CHAPTER III

Vector Spaces

As usual, a collection of objects will be called a **set**. A member of the collection is also called an **element** of the set. It is useful in practice to use short symbols to denote certain sets. For instance we denote by $\mathbf{R}$ the set of all numbers. To say that "x is a number" or that "x is an element of $\mathbf{R}$" amounts to the same thing. The set of n-tuples of numbers will be denoted by $\mathbf{R}^n$. Thus "X is an element of $\mathbf{R}^n$" and "X is an n-tuple" mean the same thing. Instead of saying that u is an element of a set S, we shall also frequently say that u **lies in** S and we write $u \in S$. If S and S' are two sets, and if every element of S' is an element of S, then we say that S' is a **subset** of S. Thus the set of rational numbers is a subset of the set of (real) numbers. To say that S is a subset of S' is to say that S is part of S'. To denote the fact that S is a subset of S', we write $S \subset S'$.

If S_1, S_2 are sets, then the **intersection** of S_1 and S_2, denoted by $S_1 \cap S_2$, is the set of elements which lie in both S_1 and S_2. The **union** of S_1 and S_2, denoted by $S_1 \cup S_2$, is the set of elements which lie in S_1 or S_2.

III, §1. Definitions

In mathematics, we meet several types of objects which can be added and multiplied by numbers. Among these are vectors (of the same dimension) and functions. It is now convenient to define in general a notion which includes these as a special case.

A **vector space** V is a set of objects which can be added and multiplied by numbers, in such a way that the sum of two elements of V is again an element of V, the product of an element of V by a number is an element of V, and the following properties are satisfied:

VS 1. *Given the elements u, v, w of V, we have*

$$(u + v) + w = u + (v + w).$$

VS 2. *There is an element of V, denoted by O, such that*

$$O + u = u + O = u$$

for all elements u of V.

VS 3. *Given an element u of V, the element $(-1)u$ is such that*

$$u + (-1)u = O.$$

VS 4. *For all elements u, v of V, we have*

$$u + v = v + u.$$

VS 5. *If c is a number, then $c(u + v) = cu + cv$.*

VS 6. *If a, b are two numbers, then $(a + b)v = av + bv$.*

VS 7. *If a, b are two numbers, then $(ab)v = a(bv)$.*

VS 8. *For all elements u of V, we have $1 \cdot u = u$ (1 here is the number one).*

We have used all these rules when dealing with vectors, or with functions but we wish to be more systematic from now on, and hence have made a list of them. Further properties which can be easily deduced from these are given in the exercises and will be assumed from now on.

The algebraic properties of elements of an arbitrary vector space are very similar to those of elements of $\mathbf{R}^2$, $\mathbf{R}^3$, or $\mathbf{R}^n$. Consequently it is customary to call elements of an arbitrary vector space also **vectors**.

If u, v are vectors (i.e. elements of the arbitrary vector space V), then the sum

$$u + (-1)v$$

is usually written $u - v$. We also write $-v$ instead of $(-1)v$.

Example 1. Fix two positive integers m, n. Let V be the set of all $m \times n$ matrices. We also denote V by $\mathrm{Mat}(m \times n)$. Then V is a vector space. It is easy to verify that all properties **VS 1** through **VS 8** are satisfied by our rules for addition of matrices and multiplication of matrices by numbers. The main thing to observe here is that addition of matrices is defined in terms of the components, and for the addition of components, the conditions analogous to **VS 1** through **VS 4** are satisfied. They are standard properties of numbers. Similarly, **VS 5** through **VS 8** are true for multiplication of matrices by numbers, because the corresponding properties for the multiplication of numbers are true.

Example 2. Let V be the set of all functions defined for all numbers. If f, g are two functions, then we know how to form their sum $f + g$. It is the function whose value at a number t is $f(t) + g(t)$. We also know how to multiply f by a number c. It is the function cf whose values at a number t is $cf(t)$. In dealing with functions, we have used properties **VS 1** through **VS 8** many times. We now realize that the set of functions is a vector space.

The function f such that $f(t) = 0$ **for all** t is the **zero function**. We emphasize the condition for all t. If a function has some of its values equal to zero, but other values not equal to 0, then it is **not** the zero function.

In practice, a number of elementary properties concerning addition of elements in a vector space are obvious because of the concrete way the vector space is given in terms of numbers, for instance as in the previous two examples. We shall now see briefly how to prove such properties just from the axioms.

It is possible to add several elements of a vector space. Suppose we wish to add four elements, say u, v, w, z. We first add any two of them, then a third, and finally a fourth. Using the rules **VS 1** and **VS 4**, we see that it does not matter in which order we perform the additions. This is exactly the same situation as we had with vectors. For example, we have

$$\begin{aligned}((u + v) + w) + z &= (u + (v + w)) + z\\ &= ((v + w) + u) + z\\ &= (v + w) + (u + z), \quad \text{etc.}\end{aligned}$$

Thus it is customary to leave out the parentheses, and write simply

$$u + v + w + z.$$

The same remark applies to the sum of any number n of elements of V.

We shall use 0 to denote the number zero, and O to denote the element of any vector space V satisfying property **VS 2**. We also call it zero, but there is never any possibility of confusion. We observe that this zero element O is uniquely determined by condition **VS 2**. Indeed, if

$$v + w = v$$

then adding $-v$ to both sides yields

$$-v + v + w = -v + v = O,$$

and the left-hand side is just $O + w = w$, so $w = O$.

Observe that for any element v in V we have

$$0v = O.$$

Proof.

$$O = v + (-1)v = (1 - 1)v = 0v.$$

Similarly, if c is a number, then

$$cO = O.$$

Proof. We have $cO = c(O + O) = cO + cO$. Add $-cO$ to both sides to get $cO = O$.

Subspaces

Let V be a vector space, and let W be a subset of V. Assume that W satisfies the following conditions.

(i) If v, w are elements of W, their sum $v + w$ is also an element of W.

(ii) If v is an element of W and c a number, then cv is an element of W.

(iii) The element O of V is also an element of W.

Then W itself is a vector space. Indeed, properties **VS 1** through **VS 8**, being satisfied for all elements of V, are satisfied also for the elements of W. We shall call W a **subspace** of V.

Example 3. Let $V = \mathbf{R}^n$ and let W be the set of vectors in V whose last coordinate is equal to 0. Then W is a subspace of V, which we could identify with $\mathbf{R}^{n-1}$.

Example 4. Let A be a vector in $\mathbf{R}^3$. Let W be the set of all elements B in $\mathbf{R}^3$ such that $B \cdot A = 0$, i.e. such that B is perpendicular to A. Then W is a subspace of $\mathbf{R}^3$. To see this, note that $O \cdot A = 0$, so that O is in W. Next, suppose that B, C are perpendicular to A. Then

$$(B + C) \cdot A = B \cdot A + C \cdot A = 0,$$

so that $B + C$ is also perpendicular to A. Finally, if x is a number, then

$$(xB) \cdot A = x(B \cdot A) = 0,$$

so that xB is perpendicular to A. This proves that W is a subspace of $\mathbf{R}^3$.

More generally, if A is a vector in $\mathbf{R}^n$, then the set of all elements B in $\mathbf{R}^n$ such that $B \cdot A = 0$ is a subspace of $\mathbf{R}^n$. The proof is the same as when $n = 3$.

Example 5. Let $\mathrm{Sym}(n \times n)$ be the set of all symmetric $n \times n$ matrices. Then $\mathrm{Sym}(n \times n)$ is a subspace of the space of all $n \times n$ matrices. Indeed, if A, B are symmetric and c is a number, then $A + B$ and cA are symmetric. Also the zero matrix is symmetric.

Example 6. If f, g are two continuous functions, then $f + g$ is continuous. If c is a number, then cf is continuous. The zero function is continuous. Hence the continuous functions form a subspace of the vector space of all functions.

If f, g are two differentiable functions, then their sum $f + g$ is differentiable. If c is a number, then cf is differentiable. The zero function is differentiable. Hence the differentiable functions form a subspace of the vector space of all functions. Furthermore, every differentiable function is continuous. Hence the differentiable functions form a subspace of the vector space of continuous functions.

Example 7. Let V be a vector space and let U, W be subspaces. We denote by $U \cap W$ the **intersection** of U and W, i.e. the set of elements which lie both in U and W. Then $U \cap W$ is a subspace. For instance, if U, W are two planes in 3-space passing through the origin, then in general, their intersection will be a straight line passing through the origin, as shown in Fig. 1.

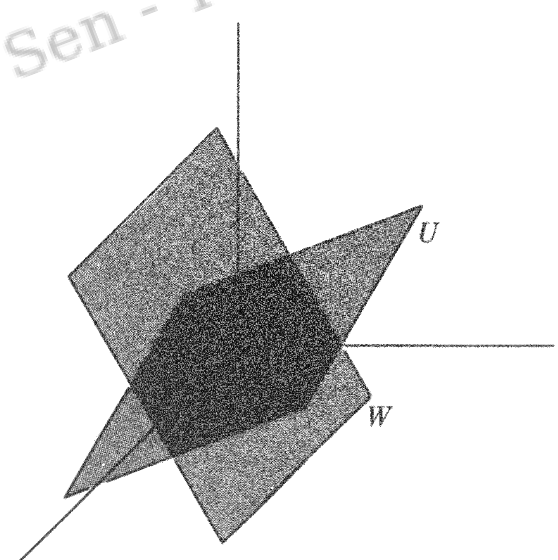


Figure 1

Example 8. Let U, W be subspaces of a vector space V. By

$$U + W$$

we denote the set of all elements $u + w$ with $u \in U$ and $w \in W$. Then we leave it to the reader to verify that $U + W$ is a subspace of V, said to be **generated by** U and W, and called the **sum** of U and W.

Exercises III, §1

1. Let $A_1, \dots, A_r$ be vectors in $\mathbf{R}^n$. Let W be the set of vectors B in $\mathbf{R}^n$ such that $B \cdot A_i = 0$ for every $i = 1, \dots, r$. Show that W is a subspace of $\mathbf{R}^n$.

2. Show that the following sets of elements in $\mathbf{R}^2$ form subspaces.
   (a) The set of all (x, y) such that $x = y$.
   (b) The set of all (x, y) such that $x - y = 0$.
   (c) The set of all (x, y) such that $x + 4y = 0$.

3. Show that the following sets of elements in $\mathbf{R}^3$ form subspaces.
   (a) The set of all (x, y, z) such that $x + y + z = 0$.
   (b) The set of all (x, y, z) such that $x = y$ and $2y = z$.
   (c) The set of all (x, y, z) such that $x + y = 3z$.

4. If U, W are subspaces of a vector space V, show that $U \cap W$ and $U + W$ are subspaces.

5. Let V be a subspace of $\mathbf{R}^n$. Let W be the set of elements of $\mathbf{R}^n$ which are perpendicular to every element of V. Show that W is a subspace of $\mathbf{R}^n$. This subspace W is often denoted by $V^\perp$, and is called V **perp**, or also the **orthogonal complement of** V.

III, §2. Linear Combinations

Let V be a vector space, and let $v_1, \dots, v_n$ be elements of V. We shall say that $v_1, \dots, v_n$ **generate** V if given an element $v \in V$ there exist numbers $x_1, \dots, x_n$ such that

$$v = x_1 v_1 + \cdots + x_n v_n.$$

Example 1. Let $E_1, \dots, E_n$ be the standard unit vectors in $\mathbf{R}^n$, so E_i has component 1 in the i-th place, and component 0 in all other places.

Then $E_1, \ldots, E_n$ generate $\mathbf{R}^n$. Proof: given $X = (x_1, \ldots, x_n) \in \mathbf{R}^n$. Then

$$X = \sum_{i=1}^{n} x_i E_i,$$

so there exist numbers satisfying the condition of the definition.

Let V be an arbitrary vector space, and let $v_1, \ldots, v_n$ be elements of V. Let $x_1, \ldots, x_n$ be numbers. An expression of type

$$x_1 v_1 + \cdots + x_n v_n$$

is called a **linear combination** of $v_1, \ldots, v_n$. The numbers $x_1, \ldots, x_n$ are then called the **coefficients** of the linear combination.

The set of all linear combinations of $v_1, \ldots, v_n$ is a subspace of V.

Proof. Let W be the set of all such linear combinations. Let $y_1, \ldots, y_n$ be numbers. Then

$$(x_1 v_1 + \cdots + x_n v_n) + (y_1 v_1 + \cdots + y_n v_n)$$
$$= (x_1 + y_1) v_1 + \cdots + (x_n + y_n) v_n.$$

Thus the sum of two elements of W is again an element of W, i.e. a linear combination of $v_1, \ldots, v_n$. Furthermore, if c is a number, then

$$c(x_1 v_1 + \cdots + x_n v_n) = c x_1 v_1 + \cdots + c x_n v_n$$

is a linear combination of $v_1, \ldots, v_n$, and hence is an element of W. Finally,

$$O = 0 v_1 + \cdots + 0 v_n$$

is an element of W. This proves that W is a subspace of V.

The subspace W consisting of all linear combinations of $v_1, \ldots, v_n$ is called the subspace **generated** by $v_1, \ldots, v_n$.

Example 2. Let v_1 be a non-zero element of a vector space V, and let w be any element of V. The set of elements

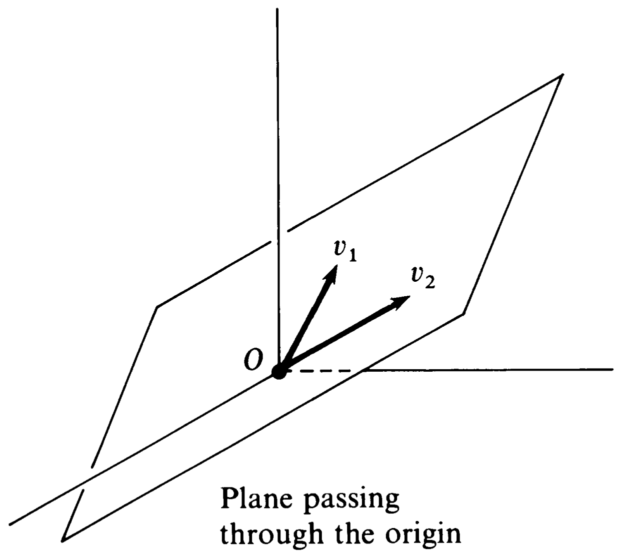
$$w + t v_1 \quad \text{with} \quad t \in \mathbf{R}$$

is called the **line passing through** w **in the direction of** v_1. We have already met such lines in Chapter I, §5. If $w = O$, then the line consisting of all scalar multiples tv_1 with $t \in \mathbf{R}$ is a subspace, generated by v_1.

Let v_1, v_2 be elements of a vector space V, and assume that neither is a scalar multiple of the other. The subspace generated by v_1, v_2 is called the **plane** generated by v_1, v_2. It consists of all linear combinations

$$t_1v_1 + t_2v_2 \quad \text{with} \quad t_1, t_2 \text{ arbitrary numbers.}$$

This plane passes through the origin, as one sees by putting $t_1 = t_2 = 0$.



Plane passing through the origin

Figure 2

We obtain the most general notion of a plane by the following operation. Let S be an arbitrary subset of V. Let P be an element of V. If we add P to all elements of S, then we obtain what is called the **translation** of S by P. It consists of all elements $P + v$ with v in S.

Example 3. Let v_1, v_2 be elements of a vector space V such that neither is a scalar multiple of the other. Let P be an element of V. We define the **plane passing through** P, **parallel to** v_1, v_2 to be the set of all elements

$$P + t_1v_1 + t_2v_2$$

where t_1, t_2 are arbitrary numbers. This notion of plane is the analogue, with two elements v_1, v_2, of the notion of parametrized line considered in Chapter I.

Warning. Usually such a plane does not pass through the origin, as shown on Fig. 3. Thus such a plane is **not** a subspace of V. If we take $P = O$, however, then the plane is a subspace.

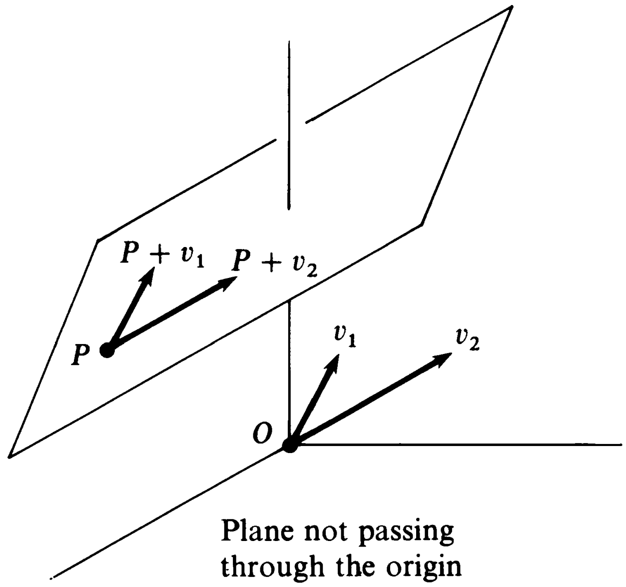


Figure 3

Sometimes it is interesting to restrict the coefficients of a linear combination. We give a number of examples below.

Example 4. Let V be a vector space and let v, u be elements of V. We define the **line segment** between v and $v + u$ to be the set of all points

$$v + tu, \qquad 0 \leqq t \leqq 1.$$

This line segment is illustrated in the following picture.

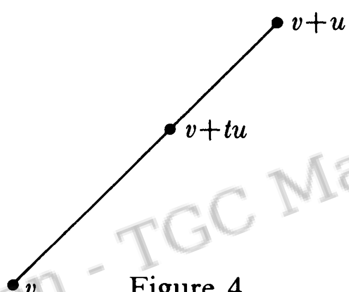
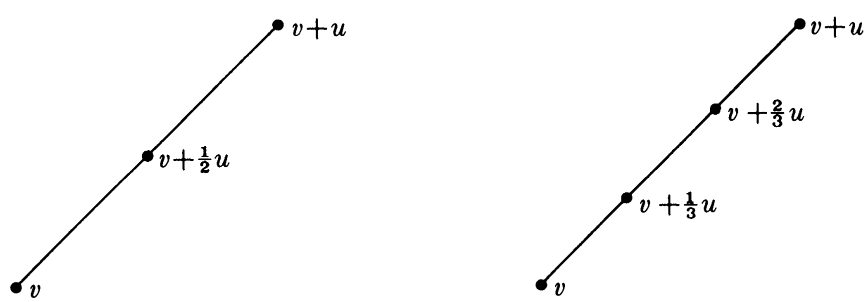


Figure 4

For instance, if $t = \frac{1}{2}$, then $v + \frac{1}{2}u$ is the point midway between v and $v + u$. Similarly, if $t = \frac{1}{3}$, then $v + \frac{1}{3}u$ is the point one third of the way between v and $v + u$ (Fig. 5).



(a) (b)

Figure 5

If v, w are elements of V, let $u = w - v$. Then the **line segment between** v and w is the set of all points $v + tu$, or

$$v + t(w - v), \qquad 0 \leqq t \leqq 1.$$

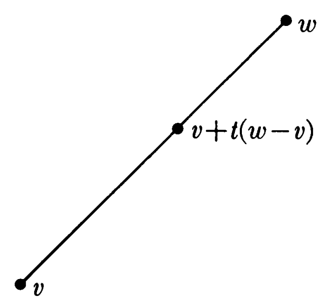


Figure 6

Observe that we can rewrite the expression for these points in the form

$$(1) \qquad (1 - t)v + tw, \qquad 0 \leqq t \leqq 1,$$

and letting $s = 1 - t$, $t = 1 - s$, we can also write it as

$$sv + (1 - s)w, \qquad 0 \leqq s \leqq 1.$$

Finally, we can write the points of our line segment in the form

$$(2) \qquad t_1 v + t_2 w \quad \text{with} \quad t_1, t_2 \geqq 0 \quad \text{and} \quad t_1 + t_2 = 1.$$

Indeed, letting $t = t_2$, we see that every point which can be written in the form (2) satisfies (1). Conversely, we let $t_1 = 1 - t$ and $t_2 = t$ and see that every point of the form (1) can be written in the form (2).

Example 5. Let v, w be elements of a vector space V. Assume that neither is a scalar multiple of the other. We define the **parallelogram spanned** by v, w to be the set of all points

$$t_1 v + t_2 w, \qquad 0 \leqq t_i \leqq 1 \quad \text{for} \quad i = 1, 2.$$

This definition is clearly justified since $t_1 v$ is a point of the segment between O and v (Fig. 7), and $t_2 w$ is a point of the segment between O

and w. For all values of t_1, t_2 ranging independently between 0 and 1, we see geometrically that $t_1v + t_2w$ describes all points of the parallelogram.

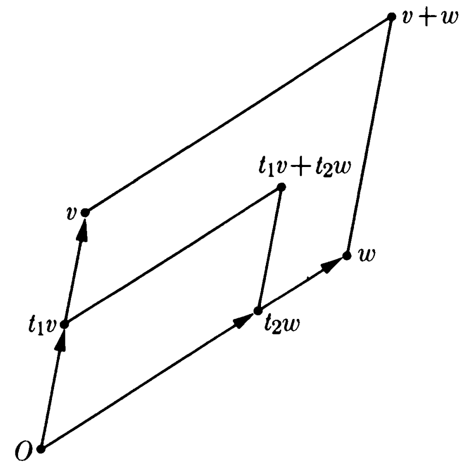


Figure 7

We obtain the most general parallelogram (Fig. 8) by taking the translation of the parallelogram just described. Thus if u is an element of V, the translation by u of the parallelogram spanned by v and w consists of all points

$$u + t_1v + t_2w, \qquad 0 \leqq t_i \leqq 1 \quad \text{for} \quad i = 1, 2.$$

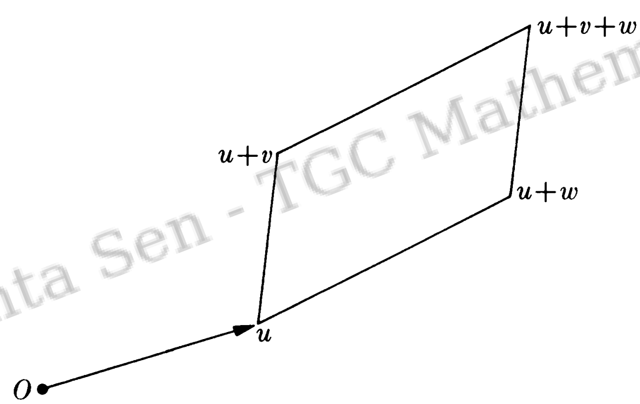


Figure 8

Similarly, in higher dimensions, let v_1, v_2, v_3 be elements of a vector space V. We define the **box spanned by these elements** to be the set of linear combinations

$$t_1v_1 + t_2v_2 + t_3v_3 \qquad \text{with} \qquad 0 \leqq t_i \leqq 1.$$

We draw the picture when v_1, v_2, v_3 are in general position:

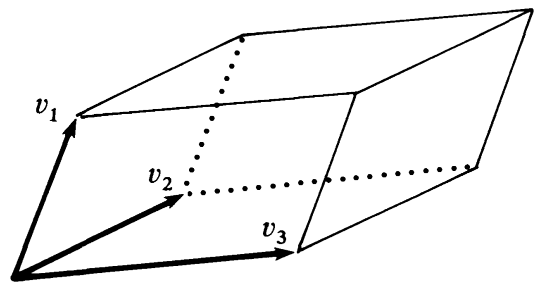


Figure 9

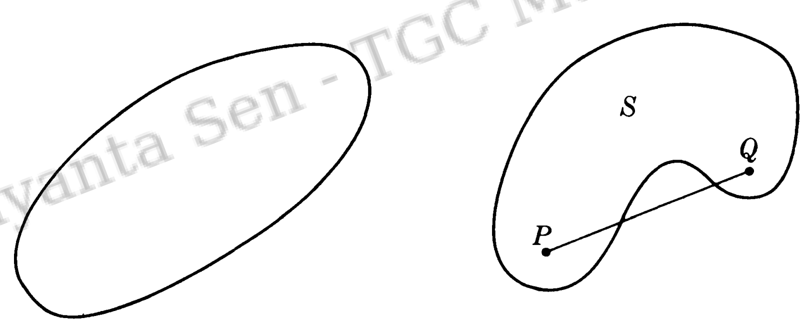
There may be degenerate cases, which will lead us into the notion of linear dependence a little later.

Exercises III, §2

1. Let $A_1, \dots, A_r$ be generators of a subspace V of $\mathbf{R}^n$. Let W be the set of all elements of $\mathbf{R}^n$ which are perpendicular to $A_1, \dots, A_r$. Show that the vectors of W are perpendicular to every element of V.
2. Draw the parallelogram spanned by the vectors $(1, 2)$ and $(-1, 1)$ in $\mathbf{R}^2$.
3. Draw the parallelogram spanned by the vectors $(2, -1)$ and $(1, 3)$ in $\mathbf{R}^2$.

III, §3. Convex Sets

Let S be a subset of a vector space V. We shall say that S is **convex** if given points P, Q in S then the line segment between P and Q is contained in S. In Fig. 10, the set on the left is convex. The set on the right is not convex since the line segment between P and Q is not entirely contained in S.



Convex set   *Not* convex

Figure 10

We recall that the line segment between P and Q consists of all points

$$(1 - t)P + tQ \qquad \text{with} \qquad 0 \leqq t \leqq 1.$$

This gives us a simple test to determine whether a set is convex or not.

Example 1. Let S be the parallelogram spanned by two vectors v_1, v_2, so S is the set of linear combinations

$$t_1 v_1 + t_2 v_2 \quad \text{with} \quad 0 \leqq t_i \leqq 1.$$

We wish to prove that S is convex. Let

$$P = t_1 v_1 + t_2 v_2 \quad \text{and} \quad Q = s_1 v_1 + s_2 v_2$$

be points in S. Then

$$\begin{aligned}(1-t)P + tQ &= (1-t)(t_1 v_1 + t_2 v_2) + t(s_1 v_1 + s_2 v_2)\\ &= (1-t)t_1 v_1 + (1-t)t_2 v_2 + ts_1 v_1 + ts_2 v_2\\ &= r_1 v_1 + r_2 v_2,\end{aligned}$$

where

$$r_1 = (1-t)t_1 + ts_1 \quad \text{and} \quad r_2 = (1-t)t_2 + ts_2.$$

But we have

$$0 \leqq (1-t)t_1 + ts_1 \leqq (1-t) + t = 1$$

and

$$0 \leqq (1-t)t_2 + ts_2 \leqq (1-t) + t = 1.$$

Hence

$$(1-t)P + tQ = r_1 v_1 + r_2 v_2 \quad \text{with} \quad 0 \leqq r_i \leqq 1.$$

This proves that $(1-t)P + tQ$ is in the parallelogram, which is therefore convex.

Example 2. Half planes. Consider a linear equation like

$$2x - 3y = 6.$$

This is the equation of a line as shown on Fig. 11.

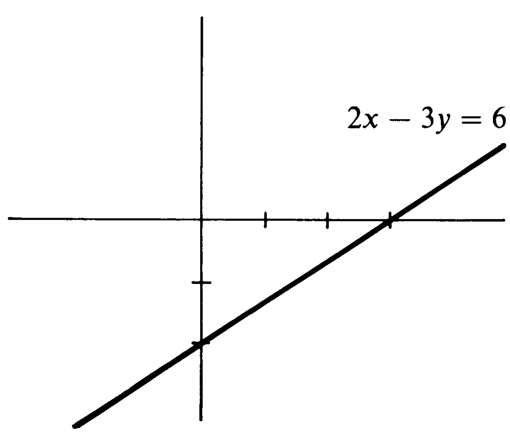


Figure 11

The inequalities

$$2x - 3y \leqq 6 \qquad \text{and} \qquad 2x - 3y \geqq 6$$

determine two half planes; one of them lies below the line and the other lies above the line, as shown on Fig. 12.

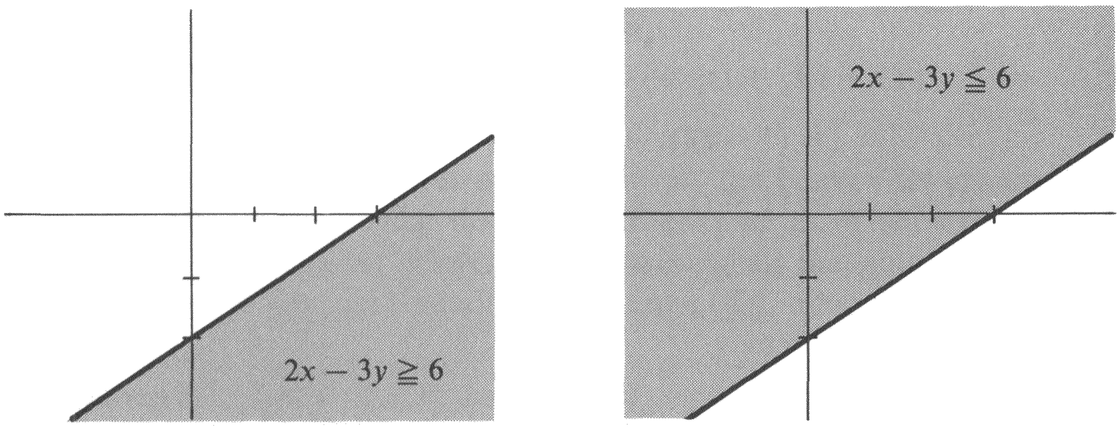


Figure 12

Let $A = (2, -3)$. We can, and should write the linear inequalities in the form

$$A \cdot X \geqq 6 \qquad \text{and} \qquad A \cdot X \leqq 6,$$

where $X = (x, y)$. Prove as Exercise 2 that each half plane is convex. This is clear intuitively from the picture, at least in $\mathbf{R}^2$, but your proof should be valid for the analogous situation in $\mathbf{R}^n$.

Theorem 3.1. *Let $P_1, \ldots, P_n$ be points of a vector space V. Let S be the set of all linear combinations*

$$t_1 P_1 + \cdots + t_n P_n$$

with $0 \leqq t_i$ and $t_1 + \cdots + t_n = 1$. Then S is convex.

Proof. Let

$$P = t_1 P_1 + \cdots + t_n P_n$$

and

$$Q = s_1 P_1 + \cdots + s_n P_n$$

with $0 \leqq t_i$, $0 \leqq s_i$, and

$$t_1 + \cdots + t_n = 1,$$
$$s_1 + \cdots + s_n = 1.$$

Let $0 \leqq t \leqq 1$. Then:

$$\begin{aligned}(1-t)P + tQ &= (1-t)t_1P_1 + \cdots + (1-t)t_nP_n \\ &\quad + ts_1P_1 + \cdots + ts_nP_n \\ &= [(1-t)t_1 + ts_1]P_1 + \cdots + [(1-t)t_n + ts_n]P_n.\end{aligned}$$

We have $0 \leqq (1-t)t_i + ts_i$ for all i, and

$$\begin{aligned}(1-t)t_1 &+ ts_1 + \cdots + (1-t)t_n + ts_n \\ &= (1-t)(t_1 + \cdots + t_n) + t(s_1 + \cdots + s_n) \\ &= (1-t) + t \\ &= 1.\end{aligned}$$

This proves our theorem.

In the next theorem, we shall prove that the set of all linear combinations

$$t_1P_1 + \cdots + t_nP_n \qquad \text{with} \qquad 0 \leqq t_i \quad \text{and} \quad t_1 + \cdots + t_n = 1$$

is the smallest convex set containing $P_1, \ldots, P_n$. For example, suppose that P_1, P_2, P_3 are three points in the plane not on a line. Then it is geometrically clear that the smallest convex set containing these three points is the triangle having these points as vertices.

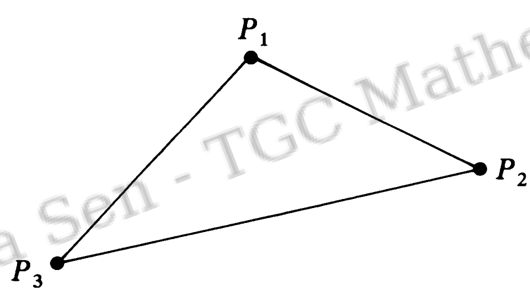


Figure 13

Thus it is natural to take as definition of a triangle the following property, valid in any vector space.

Let P_1, P_2, P_3 be three points in a vector space V, not lying on a line. Then the **triangle spanned** by these points is the set of all combinations

$$t_1P_1 + t_2P_2 + t_3P_3 \qquad \text{with} \quad 0 \leqq t_i \quad \text{and} \quad t_1 + t_2 + t_3 = 1.$$

When we deal with more than three points, then the set of linear combinations as in Theorem 3.1 looks as in the following figure.

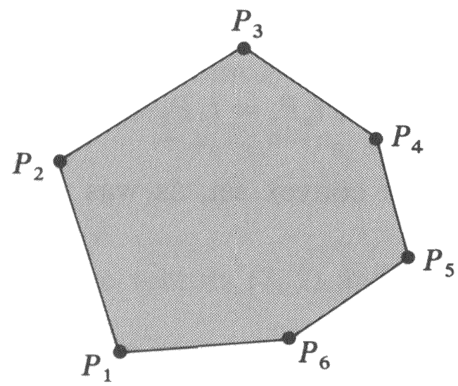


Figure 14

We shall call the convex set of Theorem 3.1 the convex set **spanned** by $P_1, \ldots, P_n$. Although we shall not need the next result, it shows that this convex set is the smallest convex set containing all the points $P_1, \ldots, P_n$. Omit the proof if you can't handle the argument by induction.

Theorem 3.2. *Let $P_1, \ldots, P_n$ be points of a vector space V. Any convex set which contains $P_1, \ldots, P_n$ also contains all linear combinations*

$$t_1 P_1 + \cdots + t_n P_n$$

with $0 \leqq t_i$ for all i and $t_1 + \cdots + t_n = 1$.

Proof. We prove this by induction. If $n = 1$, then $t_1 = 1$, and our assertion is obvious. Assume the theorem proved for some integer $n - 1 \geqq 1$. We shall prove it for n. Let $t_1, \ldots, t_n$ be numbers satisfying the conditions of the theorem. Let S' be a convex set containing $P_1, \ldots, P_n$. We must show that S' contains all linear combinations

$$t_1 P_1 + \cdots + t_n P_n.$$

If $t_n = 1$, then our assertion is trivial because $t_1 = \cdots = t_{n-1} = 0$. Suppose that $t_n \neq 1$. Then the linear combination $t_1 P_1 + \cdots + t_n P_n$ is equal to

$$(1 - t_n)\left(\frac{t_1}{1 - t_n} P_1 + \cdots + \frac{t_{n-1}}{1 - t_n} P_{n-1}\right) + t_n P_n.$$

Let

$$s_i = \frac{t_i}{1 - t_i} \qquad \text{for} \qquad i = 1, \ldots, n - 1.$$

Then $s_i \geqq 0$ and $s_1 + \cdots + s_{n-1} = 1$ so that by induction, we conclude that the point

$$Q = s_1 P_1 + \cdots + s_{n-1} P_{n-1}$$

lies in S'. But then

$$(1 - t_n)Q + t_nP_n = t_1P_1 + \cdots + t_nP_n$$

lies in S' by definition of a convex set, as was to be shown.

Exercises III, §3

1. Let S be the parallelogram consisting of all linear combinations $t_1v_1 + t_2v_2$ with $0 \leqq t_1 \leqq 1$ and $0 \leqq t_2 \leqq 1$. Prove that S is convex.
2. Let A be a non-zero vector in $\mathbf{R}^n$ and let c be a fixed number. Show that the set of all elements X in $\mathbf{R}^n$ such that $A \cdot X \geqq c$ is convex.
3. Let S be a convex set in a vector space. If c is a number, denote by cS the set of all elements cv with v in S. Show that cS is convex.
4. Let S_1 and S_2 be convex sets. Show that the intersection $S_1 \cap S_2$ is convex.
5. Let S be a convex set in a vector space V. Let w be an arbitrary element of V. Let $w + S$ be the set of all elements $w + v$ with v in S. Show that $w + S$ is convex.

III, §4. Linear Independence

Let V be a vector space, and let $v_1, \ldots, v_n$ be elements of V. We shall say that $v_1, \ldots, v_n$ are **linearly dependent** if there exist numbers $a_1, \ldots, a_n$ not all equal to 0 such that

$$a_1v_1 + \cdots + a_nv_n = O.$$

If there do not exist such numbers, then we say that $v_1, \ldots, v_n$ are **linearly independent.** In other words, vectors $v_1, \ldots, v_n$ are linearly independent if and only if the following condition is satisfied:

Let $a_1, \ldots, a_n$ be numbers such that

$$a_1v_1 + \cdots + a_nv_n = O;$$

then $a_i = 0$ for all $i = 1, \ldots, n$.

Example 1. Let $V = \mathbf{R}^n$ and consider the vectors

$$\begin{gathered} E_1 = (1, 0, \ldots, 0) \\ \vdots \\ E_n = (0, 0, \ldots, 1). \end{gathered}$$

Then $E_1, \dots, E_n$ are linearly independent. Indeed, let $a_1, \dots, a_n$ be numbers such that $a_1E_1 + \cdots + a_nE_n = O$. Since

$$a_1E_1 + \cdots + a_nE_n = (a_1, \dots, a_n),$$

it follows that all $a_i = 0$.

Example 2. Show that the vectors $(1, 1)$ and $(-3, 2)$ are linearly independent.

Let a, b be two numbers such that

$$a(1, 1) + b(-3, 2) = O.$$

Writing this equation in terms of components, we find

$$a - 3b = 0, \qquad a + 2b = 0.$$

This is a system of two equations which we solve for a and b. Subtracting the second from the first, we get $-5b = 0$, whence $b = 0$. Substituting in either equation, we find $a = 0$. Hence, a, b are both 0, and our vectors are linearly independent.

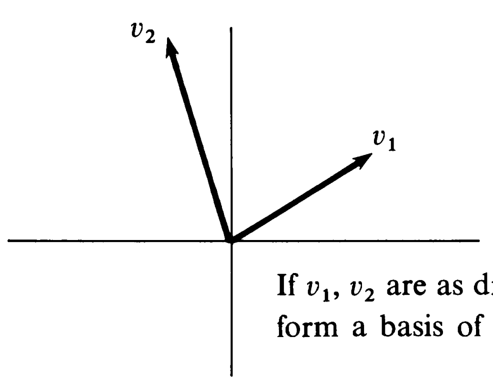
If elements $v_1, \dots, v_n$ of V generate V and in addition are linearly independent, then $\{v_1, \dots, v_n\}$ is called a **basis** of V. We shall also say that the elements $v_1, \dots, v_n$ **constitute** or **form** a basis of V.

Example 3. The vectors $E_1, \dots, E_n$ of Example 1 form a basis of $\mathbf{R}^n$. To prove this we have to prove that they are linearly independent, which was already done in Example 1; and that they generate $\mathbf{R}^n$. Given an element $A = (a_1, \dots, a_n)$ of $\mathbf{R}^n$ we can write A as a linear combination

$$A = a_1E_1 + \cdots + a_nE_n,$$

so by definition, $E_1, \dots, E_n$ generate $\mathbf{R}^n$. Hence they form a basis.

However, there are many other bases. Let us look at $n = 2$. We shall find out that any two vectors which are not parallel form a basis of $\mathbf{R}^2$. Let us first consider an example.



If v_1, v_2 are as drawn, they form a basis of $\mathbf{R}^2$.

Figure 15

Example 4. Show that the vectors $(1, 1)$ and $(-1, 2)$ form a basis of $\mathbf{R}^2$.

We have to show that they are linearly independent and that they generate $\mathbf{R}^2$. To prove linear independence, suppose that a, b are numbers such that

$$a(1, 1) + b(-1, 2) = (0, 0)$$

Then

$$a - b = 0, \qquad a + 2b = 0.$$

Subtracting the first equation from the second yields $3b = 0$, so that $b = 0$. But then from the first equation, $a = 0$, thus proving that our vectors are linearly independent.

Next, we must show that $(1, 1)$ and $(-1, 2)$ generate $\mathbf{R}^2$. Let (s, t) be an arbitrary element of $\mathbf{R}^2$. We have to show that there exist numbers x, y such that

$$x(1, 1) + y(-1, 2) = (s, t).$$

In other words, we must solve the system of equations

$$\begin{aligned} x - y &= s, \\ x + 2y &= t. \end{aligned}$$

Again subtract the first equation from the second. We find

$$3y = t - s,$$

whence

$$y = \frac{t - s}{3},$$

and finally

$$x = y + s = \frac{t - s}{3} + s.$$

This proves that $(1, 1)$ and $(-1, 2)$ generate $\mathbf{R}^2$, and concludes the proof that they form a basis of $\mathbf{R}^2$.

The general story for $\mathbf{R}^2$ is expressed in the following theorem.

Theorem 4.1. *Let (a, b) and (c, d) be two vectors in $\mathbf{R}^2$.*

(i) *They are linearly dependent if and only if $ad - bc = 0$.*
(ii) *If they are linearly independent, then they form a basis of $\mathbf{R}^2$.*

Proof. First work it out as an exercise (see Exercise 4). If you can't do it, you will find the proof in the answer section. It parallels closely the procedure of Example 4.

Let V be a vector space, and let $\{v_1, \dots, v_n)$ be a basis of V. The elements of V can be represented by n-tuples relative to this basis, as follows. If an element v of V is written as a linear combination

$$v = x_1 v_1 + \cdots + x_n v_n$$

of the basis elements, then we call $(x_1, \dots, x_n)$ the **coordinates** of v with respect to our basis, and we call x_i the i-th coordinate. The coordinates with respect to the usual basis $E_1, \dots, E_n$ of $\mathbf{R}^n$ are simply the coordinates as defined in Chapter I, §1.

The following theorem shows that there can only be one set of coordinates for a given vector.

Theorem 4.2. *Let V be a vector space. Let $v_1, \dots, v_n$ be linearly independent elements of V. Let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be numbers such that*

$$x_1 v_1 + \cdots + x_n v_n = y_1 v_1 + \cdots + y_n v_n.$$

Then we must have $x_i = y_i$ for all $i = 1, \dots, n$.

Proof. Subtract the right-hand side from the left-hand side. We get

$$x_1 v_1 - y_1 v_1 + \cdots + x_n v_n - y_n v_n = O.$$

We can write this relation also in the form

$$(x_1 - y_1)v_1 + \cdots + (x_n - y_n)v_n = O.$$

By definition, we must have $x_i - y_i = 0$ for all $i = 1, \dots, n$, thereby proving our assertion.

The theorem expresses the fact that when an element is written as a linear combination of $v_1, \dots, v_n$, then its coefficients $x_1, \dots, x_n$ are uniquely determined. This is true only when $v_1, \dots, v_n$ are linearly independent.

Example 5. Find the coordinates of $(1, 0)$ with respect to the two vectors $(1, 1)$ and $(-1, 2)$.

We must find numbers a, b such that

$$a(1, 1) + b(-1, 2) = (1, 0).$$

Writing this equation in terms of coordinates, we find

$$a - b = 1, \qquad a + 2b = 0.$$

Solving for a and b in the usual manner yields $b = -\frac{1}{3}$ and $a = \frac{2}{3}$. Hence the coordinates of $(1, 0)$ with respect to $(1, 1)$ and $(-1, 2)$ are $(\frac{2}{3}, -\frac{1}{3})$.

Example 6. The two functions e^t, e^{2t} are linearly independent. To prove this, suppose that there are numbers a, b such that

$$ae^t + be^{2t} = 0$$

(for all values of t). Differentiate this relation. We obtain

$$ae^t + 2be^{2t} = 0.$$

Subtract the first from the second relation. We obtain $be^{2t} = 0$, and hence $b = 0$. From the first relation, it follows that $ae^t = 0$, and hence $a = 0$. Hence e^t, e^{2t} are linearly independent.

Example 7. Let V be the vector space of all functions of a variable t. Let $f_1, \dots, f_n$ be n functions. To say that they are linearly dependent is to say that there exist n numbers $a_1, \dots, a_n$ not all equal to 0 such that

$$a_1 f_1(t) + \cdots + a_n f_n(t) = 0$$

for *all* values of t.

Warning. We emphasize that linear dependence for functions means that the above relation holds for all values of t. For instance, consider the relation

$$a \sin t + b \cos t = 0,$$

where a, b are two fixed numbers not both zero. There may be *some* values of t for which the above equation is satisfied. For instance, if $a \neq 0$ we then can solve

$$\frac{\sin t}{\cos t} = \frac{b}{a},$$

or in other words, $\tan t = b/a$ to get at least one solution. However, the above relation cannot hold for *all* values of t, and consequently $\sin t$, $\cos t$ are linearly independent, as functions.

Example 8. Let V be the vector space of functions generated by the two functions e^t, e^{2t}. Then the coordinates of the function

$$3e^t + 5e^{2t}$$

with respect to the basis $\{e^t, e^{2t}\}$ are $(3, 5)$.

When dealing with two vectors v, w there is another convenient way of expressing linear independence.

Theorem 4.3. *Let v, w be elements of a vector space V. They are linearly dependent if and only if one of them is a scalar multiple of the other, i.e. there is a number $c \neq 0$ such that we have $v = cw$ or $w = cv$.*

Proof. Left as an exercise, cf. Exercise 5.

In the light of this theorem, the condition imposed in various examples in the preceding section could be formulated in terms of two vectors being linearly independent.

Exercises III, §4

1. Show that the following vectors are linearly independent.
   (a) $(1, 1, 1)$ and $(0, 1, -2)$
   (b) $(1, 0)$ and $(1, 1)$
   (c) $(-1, 1, 0)$ and $(0, 1, 2)$
   (d) $(2, -1)$ and $(1, 0)$
   (e) $(\pi, 0)$ and $(0, 1)$
   (f) $(1, 2)$ and $(1, 3)$
   (g) $(1, 1, 0)$, $(1, 1, 1)$, and $(0, 1, -1)$
   (h) $(0, 1, 1)$, $(0, 2, 1)$, and $(1, 5, 3)$
2. Express the given vector X as a linear combination of the given vectors A, B, and find the coordinates of X with respect to A, B.
   (a) $X = (1, 0)$, $A = (1, 1)$, $B = (0, 1)$
   (b) $X = (2, 1)$, $A = (1, -1)$, $B = (1, 1)$
   (c) $X = (1, 1)$, $A = (2, 1)$, $B = (-1, 0)$
   (d) $X = (4, 3)$, $A = (2, 1)$, $B = (-1, 0)$
3. Find the coordinates of the vector X with respect to the vectors A, B, C.
   (a) $X = (1, 0, 0)$, $A = (1, 1, 1)$, $B = (-1, 1, 0)$, $C = (1, 0, -1)$
   (b) $X = (1, 1, 1)$, $A = (0, 1, -1)$, $B = (1, 1, 0)$, $C = (1, 0, 2)$
   (c) $X = (0, 0, 1)$, $A = (1, 1, 1)$, $B = (-1, 1, 0)$, $C = (1, 0, -1)$
4. Let (a, b) and (c, d) be two vectors in $\mathbf{R}^2$.
   (i) If $ad - bc \neq 0$, show that they are linearly independent.
   (ii) If they are linearly independent, show that $ad - bc \neq 0$.
   (iii) If $ad - bc \neq 0$ show that they form a basis of $\mathbf{R}^2$.
5. (a) Let v, w be elements of a vector space. If v, w are linearly dependent, show that there is a number c such that $w = cv$, or $v = cw$.
   (b) Conversely, let v, w be elements of a vector space, and assume that there exists a number c such that $w = cv$. Show that v, w are linearly dependent.

6. Let $A_1,\dots,A_r$ be vectors in $\mathbf{R}^n$, and assume that they are mutually perpendicular, in other words $A_i \perp A_j$ if $i \neq j$. Also assume that none of them is O. Prove that they are linearly independent.

7. Consider the vector space of all functions of a variable t. Show that the following pairs of functions are linearly independent.
(a) $1, t$ (b) t, t^2 (c) t, t^4 (d) e^t, t (e) te^t, e^{2t} (f) $\sin t, \cos t$
(g) $t, \sin t$ (h) $\sin t$, $\sin 2t$ (i) $\cos t$, $\cos 3t$

8. Consider the vector space of functions defined for $t > 0$. Show that the following pairs of functions are linearly independent.
(a) t, $1/t$ (b) e^t, $\log t$

9. What are the coordinates of the function $3 \sin t + 5 \cos t = f(t)$ with respect to the basis $\{\sin t, \cos t\}$?

10. Let D be the derivative d/dt. Let $f(t)$ be as in Exercise 9. What are the coordinates of the function $Df(t)$ with respect to the basis of Exercise 9?

In each of the following cases, exhibit a basis for the given space, and prove that it is a basis.

11. The space of 2×2 matrices.
12. The space of $m \times n$ matrices.
13. The space of $n \times n$ matrices all of whose components are 0 except possibly the diagonal components.

14. The **upper triangular matrices**, i.e. matrices of the following type:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

15. (a) The space of symmetric 2×2 matrices.
(b) The space of symmetric 3×3 matrices.
16. The space of symmetric $n \times n$ matrices.

III, §5. Dimension

We ask the question: Can we find three linearly independent elements in $\mathbf{R}^2$? For instance, are the elements

$$A = (1, 2), \qquad B = (-5, 7), \qquad C = (10, 4)$$

linearly independent? If you write down the linear equations expressing the relation

$$xA + yB + zC = O,$$

you will find that you can solve them for x, y, z not equal to 0. Namely, these equations are:

$$x - 5y + 10z = 0,$$

$$2x + 7y + \ \ 4z = 0.$$

This is a system of two homogeneous equations in three unknowns, and we know by Theorem 2.1 of Chapter II that we can find a non-trivial solution (x, y, z) not all equal to zero. Hence A, B, C are linearly dependent.

We shall see in a moment that this is a general phenomenon. In $\mathbf{R}^n$, we cannot find more than n linearly independent vectors. Furthermore, we shall see that any n linearly independent elements of $\mathbf{R}^n$ must generate $\mathbf{R}^n$, and hence form a basis. Finally, we shall also see that if one basis of a vector space has n elements, and another basis has m elements, then $m = n$. In short, two bases must have the same number of elements. This property will allow us to define the **dimension** of a vector space as the number of elements in any basis. We now develop these ideas systematically.

Theorem 5.1. *Let V be a vector space, and let $\{v_1, \ldots, v_m\}$ generate V. Let $w_1, \ldots, w_n$ be elements of V and assume that $n > m$. Then $w_1, \ldots, w_n$ are linearly dependent.*

Proof. Since $\{v_1, \ldots, v_m\}$ generate V, there exist numbers (a_{ij}) such that we can write

$$\begin{aligned} w_1 &= a_{11}v_1 + \cdots + a_{m1}v_m \\ &\vdots \\ w_n &= a_{1n}v_1 + \cdots + a_{mn}v_m. \end{aligned}$$

If $x_1, \ldots, x_n$ are numbers, then

$$\begin{aligned} &x_1w_1 + \cdots + x_nw_n \\ &\qquad = (x_1a_{11} + \cdots + x_na_{1n})v_1 + \cdots + (x_1a_{m1} + \cdots + x_na_{mn})v_m \end{aligned}$$

(just add up the coefficients of $v_1, \ldots, v_m$ vertically downward). According to Theorem 2.1 of Chapter II, the system of equations

$$\begin{aligned} x_1a_{11} + \cdots + x_na_{1n} &= 0 \\ &\vdots \\ x_1a_{m1} + \cdots + x_na_{mn} &= 0 \end{aligned}$$

has a non-trivial solution, because $n > m$. In view of the preceding remark, such a solution $(x_1, \ldots, x_n)$ is such that

$$x_1w_1 + \cdots + x_nw_n = 0.$$

as desired.

Theorem 5.2. *Let V be a vector space and suppose that one basis has n elements, and another basis has m elements. Then $m = n$.*

Proof. We apply Theorem 5.1 to the two bases. Theorem 5.1 implies that both alternatives $n > m$ and $m > n$ are impossible, and hence $m = n$.

Let V be a vector space having a basis consisting of n elements. We shall say that n is the **dimension** of V. If V consists of O alone, then V does not have a basis, and we shall say that V has dimension 0.

We may now reformulate the definitions of a line and a plane in an arbitrary vector space V. A **line passing through the origin** is simply a one-dimensional subspace. A **plane passing through the origin** is simply a two-dimensional subspace.

An arbitrary **line** is obtained as the translation of a one-dimensional subspace. An arbitrary **plane** is obtained as the translation of a two-dimensional subspace. When a basis $\{v_1\}$ has been selected for a one-dimensional space, then the points on a line are expressed in the usual form

$$P + t_1 v_1 \text{ with all possible numbers } t_1.$$

When a basis $\{v_1, v_2\}$ has been selected for a two-dimensional space, then the points on a plane are expressed in the form

$$P + t_1 v_1 + t_2 v_2 \text{ with possible numbers } t_1,\ t_2.$$

Let $\{v_1, \dots, v_n\}$ be a set of elements of a vector space V. Let r be a positive integer $\leqq n$. We shall say that $\{v_1, \dots, v_r\}$ is a **maximal** subset of linearly independent elements if $v_1, \dots, v_r$ are linearly independent, and if in addition, given any v_i with $i > r$, the elements $v_1, \dots, v_r, v_i$ are linearly dependent.

The next theorem gives us a useful criterion to determine when a set of elements of a vector space is a basis.

Theorem 5.3. *Let $\{v_1, \dots, v_n\}$ be a set of generators of a vector space V. Let $\{v_1, \dots, v_r\}$ be a maximal subset of linearly independent elements. Then $\{v_1, \dots, v_r\}$ is a basis of V.*

Proof. We must prove that $v_1, \dots, v_r$ generate V. We shall first prove that each v_i (for $i > r$) is a linear combination of $v_1, \dots, v_r$. By hypothesis, given v_i, there exists numbers $x_1, \dots, x_r, y$ not all 0 such that

$$x_1 v_1 + \cdots + x_r v_r + y v_i = O.$$

Furthermore, $y \neq 0$, because otherwise, we would have a relation of linear dependence for $v_1, \ldots, v_r$. Hence we can solve for v_i, namely

$$v_i = \frac{x_1}{-y} v_1 + \cdots + \frac{x_r}{-y} v_r,$$

thereby showing that v_i is a linear combination of $v_1, \ldots, v_r$.

Next, let v be any element of V. There exist numbers $c_1, \ldots, c_n$ such that

$$v = c_1 v_1 + \cdots + c_n v_n.$$

In this relation, we can replace each v_i $(i > r)$ by a linear combination of $v_1, \ldots, v_r$. If we do this, and then collect terms, we find that we have expressed v as a linear combination of $v_1, \ldots, v_r$. This proves that $v_1, \ldots, v_r$ generate V, and hence form a basis of V.

We shall now give criteria which allow us to tell when elements of a vector space constitute a basis.

Let $v_1, \ldots, v_n$ be linearly independent elements of a vector space V. We shall say that they form a **maximal set of linearly independent elements of** V if given any element w of V, the elements $w, v_1, \ldots, v_n$ are linearly dependent.

Theorem 5.4. *Let V be a vector space, and $\{v_1, \ldots, v_n\}$ a maximal set of linearly independent elements of V. Then $\{v_1, \ldots, v_n\}$ is a basis of V.*

Proof. We must now show that $v_1, \ldots, v_n$ generate V, i.e. that every element of V can be expressed as a linear combination of $v_1, \ldots, v_n$. Let w be an element of V. The elements $w, v_1, \ldots, v_n$ of V must be linearly dependent by hypothesis, and hence there exist numbers $x_0, x_1, \ldots, x_n$ not all 0 such that

$$x_0 w + x_1 v_1 + \cdots + x_n v_n = O.$$

We cannot have $x_0 = 0$, because if that were the case, we would obtain a relation of linear dependence among $v_1, \ldots, v_n$. Therefore we can solve for w in terms of $v_1, \ldots, v_n$, namely

$$w = -\frac{x_1}{x_0} v_1 - \cdots - \frac{x_n}{x_0} v_n.$$

This proves that w is a linear combination of $v_1, \ldots, v_n$, and hence that $\{v_1, \ldots, v_n\}$ is a basis.

Theorem 5.5. *Let V be a vector space of dimension n, and let $v_1, \ldots, v_n$ be linearly independent elements of V. Then $v_1, \ldots, v_n$ constitute a basis of V.*

Proof. According to Theorem 5.1., $\{v_1, \dots, v_n\}$ is a maximal set of linearly independent elements of V. Hence it is a basis by Theorem 5.4.

Theorem 5.6. *Let V be a vector space of dimension n and let W be a subspace, also of dimension n. Then $W = V$.*

Proof. A basis for W must also be a basis for V.

Theorem 5.7. *Let V be a vector space of dimension n. Let r be a positive integer with $r < n$, and let $v_1, \dots, v_r$ be linearly independent elements of V. Then one can find elements $v_{r+1}, \dots, v_n$ such that*

$$\{v_1, \dots, v_n\}$$

is a basis of V.

Proof. Since $r < n$ we know that $\{v_1, \dots, v_r\}$ cannot form a basis of V, and thus cannot be a maximal set of linearly independent elements of V. In particular, we can find v_{r+1} in V such that

$$v_1, \dots, v_{r+1}$$

are linearly independent. If $r + 1 < n$, we can repeat the argument. We can thus proceed stepwise (by induction) until we obtain n linearly independent elements $\{v_1, \dots, v_n\}$. These must be a basis by Theorem 5.4, and our corollary is proved.

Theorem 5.8. *Let V be a vector space having a basis consisting of n elements. Let W be a subspace which does not consist of O alone. Then W has a basis, and the dimension of W is $\leqq n$.*

Proof. Let w_1 be a non-zero element of W. If $\{w_1\}$ is not a maximal set of linearly independent elements of W, we can find an element w_2 of W such that w_1, w_2 are linearly independent. Proceeding in this manner, one element at a time, there must be an integer $m \leqq n$ such that we can find linearly independent elements $w_1, w_2, \dots, w_m$, and such that

$$\{w_1, \dots, w_m\}$$

is a maximal set of linearly independent elements of W (by Theorem 5.1 we cannot go on indefinitely finding linearly independent elements, and the number of such elements is at most n). If we now use Theorem 5.4, we conclude that $\{w_1, \dots, w_m\}$ is a basis for W.

Proposition 1. *Let V be a finite-dimensional vector space and W a subspace. Then V/W is finite-dimensional and* $\dim(V/W) = \dim V - \dim W$.

Proof. Let $w_1, \ldots, w_m$ be a basis for W; by the Basis Extension Theorem we can extend this to a basis $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$ for V (so $n = \dim V$ and $m = \dim W$). I claim that the cosets

$$v_{m+1} + W, \ldots, v_n + W \in V/W$$

form a basis for V/W; since this is a list of $n - m$ elements it will prove the theorem.

To prove that this is a basis, we need to show that it's linearly independent and that it spans. For spanning, suppose we have an arbitrary element $v + W \in V/W$, where we've written this with a representative v picked out. By using that $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$ is a basis for V we find we can (uniquely) write

$$v = a_1w_1 + \cdots + a_mw_m + a_{m+1}v_{m+1} + \cdots + a_nv_n.$$

Passing from this equality in V to one in the quotient set V/W, we have

$$\begin{aligned} v + W &= \big(a_1w_1 + \cdots + a_mw_m + a_{m+1}v_{m+1} + \cdots + a_nv_n\big) + W \\ &= a_1(w_1 + W) + \cdots + a_m(w_m + W) + a_{m+1}(v_{m+1} + W) + \cdots + a_n(v_n + W). \end{aligned}$$

But since each w_i is actually in W already, the coset $w_i + W$ is just the trivial coset W, i.e. the zero element of the vector space V/W. So we actually have

$$v + W = a_{m+1}(v_{m+1} + W) + \cdots + a_n(v_n + W).$$

Since $v + W$ is an arbitrary element of V/W this tells us the set $v_{m+1} + W, \ldots, v_n + W$ spans.

We next need to check linear independence. So assume we have a dependence relation

$$b_{m+1}(v_{m+1} + W) + \cdots + b_n(v_n + W) = (b_{m+1}v_{m+1} + \cdots + b_nv_n) + W = 0 + W$$

in V/W. By definition of equality of cosets this means

$$b_{m+1}v_{m+1} + \cdots + b_nv_n \in W,$$

and thus we can uniquely write this element as a linear combination $b_1w_1 + \cdots + b_mw_m$ in using that $\{w_1, \ldots, w_m\}$ is a basis for W. But then the equality

$$b_1w_1 + \cdots + b_mw_m = b_{m+1}v_{m+1} + \cdots + b_nv_n$$

rearranges to a dependence relation on the set $w_1, \ldots, w_m, v_{m+1}, \ldots, v_n$, which is a basis for V; so all of the coefficients b_i have to be trivial. □

The first isomorphism theorem. In class we've talked about the rank-nullity theorem: if $T : V \to W$ is a linear transformation and V is finite-dimensional, we have an equation that we can write as

$$\dim \operatorname{img}(T) = \dim V - \dim \ker(T).$$

Here, $\ker(T)$ is a subspace of V, so we can form the quotient space $V/\ker(T)$. If we look at the proposition I proved above, we also find

$$\dim V/\ker(T) = \dim V - \dim \ker(T).$$

So the rank-nullity theorem can be rephrased as saying "the image $\operatorname{img}(T)$ and the quotient space $V/\ker(T)$ always have the same dimension"! An abstract result known as the *first isomorphism theorem* says something even better, that $\operatorname{img}(T)$ and $V/\ker(T)$ are actually isomorphic in a very natural way.

Theorem 2 (First isomorphism theorem). *Let V be a vector space and $T : V \to W$ a linear transformation. Then T induces an isomorphism $\tau : V/\ker(T) \to \operatorname{img}(T)$ defined by*

$$\tau(v + \ker(T)) = T(v).$$

Proof. First of all, we need to make sure this makes sense. Since we're defining τ on the *coset* $v + \ker(T)$ in terms of the *representative* v, we need to check well-definedness, i.e. that if $v + \ker(T) = v' + \ker(T)$ then the values $T(v)$ and $T(v')$ we're trying to assign as outputs are equal. But v, v' being in the same coset means $v' - v$ is in $\ker(T)$, and thus

$$T(v') = T((v' - v) + v) = T(v' - v) + T(v) = 0 + T(v) = T(v).$$

So the map is well-defined. And since all of the values $T(v)$ lie inside of $\operatorname{img}(T)$ by definition, we don't have any problems with the codomain either.

So τ is a well-defined function; to show it's an isomorphism we need to show that it's linear, that it's injective, and that it's surjective. All of these are pretty straightforward. Linearity follows from linearity of T:

$$\tau\big((v+\ker(T))+(v'+\ker(T))\big) = \tau(v+v'+\ker(T)) = T(v+v') = T(v)+T(v') = \tau(v+\ker(T))+\tau(v'+\ker(T)),$$

$$\tau\big(a(v + \ker(T))\big) = \tau(av + \ker(T)) = T(av) = a \cdot T(v) = a\tau(v + \ker(T)).$$

For injectivity, we need to check that if $\tau(v + \ker(T)) = 0$ then $v + \ker(T) = 0$; but this is basically trivial because if $\tau(v + \ker(T)) = T(v) = 0$ then $v \in \ker(T)$ by definition. For surjectivity, any element of $\operatorname{img}(T)$ can be written as $T(v)$ for some $v \in V$ and thus is equal to $\tau(v + \operatorname{img}(T))$. $\square$

We can think of the first isomorphism theorem as a "refined version" of the rank-nullity theorem: it gives us an *explicit, specific* way of constructing an isomorphism $V/\ker(T) \cong \operatorname{img}(T)$, and knowing this isomorphism tells us $\dim V/\ker(T) = \dim \operatorname{img}(T)$ (which is a rephrasing of the rank-nullity theorem).

If we started with the rank-nullity theorem instead, the fact that $\dim V/\ker(T) = \dim \operatorname{img}(T)$ tells us that there is *some* way to construct an isomorphism $V/\ker(T) = \operatorname{img}(T)$, but doesn't tell us anything much about what such an isomorphism would look like. The first isomorphism theorem does tell us what the isomorphism is, and shows that it comes pretty directly from T itself.

The universal mapping property. If you go back to the proof of the first isomorphism theorem, really most of the work is in showing that if we start with $T : V \to W$, then we get a well-defined "induced map" $\tau : V/\ker(T) \to \operatorname{img}(T)$. That sort of argument works in a bit more generality, which gives us the following important result:

Theorem 3 (Universal mapping property for quotient spaces). *Let F be a field, V, W vector spaces over F, $T : V \to W$ a linear transformation, and $U \subseteq V$ a subspace. If $U \subseteq \ker(T)$, then there is a unique well-defined linear transformation $\tau : V/U \to W$ given by $\tau(v + U) = T(v)$.*

If $\pi : V \to V/U$ is the canonical projection (i.e. the linear transformation given by $\pi(v) = v + W$), this can be rephrased as saying that there's a unique well-defined linear transformation τ satisfying $\tau \circ \pi = T$. We can think of this as saying T "factors through" the quotient space V/U: starting with a map $V \to W$, we can actually split it up as two maps $V \to V/U \to W$.

Proof. This is basically the same proof as above (minus the last few lines). To see τ is well-defined on a coset $v + U$ we need to check that if $v + U = v' + U$ then $T(v) = T(v')$; but this follows because $v + U = v' + U$ means $v - v' \in U$ and thus $v - v' \in \ker(T)$ because U is contained in the kernel. Then we have $T(v - v') = 0$ by definition, and rearranging and using linearity gives $T(v) = T(v')$. Linearity is then a formal consequence of linearity of T:

$$\tau\big((v + U) + (v' + U)\big) = \tau(v + v' + U) = T(v + v') = T(v) + T(v') = \tau(v + U) + \tau(v' + U),$$

$$\tau\big(a(v + U)\big) = \tau(av + U) = T(av) = a \cdot T(v) = a\tau(v + U). \quad \square$$

This gives us a systematic way of constructing linear transformations on quotient spaces: to get a linear transformation $V/U \to W$, we just need to start with a linear transformation $V \to W$ which is trivial on U (i.e. has the kernel containing U). The terminology "universal mapping property" refers to any framework like this: starting with a function T satisfying some certain properties, we can conclude there exists a *unique* map τ defined in a certain way in terms of T.

Example 4. At this point, a fair question to ask is "why do I actually need to work with linear transformations defined on quotient spaces"? Like the question of "why do I actually need to work with quotient spaces", it's hard to give an answer entirely within linear algebra itself: most of the important uses of quotient spaces come up when you *apply* linear algebra to other subjects.

So I'll give an example building off of the Extended Example 1 (of the space $L^2(I)$, of "square-integrable functions $[0,1] \to \mathbb{R}$) in the "quotient vector spaces" handout. In that example, we defined $\mathcal{L}^2(I)$ to be the space of integrable functions $f : I \to \mathbb{R}$ such that $\int_0^1 |f|^2 dx < \infty$, and then as the quotient of this by the subspace U of all functions that were "almost everywhere zero".

To work with this space $L^2(I)$ in analysis, we want to be able to integrate functions on it! Say we fix some function like $\sin(2\pi x)$, and we want to consider the linear functional of "integrating against it":

$$f \mapsto \int_0^1 f(x) \sin(2\pi x) dx.$$

This makes perfect sense for any f in the actual space of functions $\mathcal{L}^2(I)$, and gives us a linear transformation $\mathcal{L}^2(I) \to \mathbb{R}$. But what we'd really like is a linear transformation $L^2(I) \to \mathbb{R}$. Fortunately, the universal mapping property lets us do this! If f is in the subspace U of "almost everywhere zero" functions, then $f(x)\sin(2\pi x)$ is also "almost everywhere zero", so its integral is zero. Thus $f \mapsto \int_0^1 f(x)\sin(2\pi x)dx$ is trivial on the subspace U, and the Universal Mapping Property tells us that we actually get a homomorphism $L^2(I) \to \mathbb{R}$ given by

$$[f] = f + U \mapsto \int_0^1 f(x) \sin(2\pi x) dx.$$

This is the functional that recovers one of the Fourier coefficients of f (which, again, makes sense: we've said that Fourier series only make sense up to "equality almost everywhere"!)

The other isomorphism theorems. From the name "the first isomorphism theorem", you can probably guess that there's a few more "isomorphism theorems" to go along with it. (The universal mapping property can sometimes be grouped in with them as well). These other isomorphism theorems are a bit less important to us in this class, but they're indispensable if you're going to be seriously working with quotient spaces.

The "second isomorphism theorem" concerns what happens when you have a vector space V and two subspaces U, W, and you take a quotient $(U + W)/W$. Your first thought might be that you can "cancel out the Ws" and just be left with something isomorphic to U - this is close to correct, but you need to compensate for any overlap between U and W.

Theorem 5 (Second isomorphism theorem)**.** *Let V be a vector space and $U, W \subseteq V$ two subspaces. Then there's an isomorphism of quotient spaces*

$$\frac{U}{U \cap W} \cong \frac{U + W}{W}$$

given by $u + (U \cap W) \mapsto u + W$.

The "third isomorphism theorem" is about quotient spaces of quotient spaces, which are pretty unpleasant to think about if you're not already really comfortable with quotient spaces.

Theorem 6 (Third isomorphism theorem)**.** *Let V be a vector space, W a subspace of V, and U a subspace of W. Then the quotient space W/U is itself a subspace of the quotient space V/U, and we have a canonical* *isomorphism*

$$\frac{V/U}{W/U} \cong V/W$$

by mapping $(v+U)+W/U$ (a coset in V/U by the subspace W/U!) to $v+W$.

There's one last theorem usually grouped with these, which is usually called the "correspondence theorem" or "lattice isomorphism theorem" and tells you about all of the subspaces in a quotient. We take the notation that $\mathrm{Sub}(V)$ denotes the collection of all subspaces of V.

Theorem 7 (Corresponcence theorem)**.** *Let V be a vector space and W a subspace of V. Then there is a bijective correspondence*

$$\mathrm{Sub}(V/W) \leftrightarrow \{U \in \mathrm{Sub}(V) : W \subseteq U \subseteq V\},$$

given by taking a subspace U with $W \subseteq U \subseteq V$ to the subspace U/W to V/W. This correspondence preserves sums and intersections: if we add or intersect two subspaces U_1/W and U_2/W of V/W we get

$$\frac{U_1}{W} + \frac{U_2}{W} = \frac{U_1 + U_2}{W} \qquad \frac{U_1}{W} \cap \frac{U_2}{W} = \frac{U_1 \cap U_2}{W}.$$

This characterizes $\mathrm{Sub}(V/W)$ in terms of a subset of $\mathrm{Sub}(V)$. Actually, the set $\mathrm{Sub}(V)$ of subspaces naturally has a partial order (by inclusion), and it's a *lattice* with respect to this partial order: any two subspaces U_1, U_2 have a *join* $U_1 + U_2$ (a "least upper bound") and a *join* $U_1 \cap U_2$ (a "greatest lower bound"). The last part of the theorem tells us that the lattice structure $\mathrm{Sub}(V/W)$ is compatible with the lattice structure on the sublattice $\{U : W \subseteq U \subseteq V\}$ of $\mathrm{Sub}(V)$, hence the name "lattice isomorphism theorem".

I'm omitting the proofs of these theorems in this section; trying to prove them yourself might be a good way to get in better practice with quotient spaces! (In all of the cases I've told you exactly what the function you need to look at is; what's left to check is that it's actually an isomorphism).

Courtesy (Contents are sourced from) **: ---**

1. S. Lang, Introduction to Linear Algebra, 2nd Ed., Springer, 2005.

2. http://pi.math.cornell.edu/~dcollins/math4310/IsomorphismTheorems.pdf