

Example B.2.4 Let F be a field and $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in F[X]$ a polynomial of degree $n \geq 1$. Then

$$R = F[X]/\langle f \rangle$$

is a vector space over F with basis $1, \alpha, \dots, \alpha^{n-1}$, where $\alpha = [X] \in R$. Multiplication by α is a linear map $\varphi : R \rightarrow R$. The matrix of φ with respect to the basis $1, \alpha, \dots, \alpha^{n-1}$ is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

The above facts are consequences of Proposition 4.6.7.