

# Review of Linear Algebra

Throughout these notes,  $F$  denotes a field (often called the *scalars* in this context).

## 1 Definition of a vector space

**Definition 1.1.** A  $F$ -vector space or simply a vector space is a triple  $(V, +, \cdot)$ , where  $(V, +)$  is an abelian group (the *vectors*), and there is a function  $F \times V \rightarrow V$  (*scalar multiplication*), whose value at  $(t, v)$  is just denoted  $t \cdot v$  or  $tv$ , such that

1. For all  $s, t \in F$  and  $v \in V$ ,  $s(tv) = (st)v$ . (An analogue of the associative law for multiplication.)
2. For all  $s, t \in F$  and  $v \in V$ ,  $(s + t)v = sv + tv$ . (Scalar multiplication distributes over scalar addition.)
3. For all  $t \in F$  and  $v, w \in V$ ,  $t(v + w) = tv + tw$ . (Scalar multiplication distributes over vector addition.)
4. For all  $v \in V$ ,  $1 \cdot v = v$ . (A kind of identity law for scalar multiplication.)

It is a straightforward consequence of the axioms that  $0v = 0$  for all  $v \in V$ , where the first 0 is the element  $0 \in F$  and the second is  $0 \in V$ , that, for all  $t \in F$ ,  $t0 = 0$  (both 0's here are the zero vector), and that, for all  $v \in V$ ,  $(-1)v = -v$ .

**Example 1.2.** (1) The  $n$ -fold Cartesian product  $F^n$  is an  $F$ -vector space, where  $F^n$  is a group under componentwise addition, i.e.  $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$ , and scalar multiplication is defined by  $t(a_1, \dots, a_n) = (ta_1, \dots, ta_n)$ .

(2) If  $X$  is a set and  $F^X$  denotes the group of functions from  $X$  to  $F$ , then  $F^X$  is an  $F$ -vector space. Here addition is defined pointwise:  $(f + g)(x) = f(x) + g(x)$ , and similarly for scalar multiplication:  $(tf)(x) = tf(x)$ .

(3) The polynomial ring  $F[x]$  is an  $F$ -vector space under addition of polynomials, where we define  $tf(x)$  to be the product of the constant polynomial  $t \in F$  with the polynomial  $f(x) \in F[x]$ . Explicitly, if  $f(x) = \sum_{i=0}^n a_n x^n$ , then  $tf(x) = \sum_{i=0}^n ta_n x^n$ .

(4) More generally, if  $R$  is any ring containing  $F$  as a subring, then  $R$  becomes an  $F$ -vector space, using the fact that  $(R, +)$  is an abelian group, and defining, for  $t \in F$  and  $r \in R$ , scalar multiplication  $tr$  to be the usual multiplication in  $R$  applied to  $t$  and  $r$ . In this case, the properties (1)–(4) of a vector space become consequences of associativity, distributivity, and the fact that  $1 \in F$  is the multiplicative identity in  $R$ . In particular, if  $E$  is a field containing  $F$  as a subfield, then  $E$  is an  $F$ -vector space in this way.

**Definition 1.3.** Let  $V$  be a vector space. An  $F$ -vector subspace of  $V$  is a subset  $W \subseteq V$  which is an additive subgroup of  $V$  which is closed under scalar multiplication (i.e. such that, for all  $v \in W$  and for all  $t \in F$ ,  $tv \in W$ ). It then follows that  $(W, +, \cdot)$  is also a vector space.

**Example 1.4.**  $\{0\}$  and  $V$  are always vector subspaces of  $V$ . The set

$$P_n = \left\{ \sum_{i=0}^n a_i x^i : a_i \in F \right\}$$

of polynomials of degree at most  $n$ , together with the zero polynomial, is a vector subspace of  $F[x]$ .

Finally, we have the analogue of homomorphisms and isomorphisms:

**Definition 1.5.** Let  $V_1$  and  $V_2$  be two  $F$ -vector spaces and let  $f: V_1 \rightarrow V_2$  be a function (= map). Then  $f$  is *linear* or a *linear map* if it is a group homomorphism from  $(V_1, +)$  to  $(V_2, +)$ , i.e. is additive, and satisfies: For all  $t \in F$  and  $v \in V_1$ ,  $f(tv) = tf(v)$ . The function  $f$  is a *linear isomorphism* if it is both linear and a bijection; in this case, it is easy to check that  $f^{-1}$  is also linear.

There is an analogue of vector spaces for more general rings:

**Definition 1.6.** Let  $R$  be a ring (always assumed commutative, with unity). Then an  $R$ -module  $M$  is a triple  $(M, +, \cdot)$ , where  $(M, +)$  is an abelian group, and there is a function  $R \times M \rightarrow M$ , whose value at  $(r, m)$  is denoted  $rm$  or  $r \cdot m$ , such that:

1. For all  $r, s \in R$  and  $m \in M$ ,  $r(sm) = (rs)m$ .

2. For all  $r, s \in R$  and  $m \in M$ ,  $(r + s)m = rm + sm$ .
3. For all  $r \in R$  and  $m, n \in M$ ,  $r(m + n) = rm + rn$ .
4. For all  $m \in M$ ,  $1 \cdot m = m$ .

Submodules and homomorphisms of  $R$ -modules are defined in the obvious way. For example,  $R^n$  is an  $R$ -module. Despite the similarity with the definition of vector spaces, general  $R$ -modules can look quite complicated. For example, a  $\mathbb{Z}$ -module is the same thing as an abelian group, and hence  $\mathbb{Z}/n\mathbb{Z}$  is a  $\mathbb{Z}$ -module. For a general ring  $R$ , if  $I$  is an ideal of  $R$ , then both  $I$  and  $R/I$  are  $R$ -modules.

## 2 Linear independence and span

Let us introduce some terminology:

**Definition 2.1.** Let  $V$  be an  $F$ -vector space and let  $v_1, \dots, v_d \in V$  be a sequence of vectors. A *linear combination* of  $v_1, \dots, v_d$  is a vector of the form  $t_1v_1 + \dots + t_dv_d$ , where the  $t_i \in F$ . The *span* of  $\{v_1, \dots, v_d\}$  is the set of all linear combinations of  $v_1, \dots, v_d$ . Thus

$$\text{span}\{v_1, \dots, v_d\} = \{t_1v_1 + \dots + t_dv_d : t_i \in F \text{ for all } i\}.$$

By definition (or logic),  $\text{span } \emptyset = \{0\}$ .

We have the following properties of span:

**Proposition 2.2.** *Let  $v_1, \dots, v_d \in V$  be a sequence of vectors. Then:*

- (i)  $\text{span}\{v_1, \dots, v_d\}$  is a vector subspace of  $V$  containing  $v_i$  for every  $i$ .
- (ii) If  $W$  is a vector subspace of  $V$  containing  $v_1, \dots, v_d$ , then

$$\text{span}\{v_1, \dots, v_d\} \subseteq W.$$

*In other words,  $\text{span}\{v_1, \dots, v_d\}$  is the smallest vector subspace of  $V$  containing  $v_1, \dots, v_d$ .*

- (iii) *For every  $v \in V$ ,  $\text{span}\{v_1, \dots, v_d\} \subseteq \text{span}\{v_1, \dots, v_d, v\}$ , and equality holds if and only if  $v \in \text{span}\{v_1, \dots, v_d\}$ .*

*Proof.* (i) Taking  $t_j = 0, j \neq i$ , and  $t_i = 1$ , we see that  $v_i \in \text{span}\{v_1, \dots, v_d\}$ . Next, given  $v = t_1v_1 + \dots + t_dv_d$  and  $w = s_1w_1 + \dots + s_dw_d \in \text{span}\{v_1, \dots, v_d\}$ ,

$$v + w = (s_1 + t_1)v_1 + \dots + (s_d + t_d)v_d \in \text{span}\{v_1, \dots, v_d\}.$$

Hence  $\text{span}\{v_1, \dots, v_d\}$  is closed under addition. Also,  $0 = 0 \cdot v_1 + \dots + 0 \cdot v_d \in \text{span}\{v_1, \dots, v_d\}$ , and, given  $v = t_1v_1 + \dots + t_dv_d \in \text{span}\{v_1, \dots, v_d\}$ ,  $-v = (-t_1)v_1 + \dots + (-t_d)v_d \in \text{span}\{v_1, \dots, v_d\}$  as well. Hence  $\text{span}\{v_1, \dots, v_d\}$  is an additive subgroup of  $V$ . Finally, for all  $v = t_1v_1 + \dots + t_dv_d \in \text{span}\{v_1, \dots, v_d\}$  and  $t \in F$ ,

$$tv = (tt_1)v_1 + \dots + (tt_d)v_d \in \text{span}\{v_1, \dots, v_d\}.$$

Hence  $\text{span}\{v_1, \dots, v_d\}$  is a vector subspace of  $V$  containing  $v_i$  for every  $i$ .

(ii) If  $W$  is a vector subspace of  $V$  containing  $v_1, \dots, v_d$ , then, for all  $t_1, \dots, t_d \in F$ ,  $t_i v_i \in W$ . Hence  $t_1v_1 + \dots + t_dv_d \in W$ . It follows that  $\text{span}\{v_1, \dots, v_d\} \subseteq W$ .

(iii) We always have  $\text{span}\{v_1, \dots, v_d\} \subseteq \text{span}\{v_1, \dots, v_d, v\}$ , since we can write  $t_1v_1 + \dots + t_dv_d = t_1v_1 + \dots + t_dv_d + 0 \cdot v$ .

Now suppose that  $\text{span}\{v_1, \dots, v_d\} = \text{span}\{v_1, \dots, v_d, v\}$ . Then in particular  $v \in \text{span}\{v_1, \dots, v_d, v\} = \text{span}\{v_1, \dots, v_d\}$ , by (i), and hence  $v \in \text{span}\{v_1, \dots, v_d\}$ , i.e.  $v$  is a linear combination of  $v_1, \dots, v_d$ . Conversely, suppose that  $v \in \text{span}\{v_1, \dots, v_d\}$ . Then by (i)  $\text{span}\{v_1, \dots, v_d\}$  is a vector subspace of  $V$  containing  $v_1, \dots, v_d$  and  $v$  and hence  $\text{span}\{v_1, \dots, v_d, v\} \subseteq \text{span}\{v_1, \dots, v_d\}$ . Thus  $\text{span}\{v_1, \dots, v_d, v\} = \text{span}\{v_1, \dots, v_d\}$ .  $\square$

**Definition 2.3.** A sequence of vectors  $w_1, \dots, w_\ell$  such that

$$V = \text{span}\{w_1, \dots, w_\ell\}$$

will be said to *span*  $V$ .

**Definition 2.4.** An  $F$ -vector space  $V$  is a *finite dimensional vector space* if there exist  $v_1, \dots, v_d \in V$  such that  $V = \text{span}\{v_1, \dots, v_d\}$ . The vector space  $V$  is *infinite dimensional* if it is not finite dimensional.

For example,  $F^n$  is finite-dimensional. But  $F[x]$  is not a finite-dimensional vector space. On the other hand, the subspace  $P_n$  of  $F[x]$  defined in Example 1.4 is a finite dimensional vector space, as it is spanned by  $1, x, \dots, x^n$ .

The next piece of terminology is there to deal with the fact that we might have chosen a highly redundant set of vectors to span  $V$ .

**Definition 2.5.** A sequence  $w_1, \dots, w_r \in V$  is *linearly independent* if the following holds: if there exist real numbers  $t_i$  such that

$$t_1 w_1 + \dots + t_r w_r = 0,$$

then  $t_i = 0$  for all  $i$ . The sequence  $w_1, \dots, w_r$  is *linearly dependent* if it is not linearly independent.

Note that the definition of linear independence does **not** depend **only** on the set  $\{w_1, \dots, w_r\}$ —if there are any repeated vectors  $w_i = w_j$ , then we can express 0 as the nontrivial linear combination  $w_i - w_j$ . Likewise if one of the  $w_i$  is zero then the set is linearly dependent.

By definition or by logic, the empty set is linearly independent. For a less obscure example,  $e_1, \dots, e_n \in F^n$  are linearly independent since if  $t_1 e_1 + \dots + t_n e_n = 0$ , then  $(t_1, \dots, t_n)$  is the zero vector and thus  $t_i = 0$  for all  $i$ . More generally, for all  $j \leq n$ , the vectors  $e_1, \dots, e_j$  are linearly independent.

**Lemma 2.6.** *The vectors  $w_1, \dots, w_r$  are linearly independent if and only if, given  $t_i, s_i \in F$ ,  $1 \leq i \leq r$ , such that*

$$t_1 w_1 + \dots + t_r w_r = s_1 w_1 + \dots + s_r w_r,$$

*then  $t_i = s_i$  for all  $i$ .*

*Proof.* If  $w_1, \dots, w_r$  are linearly independent and if  $t_1 w_1 + \dots + t_r w_r = s_1 w_1 + \dots + s_r w_r$ , then after subtracting and rearranging we have  $(t_1 - s_1)w_1 + \dots + (t_r - s_r)w_r = 0$ . Thus by the definition of linear independence  $t_i - s_i = 0$  for every  $i$ , i.e.  $s_i = t_i$ . Conversely, if the last statement of the lemma holds and if  $t_1 w_1 + \dots + t_r w_r = 0$ , then it follows from

$$t_1 w_1 + \dots + t_r w_r = 0 = 0 \cdot w_1 + \dots + 0 \cdot w_r$$

that  $t_i = 0$  for all  $i$ . Hence  $w_1, \dots, w_r$  are linearly independent. □

Clearly, if  $w_1, \dots, w_r$  are linearly independent, then so is any reordering of the vectors  $w_1, \dots, w_r$ , and likewise any smaller sequence (not allowing repeats), for example  $w_1, \dots, w_s$  with  $s \leq r$ . A related argument shows:

**Lemma 2.7.** *The vectors  $w_1, \dots, w_r$  are **not** linearly independent if and only if we can write at least one of the  $w_i$  as a linear combination of the  $w_j, j \neq i$ .*

The proof is left as an exercise.

**Definition 2.8.** Let  $V$  be an  $F$ -vector space. The vectors  $v_1, \dots, v_d$  are a *basis* of  $V$  if they are linearly independent and  $V = \text{span}\{v_1, \dots, v_d\}$ . For example, the standard basis vectors  $e_1, \dots, e_n$  are a basis for  $F^n$ . The elements  $1, x, \dots, x^n$  are a basis for  $P_n$ .

Thus to say that the vectors  $v_1, \dots, v_r$  are a basis of  $V$  is to say that every  $x \in V$  can be uniquely written as  $x = t_1 v_1 + \dots + t_r v_r$  for  $t_i \in F$ .

**Lemma 2.9** (Main counting argument). *Suppose that  $w_1, \dots, w_b$  are linearly independent vectors contained in  $\text{span}\{v_1, \dots, v_a\}$ . Then  $b \leq a$ .*

*Proof.* We shall show that, possibly after relabeling the  $v_i$ ,

$$\begin{aligned} \text{span}\{v_1, \dots, v_a\} &= \text{span}\{w_1, v_2, \dots, v_a\} = \text{span}\{w_1, w_2, v_3, \dots, v_a\} \\ &= \dots = \text{span}\{w_1, w_2, \dots, w_b, v_{b+1}, \dots, v_a\}. \end{aligned}$$

From this we will be able to conclude that  $b \leq a$ .

To begin, we may suppose that  $\{w_1, \dots, w_b\} \neq \emptyset$ . (If  $\{w_1, \dots, w_b\} = \emptyset$ , then  $b = 0$  and the conclusion  $b \leq a$  is automatic.) Moreover none of the  $w_i$  is zero. Given  $w_1$ , we can write it as a linear combination of the  $v_i$ :

$$w_1 = \sum_{i=1}^a t_i v_i.$$

Since  $w_1 \neq 0$ ,  $\{v_1, \dots, v_a\} \neq \emptyset$ , i.e.  $a \geq 1$ , and at least one of the  $t_i \neq 0$ . After relabeling the  $v_i$ , we can assume that  $t_1 \neq 0$ . Thus we can solve for  $v_1$  in terms of  $w_1$  and the  $v_i, i > 1$ :

$$v_1 = \frac{1}{t_1} w_1 + \sum_{i=2}^a \left( -\frac{t_i}{t_1} \right) v_i.$$

It follows that  $v_1 \in \text{span}\{w_1, v_2, \dots, v_a\}$ . Now using some of the properties of span listed above, we have

$$\text{span}\{w_1, v_2, \dots, v_a\} = \text{span}\{v_1, w_1, v_2, \dots, v_a\} = \text{span}\{v_1, v_2, \dots, v_a\},$$

where the second equality holds since  $w_1 \in \text{span}\{v_1, v_2, \dots, v_a\}$ .

Continuing in this way, write  $w_2$  as a vector in  $\text{span}\{w_1, v_2, \dots, v_a\}$ :

$$w_2 = t_1 w_1 + \sum_{i=2}^a t_i v_i.$$

For some  $i \geq 2$ , we must have  $t_i \neq 0$ , for otherwise we would have  $w_2 = t_1 w_1$  and thus there would exist a nontrivial linear combination  $t_1 w_1 + (-1)w_2 = 0$ , contradicting the linear independence of the  $w_i$ . After relabeling, we can assume that  $t_2 \neq 0$ ; notice that in particular we must have  $a \geq 2$ . Arguing as before, we may write

$$v_2 = -\frac{t_1}{t_2}w_1 + \frac{1}{t_2}w_2 + \sum_{i=3}^a \left(-\frac{t_i}{t_2}\right)v_i,$$

and thus we can solve for  $v_2$  in terms of  $w_1, w_2$ , and  $v_i, i \geq 3$  and so

$$\text{span}\{w_1, v_2, \dots, v_a\} = \text{span}\{w_1, w_2, v_3, \dots, v_a\}.$$

By induction, for a fixed  $i < b$ , suppose that we have showed that  $i \leq a$  and that after some relabeling of the  $v_i$  we have

$$\begin{aligned} \text{span}\{v_1, \dots, v_a\} &= \text{span}\{w_1, v_2, \dots, v_a\} = \\ &= \text{span}\{w_1, w_2, v_3, \dots, v_a\} = \dots = \text{span}\{w_1, w_2, \dots, w_i, v_{i+1}, \dots, v_a\}. \end{aligned}$$

We claim that the same is true for  $i + 1$ . Write

$$w_{i+1} = t_1 w_1 + \dots + t_i w_i + t_{i+1} v_{i+1} + \dots + t_a v_a,$$

which is possible as

$$w_{i+1} \in \text{span}\{v_1, \dots, v_a\} = \text{span}\{w_1, w_2, \dots, w_i, v_{i+1}, \dots, v_a\}.$$

At least one of the numbers  $t_{i+1}, \dots, t_a$  is nonzero, for otherwise  $w_{i+1} = t_1 w_1 + \dots + t_i w_i$ , which would say that the vectors  $w_1, \dots, w_{i+1}$  are not linearly independent. In particular this says that  $i + 1 \leq a$ . After relabeling, we may assume that  $t_{i+1} \neq 0$ . Then as before we can solve for  $v_{i+1}$  in terms of the vectors  $w_1, \dots, w_{i+1}, v_{i+2}, \dots, v_a$ . It follows that

$$\text{span}\{w_1, w_2, \dots, w_i, v_{i+1}, \dots, v_a\} = \text{span}\{w_1, w_2, \dots, w_i, w_{i+1}, v_{i+2}, \dots, v_a\}$$

and we have completed the inductive step. So for all  $i \leq b$ ,  $i \leq a$ , and in particular  $b \leq a$ .  $\square$

This rather complicated argument has the following consequences:

**Corollary 2.10.** (i) *Suppose that  $V = \text{span}\{v_1, \dots, v_n\}$  and that  $w_1, \dots, w_\ell$  are linearly independent vectors in  $V$ . Then  $\ell \leq n$ .*

- (ii) If  $V$  is a finite-dimensional  $F$ -vector space, then every two bases for  $V$  have the same number of elements—call this number the dimension of  $V$  which we write as  $\dim V$  or  $\dim_F V$  if we want to emphasize the field  $F$ . Thus for example  $\dim F^n = n$  and  $\dim P_n = n + 1$ .
- (iii) If  $V = \text{span}\{v_1, \dots, v_d\}$  then some subsequence of  $v_1, \dots, v_d$  is a basis for  $V$ . Hence  $\dim V \leq d$ , and if  $\dim V = d$  then  $v_1, \dots, v_d$  is a basis for  $V$ .
- (iv) If  $V$  is a finite-dimensional  $F$ -vector space and  $w_1, \dots, w_\ell$  are linearly independent vectors in  $V$ , then there exist vectors

$$w_{\ell+1}, \dots, w_r \in V$$

such that  $w_1, \dots, w_\ell, w_{\ell+1}, \dots, w_r$  is a basis for  $V$ . Hence  $\dim V \geq \ell$ , and if  $\dim V = \ell$  then  $w_1, \dots, w_\ell$  is a basis for  $V$ .

- (v) If  $V$  is a finite-dimensional  $F$ -vector space and  $W$  is a vector subspace of  $V$ , then  $\dim W \leq \dim V$ . Moreover  $\dim W = \dim V$  if and only if  $W = V$ .
- (vi) If  $v_1, \dots, v_d$  is a basis of  $V$ , then the function  $f: F^d \rightarrow V$  defined by

$$f(t_1, \dots, t_d) = \sum_{i=1}^d t_i v_i$$

is a linear isomorphism from  $F^d$  to  $V$ .

*Proof.* (i) Apply the lemma to the subspace  $V$  itself, which is the span of  $v_1, \dots, v_n$ , and to the linearly independent vectors  $w_1, \dots, w_\ell \in V$ , to conclude that  $\ell \leq n$ .

(ii) If  $w_1, \dots, w_b$  and  $v_1, \dots, v_a$  are two bases of  $V$ , then by definition  $w_1, \dots, w_b$  are linearly independent vectors, and  $V = \text{span}\{v_1, \dots, v_a\}$ . Thus  $b \leq a$ . But symmetrically  $v_1, \dots, v_a$  is a sequence of linearly independent vectors contained in  $V = \text{span}\{w_1, \dots, w_b\}$ , so  $a \leq b$ . Thus  $a = b$ .

(iii) If  $v_1, \dots, v_d$  are not linearly independent, then, by Lemma 2.7, one of the vectors  $v_i$  is expressed as a linear combination of the others. After relabeling we may assume that  $v_d$  is a linear combination of  $v_1, \dots, v_{d-1}$ . By (iii) of Proposition 2.2,  $\text{span}\{v_1, \dots, v_{d-1}\} = \text{span}\{v_1, \dots, v_d\}$ . Continue in this way until we find  $v_1, \dots, v_k$  with  $k \leq d$  such that  $\text{span}\{v_1, \dots, v_k\} = \text{span}\{v_1, \dots, v_d\}$  and such that  $v_1, \dots, v_k$  are linearly independent. Then by definition  $k = \dim V$  and  $k \leq d$ . Moreover  $k = d$  exactly when  $v_1, \dots, v_d$  are linearly independent, in which case  $\text{span}\{v_1, \dots, v_d\}$  is a basis.

(iv) If  $\text{span}\{w_1, \dots, w_\ell\} \neq V$ , then there exists a vector, call it  $w_{\ell+1} \in V$  with  $w_{\ell+1} \notin \text{span}\{w_1, \dots, w_\ell\}$ . It follows that the sequence  $w_1, \dots, w_\ell, w_{\ell+1}$



is still linearly independent: if there exist  $t_i \in F$ , not all 0, such that  $0 = \sum_{i=1}^{\ell+1} t_i w_i$ , then we must have  $t_{\ell+1} \neq 0$  since  $w_1, \dots, w_\ell$  are linearly independent. But that would say that  $w_{\ell+1} \in \text{span}\{w_1, \dots, w_\ell\}$ , contradicting our choice. So  $w_1, \dots, w_\ell, w_{\ell+1}$  are still linearly independent. We continue in this way. Since the number of elements in a linearly independent sequence of vectors in  $V$  is at most  $\dim V$ , this procedure has to stop after at most  $\dim V - \ell$  stages. At this point we have found a linearly independent sequence which spans  $V$  and thus is a basis. To see the last statement, note that if  $\text{span}\{w_1, \dots, w_\ell\} \neq V$ , then there exist  $\ell + 1$  linearly independent vectors in  $V$ , and hence  $\dim V \geq \ell + 1$ .

(v) Choosing a basis of  $W$  and applying (iv) (since the elements of a basis are linearly independent) we see that it can be completed to a basis of  $V$ . Thus  $\dim W \leq \dim V$ . Moreover  $\dim W = \dim V$  if and only if the basis we chose for  $W$  was already a basis for  $V$ , i.e.  $W = V$ .

(vi) A straightforward calculation shows that  $f$  is linear. It is a bijection by definition of a basis: it is surjective since the  $v_i$  span  $V$ , and it is injective since the  $v_i$  are linearly independent and by Lemma 2.6.  $\square$

**Proposition 2.11.** *If  $V$  is a finite dimensional  $F$ -vector space and  $W$  is a subset of  $V$ , then  $W$  is a vector subspace of  $V$  if and only if it is of the form  $\text{span}\{v_1, \dots, v_d\}$  for some  $v_1, \dots, v_d \in V$ .*

*Proof.* We have already noted that a set of the form  $\text{span}\{v_1, \dots, v_d\}$  is a vector subspace of  $V$ . Conversely let  $W$  be a vector subspace of  $V$ . The proof of (iv) of the above corollary shows how to find a basis of  $W$ . In particular  $W$  is of the form  $\text{span}\{v_1, \dots, v_d\}$ .  $\square$

### 3 Linear functions and matrices

Let  $f: F^n \rightarrow F^k$  be a linear function. Then

$$f(t_1, \dots, t_n) = f\left(\sum_i t_i e_i\right) = \sum_i t_i f(e_i).$$

We can write  $f(e_i)$  in terms of the basis  $e_1, \dots, e_k$  of  $F^k$ : suppose that  $f(e_i) = \sum_{j=1}^k a_{ji} e_j = (a_{1i}, \dots, a_{ki})$ . We can then associate to  $f$  an  $k \times n$  matrix with coefficients in  $F$  as follows: Define

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}.$$

Then the columns of  $A$  are the vectors  $f(e_i)$ .

More generally, suppose that  $V_1$  and  $V_2$  are two finite dimensional vector spaces, and choose bases  $v_1, \dots, v_n$  of  $V_1$  and  $w_1, \dots, w_k$  of  $V_2$ , so that  $n = \dim V_1$  and  $k = \dim V_2$ . If  $f: V_1 \rightarrow V_2$  is linear, then, given the bases  $v_1, \dots, v_n$  and  $w_1, \dots, w_k$  we again get a  $k \times n$  matrix  $A$  by the formula:  $A = (a_{ij})$ , where  $a_{ij}$  is defined by

$$f(v_i) = \sum_{j=1}^k a_{ji} w_j.$$

We say that  $A$  is the matrix associated to the linear map  $f$  and the bases  $v_1, \dots, v_n$  and  $w_1, \dots, w_k$ .

With the understanding that we have to choose bases to define the matrix associated to a linear map, composition of linear maps corresponds to multiplication of matrices. In particular, let  $f: V \rightarrow V$  be a linear map from a finite dimensional vector space  $V$  to itself. In this case, it is simplest to fix one basis  $v_1, \dots, v_n$  for  $V$ , viewing  $V$  as both the domain and range of  $f$ , and write  $A = (a_{ij})$  where  $f(v_i) = \sum_{j=1}^n a_{ji} v_j$ . Again, having fixed the basis  $v_1, \dots, v_n$  once and for all, linear maps from  $V$  to itself correspond to  $n \times n$  matrices and composition to matrix multiplication. Finally, we can define the determinant  $\det A$  of an  $n \times n$  matrix with coefficients in  $F$  by the usual formulas (for example, expansion by minors). Moreover, the  $n \times n$  matrix  $A$  is invertible  $\iff \det A \neq 0$ , and in this case there is an explicit formula for  $A^{-1}$  (Cramer's rule).