Chapter 4

The Theory of Finite Dimensional Vector Spaces

4.1 Some Basic concepts

Vector spaces which are spanned by a finite number of vectors are said to be *finite dimensional*. The purpose of this chapter is explain the elementary theory of such vector spaces, including linear independence and notion of the dimension. Indeed, the development of a workable definition for this notion was one of the first important achievements in basic algebra. We will also explain the construction of a number basic vector spaces such as direct sums, duals and quotients.

4.1.1 The Intuitive Notion of Dimension

Roughly speaking, the dimension of a vector space should describe the number of degrees of freedom an inhabitant of the space has. It is clear what this means for for subsets of $\mathbb{R}^n$ provided $n = 1, 2$ or 3. For example, the path traced out by a point moving smoothly through $\mathbb{R}^3$ is intuitively one dimensional. A smooth surface without any thickness is a two dimensional object. (On the other hand, the notion of the dimension of non-smooth paths and surfaces can be very hard to formulate. In fact, such dimensions may turn out to real, that is non-integral.) The objects we will be treating here, however, are linear, and we will see that their dimensions are defined in a natural way.

In particular, we will see that any subspace of $\mathbb{F}^n$ is finite dimensional. Since our intuition tells us that $\mathbb{R}^1$, $\mathbb{R}^2$ and $\mathbb{R}^3$ should have dimensions one,

two and three respectively, we should expect that our final definition will have the property that the dimension of $\mathbb{R}^n$ is n. Thus, the dimension of $\mathbb{F}^n$ should also be n.

4.1.2 Linear Independence

Let V denote a vector space over a field $\mathbb{F}$. Before defining the notion of the dimension of V, we need to discuss the concept of linear independence. One way of putting the definition is to say that a set of vectors is linearly independent if no one of them can be expressed as a linear combination of the others. This means that if you have two vectors, they are linearly independent when they don't lie on the same line through the origin (i.e. they aren't collinear), and three vectors are linearly independent when they don't all lie on a plane through the origin. (Of course, any three vectors lie on a plane, but the plane will not necessarily contain the origin.) Thus the situation of two, three or any finite number of vectors failing to be linearly independent will involve a constraint. Let us now formulate a definition.

Definition 4.1. Let $\mathbf{w}_1, \ldots, \mathbf{w}_k$ in V. Then we say that $\mathbf{w}_1, \ldots, \mathbf{w}_k$ are *linearly independent* (or, simply, *independent*) if and only if the vector equation

$$x_1\mathbf{w}_1 + x_2\mathbf{w}_2 + \cdots + x_k\mathbf{w}_k = \mathbf{0} \tag{4.1}$$

has only the trivial solution $x_1 = x_2 = \cdots = x_k = 0$. If a non trivial solution exists, we will call the vectors *linearly dependent* (or, simply, *dependent*).

One of the first things to notice is any set of vectors in V that includes $\mathbf{0}$ is dependent (why?). We begin with a reformulation of the concept of independence.

Proposition 4.1. *A set of vectors is linearly dependent if and only if one of them can be expressed as a linear combination of the others.*

Proof. Suppose first that one of the vectors, say $\mathbf{w}_1$, is a linear combination of the others. That is

$$\mathbf{w}_1 = a_2\mathbf{w}_2 + \cdots + a_k\mathbf{w}_k.$$

Thus

$$\mathbf{w}_1 - a_2\mathbf{w}_2 - \cdots - a_k\mathbf{w}_k = \mathbf{0},$$

so (4.1) has a solution with $x_1 = 1$, thus a non trivial solution. Therefore $\mathbf{w}_1, \ldots, \mathbf{w}_k$ are dependent. Conversely, suppose $\mathbf{w}_1, \ldots, \mathbf{w}_k$ are dependent.

This means that there is a solution $x_1, x_2, \ldots, x_k$ of (4.1), where some $x_i \neq 0$. We can assume (just by reordering the vectors) that the nonzero coefficient is x_1. Then we can write

$$\mathbf{w}_1 = a_2\mathbf{w}_2 + \ldots a_k\mathbf{w}_k,$$

where $a_i = -x_i/x_1$, so the proof is done. □

FIGURE
(LINEARLY DEPENDENT, INDEPENDENT)

The following fact gives one of the important properties of linearly independent sets.

Proposition 4.2. *Assume that $\mathbf{w}_1, \ldots, \mathbf{w}_k$ are linearly independent vectors in V and suppose $\mathbf{v}$ is in their span. Then there is exactly one linear combination of $\mathbf{w}_1, \ldots, \mathbf{w}_k$ which gives $\mathbf{v}$.*

Proof. Suppose $\mathbf{v}$ can be expressed in two ways, say

$$\mathbf{v} = r_1\mathbf{w}_1 + r_2\mathbf{w}_2 + \cdots + r_k\mathbf{w}_k$$

and

$$\mathbf{v} = s_1\mathbf{w}_1 + s_2\mathbf{w}_2 + \cdots + s_k\mathbf{w}_k$$

where the r_i and s_i are all elements of $\mathbb{F}$. By subtracting and doing a bit of algebraic manipulation, we get that

$$\mathbf{0} = \mathbf{v} - \mathbf{v} = (r_1 - s_1)\mathbf{w}_1 + (r_2 - s_2)\mathbf{w}_2 + \cdots + (r_k - s_k)\mathbf{w}_k.$$

Since the $\mathbf{w}_i$ are independent, every coefficient $r_i - s_i = 0$, which proves the Proposition. □

When $V = \mathbb{F}^n$, the definition of linear independence involves considering a linear system. Recalling that vectors in $\mathbb{F}^n$ are viewed as column vectors, consider the $n \times k$ matrix $A = (\mathbf{w}_1 \ \ldots \ \mathbf{w}_k)$. By the theory of linear systems (Chapter 2), we have

Proposition 4.3. *The vectors $\mathbf{w}_1, \ldots, \mathbf{w}_k$ in $\mathbb{F}^n$ are linearly independent exactly when the system $A\mathbf{x} = \mathbf{0}$ has no non trivial solution which is the case exactly when the rank of A is k. In particular, more than n vectors in $\mathbb{F}^n$ are linearly dependent.*

4.1.3 The Definition of a Basis

As usual let V be a vector space over a field $\mathbb{F}$.

Definition 4.2. A collection of vectors in V which is both linearly independent and spans V is called a *basis* of V.

Notice that we have not required that a basis be a finite set. Usually, however, we will deal with vector spaces that have a finite basis. One of the questions we will investigate is whether a finite dimensional vector space has a basis. Of course, $\mathbb{F}^n$ has a basis, namely the standard basis vectors, or, in other words, the columns of the identity matrix I_n over $\mathbb{F}$. A non zero vector in $\mathbb{R}^n$ spans a line, and clearly a single non zero vector is linearly independent. Hence a line has a basis consisting of a single element. A plane P through the origin is spanned by any two non collinear vectors on P, and two any two non collinear vectors on P are linearly independent. Thus P has a basis consisting of two vectors. It should noted that the trivial vector space $\{\mathbf{0}\}$ does not have a basis, since in order to contain a linearly independent subset it has to contain a nonzero vector.

Proposition 4.2 allow us to deduce an elementary property of bases.

Proposition 4.4. *The vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$ in V form a basis of V if and only if every vector $\mathbf{v}$ in V admits a unique expression*

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_r\mathbf{v}_r,$$

where $a_1, a_2, \ldots a_r$ are elements of $\mathbb{F}$.

Proof. We leave this as an exercise. □

Example 4.1. Suppose A is an $m \times n$ matrix over $\mathbb{F}$. The column space $\mathrm{col}(A)$ of A is a subspace of $\mathbb{F}^m$ which we have already considered. Using our new terminology, if A has rank n, then its columns are independent and hence form a basis of the column space. This gives a useful criterion for determining whether or not a given set of vectors in $\mathbb{F}^m$ is a basis of the subspace they span. If the rank of A is less than n, the columns are dependent, so there is still the problem of finding a basis. More generally, this is the problem of extracting a basis from a spanning set that may be dependent. We will solve this for $\mathbb{F}^m$ below.

Example 4.2. Let A be an $m \times n$ matrix over $\mathbb{F}$. As pointed out in Chapter 3, the theory of linear systems, which was developed in Chapter 2 for the case $\mathbb{F} = \mathbb{R}$, extends over word for word to a linear equation (or system) $A\mathbf{x} = \mathbf{b}$ over any field $\mathbb{F}$ and any $A \in \mathbb{F}^{m\times n}$. For example, the fundamental

solutions of $A\mathbf{x} = \mathbf{0}$ are a basis of the null space $\mathcal{N}(A)$, which is a subspace of $\mathbb{F}^n$, and we still have the identity

$$\dim \mathcal{N}(A) = n - \operatorname{rank}(A),$$

which was originally stated in (2.4).

Exercises

Exercise 4.1. Are the vectors $(0,2,1,0)^T$, $(1,0,0,1)^T$ and $(1,0,1,1)^T$ in $\mathbb{R}^4$ are independent? Can they form a basis of $\mathbb{R}^4$?

Exercise 4.2. Are $(0,0,1,0)^T$, $(1,0,0,1)^T$ and $(1,0,1,1)^T$ independent in $\mathbb{F}_2^4$?

Exercise 4.3. Show that any subset of a linearly independent set is linearly independent.

Exercise 4.4. Suppose $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are mutually orthogonal unit vectors in $\mathbb{R}^m$. Show $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are independent.

Exercise 4.5. Show that m independent vectors in $\mathbb{F}^m$ are a basis.

Exercise 4.6. Find a basis for the space $\mathbb{R}[x]$ of all polynomials with real coefficients.

Exercise 4.7. True or False: Four vectors in $\mathbb{R}^3$ are dependent. (Supply reasoning.)

Exercise 4.8. Prove the assertions made in Example 4.2 that the fundamental solutions are a basis of $\mathcal{N}(A)$ and $\dim \mathcal{N}(A) = n - \operatorname{rank}(A)$.

Exercise 4.9. Use the theory of linear systems to show the following:

(i) More than m vectors in $\mathbb{F}^m$ are dependent.

(ii) Fewer than m vectors in $\mathbb{F}^m$ cannot span $\mathbb{F}^m$.

Exercise 4.10. Let $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ be a basis of $\mathbb{R}^3$.

(a) Determine whether or not $3\mathbf{u} + 2\mathbf{v} + \mathbf{w}$, $\mathbf{u} + \mathbf{v} + 0\mathbf{w}$, and $-\mathbf{u} + 2\mathbf{v} - 3\mathbf{w}$ are independent.

(b) Find a general necessary and sufficient condition for the vectors $a_1\mathbf{u} + a_2\mathbf{v} + a_3\mathbf{w}$, $b_1\mathbf{u} + b_2\mathbf{v} + b_3\mathbf{w}$ and $c_1\mathbf{u} + c_2\mathbf{v} + c_3\mathbf{w}$ to be independent, where $a_1, a_2, \ldots, c_3$ are arbitrary scalars.

Exercise 4.11. Find a basis for the set of invertible 3×3 real matrices. (Be careful.)

4.2 Bases and Dimension

We will now (finally) define the notion of dimension and prove the basic results about bases. As we already noted above (see Exercise 4.9) $\mathbb{F}^n$ can't contain more than n independent vectors. Our definition of dimension will in fact amount to saying that the dimension of an $\mathbb{F}$-vector space V is the maximal number of independent vectors. This definition gives the right answer for the dimension of a line (one), a plane (two) and more generally $\mathbb{F}^n$ (n).

4.2.1 The Definition of Dimension

We start with the following definition.

Definition 4.3. Let V be a vector space over an arbitrary field $\mathbb{F}$. Then we say that V is *finite dimensional* if it is spanned by a finite set of vectors.

For the remainder of this section, we will only consider finite dimensional vector spaces.

Definition 4.4. The *dimension* of a finite dimensional vector space V is the number of elements in a basis of V. For convenience, we will define the dimension of the trivial vector space $\{\mathbf{0}\}$ to be 0, even though $\{\mathbf{0}\}$ doesn't have a basis. The dimension of V will be denoted by $\dim V$ or by $\dim_{\mathbb{F}} V$ in case there is a chance of confusion about which field is being considered.

This definition obviously assumes that a finite dimensional vector space (different from $\{\mathbf{0}\}$) has a basis. Less obviously, it also assumes that any two bases have the same number of elements. Hence, we have to prove these two facts before we know we may use the definition. Thses assertions will be part of the Dimension Theorem, which will be proved below.

In order to get some feeling for the definition, let's consider $\mathbb{F}^n$ as a special case. I claim that if $n > 0$, any basis of $\mathbb{F}^n$ has n elements. In fact, this is just the result of Exercise 4.9, since it says that a basis, being independent, cannot have more than n elements and, being a spanning set, has to have at least n elements. In fact, we can even say more.

Proposition 4.5. *Every basis of $\mathbb{F}^n$ contains exactly n vectors. Moreover, n linearly independent vectors in $\mathbb{F}^n$ span $\mathbb{F}^n$ and hence are a basis. Similarly n vectors in $\mathbb{F}^n$ that span $\mathbb{F}^n$ are also linearly independent and hence are also a basis.*

Proof. We already verified the first statement. Now if $\mathbf{w}_1, \ldots, \mathbf{w}_n$ are independent and $A = (\mathbf{w}_1 \ \ldots \ \mathbf{w}_n)$, then $\mathcal{N}(A) = \{\mathbf{0}\}$, so A has rank n. Since A is $n \times n$, we know A has an inverse, so the system $A\mathbf{x} = \mathbf{b}$ is solvable for any $\mathbf{b} \in \mathbb{F}^n$. Thus $\mathbf{w}_1, \ldots, \mathbf{w}_n$ span $\mathbb{F}^n$. Similarly, if $\mathbf{w}_1, \ldots, \mathbf{w}_n$ span $\mathbb{F}^n$, they have to be independent for the same reason: A is $n \times n$ of rank n. □

There is a slight sublety, however, which is illustrated by what happens when $\mathbb{F} = \mathbb{C}$. Since $\mathbb{C} = \mathbb{R}^2$, $\mathbb{C}^n$ is in some sense the same as $\mathbb{R}^{2n}$. Thus, if we ask what is the dimension of $\mathbb{C}^n$, we see that the answer could be either n or $2n$ and still be consistent with having the dimension of $\mathbb{F}^n$ be n. Hence when we speak of the dimension of $\mathbb{C}^n = \mathbb{R}^{2n}$, we need to differentiate between whether we are speaking of the real dimension (which is $2n$) or the complex dimension (which is n). In other words, $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$ while $\dim_{\mathbb{C}} \mathbb{C}^n = n$.

4.2.2 Some Examples

We now consider some examples.

Example 4.3. Let $\mathbf{e}_i$ denote the ith column of I_n. As mentioned above, the vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are the so called standard basis of $\mathbb{R}^n$. In fact, $\mathbf{e}_1, \ldots, \mathbf{e}_n$ make sense for any field $\mathbb{F}$ and, by the same reasoning, are a basis of $\mathbb{F}^n$.

Example 4.4. The dimension of a line is 1 and that of a plane is 2. The dimension of the hyperplane $a_1x_1 + \cdots + a_nx_n = 0$ in $\mathbb{R}^n$ is $n-1$, provided some $a_i \neq 0$. Note that the $n-1$ fundamental solutions form a basis of the hyperplane.

Example 4.5. Let $A = (\mathbf{w}_1 \ \mathbf{w}_2 \ \ldots \ \mathbf{w}_n)$ be $n \times n$ over $\mathbb{F}$, and suppose A has rank n. Then the columns of A are a basis of $\mathbb{F}^n$. Indeed, the columns span $\mathbb{F}^n$ since we can express an arbitrary $\mathbf{b} \in \mathbb{F}^n$ as a linear combinations of the columns due to the fact that the system $A\mathbf{x} = \mathbf{b}$ is consistent for all $\mathbf{b}$. We are also guaranteed that $\mathbf{0}$ is the unique solution of the system $A\mathbf{x} = \mathbf{0}$. Hence the columns of A are independent. Thus, the columns of an $n \times n$ matrix over $\mathbb{F}^n$ of rank n are a basis of $\mathbb{F}^n$. (Note that we have essentially just repeated part of the proof of Proposition4.5.)

Example 4.6. For any positive integer n, let $\mathcal{P}_n$ denote the space of polynomials with real coefficients of degree at most n (cf. Example 3.7). Let's determine a basis of $\mathcal{P}_3$. Consider the polynomials $1, x, x^2, x^3$. I claim they are linearly independent. To see this, we have to show that if

$$y = \sum_{i=0}^{3} a_i x^i = 0$$

for every x, then each $a_i = 0$. Now if $y = 0$, then

$$y(0) = a_0 = 0,\ y'(0) = a_1 = 0,\ y''(0) = a_2 = 0,\ y'''(0) = a_3 = 0.$$

Hence we have the asserted linear independence. It is obvious that $1, x, x^2, x^3$ span $\mathcal{P}_3$, so our job is done.

Example 4.7. Let $a_1, \ldots, a_m$ be real constants. Then the solution space of the homogeneous linear differential equation

$$y^{(m)} + a_1 y^{(m-1)} + \cdots + a_{m-1} y' + a_m y = 0$$

is a vector space over $\mathbb{R}$. It turns out, by a theorem on differential equations, that the dimension of this space is m. For example, when $m = 4$ and $a_i = 0$ for $1 \leq i \leq 4$, then we are dealing with the vector space $\mathcal{P}_3$ of the last example. The solution space of the equation $y'' + y = 0$ consists of all linear combinations of the functions $\sin x$ and $\cos x$.

4.2.3 The Dimension Theorem

We will next establish the basic result needed to show that the definition of dimension makes sense.

Theorem 4.6 (The Dimension Theorem). *Assume V is a finite dimensional vector space over a field $\mathbb{F}$ containing a non zero vector. Then V has a basis. In fact, any spanning set for V contains a basis, and any linearly independent subset of V is contained in a basis. Moreover, any two bases of V have the same number of elements.*

Proof. We first show every spanning set contains a basis. Let $\mathbf{w}_1, \ldots, \mathbf{w}_k$ span V. Of course, we may certainly assume that every $\mathbf{w}_i \neq \mathbf{0}$. Now consider the set of all subsets of $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ which also span V, and let $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ be any such subset where r is minimal. There is no problem showing this subset exists, since $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ has only 2^k subsets.

I claim that $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are independent. For, if

$$a_1\mathbf{v}_1 + \cdots + a_r\mathbf{v}_r = \mathbf{0},$$

and some $a_i \neq 0$, then

$$\mathbf{v}_i = \frac{-1}{a_i} \sum_{j \neq i} a_j \mathbf{v}_j,$$

so if $\mathbf{v}_i$ is deleted from $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$, we still have a spanning set, which contradicts the minimality of r. Thus $\mathbf{v}_1, \ldots, \mathbf{v}_r$ are independent, so every

spanning set contains a basis. In particular, since V has a finite spanning set, it has a basis.

We next show that any linearly independent set in V can be extended to a basis. Let $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be independent, and put $W = \text{span}\{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. I claim that if $\mathbf{v} \notin W$, then $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}$ are independent. To see this, suppose

$$a_1\mathbf{w}_1 + \cdots + a_m\mathbf{w}_m + b\mathbf{v} = \mathbf{0}.$$

If $b \neq 0$, it follows (as in the last argument) that $\mathbf{v} \in W$, contrary to the choice of $\mathbf{v}$. Thus $b = 0$. But then each $a_k = 0$ also since the $\mathbf{w}_k$ are independent. This proves the claim.

Now suppose $W \neq V$. We will use the basis $\mathbf{v}_1, \ldots, \mathbf{v}_r$ obtained above. If each $\mathbf{v}_i \in W$, then $W = V$ and we are done. Otherwise, let i be the first index such that $\mathbf{v}_i \notin W$. By the previous claim, $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_i$ are independent. Hence they form a basis for $W_1 = \text{span}\{\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{v}_i\}$. Clearly we may continue, at each step adding one of the $\mathbf{v}_j$, if necessary, always maintaining an independent subset of V. Eventually we have to obtain a subspace containing $\mathbf{v}_1, \ldots, \mathbf{v}_r$, so our original independent vectors $\mathbf{w}_1, \ldots, \mathbf{w}_m$ are contained in a basis.

It remains to show that two bases of V have the same number of elements. This is proved by the so called the replacement principle. Suppose $\mathbf{u}_1, \ldots, \mathbf{u}_m$ and $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are two bases of V. Without any loss of generality, suppose $m \leq n$. We can then write

$$\mathbf{v}_1 = r_1\mathbf{u}_1 + r_2\mathbf{u}_2 \cdots + r_m\mathbf{u}_m.$$

Since $\mathbf{v}_1 \neq \mathbf{0}$, some $r_i \neq 0$, so we may suppose, by renumbering indices if necessary, that $r_1 \neq 0$. I claim that this implies that $\mathbf{v}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ is also a basis of V. To see this, we must show $\mathbf{v}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ are independent and span. Suppose that

$$x_1\mathbf{v}_1 + x_2\mathbf{u}_2 \cdots + x_m\mathbf{u}_m = \mathbf{0}.$$

If $x_1 \neq 0$, then

$$\mathbf{v}_1 = y_2\mathbf{u}_2 + \cdots + y_j\mathbf{u}_m,$$

where $y_i = -x_i/x_1$. Since $r_1 \neq 0$, this gives two distinct ways of expanding $\mathbf{v}_1$ in terms of the first basis, which contradicts Proposition 4.4. Hence $x_1 = 0$. It follows immediately that all $x_i = 0$ (why?), so $\mathbf{v}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ are independent. I leave the proof that $\mathbf{v}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ span V as an exercise, hence we have produced a new basis of V where $\mathbf{v}_1$ replaces $\mathbf{u}_1$. I claim that

$\mathbf{u}_2, \ldots, \mathbf{u}_m$ can be renumbered so that $\mathbf{u}_2$ can be replaced by $\mathbf{v}_2$, giving a new basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{u}_3 \ldots, \mathbf{u}_m$ of V. To be explicit, we can write

$$\mathbf{v}_2 = r_1\mathbf{v}_1 + r_2\mathbf{u}_2 \cdots + r_m\mathbf{u}_m.$$

Then there exists an $i > 1$ such that $r_i \neq 0$ (why?). Renumbering so that $i = 2$ and applying the same reasoning as in the previous argument, we get the claim. Continuing this process, we will eventually replace all the $\mathbf{u}_i$'s, which implies that $\mathbf{v}_1, \ldots, \mathbf{v}_m$ must be a basis of V. But if $m < n$, it then follows that $\mathbf{v}_{m+1}$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m$, which contradicts the linear independence of $\mathbf{v}_1, \ldots, \mathbf{v}_n$. This is a contradiction, so we conclude $m = n$, and the Dimension Theorem is proven. □

4.2.4 An Application

Let's begin with an application. Let p be a prime and consider a finite dimensional vector space V over $\mathbb{F} = \mathbb{F}_p$. Then the dimension of V determines the number of elements of V.

Proposition 4.7. *The number of elements of V is exactly $p^{\dim_{\mathbb{F}_p} V}$.*

The proof goes as follows. Let $k = \dim V$ and choose a basis $\mathbf{w}_1, \ldots, \mathbf{w}_k$ of V, which we know is possible. Then every $\mathbf{v} \in W$ has a unique expression

$$\mathbf{v} = a_1\mathbf{w}_1 + a_2\mathbf{w}_2 + \cdots + a_k\mathbf{w}_k$$

where $a_1, a_2, \ldots, a_k$ are scalars, that is, elements of $\mathbb{F}_p$. Now it is simply a matter of counting such expressions. In fact, since $\mathbb{F}_p$ has p elements, there are p choices for each a_i, and, since different choices of the a_i give different elements of V (Proposition4.2), it follows that V contains exactly $p \cdot p \cdots p = p^k$ elements. □

Thus, for example, a line in $\mathbb{F}^n$ has p elements, a plane has p^2 and so forth.

Example 4.8. Consider for example a matrix over $\mathbb{F}_2$, for example

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Let V denote the row space of A, that is the subspace of $\mathbb{F}^4$ spanned by A's rows. Using row operations, A row reduces to the 4×4 identity matrix I_4.

We will see below that row operations leave the row space of A unchanged. Hence we conclude that the row space of A is $\mathbb{F}^4$. The original rows are a basis as are the rows of $A_{red} = I_4$.

We can apply the last result to finite fields. Let $\mathbb{F}$ be any finite field. It is clear that the characteristic of $\mathbb{F}$ is positive (since $\mathbb{F}$ is finite), so suppose it is the prime p. Now this means $\mathbb{F}_p \subset \mathbb{F}$. That is, the multiples of 1 together with 0 form a subfield, which is nothing other than $\mathbb{F}_p$. (This follows in exactly the same way as our original construction of $\mathbb{F}_p$ in Chapter 3.) But since $\mathbb{F}_p \subset \mathbb{F}$, it follows that $\mathbb{F}$ is a vector space over $\mathbb{F}_p$. In fact, since $\mathbb{F}$ is finite, its dimension over $\mathbb{F}_p$ has to be finite. Hence, by Proposition 4.7, we get

Proposition 4.8. *Let $\mathbb{F}$ be a finite field of characteristic p. Then $|\mathbb{F}| = p^n$ where n is the dimension of $\mathbb{F}$ over the prime field $\mathbb{F}_p$.*

Of course, we still do not know that there are finite fields with more than p elements. This question will be settled later. We can however give a simple example.

Example 4.9. The purpose of this example is to define a field $\mathbb{F}$ of order 4. Put $\mathbb{F} = \{0, 1, \alpha, \beta\}$, where $\beta := \alpha + 1$, and require that α be a root of the polynomial $x^2 + x + 1 = 0$. Then, for example, $\alpha\beta = \beta\alpha = 1$, so α and β both have inverses. For $x^2+x+1 = x(x+1)+1$, so $x(x+1) = (x+1)x = 1$. Also, $\alpha^3 = \beta^3 = 1$. Indeed, $\alpha^2 = \beta$, so $\alpha^3 = \alpha\beta = 1$, and similarly for β. I'll leave working out all the details of showing that in fact $\mathbb{F}$ is a field as an Exercise.

4.2.5 Some Further Properties

We next establish some more properties of finite dimensional vector spaces. First of all, we prove a fact that is obvious for $\mathbb{F}^k$.

Proposition 4.9. *Let V be a finite dimensional vector space, say $\dim V = n$. Then any subset of V containing more that n elements is dependent.*

Proof. It suffices to show that any subset of $n+1$ elements of V is dependent. Let $\mathbf{v}_1, \ldots, \mathbf{v}_{n+1}$ be independent and suppose $\mathbf{u}_1, \ldots, \mathbf{u}_n$ give a basis of V. Applying the replacement principle as in the proof of the Dimension Theorem (Theorem 4.6), we get that $\mathbf{v}_1, \ldots, \mathbf{v}_n$ give a basis, so $\mathbf{v}_1, \ldots, \mathbf{v}_{n+1}$ can't be independent. □

We also need to show the not surprising fact that every subspace of a finite dimensional vector space is also finite dimensional.

Proposition 4.10. *Every subspace W of a finite dimensional vector space V is finite dimensional. In particular, for any subspace W of V, $\dim W$ is defined and $\dim W \leq \dim V$.*

Proof. We have to show that W is finite dimensional. Consider any set of independent vectors in W, say $\mathbf{w}_1, \ldots, \mathbf{w}_m$. If these vectors don't span W, then $\mathbf{w}_1, \ldots, \mathbf{w}_m, \mathbf{w}_{m+1}$ are independent for any choice of $\mathbf{w}_{m+1} \in W$ not in the span of $\mathbf{w}_1, \ldots, \mathbf{w}_m$. If $\dim V = n$, then by Proposition 4.9, more than n elements of V are dependent, so it follows that W has to have a finite spanning set with at most n elements. The assertion that $\dim W \leq \dim V$ also follows immediately from Proposition 4.9. □

4.2.6 Extracting a Basis Constructively

Theorem 4.6 guarantees that any spanning set of a finite dimensional vector space contains a basis. In fact, the subsets which give bases are exactly the minimal spanning subsets. Frequently, however, we need an explicit method for actually extracting one of these subsets. There is an explicit method for subspaces of $\mathbb{F}^n$ which is based on row reduction. Suppose $\mathbf{w}_1, \ldots, \mathbf{w}_k \in \mathbb{F}^n$, and let W be the subspace they span. Let us construct a subset of these vectors which spans W. Consider the $n \times k$ matrix $A = (\mathbf{w}_1 \ \ldots \ \mathbf{w}_k)$. We must find columns of A which are a basis of the column space $W = \mathrm{col}(A)$.

Proposition 4.11. *The columns of A that correspond to a corner entry in A_{red} are a basis of the column space $\mathrm{col}(A)$ of A. Therefore, the dimension of $\mathrm{col}(A)$ of A is the rank of A.*

Proof. The key observation is that $A\mathbf{x} = \mathbf{0}$ if and only if $A_{red}\mathbf{x} = \mathbf{0}$ (why?). This says any expression of linear dependence among the columns of A_{red} is also an expression of linear dependence among the columns of A. The converse statement is also true. For example, if column five of A_{red} is the sum of the first four columns of A_{red}, this also holds for the first five columns of A. But it is obvious that the columns of A_{red} containing a corner entry are a basis of the column space of A_{red} (of course, this says nothing about the column space of A). Hence the corner columns are also linearly independent in W. But we just saw that every non corner column in A_{red} is a linear combination of the corner columns of A_{red}, so the same is true for A from what we said above. Therefore, the corner columns in A span W, and the proof is complete. □

This result may seem a little surprising since it involves row reducing A which of course changes $\mathrm{col}(A)$.

Example 4.10. To consider a simple example, let

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 4 & 5 & 8 \\ 7 & 8 & 14 \end{pmatrix}.$$

Then

$$A_{red} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Proposition 4.11 implies the first two columns are a basis of $\mathrm{col}(A)$. Notice that the first and third columns are dependent in both A and A_{red} as the Proposition guarantees. The Proposition says that the first two columns are a basis of the column space, but makes no assertion about the second and third columns, which in fact are also a basis.

4.2.7 The Row Space of A and the Rank of A^T

We now consider the row space of a matrix. The goal of this subsection is to relate the row space to row operations and then to derive a somewhat surprising result: namely that A and A^T have the same rank.

Definition 4.5. The *row space* of an $m \times n$ matrix A over $\mathbb{F}$ is the subspace $\mathrm{row}(A) \subset \mathbb{F}^n$ of A spanned by the rows of A.

The first fact about the row space of a matrix is about how row operations affect the row space (not!). Actually, we already let the cat out of the bag in Example 4.8.

Proposition 4.12. *Elementary row operations leave the row space of A unchanged. Consequently A and A_{red} always have the same row space. Moreover, the non-zero rows of A_{red} are a basis of* $\mathrm{row}(A)$. *Hence the dimension of the row space of A is the rank of A, that is*

$$\dim \mathrm{row}(A) = \mathrm{rank}(A).$$

Proof. The first assertion is equivalent to the statement that for any $m \times m$ elementary matrix E, $\mathrm{row}(EA) = \mathrm{row}(A)$. If E is a row swap or a row dilation, this is clear. So we only have to worry about what happens if E is an elementary row operation of the type III. Suppose E replaces the ith row $\mathbf{r}_i$ by $\mathbf{r'}_i = \mathbf{r}_i + k\mathbf{r}_j$, where $k \neq 0$ and $j \neq i$. Since the rows of EA and A are the same except that $\mathbf{r}_i$ is replaced by $\mathbf{r'}_i$, and since $\mathbf{r'}_i$ is itself a linear combination of two rows of A, every row of EA is a linear combination of

some rows of A. Hence $\text{row}(EA) \subset \text{row}(A)$. But since E^{-1} is also of type III,

$$\text{row}(A) = \text{row}((E^{-1}E)A) = \text{row}(E^{-1}(EA)) \subset \text{row}(EA),$$

so $\text{row}(EA) = \text{row}(A)$. Therefore row operations do not change the row space, and the first claim of the proposition is proved.

It follows that the non zero rows of A_{red} span $\text{row}(A)$. We will be done if the non zero rows of A_{red} are independent. But this holds for the same reason the rows of I_n are independent. Every non zero row of A_{red} has a 1 in the component corresponding to its corner entry, and in this column, all the other rows have a zero. Therefore the only linear combination of the non zero rows which can give the zero vector is the one where every coefficient is zero. Hence the non zero rows of A_{red} are also independent, so they form a basis of $\text{row}(A)$. Thus $\dim \text{row}(A)$ is the number of non zero rows of A_{red}, which is also the number of corners in A_{red}. Therefore, $\dim \text{row}(A) = \text{rank}(A)$, and this completes the proof. □

Here is a surprising corollary.

Corollary 4.13. *For any $m \times n$ matrix A over a field $\mathbb{F}$,*

$$\dim \text{row}(A) = \dim \text{col}(A).$$

Put another way, the ranks of A and A^T are the same.

Proof. We just saw that $\dim \text{row}(A)$ equals $\text{rank}(A)$. But in Proposition 4.11, we also saw that $\dim \text{col}(A)$ also equals $\text{rank}(A)$. Finally, $\text{rank}(A^T) = \dim \text{col}(A^T) = \dim \text{row}(A)$, so we are done. □

This result is unexpected. There would seem to be no connection whatsoever between $\text{row}(A)$ and $\text{col}(A)$. But now we see they have the same dimensions. Let us cap off the discussion with some examples.

Example 4.11. The 3×3 counting matrix C of Example 2.1 has reduced form

$$C_{red} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

The first two rows are a basis of $\text{row}(C)$ since they span $\text{row}(C)$ and are clearly independent (why?).

Example 4.12. Suppose $\mathbb{F} = \mathbb{F}_2$ and

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

A is already reduced so its rows are a basis of row(A), which is thus a three dimensional subspace of $\mathbb{F}^6$. A little combinatorial reasoning will allow us to compute the number of elements in row(A). In fact, the answer was already given by Proposition 4.7. Repeating the argument, there are 3 basis vectors and each has 2 possible coefficients, 0 and 1. Thus there are $2 \cdot 2 \cdot 2 = 2^3$ vectors in all. The 7 non zero vectors are

$$(100111),\ (010101),\ (001011),\ (110010),\ (101100),\ (011110),\ (1111001).$$

Note that all combinations of 0's and 1's occur in the first three components, since the corners are in these columns. In fact, the first three components tell you which linear combination is involved. Examples of this type will come up again in linear coding theory.

Exercises

Exercise 4.12. Find a basis for the subspace of $\mathbb{R}^4$ spanned by

$$(1,0,-2,1),\ (2,-1,2,1),\ (1,1,1,1),\ (0,1,0,1),\ (0,1,1,0)$$

containing the first and fifth vectors.

Exercise 4.13. Consider the matrix $A = \begin{pmatrix} 1 & 2 & 0 & 1 & 2 \\ 2 & 0 & 1 & -1 & 2 \\ 1 & 1 & -1 & 1 & 0 \end{pmatrix}$ as an element of $\mathbb{R}^{3\times 5}$.

(i) Show that the fundamental solutions are a basis of $\mathcal{N}(A)$.

(ii) Find a basis of $\mathrm{col}(A)$.

(iii) Repeat (i) and (ii) when A is considered as a matrix over $\mathbb{F}_3$.

Exercise 4.14. Suppose V is a finite dimensional vector space over a field $\mathbb{F}$, and let W be a subspace of V.

(i) Show that if $\dim W = \dim V$, then $W = V$.

(ii) Show that if $w_1, w_2, \ldots, w_k$ is a basis of W and $v \in V$ but $v \notin W$, then $w_1, w_2, \ldots, w_k, v$ are independent.

Exercise 4.15. Let $\mathbb{F}$ be any field, and suppose V and W are subspaces of $\mathbb{F}^n$.

(i) Show that $V \cap W$ is a subspace of $\mathbb{F}^n$.

(ii) Let $V + W = \{u \in \mathbb{F}^n \mid u = v + w\ \exists v \in V, w \in W\}$. Show that $V + W$ is a subspace of $\mathbb{F}^n$.

Exercise 4.16. Consider the subspace W of $\mathbb{F}_2^4$ spanned by 1011, 0110, and 1001.

(i) Find a basis of W and compute $|W|$.

(ii) Extend your basis to a basis of $\mathbb{F}_2^4$.

Exercise 4.17. Find a basis of the vector space $\mathbb{R}^{n\times n}$ of real $n \times n$ matrices.

Exercise 4.18. A square matrix A over $\mathbb{R}$ is called symmetric if $A^T = A$ and called skew symmetric if $A^T = -A$.
(a) Show that the $n \times n$ symmetric matrices form a subspace of $\mathbb{R}^{n\times n}$, and compute its dimension.
(b) Show that the $n \times n$ skew symmetric matrices form a subspace of $\mathbb{R}^{n\times n}$ and compute its dimension.
(c) Find a basis of $\mathbb{R}^{3\times 3}$ using only symmetric and skew symmetric matrices.

Exercise 4.19. Show that the set of $n \times n$ upper triangular real matrices is a subspace of $\mathbb{R}^{n\times n}$. Find a basis and its dimension.

Exercise 4.20. If A and B are $n \times n$ matrices so that B is invertible (but not necessarily A), show that the ranks of A, AB and BA are all the same.

Exercise 4.21. True or False: $\operatorname{rank}(A) \geq \operatorname{rank}(A^2)$. Explain your answer.

Exercise 4.22. Let W and X be subspaces of a finite dimensional vector space V of dimension n. What are the minimum and maximum dimensions that $W \cap X$ can have? Discuss the case where W is a hyperplane (i.e. $\dim W = n - 1$) and X is a plane (i.e. $\dim X = 2$).

Exercise 4.23. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ be mutually orthogonal unit vectors in $\mathbb{R}^n$. Are $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ a basis of $\mathbb{R}^n$?

Exercise 4.24. Given a subspace W of $\mathbb{R}^n$, define $W^\perp$ to be the set of vectors in $\mathbb{R}^n$ orthogonal to every vector in W. Show that $W^\perp$ is a subspace of $\mathbb{R}^n$ and describe a method for constructing a basis of $W^\perp$.

Exercise 4.25. Let W is a subspace of $\mathbb{R}^n$. Show that

$$\dim(W) + \dim(W^\perp) = n.$$

Exercise 4.26. Suppose W is a subspace of $\mathbb{F}^n$ of dimension k. Show the following:

(i) Any k linearly independent vectors in W span W, hence are a basis of W.

(ii) Any k vectors in W that span W are linearly independent, hence are a basis of W.

Exercise 4.27. Show that the functions

$$1, x, x^2, x^3, \ldots, x^n, \ldots$$

are linearly independent on any open interval (a, b).

Exercise 4.28. Is $\mathbb{R}$ a vector space over $\mathbb{Q}$? If so, is $\dim_{\mathbb{Q}} \mathbb{R}$ finite or infinite?

Exercise 4.29. Write out the addition and multiplication tables for the field with 4 elements described in Example 15.17. Also, show that multiplication is associative.

Exercise 4.30. Let V be a vector space over $\mathbb{F}_p$ of dimension n. Show that the number of linearly independent subsets of V with m elements is exactly $(p^n-1)(p^n-p)\cdots(p^n-p^{m-2})(p^n-p^{m-1})$. (Use Proposition 4.7 and use part of the proof of the Dimension Theorem.)

Exercise 4.31. Use Exercise 4.30 to show that the number of subspaces of dimension m in an n-dimensional vector space V over $\mathbb{F}_p$ is

$$\frac{(p^n-1)(p^n-p)\cdots(p^n-p^{m-2})(p^n-p^{m-1})}{(p^m-1)(p^m-p)\cdots(p^n-p^{m-2})(p^m-p^{m-1})}.$$

Note: the set of m-dimensional subspaces of a finite dimensional vector space is an important object called a Grassmannian. We will give the general construction of the Grassmannians in Chapter 16.

4.3 Some General Vector Space Constructions

In this section, we consider some of the standard ways of constructing new vector spaces: intersections, internal and external sums and quotients. We also will derive an interesting formula (the Hausdorff Intersection Formula) relating the dimensions of some of these spaces.

4.3.1 Intersections

Let V be a vector space over a field $\mathbb{F}$ with subspaces W and Y.

The most obvious way of building a new subspace is by taking the intersection $W \cap Y$.

Proposition 4.14. *The intersection $W \cap Y$ of the subspaces W and Y of V is also a subspace of V. More generally, the intersection of any number of subspaces of V is also a subspace.*

Proof. This is a simple exercise. □

Proposition 4.14 is simply a generalization of the fact that the solution space of a homogeneous linear system is a subspace of $\mathbb{F}^n$, the solution space is the intersection of a finite number of hyperplanes in $\mathbb{F}^n$, where each hyperplane is given by a homogeneous linear equation.

4.3.2 External and Internal Sums

First of all, let V and W be arbitrary vector spaces over the same field $\mathbb{F}$.

Definition 4.6. The *external direct sum* of V and W is the vector space denoted by $V \times W$ consisting of all pairs $(\mathbf{v}, \mathbf{w})$, where $\mathbf{v} \in V$ and $\mathbf{w} \in W$. Addition is defined by

$$(\mathbf{v}_1, \mathbf{w}_1) + (\mathbf{v}_2, \mathbf{w}_2) = (\mathbf{v}_1 + \mathbf{v}_2, \mathbf{w}_1 + \mathbf{w}_2),$$

and scalar multiplication is defined by

$$r(\mathbf{v}, \mathbf{w}) = (r\mathbf{v}, r\mathbf{w}).$$

Of course, the wide awake reader will note that $\mathbb{F} \times \mathbb{F}$ is nothing else than $\mathbb{F}^2$, while $\mathbb{F}^k \times \mathbb{F}^m = \mathbb{F}^{k+m}$. Thus the external direct sum is a generalization of the construction of $\mathbb{F}^n$. This operation can also be extended (inductively) to any number of vector spaces over $\mathbb{F}$. In fact, with this in mind, it should be clear that $\mathbb{F}^n$ is just the n-fold external direct sum of $\mathbb{F}$. It is also frequently called the n-fold Cartesian product of $\mathbb{F}$.

Note also that V and W can both be considered (in a natural way) as subspaces of $V \times W$ (why?).

Proposition 4.15. *If V and W are finite dimensional vector spaces over $\mathbb{F}$, then so is their external direct sum, and* $\dim(V \times W) = \dim V + \dim W$.

Proof. We leave this as an exercise. □

Now suppose W and Y are subspaces of the same vector space V. Then we can form the internal sum of W and Y.

Definition 4.7. The *internal sum* or simply *sum* of W and Y is the set

$$W + Y = \{\mathbf{w} + \mathbf{y} \mid \mathbf{w} \in W, \mathbf{y} \in Y\}.$$

More generally, we can in the same way form the sum of an arbitrary (finite) number of subspaces $V_1, V_2, \cdots, V_k$ of V. The sum $V_1 + \cdots + V_k$ is usually abbreviated as $\sum_{i=1}^{k} V_i$ or more simply as $\sum V_i$.

Proposition 4.16. *The sum $W = \sum_{i=1}^{k} V_i$ of the subspaces $V_1, V_2, \cdots, V_k$ of V is also a subspace of V. In fact, W is the smallest subspace of V containing each V_i.*

Proof. We leave the proof as an exercise. □

4.3.3 The Hausdorff Intersection Formula

We now ask a more interesting question: what are the dimensions of the sum $W + Y$ and the intersection $W \cap Y$ of two subspaces W and Y of V? It turns out that each depends on the other. The relation between them is called the Hausdorff Intersection Formula.

Theorem 4.17. *If W and Y are subspaces of a finite dimensional vector space V, then*

$$\dim(W + Y) = \dim W + \dim Y - \dim(W \cap Y). \tag{4.2}$$

Proof. We know $W \cap Y$ is a subspace of V, so, since V is finite dimensional, Proposition 4.9 and the Dimension Theorem tells us that $W \cap Y$ has a basis, say $\mathbf{x}_1, \ldots, \mathbf{x}_k$. We also know, by the Dimension Theorem again, that we can extend this basis to a basis of W, say $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{w}_{k+1}, \ldots, \mathbf{w}_{k+r}$, and we can do likewise for Y, getting say $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_{k+s}$. I claim

$$\mathcal{B} = \{\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{w}_{k+1}, \ldots, \mathbf{w}_{k+r}, \mathbf{y}_{k+1}, \ldots, \mathbf{y}_{k+s}\}$$

is a basis of $W + Y$. It is not hard to see that $\mathcal{B}$ spans, so we leave this to the reader. To see $\mathcal{B}$ is independent, suppose

$$\sum_{i=1}^{k} \alpha_i \mathbf{x}_i + \sum_{j=k+1}^{k+r} \beta_j \mathbf{w}_j + \sum_{m=k+1}^{k+s} \gamma_m \mathbf{y}_m = \mathbf{0}. \tag{4.3}$$

Thus

$$\sum \gamma_m \mathbf{y}_m = -\big(\sum \alpha_i \mathbf{x}_i + \sum \beta_j \mathbf{w}_j\big) \in V.$$

In other words,

$$\sum \gamma_m \mathbf{y}_m \in Y \cap W.$$

Thus

$$\sum \gamma_m \mathbf{y}_m = \sum \delta_i \mathbf{x}_i$$

for some $\delta_i \in \mathbb{F}$. Hence

$$\sum \delta_i \mathbf{x}_i + \sum (-\gamma_m) \mathbf{y}_m = \mathbf{0}.$$

Therefore, all the δ_i and γ_m are zero. In particular, (4.3) becomes the expression

$$\sum \alpha_i \mathbf{x}_i + \sum \beta_j \mathbf{v}_j = \mathbf{0}.$$

Thus all the α_i and β_j are 0 also, consequently, $\mathcal{B}$ is independent. Since $\mathcal{B}$ spans $W + Y$, it forms a basis of $W + Y$, so $\dim(W + Y) = k + r + s$. To finish the proof, we need to count dimensions. We have

$$\dim(W + Y) = k + r + s = (k + r) + (k + s) - k,$$

which is exactly $\dim W + \dim Y - \dim(W \cap Y)$. □

This leads to a deeper understanding of how subspaces intersect.

Corollary 4.18. *If W and Y are subspaces of V, then*

$$\dim(W \cap Y) \geq \dim W + \dim Y - \dim V. \tag{4.4}$$

In particular, if $\dim W + \dim Y > \dim V$, then $\dim(Y \cap W) > 0$.

Proof. Since W and Y are both subspaces of V, $\dim(W + Y) \leq \dim V$. Now substitute this into the Hausdorff Formula (4.2). □

Example 4.13. Let us illustrate a typical application of (4.4). I claim that the intersection $P_1 \cap P_2$ of two planes in $\mathbb{R}^3$ has to contain a line. For $\dim(P_1 + P_2) \geq 2 + 2 - 3 = 1$. More generally, the intersection $H_1 \cap H_2$ of two hyperplanes in $\mathbb{R}^n$ has dimension at least $2(n-1) - n = n - 2$, hence it contains an $(n-2)$-dimensional subspace. On the other hand, the intersection of two planes in $\mathbb{R}^4$ does not have to contain a line since $2 + 2 - 4 = 0$.

4.3.4 Internal Direct Sums

The final concept in this section is the notion of an internal direct sum. As usual, let V be a vector space over $\mathbb{F}$ with subspaces W and Y.

Definition 4.8. We say that V is the *internal direct sum* (or simply the *direct sum*) of W and Y if $V = W + Y$ and for any $\mathbf{v} \in V$, the expression $\mathbf{v} = \mathbf{w} + \mathbf{y}$ with $\mathbf{w} \in W$ and $\mathbf{y} \in Y$ is unique. If V is the internal direct sum of W and Y, we write $V = W \oplus Y$. More generally, we say V is the direct sum of a collection of subspaces $V_1, \ldots, V_k$ if $V = \sum V_i$ and for any $\mathbf{v} \in V$, the expression $\mathbf{v} = \sum \mathbf{v}_i$, where each $\mathbf{v}_i \in V_i$, is unique. In this case, we write $V = \bigoplus_{i=1}^{k} V_i$.

Proposition 4.19. *Suppose V is finite dimensional. Then a necessary and sufficient condition that $V = W \oplus Y$ is that $V = W + Y$ and $W \cap Y = \{\mathbf{0}\}$. Equivalently, $V = W \oplus Y$ if and only if $\dim V = \dim W + \dim Y$ and $\dim(W \cap Y) = 0$.*

Proof. First, assume $V = W + Y$ and $W \cap Y = \{\mathbf{0}\}$. To see $V = W \oplus Y$, let $\mathbf{v}$ have two expressions $\mathbf{v} = \mathbf{w} + \mathbf{y} = \mathbf{w}' + \mathbf{y}'$. Then $\mathbf{w} - \mathbf{w}' = \mathbf{y}' - \mathbf{y}$ is an element of $W \cap Y = \{\mathbf{0}\}$, so $\mathbf{w} = \mathbf{w}'$ and $\mathbf{y}' = \mathbf{y}$. Hence $V = W \oplus Y$. On the other hand, if $V = W \oplus Y$ and $W \cap Y \neq \{\mathbf{0}\}$, then any non-zero $\mathbf{w} \in W \cap Y$ has two expressions $\mathbf{w} = \mathbf{w} + \mathbf{0} = \mathbf{0} + \mathbf{w}$. This violates the definition of a direct sum, so $W \cap Y = \{\mathbf{0}\}$.

Next, suppose $\dim V = \dim W + \dim Y$ and $\dim(W \cap Y) = 0$. Then, by the Hausdorff Intersection Formula, $\dim(W + Y) = \dim W + \dim Y$. Thus $W + Y$ is a subspace of V having the same dimension as V. Therefore $V = W + Y$. Since $\dim(W \cap Y) = 0$, we have $V = W \oplus Y$. The converse is proved by reversing this argument. □

We can extend Proposition4.19 to any number of subspaces as follows.

Proposition 4.20. *Suppose V is finite dimensional and $V_1, \ldots, V_k$ are subspaces. Then $V = \bigoplus_{i=1}^{k} V_i$ if and only if $V = \sum V_i$ and for every index i,*

$$V_i \cap \Big(\sum_{j \neq i} V_j \Big) = \{\mathbf{0}\}.$$

If $\sum V_i = V$ and $\sum_{i=1}^{k} \dim V_i = \dim V$, then $V = \bigoplus_{i=1}^{k} V_i$.

Proof. We leave this as an exercise. □

Example 4.14. In the last section, we defined the orthogonal complement $V^\perp$ of a subspace V of $\mathbb{R}^n$. Recall,

$$V^\perp = \{\mathbf{w} \in \mathbb{R}^n \mid \mathbf{w} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in V\}.$$

Orthogonal complements in $\mathbb{R}^n$ provide examples of direct sums, since as we saw in Exercise 4.24, $\dim V + \dim V^\perp = n$ and $V \cap V^\perp = \{\mathbf{0}\}$ (why?). Thus, for any V,

$$\mathbb{R}^n = V \oplus V^\perp. \tag{4.5}$$

4.4 Vector Space Quotients

The final topic in this chapter is the construction of the quotient of a vector space V by a subspace W. This is a new vector space denoted as V/W. In a certain sense (despite the notation), V/W can be thought of as subtracting W from V. (Not too much should be read into this claim. Its meaning will be made clearer later.)

4.4.1 Equivalence Relations

The notion of a quotient occurs in many different contexts in algebra. It is surely one of the most fundamental ideas in the area. It is based on the idea of a equivalence relation on a set. First, recall that if S and T are sets, the *product* $S \times T$ (as defined in the previous section) is the set of all pairs (s, t), where $s \in S$ and $t \in T$.

Definition 4.9. Let S be a non-empty set. A subset E of $S \times S$ is called a *relation on* S. If E is a relation on S, and a and b are elements of S, we will say a and b are *related* by E and write aEb if and only if $(a, b) \in E$. A relation E on S is called an *equivalence relation on* S when the following three conditions hold for all $a, b, c \in S$:

(i) (reflexivity) aEa,

(ii) (symmetry) if aEb, then bEa, and

(iii) (transitivity) if aEb and bEc, then aEc.

If E is an equivalence relation on S and $a \in S$, then the *equivalence class of* a is defined to be the set of all elements $b \in S$ such that bEa.

Proposition 4.21. *If E is an equivalence relation on S, every element $a \in S$ is in an equivalence class, and two equivalence classes are either disjoint or equal. Therefore S is the disjoint union of the equivalence classes of E.*

Proof. Every element is equivalent to itself, so S is the union of its equivalence classes. We have to show that if two equivalence classes C and C' contain a common element a, then $C = C'$. Let C and C' be two equivalence classes. If $a \in C \cap C'$, then for any $c \in C$ and $c' \in C'$, we have aEc and aEc'. By (ii) and (iii), it follows that cEc'. Hence every element equivalent to c is equivalent c', and conversely. Thus $C = C'$. □

4.4.2 Cosets

Now let V be a vector space over $\mathbb{F}$ and let W be a subspace. We are going to use W to define an equivalence relation on V. Then V/W will be the set of equivalence classes. The definition is given in the following Proposition.

Proposition 4.22. *Let V be a vector space over $\mathbb{F}$ and let W be a subspace. Given $\mathbf{v}$ and $\mathbf{y}$ in V, let us say that $\mathbf{v}E_W\mathbf{y}$ if and only if $\mathbf{v}-\mathbf{y}\in W$. Then E_W is an equivalence relation on V.*

Proof. Clearly $\mathbf{v}E_W\mathbf{v}$ since $\mathbf{v}-\mathbf{v}=\mathbf{0}\in W$. If $\mathbf{v}E_W\mathbf{y}$, then $\mathbf{y}E_W\mathbf{v}$ since W is closed under scalar multiplication. Finally, if $\mathbf{v}E_W\mathbf{y}$ and $\mathbf{y}E_W\mathbf{z}$, then $\mathbf{v}E_W\mathbf{z}$ since $\mathbf{v}-\mathbf{z}=(\mathbf{v}-\mathbf{y})+(\mathbf{y}-\mathbf{z})$ and W is closed under sums. Hence E_W is an equivalence relation on V. □

Definition 4.10. Let $\mathbf{v}\in V$ be fixed. Then the *coset* of W containing $\mathbf{v}$ is defined to be the set

$$\mathbf{v}+W=\{\mathbf{v}+\mathbf{w}\mid \mathbf{w}\in W\}. \tag{4.6}$$

The notion of a coset is nothing complicated. For example, if $V=\mathbb{R}^3$ and W is a plane through $\mathbf{0}$, then the coset $\mathbf{v}+W$ is simply the plane through $\mathbf{v}$ parallel to W.

Proposition 4.23. *The equivalence classes of the equivalence relation E_W on V are precisely the cosets of W. In particular, $\mathbf{v}+W=\mathbf{y}+W$ if and only if $\mathbf{v}-\mathbf{y}\in W$.*

Proof. Let C denote the equivalence class of $\mathbf{v}$ and consider the coset $\mathbf{v}+W$. If $\mathbf{y}E_W\mathbf{v}$, then $\mathbf{y}-\mathbf{v}=\mathbf{w}\in W$. Hence $\mathbf{y}=\mathbf{v}+\mathbf{w}$, so $\mathbf{y}\in\mathbf{v}+W$. Therefore $C\subset\mathbf{v}+W$. Arguing in reverse, we also conclude that $\mathbf{v}+W\subset C$. □

We now define the quotient space V/W to be the set of all cosets of W. We want to show that cosets can be added. Given two cosets $(\mathbf{v}+W)$ and $(\mathbf{y}+W)$, define their sum by

$$(\mathbf{v}+W)+(\mathbf{y}+W)=(\mathbf{v}+\mathbf{y})+W. \tag{4.7}$$

In order that this addition be a binary operation on V/W, we have to show that the rule (4.7) is independent of the way we write each coset. That is, suppose we have $\mathbf{v}+W=\mathbf{v}'+W$ and $\mathbf{y}+W=\mathbf{y}'+W$. Then we have to show that $(\mathbf{v}+\mathbf{y})+W=(\mathbf{v}'+\mathbf{y}')+W$. But this is so if and only if

$$(\mathbf{v}+\mathbf{y})-(\mathbf{v}'+\mathbf{y}')\in W,$$

which indeed holds since

$$(\mathbf{v}+\mathbf{y})-(\mathbf{v}'+\mathbf{y}')=(\mathbf{v}-\mathbf{v}')+(\mathbf{y}-\mathbf{y}').$$

Therefore, addition is well defined. Scalar multiplication on cosets is defined by

$$a(\mathbf{v}+W)=a\mathbf{v}+W. \tag{4.8}$$

A similar argument shows that this scalar multiplication is well defined.

We can now define the quotient vector space V/W and prove one of its main properties.

Theorem 4.24. *Let V be a vector space over a field $\mathbb{F}$ and suppose W is a subspce of V. Define V/W to be the set of cosets of W in V with addition and scalar multiplication defined as in (4.7) and (4.8). Then V/W is a vector space over $\mathbb{F}$. If V is finite dimensional, then*

$$\dim V/W=\dim V-\dim W.$$

Proof. The fact that V/W satisfies the vector space axioms is straightforward, so we will omit most of the details. The zero element is $\mathbf{0}+W$, and the additive inverse $-(\mathbf{v}+W)$ of $\mathbf{v}+W$ is $-\mathbf{v}+W$. Properties such as associativity and commutativity of addition follow from corresponding properties in V.

To check the dimension formula, first choose a basis $\mathbf{w}_1,\dots,\mathbf{w}_k$ of W, and extend this to a basis

$$\mathbf{w}_1,\dots,\mathbf{w}_k,\mathbf{v}_1,\dots,\mathbf{v}_{n-k}$$

of V. Then I claim the cosets $\mathbf{v}_1+W,\dots,\mathbf{v}_{n-k}+W$ are a basis of V/W. To see they are independent, put $\mathbf{v}_i+W=\alpha_i$ if $1\le i\le n-k$, and suppose there exist $a_1,\dots,a_{n-k}\in\mathbb{F}$ such that $\sum a_i\alpha_i=\mathbf{0}+W$. This means that $\sum_{i=1}^{n-k}a_i\mathbf{v}_i\in W$. Hence there exist $b_1,\dots,b_k\in\mathbb{F}$ such that

$$\sum_{i=1}^{n-k}a_i\mathbf{v}_i=\sum_{j=1}^{k}b_j\mathbf{w}_j.$$

But the fact that the $\mathbf{v}_i$ and $\mathbf{w}_j$ comprise a basis of V implies that all a_i and b_j are zero. Therefore we have the independence. We leave the fact that $\alpha_1,\dots,\alpha_{n-k}$ span V/W as an exercise. □

Exercises

Exercise 4.32. Prove that the cosets $\alpha_1, \ldots, \alpha_{n-k}$ defined in the proof of Theorem 4.24 span V/W.

Exercise 4.33. Let V be a vector space over a finite field $\mathbb{F}_q$, where $q = p^n$, and let W be a subspace. How many cosets does W have?

Exercise 4.34. Let W be the subspace of $V = V(4, 2)$ spanned by 1001, 1101, and 0110. Write down all elements of W, and find a complete set of coset representatives for V/W. That is, find an element in each coset.

Exercise 4.35. Let A and B be arbitrary subsets of a vector space V over $\mathbb{F}$. Define their Minkowski sum to be

$$A + B = \{\mathbf{x} + \mathbf{y} \mid \mathbf{x} \in A, \quad \mathbf{y} \in B\}.$$

Show that if A and B are cosets of a subspace W of V, then so is $A + B$.

Exercise 4.36. Let V and W be any two subspaces of $\mathbb{F}^n$.

(i) Use the Hausdorff Intersection Formula to derive a formula for the quotient vector space $(V + W)/W$.

(ii) Are $(V + W)/W$ and $V/(V \cap W)$ isomorphic as vector spaces over $\mathbb{F}$? Explain.

Exercise 4.37. Find a basis of the quotient $\mathbb{R}^4/W$, where W is the subspace of $\mathbb{R}^4$ spanned by $(1, 2, 0, 1)$ and $(0, 1, 1, 0)$.

4.5 Summary

In the previous chapter, we introduced the notion of a vector space V over an arbitrary field. The purpose of this chapter was to learn some of the basic theory of vector spaces. The main topics we considered were the twin concepts of bases and dimension. A basis of V is a subset $\mathcal{B}$ of V such that every vector in V can be uniquely expressed as a linear combination of elements of $\mathcal{B}$. That is, $\mathcal{B}$ spans and is linearly independent. The main fact is that if V is finite dimensional (it is spanned by a finite subset), then any two bases have the same number of vectors. Thus the dimension of a finite dimensional V can be defined as the number of elements in a basis of V. There are two other ways of thinking about a basis. It is a minimal spanning set and a maximal linearly independent subset of V.

After we covered dimension theory, we considered several examples such as the row and column spaces of a matrix. These turned out to have the same dimension, a very surprising fact. We also constructed some new vector spaces and computed their dimensions. For example, if U and W are subspaces of V, we defined the sum $U + W$ which is a new subspace of V and computed $\dim(U + W)$. The answer is given by the Hausdorff Intersection Formula. We also defined what it means to say V is the direct sum of subspaces U and W and gave examples.

If W is a subspace of V, we may also form the quotient space V/W whose elements are called the cosets of W. Its dimension is $\dim V - dim W$. The notion of a quotient vector space uses the important fundamental idea of an equivalence relation. The idea of constructing a quotient vector space is a fundamental one, which is under constant use. Finally, we still need to derive some simple but messy formulas for changing basis. This will be done with great care in the next chapter.