Vector Space Theory

A course for second year students by

Robert Howlett

typesetting by TEX

Contents

1
Preliminaries

The topics dealt with in this introductory chapter are of a general mathematical nature, being just as relevant to other parts of mathematics as they are to vector space theory. In this course you will be expected to learn several things about vector spaces (of course!), but, perhaps even more importantly, you will be expected to acquire the ability to think clearly and express yourself clearly, for this is what mathematics is really all about. Accordingly, you are urged to read (or reread) Chapter 1 of "Proofs and Problems in Calculus" by G. P. Monro; some of the points made there are reiterated below.

§1a Logic and common sense

When reading or writing mathematics you should always remember that the mathematical symbols which are used are simply abbreviations for words. Mechanically replacing the symbols by the words they represent should result in grammatically correct and complete sentences. The meanings of a few commonly used symbols are given in the following table.

Symbols	*To be read as*
$\{ \ldots \mid \ldots \}$	the set of all ... such that ...
$=$	is
$\in$	in *or* is in
$>$	greater than *or* is greater than

Thus, for example, the following sequence of symbols

$$\{ x \in X \mid x > a \} \neq \emptyset$$

is an abbreviated way of writing the sentence

The set of all x in X such that x is greater than a is not the empty set.

When reading mathematics you should mentally translate all symbols in this fashion, and when writing mathematics you should make sure that what you write translates into meaningful sentences.

Next, you must learn how to write out proofs. The ability to construct proofs is probably the most important skill for the student of pure mathematics to acquire. And it must be realized that this ability is nothing more than an extension of clear thinking. A proof is nothing more nor less than an explanation of why something is so. When asked to prove something, your first task is to be quite clear as to what is being asserted, then you must decide why it is true, then write the reason down, in plain language. There is never anything wrong with stating the obvious in a proof; likewise, people who leave out the "obvious" steps often make incorrect deductions.

When trying to prove something, the logical structure of what you are trying to prove determines the logical structure of the proof; this observation may seem rather trite, but nonetheless it is often ignored. For instance, it frequently happens that students who are supposed to proving that a statement p is a consequence of statement q actually write out a proof that q is a consequence of p. To help you avoid such mistakes we list a few simple rules to aid in the construction of logically correct proofs, and you are urged, whenever you think you have successfully proved something, to always check that your proof has the correct logical structure.

- To prove a statement of the form

  $$\text{If } p \text{ then } q$$

  your first line should be

  $$\text{Assume that } p \text{ is true}$$

  and your last line

  $$\text{Therefore } q \text{ is true.}$$

- The statement

  $$p \text{ if and only if } q$$

  is logically equivalent to

  $$\text{If } p \text{ then } q \text{ and if } q \text{ then } p.$$

  To prove it you must do two proofs of the kind described in the preceding paragraph.

- Suppose that $P(x)$ is some statement about x. Then to prove

  $$P(x) \text{ is true for all } x \text{ in the set } S$$

your first line should be

Let x be an arbitrary element of the set S

and your last line

Therefore $P(x)$ holds.

- Statements of the form

  There exists an x such that $P(x)$ is true

  are proved producing an example of such an x.

Some of the above points are illustrated in the examples #1, #2, #3 and #4 at the end of the next section.

§1b Sets and functions

It has become traditional to base all mathematics on set theory, and we will assume that the reader has an intuitive familiarity with the basic concepts. For instance, we write $S \subseteq A$ (S is a *subset* of A) if every element of S is an element of A. If S and T are two subsets of A then the *union* of S and T is the set

$$S \cup T = \{\, x \in A \mid x \in S \text{ or } x \in T \,\}$$

and the intersection of S and T is the set

$$S \cap T = \{\, x \in A \mid x \in S \text{ and } x \in T \,\}.$$

(Note that the 'or' above is the inclusive 'or'—that which is sometimes written as 'and/or'. In this book 'or' will always be used in this sense.)

Given any two sets S and T the *Cartesian product* $S \times T$ of S and T is the set of all ordered pairs (s, t) with $s \in S$ and $t \in T$; that is,

$$S \times T = \{\, (s,t) \mid s \in S,\, t \in T \,\}.$$

The Cartesian product of S and T always exists, for any two sets S and T. This is a fact which we ask the reader to take on trust. This course is not concerned with the foundations of mathematics, and to delve into formal treatments of such matters would sidetrack us too far from our main purpose. Similarly, we will not attempt to give formal definitions of the concepts of 'function' and 'relation'.

Let A and B be sets. A *function* f from A to B is to be thought of as a rule which assigns to every element a of the set A an element $f(a)$ of the set B. The set A is called the *domain* of f and B the *codomain* (or *target*) of f. We use the notation '$f\colon A \to B$' (read 'f, from A to B') to mean that f is a function with domain A and codomain B.

A *map* is the same thing as a function. The terms *mapping* and *transformation* are also used.

A function $f\colon A \to B$ is said to be *injective* (or *one-to-one*) if and only if no two distinct elements of A yield the same element of B. In other words, f is injective if and only if for all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$.

A function $f\colon A \to B$ is said to be *surjective* (or *onto*) if and only if for every element b of B there is an a in A such that $f(a) = b$.

If a function is both injective and surjective we say that it is *bijective* (or a one-to-one correspondence).

The *image* (or *range*) of a function $f\colon A \to B$ is the subset of B consisting of all elements obtained by applying f to elements of A. That is,

$$\operatorname{im} f = \{\, f(a) \mid a \in A \,\}.$$

An alternative notation is '$f(A)$' instead of '$\operatorname{im} f$'. Clearly, f is surjective if and only if $\operatorname{im} f = B$. The word 'image' is also used in a slightly different sense: if $a \in A$ then the element $f(a) \in B$ is sometimes called the image of a under the function f.

The notation '$a \mapsto b$' means 'a maps to b'; in other words, the function involved assigns the element b to the element a. Thus, '$a \mapsto b$' (under the function f) means exactly the same as '$f(a) = b$'.

If $f\colon A \to B$ is a function and C a subset of B then the *inverse image* or *preimage* of C is the subset of A

$$f^{-1}(C) = \{\, a \in A \mid f(a) \in C \,\}.$$

(The above sentence reads 'f inverse of C is the set of all a in A such that f of a is in C.' Alternatively, one could say 'The inverse image of C under f' instead of 'f inverse of C'.)

Let $f\colon B \to C$ and $g\colon A \to B$ be functions such that domain of f is the codomain of g. The *composite* of f and g is the function $fg\colon A \to C$ given

by $(fg)(a) = f(g(a))$ for all a in A. It is easily checked that if f and g are as above and $h\colon D \to A$ is another function then the composites $(fg)h$ and $f(gh)$ are equal.

Given any set A the *identity function* on A is the function $\mathtt{i}\colon A \to A$ defined by $\mathtt{i}(a) = a$ for all $a \in A$. It is clear that if f is any function with domain A then $f\mathtt{i} = f$, and likewise if g is any function with codomain A then $\mathtt{i}g = g$.

If $f\colon B \to A$ and $g\colon A \to B$ are functions such that the composite fg is the identity on A then we say that f is a *left inverse* of g and g is a *right inverse* of f. If in addition we have that gf is the identity on B then we say that f and g are inverse to each other, and we write $f = g^{-1}$ and $g = f^{-1}$. It is easily seen that $f\colon B \to A$ has an inverse if and only if it is bijective, in which case $f^{-1}\colon A \to B$ satisfies $f^{-1}(a) = b$ if and only if $f(b) = a$ (for all $a \in A$ and $b \in B$).

Suppose that $g\colon A \to B$ and $f\colon B \to C$ are bijective functions, so that there exist inverse functions $g^{-1}\colon B \to A$ and $f^{-1}\colon C \to B$. By the properties stated above we find that

$$(fg)(g^{-1}f^{-1}) = ((fg)g^{-1})f^{-1} = (f(gg^{-1})f^{-1} = (f\mathtt{i}_B)f^{-1} = ff^{-1} = \mathtt{i}_C$$

(where $\mathtt{i}_B$ and $\mathtt{i}_C$ are the identity functions on B and C), and an exactly similar calculation shows that $(g^{-1}f^{-1})(fg)$ is the identity on A. Thus fg has an inverse, and we have proved that the composite of two bijective functions is necessarily bijective.

—*Examples*—

#1 Suppose that you wish to prove that a function $\lambda\colon X \to Y$ is injective. Consult the definition of injective. You are trying to prove the following statement:

$$\text{For all } x_1,\ x_2 \in X, \text{ if } \lambda(x_1) = \lambda(x_2) \text{ then } x_1 = x_2.$$

So the first two lines of your proof should be as follows:

$$\text{Let } x_1,\ x_2 \in X.$$
$$\text{Assume that } \lambda(x_1) = \lambda(x_2).$$

Then you will presumably consult the definition of the function λ to derive consequences of $\lambda(x_1) = \lambda(x_2)$, and eventually you will reach the final line

$$\text{Therefore } x_1 = x_2.$$

#2 Suppose you wish to prove that $\lambda\colon X \to Y$ is surjective. That is, you wish to prove

$$\text{For every } y \in Y \text{ there exists } x \in X \text{ with } \lambda(x) = y.$$

Your first line must be

$$\text{Let } y \text{ be an arbitrary element of } Y.$$

Somewhere in the middle of the proof you will have to somehow define an element x of the set X (the definition of x is bound to involve y in some way), and the last line of your proof has to be

$$\text{Therefore } \lambda(x) = y.$$

#3 Suppose that A and B are sets, and you wish to prove that $A \subseteq B$. By definition the statement '$A \subseteq B$' is logically equivalent to

$$\text{All elements of } A \text{ are elements of } B.$$

So your first line should be

$$\text{Let } x \in A$$

and your last line should be

$$\text{Therefore } x \in B.$$

#4 Suppose that you wish to prove that $A = B$, where A and B are sets. The following statements are all logically equivalent to '$A = B$':

(i) For all x, $x \in A$ if and only if $x \in B$.

(ii) (For all x)$\big($(if $x \in A$ then $x \in B$) and (if $x \in B$ then $x \in A$)$\big)$.

(iii) All elements of A are elements of B and all elements of B are elements of A.

(iv) $A \subseteq B$ and $B \subseteq A$.

You must do two proofs of the general form given in #3 above.

#5 Let $A = \{\, n \in \mathbb{Z} \mid 0 \leq n \leq 3 \,\}$ and $B = \{\, n \in \mathbb{Z} \mid 0 \leq n \leq 2 \,\}$. Prove that if $C = \{\, n \in \mathbb{Z} \mid 0 \leq n \leq 11 \,\}$ then there is a bijective map $f\colon A \times B \to C$ given by $f(a, b) = 3a + b$ for all $a \in A$ and $b \in B$.

$\gg\!\!\rightarrowtriangle$ Observe first that by the definition of the Cartesian product of two sets, $A \times B$ consists of all ordered pairs (a, b), with $a \in A$ and $b \in B$. Our

first task is to show that for every such pair (a, b), and with f as defined above, $f(a, b) \in C$.

Let $(a, b) \in A \times B$. Then a and b are integers, and so $3a + b$ is also an integer. Since $0 \leq a \leq 3$ we have that $0 \leq 3a \leq 9$, and since $0 \leq b \leq 2$ we deduce that $0 \leq 3a + b \leq 11$. So $3a + b \in \{\, n \in \mathbb{Z} \mid 0 \leq n \leq 11 \,\} = C$, as required. We have now shown that f, as defined above, is indeed a function from $A \times B$ to C.

We now show that f is injective. Let $(a, b), (a', b') \in A \times B$, and assume that $f(a, b) = f(a', b')$. Then, by the definition of f, we have $3a+b = 3a'+b'$, and hence $b'-b = 3(a-a')$. Since $a-a'$ is an integer, this shows that $b'-b$ is a multiple of 3. But since b, $b' \in B$ we have that $0 \leq b' \leq 2$ and $-2 \leq -b \leq 0$, and adding these inequalities gives $-2 \leq b' - b \leq 2$. The only multiple of 3 in this range is 0; hence $b' = b$, and the equation $3a + b = 3a' + b'$ becomes $3a = 3a'$, giving $a = a'$. Therefore $(a, b) = (a', b')$.

Finally, we must show that f is surjective. Let c be an arbitrary element of the set C, and let m be the largest multiple of 3 which is not greater than c. Then $m = 3a$ for some integer a, and $3a + 3$ (which is a multiple of 3 larger than m) must exceed c; so $3a \leq c \leq 3a + 2$. Defining $b = c - 3a$, it follows that b is an integer satisfying $0 \leq b \leq 2$; that is, $b \in B$. Note also that since $0 \leq c \leq 11$, the largest multiple of 3 not exceeding c is at least 0, and less than 12. That is, $0 \leq 3a < 12$, whence $0 \leq a < 4$, and, since a is an integer, $0 \leq a \leq 3$. Hence $a \in A$, and so $(a, b) \in A \times B$. Now $f(a, b) = 3a + b = c$, which is what was to be proved. ⊲⊣≪

#6 Let f be as defined in #5 above. Find the preimages of the following subsets of C:

$$S_1 = \{5, 11\}, \qquad S_2 = \{0, 1, 2\}, \qquad S_3 = \{0, 3, 6, 9\}.$$

≫⊳ They are $f^{-1}(S_1) = \{(1, 2), (3, 2)\}$, $f^{-1}(S_2) = \{(0, 0), (0, 1), (0, 2)\}$ and $f^{-1}(S_3) = \{(0, 0), (1, 0), (2, 0), (3, 0)\}$ respectively. ⊲⊣≪

---

§1c Relations

We move now to the concept of a *relation* on a set X. For example, '$<$' is a relation on the set of natural numbers, in the sense that if m and n are any

two natural numbers then $m < n$ is a well-defined statement which is either true or false. Likewise, 'having the same birthday as' is a relation on the set of all people. If we were to use the symbol '$\sim$' for this relation then $a \sim b$ would mean 'a has the same birthday as b' and $a \not\sim b$ would mean 'a does not have the same birthday as b'.

If $\sim$ is a relation on X then $\{\,(x, y) \mid x \sim y\,\}$ is a subset of $X \times X$, and, conversely, any subset of $X \times X$ defines a relation on X. Formal treatments of this topic usually define a relation on X to be a subset of $X \times X$.

1.1 DEFINITION Let $\sim$ be a relation on a set X.

(i) The relation $\sim$ is said to be *reflexive* if $x \sim x$ for all $x \in X$.

(ii) The relation $\sim$ is said to be *symmetric* if $x \sim y$ whenever $y \sim x$ (for all x and y in X).

(iii) The relation $\sim$ is said to be *transitive* if $x \sim z$ whenever $x \sim y$ and $y \sim z$ (for all x, y, $z \in X$).

A relation which is reflexive, symmetric and transitive is called an *equivalence relation.*

For example, the "birthday" relation above is an equivalence relation. Another example would be to define sets X and Y to be equivalent if they have the same number of elements; more formally, define $X \sim Y$ if there exists a bijection from X to Y. The reflexive property for this relation follows from the fact that identity functions are bijective, the symmetric property from the fact that the inverse of a bijection is also a bijection, and transitivity from the fact that the composite of two bijections is a bijection.

It is clear that an equivalence relation $\sim$ on a set X partitions X into nonoverlapping subsets, two elements x, $y \in X$ being in the same subset if and only if $x \sim y$. (See #6 below.) These subsets are called *equivalence classes.* The set of all equivalence classes is then called the *quotient of X by the relation $\sim$.*

When dealing with equivalence relations it frequently simplifies matters to pretend that equivalent things are equal—ignoring irrelevant aspects, as it were. The concept of 'quotient' defined above provides a mathematical mechanism for doing this. If $\overline{X}$ is the quotient of X by the equivalence relation $\sim$ then $\overline{X}$ can be thought of as the set obtained from X by identifying equivalent elements of X. The idea is that an equivalence class is a single thing which embodies things we wish to identify. See #10 and #11 below, for example.

—Examples—

#7 Suppose that $\sim$ is an equivalence relation on the set X, and for each $x \in X$ define $C(x) = \{\, y \in X \mid x \sim y \,\}$. Prove that for all y, $z \in X$, the sets $C(y)$ and $C(z)$ are equal if $y \sim z$, and have no elements in common if $y \not\sim z$. Prove furthermore that $C(x) \neq \emptyset$ for all $x \in X$, and that for every $y \in X$ there is an $x \in X$ such that $y \in C(x)$.

$\gg\!\!\rightarrow$ Let y, $z \in X$ with $y \sim z$. Let x be an arbitrary element of $C(y)$. Then by definition of $C(y)$ we have that $y \sim x$. But $z \sim y$ (by symmetry of $\sim$, since we are given that $y \sim z$), and by transitivity it follows from $z \sim y$ and $y \sim x$ that $z \sim x$. This further implies, by definition of $C(z)$, that $x \in C(z)$. Thus every element of $C(y)$ is in $C(z)$; so we have shown that $C(y) \subseteq C(z)$. On the other hand, if we let x be an arbitrary element of $C(z)$ then we have $z \sim x$, which combined with $y \sim z$ yields $y \sim x$ (by transitivity of $\sim$), and hence $x \in C(y)$. So $C(z) \subseteq C(y)$, as well as $C(y) \subseteq C(z)$. Thus $C(y) = C(z)$ whenever $y \sim z$.

Now let y, $z \in X$ with $y \not\sim z$, and let $x \in C(y) \cap C(z)$. Then $x \in C(y)$ and $x \in C(z)$, and so $y \sim x$ and $z \sim x$. By symmetry we deduce that $x \sim z$, and now $y \sim x$ and $x \sim z$ yield $y \sim z$ by transitivity. This contradicts our assumption that $y \not\sim z$. It follows that there can be no element x in $C(y) \cap C(z)$; in other words, $C(y)$ and $C(z)$ have no elements in common if $y \not\sim z$.

Finally, observe that if $x \in X$ is arbitrary then $x \in C(x)$, since by reflexivity of $\sim$ we know that $x \sim x$. Hence $C(x) \neq \emptyset$. Furthermore, for every $y \in X$ there is an $x \in X$ with $y \in C(x)$, since $x = y$ has the required property. $\leftarrow\!\!\ll$

#8 Let $f\colon X \to S$ be an arbitrary function, and define a relation $\sim$ on X by the following rule: $x \sim y$ if and only if $f(x) = f(y)$. Prove that $\sim$ is an equivalence relation. Prove furthermore that if $\overline{X}$ is the quotient of X by $\sim$ then there is a one-to-one correspondence between the sets $\overline{X}$ and $\operatorname{im} f$.

$\gg\!\!\rightarrow$ Let $x \in X$. Since $f(x) = f(x)$ it is certainly true that $x \sim x$. So $\sim$ is a reflexive relation.

Let x, $y \in X$ with $x \sim y$. Then $f(x) = f(y)$ (by the definition of $\sim$); thus $f(y) = f(x)$, which shows that $y \sim x$. So $y \sim x$ whenever $x \sim y$, and we have shown that $\sim$ is symmetric.

Now let x, y, $z \in X$ with $x \sim y$ and $y \sim z$. Then $f(x) = f(y)$ and $f(y) = f(z)$, whence $f(x) = f(z)$, and $x \sim z$. So $\sim$ is also transitive, whence

it is an eqivalence relation.

Using the notation of #7 above, $\overline{X} = \{\, C(x) \mid x \in X \,\}$ (since $C(x)$ is the equivalence class of the element $x \in X$). We show that there is a bijective function $\overline{f}\colon \overline{X} \to \operatorname{im} f$ such that if $C \in \overline{X}$ is any equivalence class, then $\overline{f}(C) = f(x)$ for all $x \in X$ such that $C = C(x)$. In other words, we wish to define $\overline{f}\colon \overline{X} \to \operatorname{im} f$ by $\overline{f}(C(x)) = f(x)$ for all $x \in X$. To show that this does give a well defined function from $\overline{X}$ to $\operatorname{im} f$, we must show that

(i) every $C \in \overline{X}$ has the form $C = C(x)$ for some $x \in X$ (so that the given formula defines $\overline{f}(C)$ for all $C \in \overline{X}$),

(ii) if $x, y \in X$ with $C(x) = C(y)$ then $f(x) = f(y)$ (so that the given formula defines $\overline{f}(C)$ uniquely in each case), and

(iii) $f(x) \in \operatorname{im} f$ (so that the the given formula does define $\overline{f}(C)$ to be an element of $\operatorname{im} f$, the set which is meant to be the codomain of $\overline{f}$.

The first and third of these points are trivial: since $\overline{X}$ is defined to be the set of all equivalence classes its elements are certainly all of the form $C(x)$, and it is immediate from the definition of the image of f that $f(x) \in \operatorname{im} f$ for all $x \in X$. As for the second point, suppose that $x, y \in X$ with $C(x) = C(y)$. Then by one of the results proved in #7 above, $y \in C(y) = C(x)$, whence $x \sim y$ by the definition of $C(x)$. And by the definition of $\sim$, this says that $f(x) = f(y)$, as required. Hence the function $\overline{f}$ is well-defined.

We must prove that $\overline{f}$ is bijective. Suppose that $C, C' \in \overline{X}$ with $\overline{f}(C) = \overline{f}(C')$. Choose $x, y \in X$ such that $C = C(x)$ and $C' = C(y)$. Then

$$f(x) = \overline{f}(C(x)) = \overline{f}(C) = \overline{f}(C') = \overline{f}(C(y)) = f(y),$$

and so $x \sim y$, by definition of $\sim$. By #7 above, it follows that $C(x) = C(y)$; that is, $C = C'$. Hence $\overline{f}$ is injective. But if $s \in \operatorname{im} f$ is arbitrary then by definition of $\operatorname{im} f$ there exists an $x \in X$ with $s = f(x)$, and now the definition of $\overline{f}$ gives $\overline{f}(C(x)) = f(x) = s$. Since $C(x) \in \overline{X}$, we have shown that for all $s \in \operatorname{im} f$ there exists $C \in \overline{X}$ with $\overline{f}(C) = s$. Thus $\overline{f}\colon \overline{X} \to \operatorname{im} f$ is surjective, as required. ⊲⋘

---

§1d Fields

Vector space theory is concerned with two different kinds of mathematical objects, called *vectors* and *scalars*. The theory has many different applications, and the vectors and scalars for one application will generally be different from

the vectors and scalars for another application. Thus the theory does not say what vectors and scalars are; instead, it gives a list of defining properties, or axioms, which the vectors and scalars have to satisfy for the theory to be applicable. The axioms that vectors have to satisfy are given in Chapter Three, the axioms that scalars have to satisfy are given below.

In fact, the scalars must form what mathematicians call a 'field'. This means, roughly speaking, that you have to be able to add scalars and multiply scalars, and these operations of addition and multiplication have to satisfy most of the familiar properties of addition and multiplication of real numbers. Indeed, in almost all the important applications the scalars are just the real numbers. So, when you see the word 'scalar', you may as well think 'real number'. But there are other sets equipped with operations of addition and multiplication which satisfy the relevant properties; two notable examples are the set of all complex numbers and the set of all rational numbers.†

1.2 DEFINITION A set F which is equipped with operations of addition and multiplication is called a *field* if the following properties are satisfied.

(i) $a + (b + c) = (a + b) + c$ for all a, b, $c \in F$.
(That is, addition is *associative*.)

(ii) There exists an element $0 \in F$ such that $a + 0 = a = 0 + a$ for all $a \in F$. (There is a *zero* element in F.)

(iii) For each $a \in F$ there is a $b \in F$ such that $a + b = 0 = b + a$.
(Each element has a *negative*.)

(iv) $a + b = b + a$ for all a, $b \in F$. (Addition is *commutative*.)

(v) $a(bc) = (ab)c$ for all a, b, $c \in F$. (Multiplication is associative.)

(vi) There exists an element $1 \in F$, which is not equal to the zero element 0, such that $1a = a = a1$ for all $a \in F$.
(There is a *unity* element in F.)

(vii) For each $a \in F$ with $a \neq 0$ there exists $b \in F$ with $ab = 1 = ba$.
(Nonzero elements have *inverses*.)

(viii) $ab = ba$ for all a, $b \in F$. (Multiplication is commutative.)

(ix) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all a, b, $c \in F$.
(Both *distributive* laws hold.)

Comments ▷▷▷

1.2.1 Although the definition is quite long the idea is simple: for a set

† A number is *rational* if it has the form n/m where n and m are integers.

to be a field you have to be able to add and multiply elements, and all the obvious desirable properties have to be satisfied.

1.2.2 It is possible to use set theory to prove the existence integers and real numbers (assuming the correctness of set theory!) and to prove that the set of all real numbers is a field. We will not, however, delve into these matters in this book; we will simply assume that the reader is familiar with these basic number systems and their properties. In particular, we will not prove that the real numbers form a field.

1.2.3 The definition is not quite complete since we have not said what is meant by the term *operation*. In general an operation on a set S is just a function from $S \times S$ to S. In other words, an operation is a rule which assigns an element of S to each ordered pair of elements of S. Thus, for instance, the rule

$$(a, b) \longmapsto \sqrt{a + b^3}$$

defines an operation on the set $\mathbb{R}$ of all real numbers: we could use the notation $a \circ b = \sqrt{a + b^3}$. Of course, such unusual operations are not likely to be of any interest to anyone, since we want operations to satisfy nice properties like those listed above. In particular, it is rare to consider operations which are not associative, and the symbol '+' is always reserved for operations which are both associative and commutative. ▷▷▷

The set of all real numbers is by far the most important example of a field. Nevertheless, there are many other fields which occur in mathematics, and so we list some examples. We omit the proofs, however, so as not to be diverted from our main purpose for too long.

—Examples—

#9 As mentioned earlier, the set $\mathbb{C}$ of all complex numbers is a field, and so is the set $\mathbb{Q}$ of all rational numbers.

#10 Any set with exactly two elements can be made into a field by defining addition and multiplication appropriately. Let S be such a set, and (for reasons that will become apparent) let us give the elements of S the names $\boxed{\text{odd}}$ and $\boxed{\text{even}}$. We now define addition by the rules

$$\boxed{\text{even}} + \boxed{\text{even}} = \boxed{\text{even}} \qquad \boxed{\text{even}} + \boxed{\text{odd}} = \boxed{\text{odd}}$$
$$\boxed{\text{odd}} + \boxed{\text{even}} = \boxed{\text{odd}} \qquad \boxed{\text{odd}} + \boxed{\text{odd}} = \boxed{\text{even}}$$

and multiplication by the rules

$$\boxed{\text{even}}\boxed{\text{even}} = \boxed{\text{even}} \qquad \boxed{\text{even}}\boxed{\text{odd}} = \boxed{\text{even}}$$
$$\boxed{\text{odd}}\boxed{\text{even}} = \boxed{\text{even}} \qquad \boxed{\text{odd}}\boxed{\text{odd}} = \boxed{\text{odd}}.$$

These definitions are motivated by the fact that the sum of any two even integers is even, and so on. Thus it is natural to associate $\boxed{\text{odd}}$ with the set of all odd integers and $\boxed{\text{even}}$ with the set of all even integers. It is straightforward to check that the field axioms are now satisfied, with $\boxed{\text{even}}$ as the zero element and $\boxed{\text{odd}}$ as the unity.

Henceforth this field will be denoted by '$\mathbb{Z}_2$' and its elements will simply be called '0' and '1'.

#11 A similar process can be used to construct a field with exactly three elements; intuitively, we wish to identify integers which differ by a multiple of three. Accordingly, let $\boxed{\text{div}}$ be the set of all integers divisible by three, $\boxed{\text{div}+1}$ the set of all integers which are one greater than integers divisible by three, and $\boxed{\text{div}-1}$ the set of all integers which are one less than integers divisible by three. The appropriate definitions for addition and multiplication of these objects are determined by corresponding properties of addition and multiplication of integers. Thus, since

$$(3k+1)(3h-1) = 3(3kh+h-k)-1$$

it follows that the product of an integer in $\boxed{\text{div}+1}$ and an integer in $\boxed{\text{div}-1}$ is always in $\boxed{\text{div}-1}$, and so we should define

$$\boxed{\text{div}+1}\boxed{\text{div}-1} = \boxed{\text{div}-1}.$$

Once these definitions have been made it is fairly easy to check that the field axioms are satisfied.

This field will henceforth be denoted by '$\mathbb{Z}_3$' and its elements by '0', '1' and '-1'. Since $1+1=-1$ in $\mathbb{Z}_3$ the element -1 is alternatively denoted by'2' (or by '5' or '-4' or, indeed, 'n' for any integer n which is one less than a multiple of 3).

#12 The above construction can be generalized to give a field with n elements for any prime number n. In fact, the construction of $\mathbb{Z}_n$ works for any n, but the field axioms are only satisfied if n is prime. Thus $\mathbb{Z}_4 = \{0,1,2,3\}$

with the operations of "addition and multiplication modulo 4" does not form a field, but $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ does form a field under addition and multiplication modulo 5. Indeed, the addition and and multiplication tables for $\mathbb{Z}_5$ are as follows:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is easily seen that $\mathbb{Z}_4$ cannot possibly be a field, because multiplication modulo 4 gives $2^2 = 0$, whereas it is a consequence of the field axioms that the product of two nonzero elements of any field must be nonzero. (This is Exercise 4 at the end of this chapter.)

#13 Define

$$F = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

with addition and multiplication of matrices defined in the usual way. (See Chapter Two for the relevant definitions.) It can be shown that F is a field.

Note that if we define $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $J = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ then F consists of all matrices of the form $aI + bJ$, where $a, b \in \mathbb{Q}$. Now since $J^2 = 2I$ (check this!) we see that the rule for the product of two elements of F is

$$(aI + bJ)(cI + dJ) = (ac + 2bd)I + (ad + bc)J \qquad \text{for all } a, b, c, d \in \mathbb{Q}.$$

If we define F' to be the set of all real numbers of the form $a + b\sqrt{2}$, where a and b are rational, then we have a similar formula for the product of two elements of F', namely

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \qquad \text{for all } a, b, c, d \in \mathbb{Q}.$$

The rules for addition in F and in F' are obviously similar as well; indeed,

$$(aI + bJ) + (cI + dJ) = (a + c)I + (b + d)J$$

and

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

Thus, as far as addition and multiplication are concerned, F and F' are essentially the same as one another. This is an example of what is known as *isomorphism* of two algebraic systems.

Note that F' is obtained by "adjoining" $\sqrt{2}$ to the field $\mathbb{Q}$, in exactly the same way as $\sqrt{-1}$ is "adjoined" to the real field $\mathbb{R}$ to construct the complex field $\mathbb{C}$.

#14 Although $\mathbb{Z}_4$ is not a field, it is possible to construct a field with four elements. We consider matrices whose entries come from the field $\mathbb{Z}_2$. Addition and multiplication of matrices is defined in the usual way, but addition and multiplication of the matrix entries must be performed modulo 2 since these entries come from $\mathbb{Z}_2$. It turns out that

$$K = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

is a field. The zero element of this field is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, and the unity element is the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. To simplify notation, let us temporarily use '0' to denote the zero matrix and '1' to denote the identity matrix, and let us also use 'ω' to denote one of the two remaining elements of K (it does not matter which). Remembering that addition and multiplication are to be performed modulo 2 in this example, we see that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and also

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

so that the fourth element of K equals $1 + \omega$. A short calculation yields the following addition and multiplication tables for K:

$+$	0	1	ω	$1+\omega$
0	0	1	ω	$1+\omega$
1	1	0	$1+\omega$	ω
ω	ω	$1+\omega$	0	1
$1+\omega$	$1+\omega$	ω	1	0

	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$1+\omega$
ω	0	ω	$1+\omega$	1
$1+\omega$	0	$1+\omega$	1	ω

#15 The set of all expressions of the form

$$\frac{a_0 + a_1X + \cdots + a_nX^n}{b_0 + b_1X + \cdots + b_mX^m}$$

where the coefficients a_i and b_i are real numbers and the b_i are not all zero, can be regarded as a field.

The last three examples in the above list are rather outré, and will not be used in this book. They were included merely to emphasize that lots of examples of fields do exist.

Exercises

1. Let A and B be nonempty sets and $f\colon A \to B$ a function.

(i) Prove that f has a left inverse if and only if it is injective.

(ii) Prove that f has a right inverse if and only if it is surjective.

(iii) Prove that if f has both a right inverse and a left inverse then they are equal.

2. Let S be a set and $\sim$ a relation on S which is both symmetric and transitive. If x and y are elements of S and $x \sim y$ then by symmetricity we must have $y \sim x$. Now by transitivity $x \sim y$ and $y \sim x$ yields $x \sim x$, and so it follows that $x \sim x$ for all $x \in S$. That is, the reflexive law is a consequence of the symmetric and transitive laws. *What is the error in this "proof"?*

3. Suppose that $\sim$ is an equivalence relation on a set X. For each $x \in X$ let $E(x) = \{\, z \in X \mid x \sim z \,\}$. Prove that if $x, y \in X$ then $E(x) = E(y)$ if $x \sim y$ and $E(x) \cap E(y) = \emptyset$ if $x \not\sim y$.

The subsets $E(x)$ of X are called *equivalence classes*. Prove that each element $x \in X$ lies in a unique equivalence class, although there may be many different y such that $x \in E(y)$.

4. Prove that if F is a field and $x, y \in F$ are nonzero then xy is also nonzero. (Hint: Use Axiom (vii).)

5. Prove that $\mathbb{Z}_n$ is not a field if n is not prime.

6. It is straightforward to check that $\mathbb{Z}_n$ satisfies all the field axioms except for part (vii) of 1.2. Prove that this axiom is satisfied if n is prime.

(Hint: Let k be a nonzero element of $\mathbb{Z}_n$. Use the fact that if $k(i-j)$ is divisible by the prime n then $i-j$ must be divisible by n to prove that $k0$, $k1$, ..., $k(n-1)$ are all distinct elements of $\mathbb{Z}_n$, and deduce that one of them must equal 1.)

7. Prove that the example in #14 above is a field. You may assume that the only solution in integers of the equation $a^2 - 2b^2 = 0$ is $a = b = 0$, as well as the properties of matrix addition and multiplication given in Chapter Two.

2

Matrices, row vectors and column vectors

Linear algebra is one of the most basic of all branches of mathematics. The first and most obvious (and most important) application is the solution of simultaneous linear equations: in many practical problems quantities which need to be calculated are related to measurable quantities by linear equations, and consequently can be evaluated by standard row operation techniques. Further development of the theory leads to methods of solving linear differential equations, and even equations which are intrinsically nonlinear are usually tackled by repeatedly solving suitable linear equations to find a convergent sequence of approximate solutions. Moreover, the theory which was originally developed for solving linear equations is generalized and built on in many other branches of mathematics.

§2a Matrix operations

A *matrix* is a rectangular array of numbers. For instance,

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 0 & 7 & 2 \\ 5 & 1 & 1 & 8 \end{pmatrix}$$

is a 3×4 matrix. (That is, it has three rows and four columns.) The numbers are called the *matrix entries* (or *components*), and they are easily specified by row number and column number. Thus in the matrix A above the $(2, 3)$-entry is 7 and the $(3, 4)$-entry is 8. We will usually use the notation 'X_{ij}' for the (i, j)-entry of a matrix X. Thus, in our example, we have $A_{23} = 7$ and $A_{34} = 8$.

A matrix with only one row is usually called a *row vector*, and a matrix with only one column is usually called a *column vector*. We will usually call them just *rows* and *columns*, since (as we will see in the next chapter) the term *vector* can also properly be applied to things which are not rows or columns. Rows or columns with n components are often called *n-tuples*.

The set of all $m \times n$ matrices over $\mathbb{R}$ will be denoted by '$\mathrm{Mat}(m \times n, \mathbb{R})$', and we refer to $m \times n$ as the *shape* of these matrices. We define $\mathbb{R}^n$ to be the

set of all column n-tuples of real numbers, and ${}^{\mathrm{t}}\mathbb{R}^n$ (which we use less frequently) to be the set of all row n-tuples. (The 't' stands for 'transpose'. The transpose of a matrix $A \in \mathrm{Mat}(m \times n, \mathbb{R})$ is the matrix ${}^{\mathrm{t}}A \in \mathrm{Mat}(n \times m, \mathbb{R})$ defined by the formula $({}^{\mathrm{t}}A)_{ij} = A_{ji}$.)

The definition of *matrix* that we have given is intuitively reasonable, and corresponds to the best way to think about matrices. Notice, however, that the essential feature of a matrix is just that there is a well-determined matrix entry associated with each pair (i, j). For the purest mathematicians, then, a matrix is simply a function, and consequently a formal definition is as follows:

2.1 Definition Let n and m be nonnegative integers. An $m \times n$ *matrix over the real numbers* is a function

$$A\colon (i, j) \mapsto A_{ij}$$

from the Cartesian product $\{1, 2, \ldots, m\} \times \{1, 2, \ldots, n\}$ to $\mathbb{R}$.

Two matrices with of the same shape can be added simply by adding the corresponding entries. Thus if A and B are both $m \times n$ matrices then $A + B$ is the $m \times n$ matrix defined by the formula

$$(A + B)_{ij} = A_{ij} + B_{ij}$$

for all $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, n\}$. Addition of matrices satisfies properties similar to those satisfied by addition of numbers—in particular, $(A + B) + C = A + (B + C)$ and $A + B = B + A$ for all $m \times n$ matrices. The $m \times n$ zero matrix, denoted by '$0_{m\times n}$', or simply '0', is the $m \times n$ matrix all of whose entries are zero. It satisfies $A + 0 = A = 0 + A$ for all $A \in \mathrm{Mat}(m \times n, \mathbb{R})$.

If λ is any real number and A any matrix over $\mathbb{R}$ then we define λA by

$$(\lambda A)_{ij} = \lambda(A_{ij}) \qquad \text{for all } i \text{ and } j.$$

Note that λA is a matrix of the same shape as A.

Multiplication of matrices can also be defined, but it is more complicated than addition and not as well behaved. The product AB of matrices A and B is defined if and only if the number of columns of A equals the

number of rows of B. Then the (i,j)-entry of AB is obtained by multiplying the entries of the i^{th} row of A by the corresponding entries of the j^{th} column of B and summing these products. That is, if A has shape $m \times n$ and B shape $n \times p$ then AB is the $m \times p$ matrix defined by

$$\begin{aligned}(AB)_{ij} &= A_{i1}B_{1j} + A_{i2}B_{2j} + \cdots + A_{in}B_{nj} \\ &= \sum_{k=1}^{n} A_{ik}B_{kj}\end{aligned}$$

for all $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, p\}$.

This definition may appear a little strange at first sight, but the following considerations should make it seem more reasonable. Suppose that we have two sets of variables, x_1, x_2, …, x_m and y_1, y_2, …, y_n, which are related by the equations

$$\begin{aligned}x_1 &= a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n \\ x_2 &= a_{21}y_1 + a_{22}y_2 + \cdots + a_{2n}y_n \\ &\vdots \\ x_m &= a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{mn}y_n.\end{aligned}$$

Let A be the $m \times n$ matrix whose (i,j)-entry is the coefficient of y_j in the expression for x_i; that is, $A_{ij} = a_{ij}$. Suppose now that the variables y_j can be similarly expressed in terms of a third set of variables z_k with coefficient matrix B:

$$\begin{aligned}y_1 &= b_{11}z_1 + b_{12}z_2 + \cdots + b_{1p}z_p \\ y_2 &= b_{21}z_1 + b_{22}z_2 + \cdots + b_{2p}z_p \\ &\vdots \\ y_n &= b_{n1}z_1 + b_{n2}z_2 + \cdots + b_{np}z_p\end{aligned}$$

where b_{ij} is the (i,j)-entry of B. Clearly one can obtain expressions for the x_i in terms of the z_k by substituting this second set of equations into the first. It is easily checked that the total coefficient of z_k in the expression for x_i is $a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}$, which is exactly the formula for the (i,k)-entry of AB. We have shown that if A is the coefficient matrix for expressing the x_i in terms of the y_j, and B the coefficient matrix for expressing the y_j in terms of the z_k, then AB is the coefficient matrix for expressing the x_i in

terms of the z_k. If one thinks of matrix multiplication in this way, none of the facts mentioned below will seem particularly surprising.

Note that if the matrix product AB is defined there is no guarantee that the product BA is defined also, and even if it is defined it need not equal AB. Furthermore, it is possible for the product of two nonzero matrices to be zero. Thus the familiar properties of multiplication of numbers do not all carry over to matrices. However, the following properties are satisfied:

(i) For each positive integer n there is an $n \times n$ *identity matrix*, commonly denoted by '$I_{n\times n}$', or simply 'I', having the properties that $AI = A$ for matrices A with n columns and $IB = B$ for all matrices B with n rows. The (i, j)-entry of I is the *Kronecker delta*, δ_{ij}, which is 1 if i and j are equal and 0 otherwise:

$$I_{ij} = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

(ii) The distributive law $A(B + C) = AB + AC$ is satisfied whenever A is an $m \times n$ matrix and B and C are $n \times p$ matrices. Similarly, $(A + B)C = AC + BC$ whenever A and B are $m \times n$ and C is $n \times p$.

(iii) If A is an $m \times n$ matrix, B an $n \times p$ matrix and C a $p \times q$ matrix then $(AB)C = A(BC)$.

(iv) If A is an $m \times n$ matrix, B an $n \times p$ matrix and λ any number, then $(\lambda A)B = \lambda(AB) = A(\lambda B)$.

These properties are all easily proved. For instance, for (iii) we have

$$\big((AB)C\big)_{ij} = \sum_{k=1}^{p} (AB)_{ik} C_{kj} = \sum_{k=1}^{p} \left(\sum_{l=1}^{n} A_{il} B_{lk} \right) C_{kj} = \sum_{k=1}^{p} \sum_{l=1}^{n} A_{il} B_{lk} C_{kj}$$

and similarly

$$\big(A(BC)\big)_{ij} = \sum_{l=1}^{n} A_{il} (BC)_{lj} = \sum_{l=1}^{n} A_{il} \left(\sum_{k=1}^{p} B_{lk} C_{kj} \right) = \sum_{l=1}^{n} \sum_{k=1}^{p} A_{il} B_{lk} C_{kj},$$

and interchanging the order of summation we see that these are equal.

The following facts should also be noted.

2.2 PROPOSITION *The j^{th} column of a product AB is obtained by multiplying the matrix A by the j^{th} column of B, and the i^{th} row of AB is the i^{th} row of A multiplied by B.*

Proof. Suppose that the number of columns of A, necessarily equal to the number of rows of B, is n. Let b_j be the j^{th} column of B; thus the k^{th} entry of b_j is B_{kj} for each k. Now by definition the i^{th} entry of the j^{th} column of AB is $(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$. But this is exactly the same as the formula for the i^{th} entry of Ab_j.

The proof of the other part is similar. □

More generally, we have the following rule concerning multiplication of "partitioned matrices", which is fairly easy to see although a little messy to state and prove. Suppose that the $m \times n$ matrix A is subdivided into blocks $A^{(rs)}$ as shown, where $A^{(rs)}$ has shape $m_r \times n_s$:

$$A = \begin{pmatrix} A^{(11)} & A^{(12)} & \dots & A^{(1q)} \\ A^{(21)} & A^{(22)} & \dots & A^{(2q)} \\ \vdots & \vdots & & \vdots \\ A^{(p1)} & A^{(p2)} & \dots & A^{(pq)} \end{pmatrix}.$$

Thus we have that $m = \sum_{r=1}^{p} m_r$ and $n = \sum_{s=1}^{q} n_s$. Suppose also that B is an $n \times l$ matrix which is similarly partitioned into submatrices $B^{(st)}$ of shape $n_s \times l_t$. Then the product AB can be partitioned into blocks of shape $m_r \times l_t$, where the (r,t)-block is given by the formula $\sum_{s=1}^{q} A^{(rs)}B^{(st)}$. That is,

$$\begin{pmatrix} A^{(11)} & A^{(12)} & \dots & A^{(1q)} \\ A^{(21)} & A^{(22)} & \dots & A^{(2q)} \\ \vdots & \vdots & & \vdots \\ A^{(p1)} & A^{(p2)} & \dots & A^{(pq)} \end{pmatrix} \begin{pmatrix} B^{(11)} & B^{(12)} & \dots & B^{(1u)} \\ B^{(21)} & B^{(22)} & \dots & B^{(2u)} \\ \vdots & \vdots & & \vdots \\ B^{(q1)} & B^{(q2)} & \dots & B^{(qu)} \end{pmatrix}$$

$$(\$) \qquad = \begin{pmatrix} \sum_{s=1}^{q} A^{(1s)}B^{(s1)} & \dots & \sum_{s=1}^{q} A^{(1s)}B^{(su)} \\ \vdots & & \vdots \\ \sum_{s=1}^{q} A^{(ps)}B^{(s1)} & \dots & \sum_{s=1}^{q} A^{(ps)}B^{(sq)} \end{pmatrix}.$$

The proof consists of calculating the (i,j)-entry of each side, for arbitrary i and j. Define

$$M_0 = 0,\ M_1 = m_1,\ M_2 = m_1 + m_2,\ \dots,\ M_p = m_1 + m_2 + \cdots + m_p$$

and similarly

$$N_0 = 0,\ N_1 = n_1,\ N_2 = n_1 + n_2,\ \ldots,\ N_q = n_1 + n_2 + \cdots + n_q$$
$$L_0 = 0,\ L_1 = l_1,\ \ L_2 = l_1 + l_2,\ \ \ldots,\ L_u = l_1 + l_2 + \cdots + l_u.$$

Given that i lies between $M_0 + 1 = 1$ and $M_p = m$, there exists an r such that i lies between $M_{r-1} + 1$ and M_r. Write $i' = i - M_{r-1}$. We see that the i^{th} row of A is partitioned into the $i'^{\,\text{th}}$ rows of $A^{(r1)}$, $A^{(r2)}$, $\ldots$, $A^{(rq)}$. Similarly we may locate the j^{th} column of B by choosing t such that j lies between L_{t-1} and L_t, and we write $j' = j - L_{t-1}$. Now we have

$$\begin{aligned}
(AB)_{ij} &= \sum_{k=1}^{n} A_{ik}B_{kj} \\
&= \sum_{s=1}^{q} \left(\sum_{k=N_{s-1}+1}^{N_s} A_{ik}B_{kj} \right) \\
&= \sum_{s=1}^{q} \left(\sum_{k=1}^{n_s} (A^{(rs)})_{i'k} (B^{(st)})_{kj'} \right) \\
&= \sum_{s=1}^{q} (A^{(rs)}B^{(st)})_{i'j'} \\
&= \left(\sum_{s=1}^{q} A^{(rs)}B^{(st)} \right)_{i'j'}
\end{aligned}$$

which is the (i, j)-entry of the partitioned matrix (\$) above.

—Example—

#1 Verify the above rule for multiplication of partitioned matrices by computing the matrix product

$$\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 3 \\ 5 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 4 & 1 & 4 & 1 \end{pmatrix}$$

using the following partitioning:

$$\left(\begin{array}{cc|c} 2 & 4 & 1 \\ 1 & 3 & 3 \\ \hline 5 & 0 & 1 \end{array}\right) \left(\begin{array}{cccc} 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 2 & 3 \\ 4 & 1 & 4 & 1 \end{array}\right).$$

≫⊳ We find that

$$\begin{aligned}
&\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix} + \begin{pmatrix} 1 \\ 3 \end{pmatrix}\begin{pmatrix} 4 & 1 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 6 & 10 & 14 \\ 1 & 4 & 7 & 10 \end{pmatrix} + \begin{pmatrix} 4 & 1 & 4 & 1 \\ 12 & 3 & 12 & 3 \end{pmatrix} \\
&= \begin{pmatrix} 6 & 7 & 14 & 15 \\ 13 & 7 & 19 & 13 \end{pmatrix}
\end{aligned}$$

and similarly

$$\begin{aligned}
&\begin{pmatrix} 5 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix} + \begin{pmatrix} 1 \end{pmatrix}\begin{pmatrix} 4 & 1 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 5 & 5 & 5 & 5 \end{pmatrix} + \begin{pmatrix} 4 & 1 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 9 & 6 & 9 & 6 \end{pmatrix},
\end{aligned}$$

so that the answer is

$$\begin{pmatrix} 6 & 7 & 14 & 15 \\ 13 & 7 & 19 & 13 \\ 9 & 6 & 9 & 6 \end{pmatrix},$$

as can easily be checked directly. ⊲≪

Comment ⊳⊳⊳

2.2.1 Looking back on the proofs in this section one quickly sees that the only facts about real numbers which are made use of are the associative, commutative and distributive laws for addition and multiplication, existence of 1 and 0, and the like; in short, these results are based simply on the field axioms. Everything in this section is true for matrices over any field. ⊳⊳⊳

§2b Simultaneous equations

In this section we review the procedure for solving simultaneous linear equations. Given the system of equations

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\
&\vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m
\end{aligned} \tag{2.2.2}$$

the first step is to replace it by a *reduced echelon* system which is equivalent to the original. Solving reduced echelon systems is trivial. An algorithm is described below for obtaining the reduced echelon system corresponding to a given system of equations. The algorithm makes use of *elementary row operations*, of which there are three kinds:

1. Replace an equation by itself plus a multiple of another.
2. Replace an equation by a nonzero multiple of itself.
3. Write the equations down in a different order.

The most important thing about row operations is that the new equations should be consequences of the old, and, conversely, the old equations should be consequences of the new, so that the operations do not change the solution set. It is clear that the three kinds of elementary row operations do satisfy this requirement; for instance, if the fifth equation is replaced by itself minus twice the second equation, then the old equations can be recovered from the new by replacing the new fifth equation by itself plus twice the second.

It is usual when solving simultaneous equations to save ink by simply writing down the coefficients, omitting the variables, the plus signs and the equality signs. In this shorthand notation the system 2.2.2 is written as the *augmented matrix*

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ & & \cdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right). \tag{2.2.3}$$

It should be noted that the system of equations 2.2.2 can also be written as the single matrix equation

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \cdots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

where the matrix product on the left hand side is as defined in the previous section. For the time being, however, this fact is not particularly relevant, and 2.2.3 should simply be regarded as an abbreviated notation for 2.2.2.

The *leading entry* of a nonzero row of a matrix is the first (that is, leftmost) nonzero entry. An *echelon matrix* is a matrix with the following properties:

(i) All nonzero rows must precede all zero rows.

(ii) For all i, if rows i and $i+1$ are nonzero then the leading entry of row $i+1$ must be further to the right—that is, in a higher numbered column—than the leading entry of row i.

A reduced echelon matrix has two further properties:

(iii) All leading entries must be 1.

(iv) A column which contains the leading entry of any row must contain no other nonzero entry.

Once a system of equations is obtained for which the augmented matrix is reduced echelon, proceed as follows to find the general solution. If the last leading entry occurs in the final column (corresponding to the right hand side of the equations) then the equations have no solution (since we have derived the equation 0=1), and we say that the system is *inconsistent*. Otherwise each nonzero equation determines the variable corresponding to the leading entry uniquely in terms the other variables, and those variables which do not correspond to the leading entry of any row can be given arbitrary values. To state this precisely, suppose that rows 1, 2, ..., k are the nonzero rows, and suppose that their leading entries occur in columns i_1, i_2, ..., i_k respectively. We may call x_{i_1}, x_{i_2}, ..., x_{i_k} the *pivot* or *basic* variables and the remaining $n-k$ variables the *free* variables. The most general solution is obtained by assigning arbitrary values to the free variables, and solving equation 1 for x_{i_1}, equation 2 for x_{i_2}, ..., and equation k for x_{i_k}, to obtain the values of the basic variables. Thus the general solution of consistent system has $n-k$ degrees of freedom, in the sense that it involves $n-k$ arbitrary parameters. In particular a consistent system has a unique solution if and only if $n-k=0$.

—Example—

#2 Suppose that after performing row operations on a system of five equations in the nine variables x_1, x_2, ..., x_9, the following reduced echelon augmented matrix is obtained:

$$\left(\begin{array}{ccccccccc|c} 0 & 0 & 1 & 2 & 0 & 0 & -2 & -1 & 0 & 8 \\ 0 & 0 & 0 & 0 & 1 & 0 & -4 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right). \tag{2.2.4}$$

The leading entries occur in columns 3, 5, 6 and 9, and so the basic variables are x_3, x_5, x_6 and x_9. Let $x_1=\alpha$, $x_2=\beta$, $x_4=\gamma$, $x_7=\delta$ and $x_8=\varepsilon$, where

α, β, γ, δ and ε are arbitrary parameters. Then the equations give

$$\begin{aligned} x_3 &= 8 - 2\gamma + 2\delta + \varepsilon \\ x_5 &= 2 + 4\delta \\ x_6 &= -1 - \delta - 3\varepsilon \\ x_9 &= 5 \end{aligned}$$

and so the most general solution of the system is

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ 8 - 2\gamma + 2\delta + \varepsilon \\ \gamma \\ 2 + 4\delta \\ -1 - \delta - 3\varepsilon \\ \delta \\ \varepsilon \\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 0 \\ 8 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \\ 5 \end{pmatrix} + \alpha \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 0 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \delta \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 4 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \varepsilon \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -3 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

It is not wise to attempt to write down this general solution directly from the reduced echelon system 2.2.4. Although the actual numbers which appear in the solution are the same as the numbers in the augmented matrix, apart from some changes in sign, some care is required to get them in the right places!

Comments ▷▷▷

2.2.5 In general there are many different choices for the row operations to use when putting the equations into reduced echelon form. It can be

shown, however, that the reduced echelon form itself is uniquely determined by the original system: it is impossible to change one reduced echelon system into another by row operations.

2.2.6 We have implicitly assumed that the coefficients a_{ij} and b_i which appear in the system of equations 2.2.2 are real numbers, and that the unknowns x_j are also meant to be real numbers. However, it is easily seen that the process used for solving the equations works equally well for any field. ▷▷▷

There is a straightforward algorithm for obtaining the reduced echelon system corresponding to a given system of linear equations. The idea is to use the first equation to eliminate x_1 from all the other equations, then use the second equation to eliminate x_2 from all subsequent equations, and so on. For the first step it is obviously necessary for the coefficient of x_1 in the first equation to be nonzero, but if it is zero we can simply choose to call a different equation the "first". Similar reorderings of the equations may be necessary at each step.

More exactly, and in the terminology of row operations, the process is as follows. Given an augmented matrix with m rows, find a nonzero entry in the first column. This entry is called the first *pivot*. Swap rows to make the row containing this first pivot the first row. (Strictly speaking, it is possible that the first column is entirely zero; in that case use the next column.) Then subtract multiples of the first row from all the others so that the new rows have zeros in the first column. Thus, all the entries below the first pivot will be zero. Now repeat the process, using the $(m-1)$-rowed matrix obtained by ignoring the first row. That is, looking only at the second and subsequent rows, find a nonzero entry in the second column. If there is none (so that elimination of x_1 has accidentally eliminated x_2 as well) then move on to the third column, and keep going until a nonzero entry is found. This will be the second pivot. Swap rows to bring the second pivot into the second row. Now subtract multiples of the second row from all subsequent rows to make the entries below the second pivot zero. Continue in this way (using next the $m-2$-rowed matrix obtained by ignoring the first two rows) until no more pivots can be found.

When this has been done the resulting matrix will be in echelon form, but (probably) not reduced echelon form. The reduced echelon form is readily obtained, as follows. Start by dividing all entries in the last nonzero row by the leading entry—the pivot—in the row. Then subtract multiples of this

row from all the preceding rows so that the entries above the pivot become zero. Repeat this for the second to last nonzero row, then the third to last, and so on. It is important to note the following:

2.2.7 *The algorithm involves dividing by each of the pivots.*

§2c Partial pivoting

As commented above, the procedure described in the previous section applies equally well for solving simultaneous equations over any field. Differences between different fields manifest themselves only in the different algorithms required for performing the operations of addition, subtraction, multiplication and division in the various fields. For this section, however, we will restrict our attention exclusively to the field of real numbers (which is, after all, the most important case).

Practical problems often present systems with so many equations and so many unknowns that it is necessary to use computers to solve them. Usually, when a computer performs an arithmetic operation, only a fixed number of significant figures in the answer are retained, so that each arithmetic operation performed will introduce a minuscule round-off error. Solving a system involving hundreds of equations and unknowns will involve millions of arithmetic operations, and there is a definite danger that the cumulative effect of the minuscule approximations may be such that the final answer is not even close to the true solution. This raises questions which are extremely important, and even more difficult. We will give only a very brief and superficial discussion of them.

We start by observing that it is sometimes possible that a minuscule change in the coefficients will produce an enormous change in the solution, or change a consistent system into an inconsistent one. Under these circumstances the unavoidable roundoff errors in computation will produce large errors in the solution. In this case the matrix is *ill-conditioned*, and there is nothing which can be done to remedy the situation.

Suppose, for example, that our computer retains only three significant figures in its calculations, and suppose that it encounters the following system of equations:

$$\begin{aligned} x + \qquad 5z &= 0 \\ 12y + 12z &= 36 \\ .01x + 12y + 12z &= 35.9 \end{aligned}$$

Using the algorithm described above, the first step is to subtract .01 times the first equation from the third. This should give $12y + 11.95z = 35.9$, but the best our inaccurate computer can get is either $12y + 11.9z = 35.9$ or $12y + 12z = 35.9$. Subtracting the second equation from this will either give $0.1z = 0.1$ or $0z = 0.1$, instead of the correct $0.05z = 0.1$. So the computer will either get a solution which is badly wrong, or no solution at all. The problem with this system of equations—at least, for such an inaccurate computer—is that a small change to the coefficients can dramatically change the solution. As the equations stand the solution is $x = -10$, $y = 1$, $z = 2$, but if the coefficient of z in the third equation is changed from 12 to 12.1 the solution becomes $x = 10$, $y = 5$, $z = -2$.

Solving an ill-conditioned system will necessarily involve dividing by a number that is close to zero, and a small error in such a number will produce a large error in the answer. There are, however, occasions when we may be tempted to divide by a number that is close to zero when there is in fact no need to. For instance, consider the equations

2.2.8
$$\begin{aligned} .01x + 100y &= 100 \\ x + y &= 2 \end{aligned}$$

If we select the entry in the first row and first column of the augmented matrix as the first pivot, then we will subtract 100 times the first row from the second, and obtain

$$\left(\begin{array}{cc|c} .01 & 100 & 100 \\ 0 & -9999 & -9998 \end{array}\right).$$

Because our machine only works to three figures, -9999 and -9998 will both be rounded off to 10000. Now we divide the second row by -10000, then subtract 100 times the second row from the first, and finally divide the first row by .01, to obtain the reduced echelon matrix

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 1 \end{array}\right).$$

That is, we have obtained $x = 0$, $y = 1$ as the solution. Our value of y is accurate enough; our mistake was to substitute this value of y into the first equation to obtain a value for x. Solving for x involved dividing by .01, and the small error in the value of y resulted in a large error in the value of x.

A much more accurate answer is obtained by selecting the entry in the second row and first column as the first pivot. After swapping the two rows, the row operation procedure continues as follows:

$$\left(\begin{array}{cc|c} 1 & 1 & 2 \\ .01 & 100 & 100 \end{array}\right) \xrightarrow{R_2 := R_2 - .01R_1} \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 100 & 100 \end{array}\right)$$
$$\xrightarrow[R_1 := R_1 - R_2]{R_2 := \frac{1}{100}R_2} \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right).$$

We have avoided the numerical instability that resulted from dividing by .01, and our answer is now correct to three significant figures.

In view of these remarks and the comment 2.2.7 above, it is clear that when deciding which of the entries in a given column should be the next pivot, we should avoid those that are too close to zero.

Of all possible pivots in the column, always choose that which has the largest absolute value.

Choosing the pivots in this way is called *partial pivoting*. It is this procedure which is used in most practical problems.†

Some refinements to the partial pivoting algorithm may sometimes be necessary. For instance, if the system 2.2.8 above were modified by multiplying the whole of the first equation by 200 then partial pivoting as described above would select the entry in the first row and first column as the first pivot, and we would encounter the same problem as before. The situation can be remedied by scaling the rows before commencing pivoting, by dividing each row through by its entry of largest absolute value. This makes the rows commensurate, and reduces the likelihood of inaccuracies resulting from adding numbers of greatly differing magnitudes.

Finally, it is worth noting that although the claims made above seem reasonable, it is hard to justify them rigorously. This is because the best algorithm is not necessarily the best for all systems. There will always be cases where a less good algorithm happens to work well for a particular system. It is a daunting theoretical task to define the "goodness" of an algorithm in any reasonable way, and then use the concept to compare algorithms.

† In *complete pivoting* all the entries of all the remaining columns are compared when choosing the pivots. The resulting algorithm is slightly safer, but much slower.

§2d Elementary matrices

In this section we return to a discussion of general properties of matrices: properties that are true for matrices over any field. Accordingly, we will not specify any particular field; instead, we will use the letter 'F' to denote some fixed but unspecified field, and the elements of F will be referred to as 'scalars'. This convention will remain in force for most of the rest of this book, although from time to time we will restrict ourselves to the case $F = \mathbb{R}$, or impose some other restrictions on the choice of F. It is conceded, however, that the extra generality that we achieve by this approach is not of great consequence for the most common applications of linear algebra, and the reader is encouraged to think of scalars as ordinary numbers (since they usually are).

2.3 Definition Let m and n be positive integers. An *elementary row operation* is a function $\rho\colon \mathrm{Mat}(m \times n, F) \to \mathrm{Mat}(m \times n, F)$ such that either $\rho = \rho_{ij}$ for some $i, j \in \mathcal{I} = \{1, 2, \ldots, m\}$, or $\rho = \rho_i^{(\lambda)}$ for some $i \in \mathcal{I}$ and some nonzero scalar λ, or $\rho = \rho_{ij}^{(\lambda)}$ for some $i, j \in \mathcal{I}$ and some scalar λ, where ρ_{ij}, $\rho_{ij}^{(\lambda)}$ and $\rho_i^{(\lambda)}$ are defined as follows:

(i) $\rho_{ij}(A)$ is the matrix obtained from A by swapping the i^{th} and j^{th} rows;

(ii) $\rho_i^{(\lambda)}(A)$ is the matrix obtained from A by multiplying the i^{th} row by λ;

(iii) $\rho_{ij}^{(\lambda)}(A)$ is the matrix obtained from A by adding λ times the i^{th} row to the j^{th} row.

Comment ▷▷▷

2.3.1 Elementary column operations are defined similarly. ▷▷▷

2.4 Definition An *elementary matrix* is any matrix obtainable by applying an elementary row operation to an identity matrix. We use the following notation:

$$E_{ij} = \rho_{ij}(I), \qquad E_i^{(\lambda)} = \rho_i^{(\lambda)}(I), \qquad E_{ij}^{(\lambda)} = \rho_{ij}^{(\lambda)}(I),$$

where I denotes an identity matrix.

It can be checked that all elementary row operations have inverses. So it follows that they are bijective functions. The inverses are in fact also elementary row operations:

2.5 PROPOSITION *We have* $\rho_{ij}^{-1} = \rho_{ij}$ *and* $(\rho_{ij}^{(\lambda)})^{-1} = \rho_{ij}^{(-\lambda)}$ *for all* i, j *and* λ, *and if* $\lambda \neq 0$ *then* $(\rho_i^{(\lambda)})^{-1} = \rho_i^{(\lambda^{-1})}$.

The principal theorem about elementary row operations is that the effect of each is the same as premultiplication by the corresponding elementary matrix:

2.6 THEOREM *If* A *is a matrix of* m *rows and* $\mathcal{I}$ *is as in 2.3 then for all* i, $j \in \mathcal{I}$ *and* $\lambda \in F$ *we have that* $\rho_{ij}(A) = E_{ij}A$, $\rho_i^{(\lambda)}(A) = E_i^{(\lambda)}A$ *and* $\rho_{ij}^{(\lambda)}(A) = E_{ij}^{(\lambda)}A$.

Once again there must be corresponding results for columns. However, we do not have to define "column elementary matrices", since it turns out that the result of applying an elementary column operation to an identity matrix I is the same as the result of applying an appropriate elementary row operation to I. Let us use the following notation for elementary column operations:

(i) γ_{ij} swaps columns i and j,

(ii) $\gamma_i^{(\lambda)}$ multiplies column i by λ,

(iii) $\gamma_{ij}^{(\lambda)}$ adds λ times column i to column j.

We find that

2.7 THEOREM *If* γ *is an elementary column operation then* $\gamma(A) = A\gamma(I)$ *for all* A *and the appropriate* I. *Furthermore,* $\gamma_{ij}(I) = E_{ij}$, $\gamma_i^{(\lambda)}(I) = E_i^{(\lambda)}$ *and* $\gamma_{ij}^{(\lambda)}(I) = E_{ji}^{(\lambda)}$.

(Note that i and j occur in different orders on the two sides of the last equation in this theorem.)

—Example—

#3 Performing the elementary row operation $\rho_{21}^{(2)}$ (adding twice the second row to the first) on the 3×3 identity matrix yields the matrix

$$E = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So if A is any matrix with three rows then EA should be the result of performing $\rho_{21}^{(2)}$ on A. Thus, for example

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \end{pmatrix} = \begin{pmatrix} a+2e & b+2f & c+2g & d+2h \\ e & f & g & h \\ i & j & k & l \end{pmatrix},$$

which is indeed the result of adding twice the second row to the first. Observe that E is also obtainable by performing the elementary column operation $\gamma_{12}^{(2)}$ (adding twice the first column to the second) on the identity. So if B is any matrix with three columns, BE is the result of performing $\gamma_{12}^{(2)}$ on B. For example,

$$\begin{pmatrix} p & q & r \\ s & t & u \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} p & 2p+q & r \\ s & 2s+t & u \end{pmatrix}.$$

The pivoting algorithm described in the previous section gives the following fact.

2.8 Proposition *For each $A \in \mathrm{Mat}(m \times n, F)$ there exists a sequence of $m \times m$ elementary matrices E_1, E_2, …, E_k such that $E_k E_{k-1} \dots E_1 A$ is a reduced echelon matrix.*

If A is an $n \times n$ matrix then an *inverse* of A is a matrix B satisfying $AB = BA = I$. Matrices which have inverses are said to be *invertible*. It is easily proved that a matrix can have at most one inverse; so there can be no ambiguity in using the notation 'A^{-1}' for the inverse of an invertible A. Elementary matrices are invertible, and, as one would expect in view of 2.5, $E_{ij}^{-1} = E_{ij}$, $(E_i^{(\lambda)})^{-1} = E_i^{(\lambda^{-1})}$ and $(E_{ij}^{(\lambda)})^{-1} = E_{ij}^{(-\lambda)}$. A matrix which is a product of invertible matrices is also invertible, and we have $(AB)^{-1} = B^{-1}A^{-1}$.

The proofs of all the above results are easy and are omitted. In contrast, the following important fact is definitely nontrivial.

2.9 Theorem *If A, $B \in \mathrm{Mat}(n \times n, F)$ and if $AB = I$ then it is also true that $BA = I$. Thus A and B are inverses of each other.*

Proof. By 2.8 there exist $n \times n$ matrices T and R such that R is reduced echelon, T is a product of elementary matrices, and $TA = R$. Let r be the

number of nonzero rows of R, and let the leading entry of the i^{th} nonzero row occur in column j_i.

Since the leading entry of each nonzero row of R is further to the right than that of the preceding row, we must have $1 \leq j_1 < j_2 < \cdots < j_r \leq n$, and if all the rows of R are nonzero (so that $r = n$) this forces $j_i = i$ for all i. So either R has at least one zero row, or else the leading entries of the rows occur in the diagonal positions.

Since the leading entries in a reduced echelon matrix are all 1, and since all the other entries in a column containing a leading entry must be zero, it follows that if all the diagonal entries of R are leading entries then R must be just the identity matrix. So in this case we have $TA = I$. This gives $T = TI = T(AB) = (TA)B = IB = B$, and we deduce that $BA = I$, as required.

It remains to prove that it is impossible for R to have a zero row. Note that T is invertible, since it is a product of elementary matrices, and since $AB = I$ we have $R(BT^{-1}) = TABT^{-1} = TT^{-1} = I$. But the i^{th} row of $R(BT^{-1})$ is obtained by multiplying the i^{th} row of R by BT^{-1}, and will therefore be zero if the i^{th} row of R is zero. Since $R(BT^{-1}) = I$ certainly does not have a zero row, it follows that R does not have a zero row. □

Note that Theorem 2.9 applies to square matrices only. If A and B are not square it is in fact impossible for both AB and BA to be identity matrices, as the next result shows.

2.10 Theorem *If the matrix A has more rows than columns then it is impossible to find a matrix B such that $AB = I$.*

The proof, which we omit, is very similar to the last part of the proof of 2.9, and hinges on the fact that the reduced echelon matrix obtained from A by pivoting must have a zero row.

§2e Determinants

We will have more to say about determinants in Chapter Eight; for the present, we confine ourselves to describing a method for calculating determinants and stating some properties which we will prove in Chapter Eight.

Associated with every square matrix is a scalar called the *determinant* of the matrix. A 1×1 matrix is just a scalar, and its determinant is equal

to itself. For 2×2 matrices the rule is

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

We now proceed recursively. Let A be an $n \times n$ matrix, and assume that we know how to calculate the determinants of $(n-1) \times (n-1)$ matrices. We define the $(i,j)^{\text{th}}$ *cofactor* of A, denoted '$\operatorname{cof}_{ij}(A)$', to be $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the i^{th} row and j^{th} column of A. So, for example, if n is 3 we have

$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}$$

and we find that

$$\operatorname{cof}_{21}(A) = (-1)^3 \det \begin{pmatrix} A_{12} & A_{13} \\ A_{32} & A_{33} \end{pmatrix} = -A_{12}A_{33} + A_{13}A_{32}.$$

The determinant of A (for any n) is given by the so-called *first row expansion*:

$$\begin{aligned} \det A &= A_{11} \operatorname{cof}_{11}(A) + A_{12} \operatorname{cof}_{12}(A) + \cdots + A_{1n} \operatorname{cof}_{1n}(A) \\ &= \sum_{i=1}^{n} A_{1i} \operatorname{cof}_{1i}(A). \end{aligned}$$

(A better practical method for calculating determinants will be presented later.)

It turns out that a matrix A is invertible if and only if $\det A \neq 0$, and if $\det A \neq 0$ then the inverse of A is given by the formula

$$A^{-1} = \frac{1}{\det A} \operatorname{adj} A$$

where $\operatorname{adj} A$ (the *adjoint* matrix†) is the transposed matrix of cofactors; that is,

$$(\operatorname{adj} A)_{ij} = \operatorname{cof}_{ji}(A).$$

† called the *adjugate* matrix in an earlier edition of this book, since some misguided mathematicians use the term 'adjoint matrix' for the conjugate transpose of a matrix.

In particular, in the 2×2 case this says that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

provided that $ad - bc \neq 0$, a formula that can easily be verified directly. We remark that it is foolhardy to attempt to use the cofactor formula to calculate inverses of matrices, except in the 2×2 case and (occasionally) the 3×3 case; a much quicker method exists using row operations.

The most important properties of determinants are as follows.

(i) A square matrix A has an inverse if and only if $\det A \neq 0$.

(ii) Let A and B be $n \times n$ matrices. Then $\det(AB) = \det A \det B$.

(iii) Let A be an $n \times n$ matrix. Then $\det A = 0$ if and only if there exists a nonzero $n \times 1$ matrix x (that is, a column) satisfying the equation $Ax = 0$.

This last property is particularly important for the next section.

—***Example***—

#4 Calculate $\operatorname{adj} A$ and $(\operatorname{adj} A)A$ for the following matrix A:

$$A = \begin{pmatrix} 3 & -1 & 4 \\ -2 & -2 & 3 \\ 7 & 3 & -2 \end{pmatrix}.$$

⋙▷ The cofactors are as follows:

$$(-1)^2 \det\begin{pmatrix} -2 & 3 \\ 3 & -2 \end{pmatrix} = -5 \quad (-1)^3 \det\begin{pmatrix} -2 & 3 \\ 7 & -2 \end{pmatrix} = 17 \quad (-1)^4 \det\begin{pmatrix} -2 & -2 \\ 7 & 3 \end{pmatrix} = 8$$

$$(-1)^3 \det\begin{pmatrix} -1 & 4 \\ 3 & -2 \end{pmatrix} = 10 \quad (-1)^4 \det\begin{pmatrix} 3 & 4 \\ 7 & -2 \end{pmatrix} = -34 \quad (-1)^5 \det\begin{pmatrix} 3 & -1 \\ 7 & 3 \end{pmatrix} = -16$$

$$(-1)^4 \det\begin{pmatrix} -1 & 4 \\ -2 & 3 \end{pmatrix} = 5 \quad (-1)^5 \det\begin{pmatrix} 3 & 4 \\ -2 & 3 \end{pmatrix} = -17 \quad (-1)^6 \det\begin{pmatrix} 3 & -1 \\ -2 & -2 \end{pmatrix} = -8.$$

So the transposed matrix of cofactors is

$$\operatorname{adj} A = \begin{pmatrix} -5 & 10 & -16 \\ 17 & -34 & -17 \\ 8 & -16 & -8 \end{pmatrix}.$$

Hence we find that

$$\begin{aligned}(\operatorname{adj} A)A &= \begin{pmatrix} -5 & 10 & 5 \\ 17 & -34 & -17 \\ 8 & -16 & -8 \end{pmatrix} \begin{pmatrix} 3 & -1 & 4 \\ -2 & -2 & 3 \\ 7 & 3 & -2 \end{pmatrix} \\ &= \begin{pmatrix} -15-20+35 & 5-20+15 & -20+30-10 \\ 51+68-119 & -17+68-51 & 68-102+34 \\ 24+32-56 & -8+32-24 & 32-48+16 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.\end{aligned}$$

Since $(\operatorname{adj} A)A$ should equal $(\det A)I$, we conclude that $\det A = 0$. ⊲⊢≪

---

§2f Introduction to eigenvalues

2.11 Definition Let $A \in \operatorname{Mat}(n \times n, F)$. A scalar λ is called an *eigenvalue* of A if there exists a nonzero $v \in F^n$ such that $Av = \lambda v$. Any such v is called an *eigenvector*.

Comments ▷▷▷

2.11.1 Eigenvalues are sometimes called *characteristic roots* or *characteristic values*, and the words 'proper' and 'latent' are occasionally used instead of 'characteristic'.

2.11.2 Since the field $\mathbb{Q}$ of all rational numbers is contained in the field $\mathbb{R}$ of all real numbers, a matrix over $\mathbb{Q}$ can also be regarded as a matrix over $\mathbb{R}$. Similarly, a matrix over $\mathbb{R}$ can be regarded as a matrix over $\mathbb{C}$, the field of all complex numbers. It is a perhaps unfortunate fact that there are some rational matrices that have eigenvalues which are real or complex but not rational, and some real matrices which have non-real complex eigenvalues.

◁◁◁

2.12 Theorem *Let $A \in \operatorname{Mat}(n \times n, F)$. A scalar λ is an eigenvalue of A if and only if* $\det(A - \lambda I) = 0$.

Proof. For all $v \in F^n$ we have that $Av = \lambda v$ if and only if

$$(A - \lambda I)v = Av - \lambda v = 0.$$

By the last property of determinants mentioned in the previous section, a nonzero such v exists if and only if $\det(A - \lambda I) = 0$. □

—***Example***—

#5 Find the eigenvalues and corresponding eigenvectors of $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$.

⋙▷ We must find the values of λ for which $\det(A - \lambda I) = 0$. Now

$$\det(A - \lambda I) = \det \begin{pmatrix} 3-\lambda & 1 \\ 1 & 3-\lambda \end{pmatrix} = (3-\lambda)^2 - 1.$$

So $\det(A - \lambda I) = (4 - \lambda)(2 - \lambda)$, and the eigenvalues are 4 and 2.

To find eigenvectors corresponding to the eigenvalue 2 we must find nonzero columns v satisfying $(A - 2I)v = 0$; that is, we must solve

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

Trivially we find that all solutions are of the form $\begin{pmatrix} \xi \\ -\xi \end{pmatrix}$, and hence that any nonzero ξ gives an eigenvector. Similarly, solving

$$\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

we find that the columns of the form $\begin{pmatrix} \xi \\ \xi \end{pmatrix}$ with $\xi \neq 0$ are the eigenvectors corresponding to 4 . ⋘◁

As we discovered in the above example the equation $\det(A - \lambda I) = 0$, which we must solve in order to find the eigenvalues of A, is a polynomial equation for λ. It is called the *characteristic equation* of A. The polynomial involved is of considerable theoretical importance.

2.13 Definition Let $A \in \mathrm{Mat}(n \times n, F)$ and let x be an indeterminate. The polynomial $f(x) = \det(A - xI)$ is called the *characteristic polynomial* of A.

Some authors define the characteristic polynomial to be $\det(xI - A)$, which is the same as ours if n is even, the negative of ours if n is odd. Observe

that the characteristic roots (eigenvalues) are the roots of the characteristic polynomial.

A square matrix A is said to be *diagonal* if $A_{ij} = 0$ whenever $i \neq j$. As we shall see in examples below and in the exercises, the following problem arises naturally in the solution of systems simultaneous differential equations:

2.13.1 Given a square matrix A, find an invertible matrix P such that $P^{-1}AP$ is diagonal.

Solving this problem is sometimes called "diagonalizing A". Eigenvalue theory is used to do it.

—***Examples***—

#6 Diagonalize the matrix $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$.

≫→ We have calculated the eigenvalues and eigenvectors of A in #5 above, and so we know that

$$\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 2 \\ -2 \end{pmatrix}$$

and

$$\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$$

and using Proposition 2.2 to combine these into a single matrix equation gives

2.13.2
$$\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ -2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}.$$

Defining now

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

we see that $\det P = 2 \neq 0$, and hence P^{-1} exists. It follows immediately from 2.13.2 that $P^{-1}AP = \operatorname{diag}(2, 4)$. ←≪

#7 Solve the simultaneous differential equations

$$x'(t) = 3x(t) + y(t)$$
$$y'(t) = x(t) + 3y(t).$$

⋙▷ We may write the equations as

$$\frac{d}{dt}\begin{pmatrix} x \\ y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix}$$

where A is the matrix from our previous example. The method is to find a change of variables which simplifies the equations. Choose new variables u and v related to x and y by

$$\begin{pmatrix} x \\ y \end{pmatrix} = P\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} p_{11}u + p_{12}v \\ p_{21}u + p_{22}v \end{pmatrix}$$

where p_{ij} is the $(i,j)^{\text{th}}$ entry of P. We require P to be invertible, so that it is possible to express u and v in terms of x and y, and the entries of P must constants, but there are no other restrictions. Differentiating, we obtain

$$\frac{d}{dt}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \frac{d}{dt}(p_{11}u + p_{12}v) \\ \frac{d}{dt}(p_{21}u + p_{22}v) \end{pmatrix} = \begin{pmatrix} p_{11}u' + p_{12}v' \\ p_{21}u' + p_{22}v' \end{pmatrix} = P\begin{pmatrix} u' \\ v' \end{pmatrix}$$

since the p_{ij} are constants. In terms of u and v the equations now become

$$P\begin{pmatrix} u' \\ v' \end{pmatrix} = AP\begin{pmatrix} u \\ v \end{pmatrix}$$

or, equivalently,

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = P^{-1}AP\begin{pmatrix} u \\ v \end{pmatrix}.$$

That is, in terms of the new variables the equations are of exactly the same form as before, but the coefficient matrix A has been replaced by $P^{-1}AP$. We naturally wish choose the matrix P in such a way that $P^{-1}AP$ is as simple as possible, and as we have seen in the previous example it is possible (in this case) to arrange that $P^{-1}AP$ is diagonal. To do so we choose P to be any invertible matrix whose columns are eigenvectors of A. Hence we define

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

(which means that $x = u + v$ and $y = -u + v$).

Our new equations now are

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

or, on expanding, $u' = 2u$ and $v' = 4v$. The solution to this is $u = He^{2t}$ and $v = Ke^{4t}$ where H and K are arbitrary constants, and this gives

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} He^{2t} \\ Ke^{4t} \end{pmatrix} = \begin{pmatrix} He^{2t} + Ke^{4t} \\ -He^{2t} + Ke^{4t} \end{pmatrix}$$

so that the most general solution to the original problem is $x = He^{2t} + Ke^{4t}$ and $y = -He^{2t} + Ke^{4t}$, where H and K are arbitrary constants. ⊲⊣≪

#8 Another typical application involving eigenvalues is the *Leslie population model*. We are interested in how the size of a population varies as time passes. At regular intervals the number of individuals in various age groups is counted. At time t let

$$\begin{aligned} x_1(t) &= \text{the number of individuals aged between 0 and 1} \\ x_2(t) &= \text{the number of individuals aged between 1 and 2} \\ &\vdots \\ x_n(t) &= \text{the number of individuals aged between } n-1 \text{ and } n \end{aligned}$$

where n is the maximum age ever attained. Censuses are taken at times $t = 0, 1, 2, \ldots$ and it is observed that

$$\begin{aligned} x_2(i+1) &= b_1 x_1(i) \\ x_3(i+1) &= b_2 x_2(i) \\ &\vdots \\ x_n(i+1) &= b_{n-1} x_{n-1}(i). \end{aligned}$$

Thus, for example, $b_1 = 0.95$ would mean that 95% of those aged between 0 and 1 at one census survive to be aged between 1 and 2 at the next. We also find that

$$x_1(i+1) = a_1 x_1(i) + a_2 x_2(i) + \cdots + a_n x_n(i)$$

for some constants $a_1, a_2, \ldots, a_n$. That is, the a_i measure the contributions to the birth rate from the different age groups. In matrix notation

$$\begin{pmatrix} x_1(i+1) \\ x_2(i+1) \\ x_3(i+1) \\ \vdots \\ x_n(i+1) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{n-1} & a_n \\ b_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & b_2 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & b_{n-1} & 0 \end{pmatrix} \begin{pmatrix} x_1(i) \\ x_2(i) \\ x_3(i) \\ \vdots \\ x_n(i) \end{pmatrix}$$

or $\underset{\sim}{x}(i+1) = L\underset{\sim}{x}(i)$, where $\underset{\sim}{x}(t)$ is the column with $x_j(t)$ as its j^{th} entry and

$$L = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_{n-1} & a_n \\ b_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & b_2 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & b_{n-1} & 0 \end{pmatrix}$$

is the *Leslie matrix*.

Assuming this relationship between $\underset{\sim}{x}(i+1)$ and $\underset{\sim}{x}(i)$ persists indefinitely we see that $\underset{\sim}{x}(k) = L^k\underset{\sim}{x}(0)$. We are interested in the behaviour of $L^k\underset{\sim}{x}(0)$ as $k \to \infty$. It turns out that in fact this behaviour depends on the largest eigenvalue of L, as we can see in an oversimplified example.

Suppose that $n = 2$ and $L = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. That is, there are just two age groups (young and old), and

(i) all young individuals survive to become old in the next era ($b_1 = 1$),

(ii) on average each young individual gives rise to one offspring in the next era, and so does each old individual ($a_1 = a_2 = 1$).

The eigenvalues of L are $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$, and the corresponding eigenvectors are $\begin{pmatrix} (1+\sqrt{5})/2 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} (1-\sqrt{5})/2 \\ 1 \end{pmatrix}$ respectively.

Suppose that there are initially one billion young and one billion old individuals. This tells us $\underset{\sim}{x}(0)$. By solving equations we can express $\underset{\sim}{x}(0)$ in terms of the eigenvectors:

$$\underset{\sim}{x}(0) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1+\sqrt{5}}{2\sqrt{5}} \begin{pmatrix} (1+\sqrt{5})/2 \\ 1 \end{pmatrix} - \frac{1-\sqrt{5}}{2\sqrt{5}} \begin{pmatrix} (1-\sqrt{5})/2 \\ 1 \end{pmatrix}.$$

We deduce that

$$\begin{aligned}\underset{\sim}{x}(k) &= L^k \underset{\sim}{x}(0) \\ &= \frac{1+\sqrt{5}}{2\sqrt{5}} L^k \begin{pmatrix} (1+\sqrt{5})/2 \\ 1 \end{pmatrix} - \frac{1-\sqrt{5}}{2\sqrt{5}} L^k \begin{pmatrix} (1-\sqrt{5})/2 \\ 1 \end{pmatrix} \\ &= \frac{1+\sqrt{5}}{2\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^k \begin{pmatrix} (1+\sqrt{5})/2 \\ 1 \end{pmatrix} \\ &\qquad - \frac{1-\sqrt{5}}{2\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^k \begin{pmatrix} (1-\sqrt{5})/2 \\ 1 \end{pmatrix}.\end{aligned}$$

But $\big((1-\sqrt{5})/2\big)^k$ becomes insignificant in comparison with $\big((1+\sqrt{5})/2\big)^k$ as $k \to \infty$. We see that for k large

$$\underset{\sim}{x}(k) \approx \frac{1}{\sqrt{5}} \begin{pmatrix} \big((1+\sqrt{5})/2\big)^{k+2} \\ \big((1+\sqrt{5})/2\big)^{k+1} \end{pmatrix}.$$

So in the long term the ratio of young to old approaches $(1+\sqrt{5})/2$, and the size of the population is multiplied by $(1+\sqrt{5})/2$ (the largest eigenvalue) per unit time.

#9 Let $f(x, y)$ be a smooth real valued function of two real variables, and suppose that we are interested in the behaviour of f near some fixed point. Choose that point to be the origin of our coordinate system. Under appropriate conditions $f(x, y)$ can be approximated by a Taylor series

$$f(x, y) \approx p + qx + ry + sx^2 + 2txy + uy^2 + \cdots$$

where higher order terms become less and less significant as (x, y) is made closer and closer to $(0, 0)$. For the first few terms we can conveniently use matrix notation, and write

2.13.3 $$f(\underset{\sim}{x}) \approx p + L\underset{\sim}{x} + {}^{\mathrm{t}}\underset{\sim}{x}\, Q\underset{\sim}{x}$$

where $L = \begin{pmatrix} q & r \end{pmatrix}$ and $Q = \begin{pmatrix} s & t \\ t & u \end{pmatrix}$, and $\underset{\sim}{x}$ is the two-component column with entries x and y. Note that the entries of L are given by the first order partial derivatives of f at $\underset{\sim}{0}$, and the entries of Q are given by the second

order partial derivatives of f at $\underset{\sim}{0}$. Furthermore, 2.13.3 is equally valid when $\underset{\sim}{x}$ has more than two components.

In the case that $\underset{\sim}{0}$ is a *critical point* of f the terms of degree 1 disappear, and the behaviour of f near $\underset{\sim}{0}$ is determined by the *quadratic form* ${}^{\mathrm{t}}\underset{\sim}{x}\,Q\underset{\sim}{x}$. To understand ${}^{\mathrm{t}}\underset{\sim}{x}\,Q\underset{\sim}{x}$ it is important to be able to rotate the axes so as to eliminate product terms like xy and be left only with the square terms. We will return to this problem in Chapter Five, and show that it can always be done. That the eigenvalues of the matrix Q are of crucial importance can be seen easily in the two variable case, as follows.

Rotating the axes through an angle θ introduces new variables x' and y' related to the old variables by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

or, equivalently

$$\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} x' & y' \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

That is, $\underset{\sim}{x} = T\underset{\sim}{x}'$ and ${}^{\mathrm{t}}\underset{\sim}{x} = {}^{\mathrm{t}}(\underset{\sim}{x}'){}^{\mathrm{t}}T$. Substituting this into the expression for our quadratic form gives

$${}^{\mathrm{t}}(\underset{\sim}{x}') \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} s & t \\ t & u \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \underset{\sim}{x}'$$

or ${}^{\mathrm{t}}(\underset{\sim}{x}')\,{}^{\mathrm{t}}TQT\underset{\sim}{x}'$. Our aim is to choose θ so that $Q' = {}^{\mathrm{t}}TQT$ is diagonal. Since it happens that the transpose of the rotation matrix T coincides with its inverse, this is the same problem introduced in 2.13.1 above. It is because Q is its own transpose that a diagonalizing matrix T can be found satisfying $T^{-1} = {}^{\mathrm{t}}T$.

The diagonal entries of the diagonal matrix Q' are just the eigenvalues of Q. It can be seen that if the eigenvalues are both positive then the critical point 0 is a local minimum. The corresponding fact is true in the n-variable case: if all eigenvalues of Q are positive then we have a local minimum. Likewise, if all are negative then we have a local maximum. If some eigenvalues are negative and some are positive it is neither a maximum nor a minimum. Since the determinant of Q' is the product of the eigenvalues,

and since $\det Q = \det Q'$, it follows in the two variable case that we have a local maximum or minimum if and only if $\det Q > 0$. For n variables the test is necessarily more complicated.

#10 We remark also that eigenvalues are of crucial importance in questions of numerical stability in the solving of equations. If x and b are related by $Ax = b$ where A is a square matrix, and if it happens that A has an eigenvalue very close to zero and another eigenvalue with a large absolute value, then it is likely that small changes in either x or b will produce large changes in the other. For example, if

$$A = \begin{pmatrix} 100 & 0 \\ 0 & 0.01 \end{pmatrix}$$

then changing the first component of x by 0.1 changes the first component of b by 10, while changing the second component of b by 0.1 changes the second component of x by 10. If, as in this example, the matrix A is equal to its own transpose, the *condition number* of A is defined as the ratio of the largest eigenvalue of A to the smallest eigenvalue of A, and A is ill-conditioned (see §2c) if the condition number is too large.

Whilst on numerical matters, we remark that numerical calculation of eigenvalues is an important practical problem. One method is to make use of the fact that (usually) if A is a square matrix and x a column then as $k \to \infty$ the columns $A^k x$ tend to approach scalar multiples of an eigenvector. (We saw this in #8 above.) In practice, especially for large matrices, the best numerical methods for calculating eigenvalues do not depend upon direct solution of the characteristic equation.

Exercises

1. Prove that matrix addition is associative ($A + (B + C) = (A + B) + C$ for all A, B and C) and commutative ($A + B = B + A$ for all A and B).

2. Prove that if A is an $m \times n$ matrix and I_m and I_n are (respectively) the $m \times m$ and $n \times n$ identity matrices then $AI_n = A = I_m A$.

3. Prove that if A, B and C are matrices of appropriate shapes and λ and μ are arbitrary numbers then $A(\lambda B + \mu C) = \lambda(AB) + \mu(AC)$.

4. Use the properties of matrix addition and multiplication from the previous exercises together with associativity of matrix multiplication to prove that a square matrix can have at most one inverse.

5. Check, by tedious expansion, that the formula $A(\operatorname{adj} A) = (\det A)I$ is valid for any 3×3 matrix A.

6. Prove that ${}^{\mathrm{t}}(AB) = ({}^{\mathrm{t}}B)({}^{\mathrm{t}}A)$ for all matrices A and B such that AB is defined. Prove that if the entries of A and B are complex numbers then $\overline{AB} = \overline{A}\,\overline{B}$. (If X is a complex matrix then $\overline{X}$ is the matrix whose (i,j)-entry is the complex conjugate of X_{ij}.)

7. A particle moves in the plane, its coordinates at time t being $(x(t), y(t))$ where x and y are differentiable functions on $[0, \infty)$. Suppose that

$$(*) \qquad \begin{aligned} x'(t) &= \quad -2y(t) \\ y'(t) &= x(t) + 3y(t) \end{aligned}$$

Show (by direct calculation) that the equations $(*)$ can be solved by putting $x(t) = 2z(t) - w(t)$ and $y(t) = -z(t) + w(t)$, and obtaining differential equations for z and w.

8. (i) Show that if ξ is an eigenvalue of the 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then ξ is a solution of the quadratic equation

$$x^2 - (a+d)x + (ad - bc) = 0.$$

Hence find the eigenvalues of the matrix $\begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix}$.

(ii) Find an eigenvector for each of these eigenvalues.

9. (i) Suppose that A is an $n \times n$ matrix and that $\xi_1, \xi_2, \ldots, \xi_n$ are eigenvalues for A. For each i let v_i be an eigenvector corresponding to the eigenvalue ξ, and let P be the $n \times n$ matrix whose n columns are $v_1, v_2, \ldots, v_n$ (in that order). Show that $AP = PD$, where D is the diagonal matrix with diagonal entries $\xi_1, \xi_2, \ldots, \xi_n$. (That is, $D_{ij} = \xi_i \delta_{ij}$, where δ_{ij} is the Kronecker delta.)

(*ii*) Use the previous exercise to find a matrix P such that

$$\begin{pmatrix} 0 & -2 \\ 1 & 3 \end{pmatrix} P = P \begin{pmatrix} \xi & 0 \\ 0 & \nu \end{pmatrix}$$

where ξ and ν are the eigenvalues of the matrix on the left. (Note the connection with Exercise 7.)

10. Calculate the eigenvalues of the following matrices, and for each eigenvalue find an eigenvector.

(a) $\begin{pmatrix} 4 & 2 \\ -1 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 2 & -2 & 7 \\ 0 & -1 & 4 \\ 0 & 0 & 5 \end{pmatrix}$ (c) $\begin{pmatrix} -7 & -2 & 6 \\ -2 & 1 & 2 \\ -10 & -2 & 9 \end{pmatrix}$

11. Solve the system of differential equations

$$\begin{aligned} x' &= -7x - 2y + 6z \\ y' &= -2x + y + 2z \\ z' &= -10x - 2y + 9z. \end{aligned}$$

12. Let A be an $n \times n$ matrix. Prove that the characteristic polynomial $c_A(x)$ of A has degree n. Prove also that the leading coefficient of $c_A(x)$ is $(-1)^n$, the coefficient of x^{n-1} is $(-1)^{n-1} \sum_{i=1}^{n} A_{ii}$, and the constant term is $\det A$. (Hint: Use induction on n.)

3
Introduction to vector spaces

Pure Mathematicians love to generalize ideas. If they manage, by means of a new trick, to prove some conjecture, they always endeavour to get maximum mileage out of the idea by searching for other situations in which it can be used. To do this successfully one must discard unnecessary details and focus attention only on what is really needed to make the idea work; furthermore, this should lead both to simplifications and deeper understanding. It also leads naturally to an axiomatic approach to mathematics, in which one lists initially as axioms all the things which have to hold before the theory will be applicable, and then attempts to derive consequences of these axioms. Potentially this kills many birds with one stone, since good theories are applicable in many different situations.

We have alreay used the axiomatic approach in Chapter 1 in the definition of 'field', and in this chapter we proceed to the definition of 'vector space'. We start with a discussion of linearity, since one of the major reasons for introducing vector spaces is to provide a suitable context for discussion of this concept.

§3a Linearity

A common mathematical problem is to solve a system of equations of the form

3.0.1 $$T(x) = 0.$$

Depending on the context the unknown x could be a number, or something more complicated, such as an n-tuple, a function, or even an n-tuple of functions. For instance the simultaneous linear equations

3.0.2 $$\begin{pmatrix} 3 & 1 & 1 & 1 \\ -1 & 1 & -1 & 2 \\ 4 & 4 & 0 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

have the form 3.0.1 with x a 4-tuple, and the differential equation

3.0.3 $$t^2\, d^2x/dt^2 + t\, dx/dt + (t^2-4)x = 0$$

is an example in which x is a function. Similarly, the pair of simultaneous differential equations

$$df/dt = 2f + 3g$$
$$dg/dt = 2f + 7g$$

could be rewritten as

3.0.4 $$\frac{d}{dt}\begin{pmatrix} f \\ g \end{pmatrix} - \begin{pmatrix} 2 & 3 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

which is also has the form 3.0.1, with x being an ordered pair of functions.

Whether or not one can solve the system 3.0.1 obviously depends on the nature of the expression $T(x)$ on the left hand side. In this course we will be interested in cases in which $T(x)$ is *linear* in x.

3.1 Definition An expression $T(x)$ is said to be *linear in the variable* x if

$$T(x_1 + x_2) = T(x_1) + T(x_2)$$

for all values x_1 and x_2 of the variable, and

$$T(\lambda x) = \lambda T(x)$$

for all values of x and all scalars λ.

If we let $T(x)$ denote the expression on the left hand side of the equation 3.0.3 above we find that

$$\begin{aligned} T(x_1+x_2) &= t^2\frac{d^2}{dt^2}(x_1+x_2) + t\frac{d}{dt}(x_1+x_2) + (t^2-4)(x_1+x_2) \\ &= t^2(d^2x_1/dt^2 + d^2x_2/dt^2) + t(dx_1/dt + dx_2/dt) \\ &\qquad + (t^2-4)x_1 + (t^2-4)x_2 \\ &= \big(t^2d^2x_1/dt^2 + tdx_1/dt + (t^2-4)x_1\big) \\ &\qquad + \big(t^2d^2x_2/dt^2 + tdx_2/dt + (t^2-4)x_2\big) \\ &= T(x_1) + T(x_2) \end{aligned}$$

and

$$\begin{aligned} T(\lambda x) &= t^2\frac{d^2}{dt^2}(\lambda x) + t\frac{d}{dt}(\lambda x) + (t^2-4)\lambda x \\ &= \lambda(t^2d^2x/dt^2 + tdx/dt + (t^2-4)x) \\ &= \lambda T(x). \end{aligned}$$

Thus $T(x)$ is a linear expression, and for this reason 3.0.3 is called a *linear differential equation*. It is left for the reader to check that 3.0.2 and 3.0.4 above are also linear equations.

—***Example***—

#1 Suppose that T is linear in x, and let $x = x_0$ be a particular solution of the equation $T(x) = a$. Show that the general solution of $T(x) = a$ is $x = x_0 + y$ for $y \in S$, where S is the set of all solutions of $T(y) = 0$.

⋙▷ We are given that $T(x_0) = a$. Let $y \in S$, and put $x = x_0 + y$. Then $T(y) = 0$, and linearity of T yields

$$T(x) = T(x_0 + y) = T(x_0) + T(y) = a + 0 = a,$$

and we have shown that $x = x_0 + y$ is a solution of $T(x) = a$ whenever $y \in S$.

Now suppose that x is any solution of $T(x) = a$, and define $y = x - x_0$. Then we have that $x = x_0 + y$, and by linearity of T we find that

$$T(y) = T(x - x_0) = T(x) - T(x_0) = a - a = 0,$$

so that $y \in S$. Hence all solutions of $T(x) = a$ have the given form. ◁⋘

Our definition of linearity may seem reasonable at first sight, but a closer inspection reveals some deficiencies. The term 'expression in x' is a little imprecise; in fact T is simply a function, and we should really have said something like this:

3.1.1 A function $T: V \to W$ is linear if $T(x_1 + x_2) = T(x_1) + T(x_2)$ and $T(\lambda x) = \lambda T(x)$ for all $x_1, x_2, x \in V$ and all scalars λ.

For this to be meaningful V and W have to both be equipped with operations of addition, and one must also be able to multiply elements of V and W by scalars.

The set of all $m \times n$ matrices (where m and n are fixed) provides an example of a set equipped with addition and scalar multiplication: with the definitions as given in Chapter 1, the sum of two $m \times n$ matrices is another $m \times n$ matrix, and a scalar multiple of an $m \times n$ matrix is an $m \times n$ matrix. We have also seen that addition and scalar multiplication of rows and columns arises naturally in the solution of simultaneous equations; for

instance, we expressed the general solution of 2.2.4 in terms of addition and scalar multiplication of columns. Finally, we can define addition and scalar multiplication for real valued differentiable functions. If x and y are such functions then $x + y$ is the real valued differentiable function defined by $(x + y)(t) = x(t) + y(t)$, and if $\lambda \in \mathbb{R}$ then λx is the function defined by $(\lambda x)(t) = \lambda x(t)$; these definitions were implicit in our discussion of 3.0.3 above.

Roughly speaking, a vector space is a set for which addition and scalar multiplication are defined in some sensible fashion. By "sensible" I mean that a certain list of obviously desirable properties must be satisfied. It will then make sense to ask whether a function from one vector space to another is linear in the sense of 3.1.1.

§3b Vector axioms

In accordance with the above discussion, a vector space should be a set (whose elements will be called *vectors*) which is equipped with an operation of addition, and a scalar multiplication function which determines an element λx of the vector space whenever x is an element of the vector space and λ is a scalar. That is, if x and y are two vectors then their sum $x + y$ must exist and be another vector, and if x is a vector and λ a scalar then λx must exist and be vector.

3.2 Definition Let F be a field. A set V is called a *vector space over* F if there is an operation of addition

$$(x, y) \longmapsto x + y$$

on V, and a scalar multiplication function

$$(\lambda, x) \longmapsto \lambda x$$

from $F \times V$ to V, such that the following properties are satisfied.

(i) $(u + v) + w = u + (v + w)$ for all u, v, $w \in V$.
(ii) $u + v = v + u$ for all u, $v \in V$.
(iii) There exists an element $0 \in V$ such that $0 + v = v$ for all $v \in V$.
(iv) For each $v \in V$ there exists a $u \in V$ such that $u + v = 0$.
(v) $1v = v$ for all $v \in V$.
(vi) $\lambda(\mu v) = (\lambda\mu)v$ for all λ, $\mu \in F$ and all $v \in V$.
(vii) $(\lambda + \mu)v = \lambda v + \mu v$ for all λ, $\mu \in F$ and all $v \in V$.

(viii) $\lambda(u+v) = \lambda u + \lambda v$ for all $\lambda \in F$ and all $u, v \in V$.

Comments ▷▷▷

3.2.1 The field of scalars F and the vector space V both have zero elements which are both commonly denoted by the symbol '0'. With a little care one can always tell from the context whether 0 means the zero scalar or the zero vector. Sometimes we will distinguish notationally between vectors and scalars by writing a tilde underneath vectors; thus $\underset{\sim}{0}$ would denote the zero of the vector space under discussion.

3.2.2 The 1 which appears in axiom (v) is the scalar 1; there is no vector 1. ▷▷▷

—***Examples***—

#2 Let $\mathcal{P}$ be the Euclidean plane and choose a fixed point $O \in \mathcal{P}$. The set of all line segments OP, as P varies over all points of the plane, can be made into a vector space over $\mathbb{R}$, called the space of position vectors relative to O. The sum of two line segments is defined by the parallelogram rule; that is, for $P, Q \in \mathcal{P}$ find the point R such that $OPRQ$ is a parallelogram, and define $OP + OQ = OR$. If λ is a positive real number then λOP is the line segment OS such that S lies on OP or OP produced and the length of OS is λ times the length of OP. For negative λ the product λOP is defined similarly (giving a point on PO produced).

The proofs that the vector space axioms are satisfied are nontrivial exercises in Euclidean geometry. The same construction is also applicable in three dimensional Euclidean space.

#3 The set $\mathbb{R}^3$, consisting of all ordered triples of real numbers, is an example of a vector space over $\mathbb{R}$. Addition and scalar multiplication are defined in the usual way:

$$\begin{pmatrix} x_1 \\ y_1 \\ z_2 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ z_1 + z_2 \end{pmatrix}$$

$$\lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \\ \lambda z \end{pmatrix}$$

for all real numbers λ, x, x_1, ... etc.. It is trivial to check that the axioms listed in the definition above are satisfied. Of course, the use of Cartesian

coordinates shows that this vector space is essentially the same as position vectors in Euclidean space; you should convince yourself that componentwise addition really does correspond to the parallelogram law.

#4 The set $\mathbb{R}^n$ of all n-tuples of real numbers is a vector space over $\mathbb{R}$ for all positive integers n. Everything is completely analogous to $\mathbb{R}^3$. (Recall that we have defined

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \;\middle|\; x_i \in \mathbb{R} \text{ for all } i \right\}$$

$$^{\mathrm{t}}\mathbb{R}^n = \{ \begin{pmatrix} x_1 & x_2 & \dots & x_n \end{pmatrix} \mid x_i \in \mathbb{R} \text{ for all } i \}.$$

It is clear that $^{\mathrm{t}}\mathbb{R}^n$ is also a vector space.)

#5 If F is any field then F^n and $^{\mathrm{t}}F^n$ are both vector spaces over F. These spaces of n-tuples are the most important examples of vector spaces, and the first examples to think of when trying to understand theoretical results.

#6 Let S be any set and let $\mathcal{S}$ be the set of all functions from S to F (where F is a field). If $f, g \in \mathcal{S}$ and $\lambda \in F$ define $f + g$, $\lambda f \in \mathcal{S}$ as follows:

$$(f+g)(a) = f(a) + g(a)$$
$$(\lambda f)(a) = \lambda\big(f(a)\big)$$

for all $a \in S$. (Note that addition and multiplication on the right hand side of these equations take place in F; you do not have to be able to add and multiply elements of S for the definitions to make sense.) It can now be shown these definitions of addition and scalar multiplication make $\mathcal{S}$ into a vector space over F; to do this we must verify that all the axioms are satisfied. In each case the proof is routine, based on the fact that F satisfies the field axioms.

(i) Let $f, g, h \in \mathcal{S}$. Then for all $a \in S$,

$$\begin{aligned} \big((f+g)+h\big)(a) &= (f+g)(a) + h(a) && \text{(by definition addition on } \mathcal{S}) \\ &= (f(a)+g(a)) + h(a) && \text{(same reason)} \\ &= f(a) + (g(a)+h(a)) && \text{(addition in } F \text{ is associative)} \\ &= f(a) + (g+h)(a) && \text{(definition of addition on } \mathcal{S}) \\ &= \big(f+(g+h)\big)(a) && \text{(same reason)} \end{aligned}$$

and so $(f+g)+h = f+(g+h)$.

(ii) Let f, $g \in \mathcal{S}$. Then for all $a \in S$,

$$\begin{aligned}(f+g)(a) &= f(a)+g(a) && \text{(by definition)}\\ &= g(a)+f(a) && \text{(since addition in } F \text{ is commutative)}\\ &= (g+f)(a) && \text{(by definition)},\end{aligned}$$

so that $f+g = g+f$.

(iii) Define $z\colon S \to F$ by $z(a) = 0$ (the zero element of F) for all $a \in S$. We must show that this *zero function* z satisfies $f+z = f$ for all $f \in \mathcal{S}$. For all $a \in S$ we have

$$(f+z)(a) = f(a)+z(a) = f(a)+0 = f(a)$$

by the definition of addition in $\mathcal{S}$ and the Zero Axiom for fields, whence the result.

(iv) Suppose that $f \in \mathcal{S}$. Define $g \in \mathcal{S}$ by $g(a) = -f(a)$ for all $a \in S$. Then for all $a \in S$,

$$(g+f)(a) = g(a)+f(a) = 0 = z(a),$$

so that $g+f = z$. Thus each element of $\mathcal{S}$ has a negative.

(v) Suppose that $f \in \mathcal{S}$. By definition of scalar multiplication for $\mathcal{S}$ and the Identity Axiom for fields, we have, for all $a \in S$,

$$(1f)(a) = 1\big(f(a)\big) = f(a)$$

and therefore $1f = f$.

(vi) Let λ, $\mu \in F$ and $f \in \mathcal{S}$. Then for all $a \in S$,

$$\big(\lambda(\mu f)\big)(a) = \lambda\big((\mu f)(a)\big) = \lambda(\mu\, f(a)) = (\lambda\mu)\, f(a) = \big((\lambda\mu)f\big)(a)$$

by the definition of scalar multiplication for $\mathcal{S}$ and associativity of multiplication in the field F. Thus $\lambda(\mu f) = (\lambda\mu)f$.

(vii) Let λ, $\mu \in F$ and $f \in \mathcal{S}$. Then for all $a \in S$,

$$\begin{aligned}\big((\lambda+\mu)f\big)(a) = (\lambda+\mu)\big(f(a)\big) &= \lambda\, f(a)+\mu\, f(a)\\ &= (\lambda f)(a)+(\mu f)(a) = (\lambda f+\mu f)(a)\end{aligned}$$

by the definition of addition and scalar multiplication for $\mathcal{S}$ and the distributive law in F. Thus $(\lambda+\mu)f = \lambda f + \mu f$.

(viii) Let $\lambda \in F$ and $f, g \in \mathcal{S}$. Then for all $a \in S$,

$$\begin{aligned}\big(\lambda(f+g)\big)(a) &= \lambda\big((f+g)(a)\big) = \lambda\big(f(a)+g(a)\big)\\ &= \lambda\, f(a) + \lambda\, g(a) = (\lambda f)(a) + (\lambda g)(a) = (\lambda f + \lambda g)(a),\end{aligned}$$

whence $\lambda(f+g) = \lambda f + \lambda g$.

Observe that if $S = \{1, 2, \ldots, n\}$ then the set $\mathcal{S}$ is essentially the same as F^n, since an n-tuple $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ in F^n may be identified with the function $f\colon\{1, 2, \ldots, n\} \to F$ given by $f(i) = a_i$ for $i = 1, 2, \ldots, n$; it is readily checked that the definitions of addition and scalar multiplication for n-tuples are consistent with the definitions of addition and scalar multiplication for functions. (Indeed, since we have defined a column to be an $n \times 1$ matrix, and a matrix to be a function, F^n is in fact the set of all functions from $S \times \{1\}$ to F. There is an obvious bijective correspondence between the sets S and $S \times \{1\}$.)

#7 The set $\mathcal{C}$ of all continuous functions $f\colon\mathbb{R} \to \mathbb{R}$ is a vector space over $\mathbb{R}$, addition and scalar multiplication being defined as in the previous example. It is necessary to show that these definitions do give well defined functions $\mathcal{C} \times \mathcal{C} \to \mathcal{C}$ (for addition) and $\mathbb{R} \times \mathcal{C} \to \mathcal{C}$ (for scalar multiplication). In other words, one must show that if f and g are continuous and $\lambda \in \mathbb{R}$ then $f+g$ and λf are continuous. This follows from elementary calculus. It is necessary also to show that the vector space axioms are satisfied; this is routine to do, and similar to the previous example.

#8 The set of all continuously differentiable functions from $\mathbb{R}$ to $\mathbb{R}$, the set of all three times differentiable functions from $(-1, 1)$ to $\mathbb{R}$, and the set of all integrable functions from $[0, 10]$ to $\mathbb{R}$ are further examples of vector spaces over $\mathbb{R}$, and there are many similar examples. It is also straightforward to show that the set of all polynomial functions from $\mathbb{R}$ to $\mathbb{R}$ is a vector space over $\mathbb{R}$.

#9 The solution set of a linear equation $T(x) = 0$ is always a vector space.

Thus, for instance, the subset of $\mathbb{R}^3$ consisting of all triples $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ such that

$$\begin{pmatrix} 1 & 0 & 5 \\ 2 & 1 & 2 \\ 4 & 4 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

is a vector space.

Stating the result more precisely, if V and W are vector spaces over a field F and $T: V \to W$ is a linear function then the set

$$U = \{\, x \in V \mid T(x) = 0 \,\}$$

is a vector space over F, relative to addition and scalar multiplication functions "inherited" from V. To prove this one must first show that if x, $y \in U$ and $\lambda \in F$ then $x + y$, $\lambda x \in U$ (so that we do have well defined addition and scalar multiplication functions for U), and then check the axioms. If $T(x) = T(y) = 0$ and $\lambda \in F$ then linearity of T gives

$$T(x + y) = T(x) + T(y) = 0 + 0 = 0$$
$$T(\lambda x) = \lambda T(x) = \lambda 0 = 0$$

so that $x + y$, $\lambda x \in U$. The proofs that each of the vector space axioms are satisfied in U are relatively straightforward, based in each case on the fact that the same axiom is satisfied in V. A complete proof will be given below (see 3.13).

To conclude this section we list some examples of functions which are linear. For some unknown reason it is common in vector space theory to speak of 'linear transformations' rather than 'linear functions', although the words 'transformation' and 'function' are actually synonomous in mathematics. As explained above, the domain and codomain of a linear transformation should both be vector spaces (such as the vector spaces given in the examples above). The definition of 'linear transformation' was essentially given in 3.1.1 above, but there is no harm in writing it down again:

3.3 DEFINITION Let V and W be vector spaces over the field F. A function $T: V \to W$ is called a *linear transformation* if $T(u+v) = T(u) + T(v)$ and $T(\lambda u) = \lambda T(u)$ for all u, $v \in V$ and all $\lambda \in F$.

Comment ▷▷▷

3.3.1 A function T which satisfies $T(u+v) = T(u)+T(v)$ for all u and v is sometimes said to *preserve addition*. Likewise, a function T satisfying $T(\lambda v) = \lambda T(v)$ for all λ and v is said to *preserve scalar multiplication*.

◁◁◁

—Examples—

#10 Let $T: \mathbb{R}^3 \to \mathbb{R}^2$ be defined by

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y+z \\ 2x-y \end{pmatrix}.$$

Let u, $v \in \mathbb{R}^3$ and $\lambda \in \mathbb{R}$. Then

$$u = \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \qquad v = \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}$$

for some x_i, y_i, $z_i \in \mathbb{R}$, and we have

$$\begin{aligned} T(u+v) = T\begin{pmatrix} x_1+x_2 \\ y_1+y_2 \\ z_1+z_2 \end{pmatrix} &= \begin{pmatrix} x_1+x_2+y_1+y_2+z_1+z_2 \\ 2(x_1+x_2)-(y_1+y_2) \end{pmatrix} \\ &= \begin{pmatrix} x_1+y_1+z_1 \\ 2x_1-y_1 \end{pmatrix} + \begin{pmatrix} x_2+y_2+z_2 \\ 2x_2-y_2 \end{pmatrix} = T(u)+T(v), \end{aligned}$$

$$\begin{aligned} T(\lambda u) = T\begin{pmatrix} \lambda x_1 \\ \lambda y_1 \\ \lambda z_1 \end{pmatrix} &= \begin{pmatrix} \lambda x_1+\lambda y_1+\lambda z_1 \\ 2\lambda x_1-\lambda y_1 \end{pmatrix} \\ &= \begin{pmatrix} \lambda(x_1+y_1+z_1) \\ \lambda(2x_1-y_1) \end{pmatrix} = \lambda\begin{pmatrix} x_1+y_1+z_1 \\ 2x_1-y_1 \end{pmatrix} = \lambda T(u). \end{aligned}$$

Since these equations hold for all u, v and λ it follows that T is a linear transformation.

Note that the definition of this function T could be rewritten as

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Writing $A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -1 & 0 \end{pmatrix}$, the calculations above amount to showing that $A(u+v) = Au + Av$ and $A(\lambda u) = \lambda(Au)$ for all $u, v \in \mathbb{R}^3$ and all $\lambda \in \mathbb{R}$, facts which we have already noted in Chapter One.

#11 Let F be any field and A any matrix of m rows and n columns with entries from F. If the function $f\colon F^n \to F^m$ is defined by $f(\underset{\sim}{x}) = A\underset{\sim}{x}$ for all $\underset{\sim}{x} \in F^n$, then f is a linear transformation. The proof of this is straightforward, using Exercise 3 from Chapter 2. The calculations are reproduced below, in case you have not done that exercise. We use the notation $(\underset{\sim}{v})_i$ for the i^{th} entry of a column $\underset{\sim}{v}$.

Let $\underset{\sim}{u}$, $\underset{\sim}{v} \in F^n$ and $\lambda \in F$. Then

$$\begin{aligned}(f(\underset{\sim}{u}+\underset{\sim}{v}))_i = (A(\underset{\sim}{u}+\underset{\sim}{v}))_i &= \sum_{j=1}^{n} A_{ij}\,(\underset{\sim}{u}+\underset{\sim}{v})_j = \sum_{j=1}^{n} A_{ij}\big((\underset{\sim}{u})_j + (\underset{\sim}{v})_j\big) \\ &= \sum_{j=1}^{n} A_{ij}(\underset{\sim}{u})_j + A_{ij}(\underset{\sim}{v})_j = \sum_{j=1}^{n} A_{ij}(\underset{\sim}{u})_j + \sum_{j=1}^{n} A_{ij}(\underset{\sim}{v})_j \\ &= (A\underset{\sim}{u})_i + (A\underset{\sim}{v})_i = (f(\underset{\sim}{u}))_i + (f(\underset{\sim}{v}))_i = (f(\underset{\sim}{u}) + f(\underset{\sim}{v}))_i\end{aligned}$$

Similarly,

$$\begin{aligned}(f(\lambda\underset{\sim}{u}))_i = (A(\lambda\underset{\sim}{u}))_i &= \sum_{j=1}^{n} A_{ij}\,(\lambda\underset{\sim}{u})_j = \sum_{j=1}^{n} A_{ij}\lambda\big((\underset{\sim}{u})_j\big) \\ &= \lambda\sum_{j=1}^{n} A_{ij}(\underset{\sim}{u})_j = \lambda\,(A\underset{\sim}{u})_i = \lambda\,(f(\underset{\sim}{u}))_i = (\lambda f(\underset{\sim}{u}))_i\,.\end{aligned}$$

This holds for all i; so $f(\underset{\sim}{u}+\underset{\sim}{v}) = f(\underset{\sim}{u}) + f(\underset{\sim}{v})$ and $f(\lambda\underset{\sim}{u}) = \lambda f(\underset{\sim}{u})$, and therefore f is linear.

#12 Let $\mathcal{F}$ be the set of all functions with domain $\mathbb{Z}$(the set of all integers) and codomain $\mathbb{R}$. By #6 above we know that $\mathcal{F}$ is a vector space over $\mathbb{R}$. Let $G\colon \mathcal{F} \to \mathbb{R}^2$ be defined by

$$G(f) = \begin{pmatrix} f(-1) \\ f(2) \end{pmatrix}$$

for all $f \in \mathcal{F}$. Then if f, $g \in \mathcal{F}$ and $\lambda \in \mathbb{R}$ we have

$$\begin{aligned} G(f+g) &= \begin{pmatrix} (f+g)(-1) \\ (f+g)(2) \end{pmatrix} && \text{(by definition of } G\text{)} \\ &= \begin{pmatrix} f(-1)+g(-1) \\ f(2)+g(2) \end{pmatrix} && \text{(by the definition of addition of functions)} \\ &= \begin{pmatrix} f(-1) \\ f(2) \end{pmatrix} + \begin{pmatrix} g(-1) \\ g(2) \end{pmatrix} && \text{(by the definition of addition of columns)} \\ &= G(f)+G(g), \end{aligned}$$

and similarly

$$\begin{aligned} G(\lambda f) &= \begin{pmatrix} (\lambda f)(-1) \\ (\lambda f)(2) \end{pmatrix} && \text{(definition of } G\text{)} \\ &= \begin{pmatrix} \lambda\big(f(-1)\big) \\ \lambda\big(f(2)\big) \end{pmatrix} && \text{(definition of scalar multiplication for functions)} \\ &= \lambda \begin{pmatrix} f(-1) \\ f(2) \end{pmatrix} && \text{(definition of scalar multiplication for columns)} \\ &= \lambda G(f), \end{aligned}$$

and it follows that G is linear.

#13 Let $\mathcal{C}$ be the vector space consisting of all continuous functions from the open interval $(-1, 7)$ to $\mathbb{R}$, and define $I\colon \mathcal{C} \to \mathbb{R}$ by $I(f) = \int_0^4 f(x)\,dx$. Let f, $g \in \mathcal{C}$ and $\lambda \in \mathbb{R}$. Then

$$\begin{aligned} I(f+g) &= \int_0^4 (f+g)(x)\,dx \\ &= \int_0^4 f(x)+g(x)\,dx \\ &= \int_0^4 f(x)\,dx + \int_0^4 g(x)\,dx && \text{(by basic integral calculus)} \\ &= I(f)+I(g), \end{aligned}$$

and similarly

$$I(\lambda f) = \int_0^4 (\lambda f)(x)\,dx$$

$$\begin{aligned} &= \int_0^4 \lambda\big(f(x)\big)\,dx \\ &= \lambda \int_0^4 f(x)\,dx \\ &= \lambda I(f), \end{aligned}$$

whence I is linear.

#14 It is as well to finish with an example of a function which is *not* linear. If $\mathcal{S}$ is the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, then the function $T\colon \mathcal{S} \to \mathbb{R}$ defined by $T(f) = 1 + f(4)$ is not linear. For instance, if $f \in \mathcal{S}$ is defined by $f(x) = x$ for all $x \in \mathbb{R}$ then

$$T(2f) = 1 + (2f)(4) = 1 + 2\big(f(4)\big) \neq 2 + 2\big(f(4)\big) = 2(1 + f(4)) = 2T(f),$$

so that T does not preserve scalar multiplication. Hence T is not linear. (In fact, T does not preserve addition either.)

---

§3c Trivial consequences of the axioms

Having defined vector spaces in the previous section, our next objective is to prove theorems about vector spaces. In doing this we must be careful to make sure that our proofs use only the axioms and nothing else, for only that way can we be sure that every system which satisfies the axioms will also satisfy all the theorems that we prove. An unfortunate consequence of this is that we must start by proving trivialities, or, rather, things which seem to be trivialities because they are familiar to us in slightly different contexts. It is necessary to prove that these things are indeed consequences of the vector space axioms. It is also useful to learn the art of constructing proofs by doing proofs of trivial facts before trying to prove difficult theorems.

Throughout this section F will be a field and V a vector space over F.

3.4 Proposition *For all u, v, $w \in V$, if $v + u = w + u$ then $v = w$.*

Proof. Assume that $v + u = w + u$. By Axiom (iv) in Definition 3.2 there exists $t \in V$ such that $u + t = \underset{\sim}{0}$. Now adding t to both sides of the equation

gives

$$\begin{aligned} (v+u)+t &= (w+u)+t \\ v+(u+t) &= w+(u+t) && \text{(by Axiom (i))} \\ v+\underset{\sim}{0} &= w+\underset{\sim}{0} && \text{(by the choice of } t\text{)} \\ v &= w && \text{(by Axiom (iii)).} \end{aligned}$$

□

3.5 Proposition *For each $v \in V$ there is a unique $t \in V$ which satisfies $t+v=\underset{\sim}{0}$.*

Proof. The existence of such a t for each v is immediate from Axioms (iv) and (ii). Uniqueness follows from 3.4 above since if $t+v=\underset{\sim}{0}$ and $t'+v=\underset{\sim}{0}$ then, by 3.4, $t=t'$. □

By Proposition 3.5 there is no ambiguity in using the customary notation '$-v$' for the negative of a vector v, and we will do this henceforward.

3.6 Proposition *If $u, v \in V$ and $u+v=v$ then $u=\underset{\sim}{0}$.*

Proof. Assume that $u+v=v$. Then by Axiom (iii) we have $u+v=\underset{\sim}{0}+v$, and by 3.4, $v=\underset{\sim}{0}$. □

We comment that 3.6 shows that V cannot have more than one zero element.

3.7 Proposition *Let $\lambda \in F$ and $v \in V$. Then $\lambda\underset{\sim}{0}=\underset{\sim}{0}=0v$, and, conversely, if $\lambda v=\underset{\sim}{0}$ then either $\lambda=0$ or $v=\underset{\sim}{0}$. We also have $(-1)v=-v$.*

Proof. By definition of $\underset{\sim}{0}$ we have $\underset{\sim}{0}+\underset{\sim}{0}=\underset{\sim}{0}$, and therefore

$$\begin{aligned} \lambda(\underset{\sim}{0}+\underset{\sim}{0}) &= \lambda\underset{\sim}{0} \\ \lambda\underset{\sim}{0}+\lambda\underset{\sim}{0} &= \lambda\underset{\sim}{0} && \text{(by Axiom (viii))} \\ \lambda\underset{\sim}{0} &= \underset{\sim}{0} && \text{(by 3.6).} \end{aligned}$$

By the field axioms (see (ii) of Definition 1.2) we have 0+0=0, and so by Axiom (vii) (in Definition 3.2)

$$0v+0v=(0+0)v=0v,$$

whence $0v = \underset{\sim}{0}$ by 3.6. For the converse, suppose that $\lambda v = \underset{\sim}{0}$ and $\lambda \neq 0$. Field axioms guarantee that λ^{-1} exists, and we deduce that

$$v = 1v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1}\underset{\sim}{0} = \underset{\sim}{0}.$$

For the last part, observe that we have $(-1) + 1 = 0$ by field axioms, and therefore

$$(-1)v + v = (-1)v + 1v = ((-1) + 1)v = 0v = \underset{\sim}{0}$$

by Axioms (v) and (vii) and the first part. By 3.5 above we deduce that $(-1)v = -v$. □

§3d Subspaces

If V is a vector space over a field F and U is a subset of V we may ask whether the operation of addition on V gives rise to an operation of addition on U. Since an operation on U is a function $U \times U \to U$, it does so if and only if adding two elements of U always gives another element of U. Likewise, the scalar multiplication function for V gives rise to a scalar multiplication function for U if and only if multiplying an element of U by a scalar always gives another element of U.

3.8 Definition A subset U of a vector space V is said to be *closed* under addition and scalar multiplication if

(i) $u_1 + u_2 \in U$ for all $u_1, u_2 \in U$

(ii) $\lambda u \in U$ for all $u \in U$ and all scalars λ.

If a subset U of V is closed in this sense, it is natural to ask whether U is a vector space relative to the addition and scalar multiplication inherited from V; if it is we say that U is a subspace of V.

3.9 Definition A subset U of a vector space V is called a *subspace* of V if U is itself a vector space relative to addition and scalar multiplication inherited from V.

It turns out that a subset which is closed under addition and scalar multiplication is always a subspace, provided only that it is nonempty.

3.10 THEOREM *If V is a vector space and U a subset of V which is nonempty and closed under addition and scalar multiplication, then U is a subspace of V.*

Proof. It is necessary only to verify that the inherited operations satisfy the vector space axioms. In most cases the fact that a given axiom is satisfied in V trivially implies that the same axiom is satisfied in U.

Let $x, y, z \in U$. Then $x, y, z \in V$, and so by Axiom (i) for V it follows that $(x + y) + z = x + (y + z)$. Thus Axiom (i) holds in U.

Let $x, y \in U$. Then $x, y \in V$, and so $x + y = y + x$. Thus Axiom (ii) holds.

The next task is to prove that U has a zero element. Since V is a vector space we know that V has a zero element, which we will denote by '$\underset{\sim}{0}$', but at first sight it seems possible that $\underset{\sim}{0}$ may fail to be in the subset U. However, since U is nonempty there certainly exists at least one element in U. Let x be such an element. By closure under scalar multiplication we have that $0x \in U$. But Proposition 3.7 gives $0x = \underset{\sim}{0}$ (since x is an element of V), and so, after all, it is necessarily true that $\underset{\sim}{0} \in U$. It is now trivial that $\underset{\sim}{0}$ is also a zero element for U, since if $y \in U$ is arbitrary then $y \in V$ and Axiom (iii) for V gives $\underset{\sim}{0} + y = y$.

For Axiom (iv) we must prove that each $x \in U$ has a negative in U. Since Axiom (iv) for V guarantees that x has a negative in V and since the zero of U is the same as the zero of V, it suffices to show that $-x \in U$. But $x \in U$ gives $(-1)x \in U$ (by closure under scalar multiplication), and $-x = (-1)x$ (by 3.7); so the result follows.

The remaining axioms are trivially proved by arguments similar to those used for axioms (i) and (ii). □

Comments ▷▷▷

3.10.1 It is easily seen that if V is a vector space then the set V itself is a subspace of V, and the set $\{0\}$ (consisting of just the zero element of V) is also a subspace of V.

3.10.2 In #9 above we claimed that if V and W are vector spaces over F and $T: V \to W$ a linear transformation then the set $U = \{\, v \in V \mid T(v) = 0 \,\}$ is a subspace of V. In view of 3.10 it is no longer necessary to check all eight vector space axioms in order to prove this; it suffices, instead, to prove merely that U is nonempty and closed under addition and scalar multiplication.

▷▷▷

—Examples—

#15 Let $F = \mathbb{R}$, $V = \mathbb{R}^3$ and $U = \{ \begin{pmatrix} x \\ y \\ x+y \end{pmatrix} \mid x, y \in \mathbb{R} \}$. Prove that U is a subspace of V.

⋙▷ In view of Theorem 3.10, we must prove that U is nonempty and closed under addition and scalar multiplication.

It is clear that U is nonempty: $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in U$.

Let u, v be arbitrary elements of U. Then

$$u = \begin{pmatrix} x \\ y \\ x+y \end{pmatrix}, \qquad v = \begin{pmatrix} x' \\ y' \\ x'+y' \end{pmatrix}$$

for some x, y, x', $y' \in \mathbb{R}$, and we see that

$$u + v = \begin{pmatrix} x'' \\ y'' \\ x''+y'' \end{pmatrix} \qquad (\text{where } x'' = x + x',\ y'' = y + y'),$$

and this is an element of U. Hence U is closed under addition.

Let if u be an arbitrary element of U and λ an arbitrary scalar. Then $u = \begin{pmatrix} x \\ y \\ x+y \end{pmatrix}$ for some x, $y \in \mathbb{R}$, and

$$\lambda u = \begin{pmatrix} \lambda x \\ \lambda y \\ \lambda(x+y) \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda y \\ \lambda x + \lambda y \end{pmatrix} \in U.$$

Thus U is closed under scalar multiplication. ◁⋘

#16 Use the result proved in #6 and elementary calculus to prove that the set $\mathcal{C}$ of all real valued continuous functions on the closed interval $[0, 1]$ is a vector space over $\mathbb{R}$.

⋙▷ By #6 the set $\mathcal{S}$ of all real valued functions on $[0, 1]$ is a vector space over $\mathbb{R}$; so it will suffice to prove that $\mathcal{C}$ is a subspace of $\mathcal{S}$. By Theorem 3.10

then it suffices to prove that $\mathcal{C}$ is nonempty and closed under addition and scalar multiplication.

The zero function is clearly continuous; so $\mathcal{C}$ is nonempty.

Let $f, g \in \mathcal{C}$ and $t \in \mathbb{R}$. For all $a \in [0,1]$ we have

$$\begin{aligned}
\lim_{x\to a}(f+g)(x) &= \lim_{x\to a}\big(f(x)+g(x)\big) && \text{(definition of } f+g\text{)}\\
&= \lim_{x\to a} f(x) + \lim_{x\to a} g(x) && \text{(basic calculus)}\\
&= f(a)+g(a) && \text{(since } f, g \text{ are continuous)}\\
&= (f+g)(a)
\end{aligned}$$

and similarly

$$\begin{aligned}
\lim_{x\to a}(tf)(x) &= \lim_{x\to a} t\big(f(x)\big) && \text{(definition of } tf\text{)}\\
&= t\lim_{x\to a} f(x) && \text{(basic calculus)}\\
&= t\big(f(a)\big) && \text{(since } f \text{ is continuous)}\\
&= (tf)(a),
\end{aligned}$$

so that $f+g$ and tf are continuous. Hence $\mathcal{C}$ is closed under addition and scalar multiplication. ⊲⋘

Since one of the major reasons for introducing vector spaces was to elucidate the concept of 'linear transformation', much of our time will be devoted to the study of linear transformations. Whenever T is a linear transformation, it is always of interest to find those vectors x such that $T(x)$ is zero.

3.11 Definition Let V and W be vector spaces over a field F and let $T\colon V \to W$ be a linear transformation. The subset of V

$$\ker T = \{\, x \in V \mid T(x) = 0_W \,\}$$

is called the *kernel* of T.

In this definition '0_W' denotes the zero element of the space W. Since the domain V and codomain W of the transformation T may very well be different vector spaces, there are two different kinds of vectors simultaneously

under discussion. Thus, for instance, it is important not to confuse the zero element of V with the zero element of W, although it is normal to use the same symbol '0' for each. Occasionally, as here, we will append a subscript to indicate which zero vector we are talking about.

By definition the kernel of T consists of those vectors in V which are mapped to the zero vecor of W. It is natural to ask whether the zero of V is one of these. In fact, it always is.

3.12 PROPOSITION *Let V and W be vector spaces over F and let 0_V and 0_W be the zero elements of V and W respectively. If $T: V \to W$ is a linear transformation then $T(0_V) = 0_W$.*

Proof. Certainly T must map 0_V to some element of W; let $w = T(0_V)$ be this element. Since $0_V + 0_V = 0_V$ we have

$$w = T(0_V) = T(0_V + 0_V) = T(0_V) + T(0_V) = w + w$$

since T preserves addition. By 3.6 it follows that $w = 0$. □

We now prove the theorem which was foreshadowed in #9:

3.13 THEOREM *If $T: V \to W$ is a linear transformation then $\ker T$ is a subspace of V.*

Proof. By 3.12 we know that $0_V \in \ker T$, and therefore $\ker T$ is nonempty. By 3.10 it remains to prove that $\ker T$ is closed under addition and scalar multiplication.

Suppose that $u, v \in \ker T$ and λ is a scalar. Then by linearity of T,

$$T(u + v) = T(u) + T(v) = 0_W + 0_W = 0_W$$

and

$$T(\lambda u) = \lambda T(u) = \lambda 0_W = 0_W$$

(by 3.7 above). Thus $u + v$ and λu are in $\ker T$, and it follows that $\ker T$ is closed under addition and scalar multiplication, as required. □

—Examples—

#17 The solution set of the simultaneous linear equations

$$x + y + z = 0$$
$$x - 2y - z = 0$$

may be viewed as the kernel of the linear transformation $T\colon \mathbb{R}^3 \to \mathbb{R}^2$ given by

$$T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -2 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

and is therefore a subspace of $\mathbb{R}^3$.

#18 Let $\mathcal{D}$ be the vector space of all differentiable real valued functions on $\mathbb{R}$, and let $\mathcal{F}$ be the vector space of all real valued functions on $\mathbb{R}$. For each $f \in \mathcal{D}$ define $Tf \in \mathcal{F}$ by $(Tf)(x) = f'(x) + (\cos x)f(x)$. Show that $f \mapsto Tf$ is a linear map from $\mathcal{D}$ to $\mathcal{F}$, and calculate its kernel.

≫→ Let f, $g \in \mathcal{D}$ and λ, $\mu \in \mathbb{R}$. Then for all $x \in \mathbb{R}$ we have

$$\begin{aligned}(T(\lambda f + \mu g))(x) &= (\lambda f + \mu g)'(x) + (\cos x)(\lambda f + \mu g)(x) \\ &= \frac{d}{dx}(\lambda f(x) + \mu g(x)) + (\cos x)(\lambda f(x) + \mu g(x)) \\ &= \lambda f'(x) + \lambda(\cos x)f(x) + \mu g'(x) + \mu(\cos x)g(x) \\ &= \lambda((Tf)(x)) + \mu((Tg)(x)) \\ &= (\lambda(Tf) + \mu(Tg))(x),\end{aligned}$$

and it follows that $T(\lambda f + \mu g) = \lambda(Tf) + \mu(Tg)$. Hence T is linear.

By definition, the kernel of T is the set of all functions $f \in \mathcal{D}$ such that $Tf = 0$. Hence, finding the kernel of T means solving the differential equation $f'(x) + (\cos x)f(x) = 0$. Techniques for solving differential equations are dealt with in other courses. In this case the method is to multiply through by the "integrating factor" $e^{\sin x}$, and then integrate. This gives $f(x)e^{\sin x} = C$, where C is any constant. Hence the kernel consists of all functions f such that $f(x) = Ce^{-\sin x}$ for some constant C. Note that the sum of two functions of this form (corresponding to two constants C_1 and C_2) is again of the same form. Similarly, any scalar multiple of a function of this form has the same form. Thus the kernel of T is indeed a subspace of $\mathcal{D}$, as we knew (by Theorem 3.13) that it would be. ←≪

Theorem 3.13 says that the kernel of a linear transformation T is a subspace of the domain of T; our next result is, in a sense, dual to 3.13, and says that the image of a linear transformation is a subspace of the codomain.

3.14 THEOREM *If $T: V \to W$ is a linear transformation then the image of T is a subspace of W.*

Proof. Recall (see §0c) that the image of T is the set

$$\operatorname{im} T = \{ T(v) \mid v \in V \}.$$

We have by 3.12 that $T(0_V) = 0_W$, and hence $0_W \in \operatorname{im} T$. So $\operatorname{im} T \neq \emptyset$. Let $x, y \in \operatorname{im} T$ and let λ be a scalar. By definition of $\operatorname{im} T$ there exist $u, v \in V$ with $T(u) = x$ and $T(v) = y$, and now linearity of T gives

$$x + y = T(u) + T(v) = T(u + v)$$

and

$$\lambda x = \lambda T(u) = T(\lambda u),$$

so that $x + y$, $\lambda x \in \operatorname{im} T$. Hence $\operatorname{im} T$ is closed under addition and scalar multiplication. □

—Example—

#19 Let $T: \mathbb{R}^2 \to \mathbb{R}^3$ be defined by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 4 & -10 \\ -2 & 9 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

By #11 we know that T is a linear transformation, and so its image is a subspace of $\mathbb{R}^3$. The image in fact consists of all triples $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ such that there exist $x, y \in \mathbb{R}$ such that

$$(*) \qquad \begin{aligned} x - 3y &= a \\ 4x - 10y &= b \\ -2x + 9y &= c. \end{aligned}$$

It turns out that this is the same as the set

$$\left\{ \begin{pmatrix} a \\ b \\ c \end{pmatrix} \;\middle|\; 16a - 3b + 2c = 0 \right\}.$$

One way to prove this is to form the augmented matrix corresponding to the system $(*)$ and apply row operations to obtain an echelon matrix. The result is

$$\left(\begin{array}{cc|c} 1 & -3 & a \\ 0 & 2 & b - 4a \\ 0 & 0 & 16a - 3b + 2c \end{array}\right).$$

Thus equations are consistent if and only if $16a - 3b + 2c = 0$, as claimed.

Our final result for this section gives a useful criterion for determining whether a linear transformation is injective.

3.15 Proposition *A linear transformation is injective if and only if its kernel is the zero subspace,* $\{\underset{\sim}{0}\}$.

Proof. Let $\theta: V \to W$ be a linear transformation. Assume first that θ is injective.

We have proved in 3.13 that the kernel of θ is a subspace of V; hence it contains the zero of V. That is, $\theta(\underset{\sim}{0}) = \underset{\sim}{0}$. (This was proved explicitly in the proof of 3.13. Here we will use the same notation, $\underset{\sim}{0}$, for the zero elements of V and W—this should cause no confusion.) Now let v be an arbitrary element of $\ker\theta$. Then we have

$$\theta(v) = \underset{\sim}{0} = \theta(\underset{\sim}{0}),$$

and since θ is injective it follows that $v = \underset{\sim}{0}$. Hence $\underset{\sim}{0}$ is the only element of $\ker\theta$, and so $\ker\theta = \{\underset{\sim}{0}\}$, as required.

For the converse, assume that $\ker\theta = \{\underset{\sim}{0}\}$. We seek to prove that θ is injective; so assume that $u, v \in V$ with $\theta(u) = \theta(v)$. By linearity of θ we obtain

$$\theta(u - v) = \theta(u) + \theta(-v) = \theta(u) - \theta(v) = \underset{\sim}{0},$$

so that $u - v \in \ker\theta$. Hence $u - v = \underset{\sim}{0}$, and $u = v$. Hence θ is injective. □

For completeness we state the analogous result for surjective linear transformations, although it is immediate from the definitions concerned.

3.16 PROPOSITION *A linear transformation is surjective if and only if its image is the whole codomain.*

§3e Linear combinations

Let $v_1, v_2, \ldots, v_n$ and w be vectors in some space V. We say that w is a *linear combination* of $v_1, v_2, \ldots, v_n$ if $w = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$ for some scalars $\lambda_1, \lambda_2, \ldots, \lambda_n$. This concept is, in a sense, the fundamental concept of vector space theory, since it is made up of addition and scalar multiplication.

3.17 DEFINITION The vectors $v_1, v_2, \ldots, v_n$ are said to *span* V if every element $w \in V$ can be expressed as a linear combination of the v_i.

For example, the set S of all triples $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ such that $x + y + z = 0$ is a subspace of $\mathbb{R}^3$, and it is easily checked that the triples

$$u = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \; v = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \text{ and } w = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$$

span S. For example, if $x + y + z = 0$ then

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \frac{y-z}{3} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} + \frac{z-x}{3} \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} + \frac{x-y}{3} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}.$$

In this example it can be seen that there are infinitely many ways of expressing each element of the set S in terms of u, v and w. Indeed, since $u + v + w = 0$, if any number α is added to each of the coefficients of u, v and w, then the answer will not be altered. Thus one can arrange for the coefficient of u to be zero, and it follows that in fact S is spanned by v and w. (It is equally true that u and v span S, and that u and w span S.) It is usual to try to find spanning sets which are minimal, so that no element of the spanning set is expressible in terms of the others. The elements of a minimal spanning set are then linearly independent, in the following sense.

3.18 DEFINITION We say that vectors $v_1, v_2, \ldots, v_r$ are *linearly independent* if the only solution of

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_r v_r = 0$$

is given by

$$\lambda_1 = \lambda_2 = \cdots = \lambda_r = 0.$$

For example, the triples u and v above are linearly independent, since if

$$\lambda \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

then inspection of the first two components immediately gives $\lambda = \mu = 0$.

Vectors $v_1, v_2, \ldots, v_r$ are *linearly dependent* if they are not linearly independent; that is, if there is a solution of $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_r v_r = 0$ for which the scalars λ_i are not all zero.

—Example—

#20 Show that the functions f, g and h defined by

$$\left.\begin{aligned} f(x) &= \sin x \\ g(x) &= \sin(x + \tfrac{\pi}{4}) \\ h(x) &= \sin(x + \tfrac{\pi}{2}) \end{aligned}\right\} \quad \text{for all } x \in \mathbb{R}$$

are linearly dependent over $\mathbb{R}$.

$\gg\!\!\rightarrow$ We attempt to find $\alpha, \beta, \gamma \in \mathbb{R}$ which are not all zero, and which satisfy $\alpha f + \beta g + \gamma h = 0$. We require

3.18.1 $$\alpha f(x) + \beta g(x) + \gamma h(x) = 0 \qquad \text{for all } x \in \mathbb{R},$$

in other words

$$\alpha \sin x + \beta \sin(x + \tfrac{\pi}{4}) + \gamma \sin(x + \tfrac{\pi}{2}) = 0 \qquad \text{for all } x \in \mathbb{R}.$$

By some well known trigonometric formulae we find that

$$\sin(x + \tfrac{\pi}{4}) = \sin x \cos\tfrac{\pi}{4} + \cos x \sin\tfrac{\pi}{4} = \tfrac{1}{\sqrt{2}} \sin x + \tfrac{1}{\sqrt{2}} \cos x$$

and similarly

$$\sin(x + \tfrac{\pi}{2}) = \sin x \cos \tfrac{\pi}{2} + \cos x \sin \tfrac{\pi}{2} = \cos x,$$

and so our equations become

$$(\alpha + \tfrac{\beta}{\sqrt{2}}) \sin x + (\tfrac{\beta}{\sqrt{2}} + \gamma) \cos x = 0 \qquad \text{for all } x \in \mathbb{R}.$$

Clearly $\alpha = 1$, $\beta = -\sqrt{2}$ and $\gamma = 1$ solves this, since the coefficients of $\sin x$ and $\cos x$ both become zero. Hence 3.18.1 has a nontrivial solution, and f, g and h are linearly dependent, as claimed. ⊲⋘

3.19 Definition If $v_1, v_2, \ldots, v_n$ are linearly independent and span V we say that they form a *basis* of V. The number n is called the *dimension*.

If a vector space V has a basis consisting of n vectors then a general element of V can be completely described by specifying n scalar parameters (the coefficients of the basis elements). The dimension can thus be thought of as the number of "degrees of freedom" in the space. For example, the subspace S of $\mathbb{R}^3$ described above has two degrees of freedom, since it has a basis consisting of the two elements u and v. Choosing two scalars λ and μ determines an element $\lambda u + \mu v$ of S, and each element of S is uniquely expressible in this form. Geometrically, S represents a plane through the origin, and so it certainly ought to be a two-dimensional space.

One of our major tasks is to show that the dimension is an invariant of a vector space. That is, any two bases must have the same number of elements. We will do this in the next chapter; see also Exercise 5 below.

We have seen in #11 above that if $A \in \mathrm{Mat}(m \times n, F)$ then $T(x) = Ax$ defines a linear transformation $T\colon F^n \to F^m$. The set $S = \{\, Ax \mid x \in F^n \,\}$ is the image of T; so (by 3.14) it is a subspace of F^m. Let $a_1, a_2, \ldots, a_n$ be the columns of A. Since A is an $m \times n$ matrix these columns all have m components; that is, $a_i \in F^m$ for each i. By multiplication of partitioned matrices we find that

$$A \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} a_1 & | & a_2 & | & \cdots & | & a_n \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n,$$

and we deduce that S is precisely the set of all linear combinations of the columns of A.

3.20 DEFINITION If $A \in \mathrm{Mat}(m \times n, F)$ the *column space*, $\mathrm{CS}(A)$, of the matrix A is the subspace of F^m consisting of all linear combinations of the columns of A. The *row space*, $\mathrm{RS}(A)$ is the subspace of ${}^{\mathrm{t}}F^n$ consisting of all linear combinations of the rows of A.

Comment ▷▷▷
3.20.1 Observe that the system of equations $Ax = b$ is consistent if and only if b is in the column space of A. ▷▷▷

3.21 PROPOSITION *Let $A \in \mathrm{Mat}(m \times n, F)$ and $B \in \mathrm{Mat}(n \times p, F)$. Then*
(i) $\mathrm{RS}(AB) \subseteq \mathrm{RS}(B)$, *and*
(ii) $\mathrm{CS}(AB) \subseteq \mathrm{CS}(A)$.

Proof. Let the (i, j)-entry of A be α_{ij} and let the i^{th} row of B be $\underset{\sim}{b}_i$. It is a general fact that

$$\text{the } i^{\text{th}} \text{ row of } AB = \big(i^{\text{th}} \text{ row of } A\big)B,$$

and since the i^{th} row of A is $(\, a_{i1} \quad a_{i2} \quad \dots \quad a_{in} \,)$ we have

$$\begin{aligned} i^{\text{th}} \text{ row of } AB &= (\, a_{i1} \quad a_{i2} \quad \dots \quad a_{in} \,) \begin{pmatrix} \underset{\sim}{b}_1 \\ \underset{\sim}{b}_2 \\ \vdots \\ \underset{\sim}{b}_n \end{pmatrix} \\ &= \alpha_{i1}\underset{\sim}{b}_1 + \alpha_{i2}\underset{\sim}{b}_2 + \cdots + \alpha_{in}\underset{\sim}{b}_n \\ &\in \mathrm{RS}(B). \end{aligned}$$

In words, we have shown that the i^{th} row of AB is a linear combination of the rows of B, the scalar coefficients being the entries in the i^{th} row of A. So all rows of AB are in the row space of B, and since the row space of B is closed under addition and scalar multiplication it follows that all linear combinations of the rows of AB are also in the row space of B. That is, $\mathrm{RS}(AB) \subseteq \mathrm{RS}(B)$.

The proof of (ii) is similar and is omitted. □

—Example—

#21 Prove that if A is an $m \times n$ matrix and B an $n \times p$ matrix then the i^{th} row of AB is $\underset{\sim}{a}B$, where $\underset{\sim}{a}$ is the i^{th} row of A.

⋙▷ Note that since $\underset{\sim}{a}$ is a $1 \times n$ row vector and B is an $n \times m$ matrix, $\underset{\sim}{a}B$ is a $1 \times m$ row vector. The j^{th} entry of $\underset{\sim}{a}B$ is $\sum_{k=1}^{n} a_k B_{kj}$, where a_k is the k^{th} entry of $\underset{\sim}{a}$. But since $\underset{\sim}{a}$ is the i^{th} row of A, the k^{th} entry of $\underset{\sim}{a}$ is in fact the (i,k)-entry of A. So we have shown that the j^{th} entry of $\underset{\sim}{a}B$ is $\sum_{k=1}^{n} A_{ik}B_{kj}$, which is equal to $(AB)_{ij}$, the j^{th} entry of the i^{th} row of AB. So we have shown that for all j, the i^{th} row of AB has the same j^{th} entry as $\underset{\sim}{a}B$; hence $\underset{\sim}{a}B$ equals the i^{th} row of AB, as required. ◁⋘

3.22 Corollary *Suppose that $A \in \text{Mat}(n \times n, F)$ is invertible, and let $B \in \text{Mat}(n \times p, F)$ be arbitrary. Then* $\text{RS}(AB) = \text{RS}(B)$.

Proof. By 3.21 we have $\text{RS}(AB) \subseteq \text{RS}(B)$. Moreover, applying 3.21 with A^{-1}, AB in place of A, B gives $\text{RS}(A^{-1}(AB)) \subseteq \text{RS}(AB)$. Thus we have shown that $\text{RS}(B) \subseteq \text{RS}(AB)$ and $\text{RS}(AB) \subseteq \text{RS}(B)$, as required. □

From 3.22 it follows that if A is invertible then the function "premultiplication by A", which takes B to AB, does not change the row space. (It is trivial to prove also the column space analogue: postmultiplication by invertible matrices leaves the column space unchanged.) Since performing row operations on a matrix is equivalent to premultiplying by elementary matrices, and elementary matrices are invertible, it follows that row operations do not change the row space of a matrix. Hence the reduced echelon matrix E which is the end result of the pivoting algorithm described in Chapter 2 has the same row space as the original matrix A. The nonzero rows of E therefore span the row space of A. We leave it as an exercise for the reader to prove that the nonzero rows of E are also linearly independent, and therefore form a basis for the row space of A.

—Examples—

#22 Find a basis for the row space of the matrix

$$\begin{pmatrix} 1 & -3 & 5 & 5 \\ -2 & 2 & 1 & -3 \\ -3 & 1 & 7 & 1 \end{pmatrix}.$$

≫⊳

$$\begin{pmatrix} 1 & -3 & 5 & 5 \\ -2 & 2 & 1 & -3 \\ -3 & 1 & 7 & -1 \end{pmatrix} \xrightarrow[R_3:=R_3+3R_1]{R_2:=R_2+2R_1} \begin{pmatrix} 1 & -3 & 5 & 5 \\ 0 & -4 & 11 & 7 \\ 0 & -8 & 22 & 14 \end{pmatrix}$$

$$\xrightarrow{R_3:=R_3-2R_2} \begin{pmatrix} 1 & -3 & 5 & 5 \\ 0 & -4 & 11 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since row operations do not change the row space, the echelon matrix we have obtained has the same row space as the original matrix A. Hence the row space consists of all linear combinations of the rows $(\,1 \quad -3 \quad 5 \quad 5\,)$ and $(\,0 \quad -4 \quad 11 \quad 7\,)$, since the zero row can clearly be ignored when computing linear combinations of the rows. Furthermore, because the matrix is echelon, it follows that its nonzero rows are linearly independent. Indeed, if

$$\lambda(\,1 \quad -3 \quad 5 \quad 5\,) + \mu(\,0 \quad -4 \quad 11 \quad 7\,) = (\,0 \quad 0 \quad 0 \quad 0\,)$$

then looking at the first entry we see immediately that $\lambda = 0$, whence (from the second entry) μ must be zero also. Hence the two nonzero rows of the echelon matrix form a basis of $\mathrm{RS}(A)$. ⊲≪

#23 Is the column vector $v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ in the column space of the matrix $A = \begin{pmatrix} 2 & -1 & 4 \\ -1 & 3 & -1 \\ 4 & 3 & 2 \end{pmatrix}$?

≫⊳ The question can be rephrased as follows: can v be expressed as a linear combination of the columns of A? That is, do the equations

$$x \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix} + y \begin{pmatrix} -1 \\ 3 \\ 3 \end{pmatrix} + z \begin{pmatrix} 4 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

have a solution? Since these equations can also be written as

$$\begin{pmatrix} 2 & -1 & 4 \\ -1 & 3 & -1 \\ 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

our task is to determine whether or not these equations are consistent. (This is exactly the point made in 3.20.1 above.)

We simply apply standard row operation techniques:

$$\left(\begin{array}{ccc|c} 2 & -1 & 4 & 1 \\ -1 & 3 & -1 & 1 \\ 4 & 3 & 2 & 1 \end{array}\right) \xrightarrow[R_3:=R_3+4R_1]{\substack{R_1\leftrightarrow R_2 \\ R_2:=R_2+2R_1}} \left(\begin{array}{ccc|c} -1 & 3 & -1 & 1 \\ 0 & 5 & 2 & 3 \\ 0 & 15 & -2 & 5 \end{array}\right)$$

$$\xrightarrow{R_3:=R_3-3R_2} \left(\begin{array}{ccc|c} -1 & 3 & -1 & 1 \\ 0 & 5 & 2 & 3 \\ 0 & 0 & -8 & -4 \end{array}\right)$$

Now the coefficient matrix has been reduced to echelon form, and there is no row for which the left hand side of the equation is zero and the right hand side nonzero. Hence the equations must be consistent. Thus v is in the column space of A. Although the question did not ask for the coefficients x, y and z to be calculated, let us nevertheless do so, as a check. The last equation of the echelon system gives $z = 1/2$, substituting this into the second equation gives $y = 2/5$, and then the first equation gives $x = -3/10$. It is easily checked that

$$(-3/10)\begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix} + (2/5)\begin{pmatrix} -1 \\ 3 \\ 3 \end{pmatrix} + (1/2)\begin{pmatrix} 4 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

⇦≪

Exercises

1. Prove that the set T of all solutions of the simultaneous equations

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

is a subspace of $\mathbb{R}^4$.

2. Prove that if A is an $m \times n$ matrix over $\mathbb{R}$ then the solution set of $Av = 0$ is a subspace of $\mathbb{R}^n$.

3. Let A be an $n \times n$ matrix over $\mathbb{R}$, and λ any eigenvalue of A. Prove that if S is the subset of $\mathbb{R}^n$ which consists of the zero column and all eigenvectors associated to the eigenvalue λ then S is a subspace of $\mathbb{R}^n$.

4. Prove that the nonzero rows of an echelon matrix are necessarily linearly independent.

5. Let $v_1, v_2, \ldots, v_m$ and $w_1, w_2, \ldots, w_n$ be two bases of a vector space V, let A be the $m \times n$ coefficient matrix obtained when the v_i are expressed as linear combinations of the w_j, and let B be the $n \times m$ coefficient matrix obtained when the w_j are expressed as linear combinations of the v_i. Combine these equations to express the v_i as linear combinations of themselves, and then use linear independence of the v_i to deduce that $AB = I$. Similarly, show that $BA = I$, and use 2.10 to deduce that $m = n$.

6. In each case decide whether or not the set S is a vector space over the field F, relative to obvious operations of addition and scalar multiplication.

(*i*) $S = \mathbb{C}$ (complex numbers), $F = \mathbb{R}$.

(*ii*) $S = \mathbb{C}$, $F = \mathbb{C}$.

(*iii*) $S = \mathbb{R}$, $F = \mathbb{Q}$ (rational numbers).

(*iv*) $S = \mathbb{R}[X]$ (polynomials over $\mathbb{R}$ in the variable X—that is, expressions of the form $a_0 + a_1X + \cdots + a_nX^n$ with $(a_i \in \mathbb{R})$), $F = \mathbb{R}$.

(*v*) $S = \mathrm{Mat}(n, \mathbb{C})$ ($n \times n$ matrices over $\mathbb{C}$), $F = \mathbb{R}$.

7. Let V be a vector space and S any set. Show that the set of all functions from S to V can be made into a vector space in a natural way.

8. Which of the following functions are linear transformations?

(*i*) $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$,

(*ii*) $S\colon \mathbb{R}^2 \to \mathbb{R}^2$ defined by $S\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$,

(*iii*) $g\colon \mathbb{R}^2 \to \mathbb{R}^3$ defined by $g\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x + y \\ y \\ x - y \end{pmatrix}$,

(*iv*) $f\colon \mathbb{R} \to \mathbb{R}^2$ defined by $f(x) = \begin{pmatrix} x \\ x + 1 \end{pmatrix}$.

9. Let V be a vector space and let S and T be subspaces of V.

(i) Prove that $S \cap T$ is a subspace of V.

(ii) Let $S + T = \{\, x + y \mid x \in S \text{ and } y \in T \,\}$. Prove that $S + T$ is a subspace of V.

10. (i) Let U, V, W be vector spaces over a field F, and let $f\colon V \to W$, $g\colon U \to V$ be linear transformations. Prove that $fg\colon U \to W$ defined by

$$(fg)(u) = f\big(g(u)\big) \qquad \text{for all } u \in U$$

is a linear transformation.

(ii) Let $U = \mathbb{R}^2$, $V = \mathbb{R}^3$, $W = \mathbb{R}^5$ and suppose that f, g are defined by

$$f\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 2 & 1 & 0 \\ -1 & -1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

$$g\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Give a formula for $(fg)\begin{pmatrix} a \\ b \end{pmatrix}$.

11. Let V, W be vector spaces over F.

(i) Prove that if ϕ and ψ are linear transformations from V to W then $\phi + \psi\colon V \to W$ defined by

$$(\phi + \psi)(v) = \phi(v) + \psi(v) \qquad \text{for all } v \in V$$

is also a linear transformation.

(ii) Prove that if $\phi\colon V \to W$ is a linear transformation and $\alpha \in F$ then $\alpha\phi\colon V \to W$ defined by

$$(\alpha\phi)(v) = \alpha\big(\phi(v)\big) \qquad \text{for all } v \in V$$

is also a linear transformation.

12. Prove that the set U of all functions $f\colon \mathbb{R} \to \mathbb{R}$ which satisfy the differential equation $f''(t) - f(t) = 0$ is a vector subspace of the vector space of all real-valued functions on $\mathbb{R}$.

13. Let V be a vector space and let S and T be subspaces of V.

(*i*) Prove that if addition and scalar multiplication are defined in the obvious way then

$$V^2 = \{\begin{pmatrix} u \\ v \end{pmatrix} \mid u, v \in V\}$$

becomes a vector space. Prove that

$$S \dot{+} T = \{\begin{pmatrix} u \\ v \end{pmatrix} \mid u \in S,\ v \in T\}$$

is a subspace of V^2.

(*ii*) Prove that $f\colon S \dot{+} T \to V$ defined by

$$f\begin{pmatrix} u \\ v \end{pmatrix} = u + v$$

is a linear transformation. Calculate $\ker f$ and $\operatorname{im} f$.

14. (*i*) Let F be any field. Prove that for any $a \in F$ the function $f\colon F \to F$ given by $f(x) = ax$ for all $x \in F$ is a linear transformation. Prove also that any linear transformation from F to F has this form. (Note that this implicitly uses the fact that F is a vector space over itself.)

(*ii*) Prove that if f is any linear transformation from F^2 to F^2 then there exists a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (where $a, b, c, d \in F$) such that $f(x) = Ax$ for all $x \in F^2$.

(Hint: the formulae $f\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$ and $f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}$ define the coefficients of A.)

(*iii*) Can these results be generalized to deal with linear transformations from F^n to F^m for arbitrary n and m?

4

The structure of abstract vector spaces

This chapter probably constitutes the hardest theoretical part of the course; in it we investigate bases in arbitrary vector spaces, and use them to relate abstract vector spaces to spaces of n-tuples. Throughout the chapter, unless otherwise stated, V will be a vector space over the field F.

§4a Preliminary lemmas

If n is a nonnegative integer and for each positive integer $i \leq n$ we are given a vector $v_i \in V$ then we will say that $(v_1, v_2, \ldots, v_n)$ is a sequence of vectors. It is convenient to formulate most of the results in this chapter in terms of sequences of vectors, and we start by restating the definitions from §3e in terms of sequences.

4.1 Definition Let $(v_1, v_2, \ldots, v_n)$ be a sequence of vectors in V.

(i) An element $w \in V$ is a *linear combination* of $(v_1, v_2, \ldots, v_n)$ if there exist scalars λ_i such that $w = \sum_{i=1}^{n} \lambda_i v_i$.

(ii) The subset of V consisting of all linear combinations of $(v_1, v_2, \ldots, v_n)$ is called the *span* of $(v_1, v_2, \ldots, v_n)$:

$$\mathrm{Span}(v_1,\, v_2,\, \ldots,\, v_n) = \{\, \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in F \,\}.$$

If $\mathrm{Span}(v_1, v_2, \ldots, v_n) = V$ then $(v_1, v_2, \ldots, v_n)$ is said to *span* V.

(iii) The sequence $(v_1, v_2, \ldots, v_n)$ is said to be *linearly independent* if the only solution of

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \underset{\sim}{0} \qquad (\lambda_1,\, \lambda_2,\, \ldots,\, \lambda_n \in F)$$

is given by

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0.$$

(iv) The sequence $(v_1, v_2, \ldots, v_n)$ is said to be a *basis* of V if it is linearly independent and spans V.

Comments ▷▷▷

4.1.1 The sequence of vectors $(v_1, v_2, \ldots, v_n)$ is said to be *linearly dependent* if it is not linearly independent; that is, if there is a solution of $\sum_{i=1}^{n} \lambda_i v_i = \underset{\sim}{0}$ for which at least one of the λ_i is nonzero.

4.1.2 It is not difficult to prove that $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ is always a subspace of V; it is commonly called *the subspace generated by* v_1, v_2, …, v_n. (The word 'generate' is often used as a synonym for 'span'.) We say that the vector space V is *finitely generated* if there exists a finite sequence $(v_1, v_2, \ldots, v_n)$ of vectors in V such that $V = \mathrm{Span}(v_1, v_2, \ldots, v_n)$.

4.1.3 Let $V = F^n$ and define $e_i \in V$ to be the column with 1 as its i^{th} entry and all other entries zero. It is easily proved that $(e_1, e_2, \ldots, e_n)$ is a basis of F^n. We will call this basis the *standard basis* of F^n.

4.1.4 The notation '$(v_1, v_2, \ldots, v_n)$' is not meant to imply that $n \geq 2$, and indeed we want all our statements about sequences of vectors to be valid for one-term sequences, and even for the sequence which has no terms. Each $v \in V$ gives rise to a one-term sequence (v), and a linear combination of (v) is just a scalar multiple of v; thus $\mathrm{Span}(v) = \{\, \lambda v \mid \lambda \in F \,\}$. The sequence $(\underset{\sim}{0})$ is certainly not linearly independent, since $\lambda = 1$ is a nonzero solution of $\lambda \underset{\sim}{0} = \underset{\sim}{0}$. However, if $v \neq \underset{\sim}{0}$ then by 3.7 we know that the only solution of $\lambda v = \underset{\sim}{0}$ is $\lambda = 0$. Thus the sequence (v) is linearly independent if and only if $v \neq \underset{\sim}{0}$.

4.1.5 Empty sums are always given the value zero; so it seems reasonable that an empty linear combination should give the zero vector. Accordingly we adopt the convention that the empty sequence generates the subspace $\{\underset{\sim}{0}\}$. Furthermore, the empty sequence is considered to be linearly independent; so it is a basis for $\{\underset{\sim}{0}\}$.

4.1.6 (This is a rather technical point.) It may seem a little strange that the above definitions have been phrased in terms of a *sequence* of vectors $(v_1, v_2, \ldots, v_n)$ rather than a *set* of vectors $\{v_1, v_2, \ldots, v_n\}$. The reason for our choice can be illustrated with a simple example, in which $n = 2$. Suppose that v is a nonzero vector, and consider the two-term sequence (v, v). The equation $\lambda_1 v + \lambda_2 v = \underset{\sim}{0}$ has a nonzero solution—namely, $\lambda_1 = 1$, $\lambda_2 = -1$. Thus, by our definitions, (v, v) is a linearly dependent sequence of vectors. A definition of linear independence for sets of vectors would encounter the

problem that $\{v, v\} = \{v\}$: we would be forced to say that $\{v, v\}$ is linearly independent. The point is that sets A and B are equal if and only if each element of A is an element of B and vice versa, and writing an element down again does not change the set; on the other hand, sequences $(v_1, v_2, \ldots, v_n)$ and $(u_1, u_2, \ldots, u_m)$ are equal if and only if $m = n$ and $u_i = v_i$ for each i.

4.1.7 Despite the remarks just made in 4.1.6, the concept of 'linear combination' could have been defined perfectly satisfactorily for sets; indeed, if $(v_1, v_2, \ldots, v_n)$ and $(u_1, u_2, \ldots, u_m)$ are sequences of vectors such that $\{v_1, v_2, \ldots, v_n\} = \{u_1, u_2, \ldots, u_m\}$, then a vector v is a linear combination of $(v_1, v_2, \ldots, v_n)$ if and only if it is a linear combination of $(u_1, u_2, \ldots, u_m)$.

4.1.8 One consequence of our terminology is that the order in which elements of a basis are listed is important. If $v_1 \neq v_2$ then the sequences (v_1, v_2, v_3) and (v_2, v_1, v_3) are not equal. It is true that if a sequence of vectors is linearly independent then so is any rearrangement of that sequence, and if a sequence spans V then so does any rearrangement. Thus a rearrangement of a basis is also a basis—but a different basis. Our terminology is a little at odds with the mathematical world at large in this regard: what we are calling a *basis* most authors call an *ordered basis*. However, for our discussion of matrices and linear transformations in Chapter 6, it is the concept of an ordered basis which is appropriate. ▷▷▷

Our principal goal in this chapter is to prove that every finitely generated vector space has a basis and that any two bases have the same number of elements. The next two lemmas will be used in the proofs of these facts.

4.2 Lemma *Suppose that $v_1, v_2, \ldots, v_n \in V$, and let $1 \leq j \leq n$. Write $S = \mathrm{Span}(v_1, v_2, \ldots, v_n)$ and $S' = \mathrm{Span}(v_1, v_2, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$. Then*

(i) $S' \subseteq S$,

(ii) if $v_j \in S'$ then $S' = S$,

(iii) if the sequence $(v_1, v_2, \ldots, v_n)$ is linearly independent, then so also is $(v_1, v_2, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$.

Comment ▷▷▷

4.2.1 By '$(v_1, v_2, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$' we mean the sequence which is obtained from $(v_1, v_2 \ldots, v_n)$ by deleting v_j; the notation is not meant to imply that $2 < j < n$. However, n must be at least 1, so that there is a term to delete. ▷▷▷

Proof of 4.2. (i) If $v \in S'$ then for some scalars λ_i,

$$\begin{aligned} v &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{j-1} v_{j-1} + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n \\ &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{j-1} v_{j-1} + 0 v_j + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n \\ &\in S. \end{aligned}$$

Every element of S' is in S; that is, $S' \subseteq S$.

(ii) Assume that $v_j \in S'$. This gives

$$v_j = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{j-1} v_{j-1} + \alpha_{j+1} v_{j+1} + \cdots + \alpha_n v_n$$

for some scalars α_i. Now let v be an arbitrary element of S. Then for some λ_i we have

$$\begin{aligned} v &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \\ &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{j-1} v_{j-1} \\ &\qquad + \lambda_j(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{j-1} v_{j-1} + \alpha_{j+1} v_{j+1} + \cdots + \alpha_n v_n) \\ &\qquad\quad + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n \\ &= (\lambda_1 + \lambda_j \alpha_1) v_1 + (\lambda_2 + \lambda_j \alpha_2) v_2 + \cdots + (\lambda_{j-1} + \lambda_j \alpha_{j-1}) v_{j-1} \\ &\qquad + (\lambda_{j+1} + \lambda_j \alpha_{j+1}) v_{j+1} + \cdots + (\lambda_n + \lambda_j \alpha_n) v_n \\ &\in S'. \end{aligned}$$

This shows that $S \subseteq S'$, and, since the reverse inclusion was proved in (i), it follows that $S' = S$.

(iii) Assume that $(v_1, v_2 \ldots, v_n)$ is linearly independent, and suppose that

$$(\$) \qquad \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{j-1} v_{j-1} + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n = \underset{\sim}{0}$$

where the coefficients λ_i are elements of F. Then

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{j-1} v_{j-1} + 0 v_j + \lambda_{j+1} v_{j+1} + \cdots + \lambda_n v_n = \underset{\sim}{0}$$

and, by linear independence of $(v_1, v_2, \ldots, v_n)$, all the coefficients in this equation must be zero. Hence

$$\lambda_1 = \lambda_2 = \cdots = \lambda_{j-1} = \lambda_{j+1} = \cdots = \lambda_n = 0.$$

Since we have shown that this is the only solution of ($), we have shown that $(v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$ is linearly independent. □

A *subsequence* of a sequence is a sequence obtained by deleting terms from the original. (This is meant to include the possibility that the number of terms deleted is zero; thus a sequence is considered to be a subsequence of itself.) Repeated application of 4.2 (iii) gives

4.3 Corollary *Any subsequence of a linearly independent sequence is linearly independent.*

In a similar vein to 4.2, and only slightly harder, we have:

4.4 Lemma *Suppose that* $v_1, v_2, \ldots, v_r \in V$ *are such that the sequence* $(v_1, v_2, \ldots, v_{r-1})$ *is linearly independent, but* $(v_1, v_2, \ldots, v_r)$ *is linearly dependent. Then* $v_r \in \mathrm{Span}(v_1, v_2, \ldots, v_{r-1})$.

Proof. Since $(v_1, v_2, \ldots, v_r)$ is linearly dependent there exist coefficients $\lambda_1, \lambda_2, \ldots, \lambda_r$ which are not all zero and which satisfy

$$(**) \qquad \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_r v_r = \underset{\sim}{0}.$$

If $\lambda_r = 0$ then $\lambda_1, \lambda_2, \ldots, \lambda_{r-1}$ are not all zero, and, furthermore, $(**)$ gives

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{r-1} v_{r-1} = \underset{\sim}{0}.$$

But this contradicts the assumption that $(v_1, v_2, \ldots, v_{r-1})$ is linearly independent. Hence $\lambda_r \neq 0$, and rearranging $(**)$ gives

$$\begin{aligned} v_r &= -\lambda_r^{-1}(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{r-1} v_{r-1}) \\ &\in \mathrm{Span}(v_1, v_2, \ldots, v_{r-1}). \end{aligned}$$

□

§4b Basis theorems

This section consists of a list of the main facts about bases which every student should know, collected together for ease of reference. The proofs will be given in the next section.

4.5 Theorem *Every finitely generated vector space has a basis.*

4.6 Proposition *If* $(w_1, w_2, \ldots, w_m)$ *and* $(v_1, v_2, \ldots, v_n)$ *are both bases of* V *then* $m = n$.

As we have already remarked, if V has a basis then the number of elements in any basis of V is called the *dimension* of V, denoted '$\dim V$'.

4.7 PROPOSITION *Suppose that* $(v_1, v_2, \ldots, v_n)$ *spans* V*, and no proper subsequence of* $(v_1, v_2, \ldots, v_n)$ *spans* V*. Then* $(v_1, v_2, \ldots, v_n)$ *is a basis of* V*.*

Dual to 4.7 we have

4.8 PROPOSITION *Suppose that* $(v_1, v_2, \ldots, v_n)$ *is a linearly independent sequence in* V *which is not a proper subsequence of any other linearly independent sequence. Then* $(v_1, v_2, \ldots, v_n)$ *is a basis of* V*.*

4.9 PROPOSITION *If a sequence* $(v_1, v_2, \ldots, v_n)$ *spans* V *then some subsequence of* $(v_1, v_2, \ldots, v_n)$ *is a basis.*

Again there is a dual result: any linearly independent sequence extends to a basis. However, to avoid the complications of infinite dimensional spaces, we insert the proviso that the space is finitely generated.

4.10 PROPOSITION *If* $(v_1, v_2, \ldots, v_n)$ *a linearly independent sequence in a finitely generated vector space* V *then there exist* v_{n+1}*,* v_{n+2}*,* $\ldots$*,* v_d *in* V *such that* $(v_1, v_2, \ldots, v_n, v_{n+1}, \ldots, v_d)$ *is a basis of* V*.*

4.11 PROPOSITION *If* V *is a finitely generated vector space and* U *is a subspace of* V *then* U *is also finitely generated, and* $\dim U \leq \dim V$*. Furthermore, if* $U \neq V$ *then* $\dim U < \dim V$*.*

4.12 PROPOSITION *Let* V *be a finitely generated vector space of dimension* d *and* $\boldsymbol{s} = (v_1, v_2, \ldots, v_n)$ *a sequence of elements of* V*.*

(i) If $n < d$ *then* $\boldsymbol{s}$ *does not span* V*.*

(ii) If $n > d$ *then* $\boldsymbol{s}$ *is not linearly independent.*

(iii) If $n = d$ *then* $\boldsymbol{s}$ *spans* V *if and only if* $\boldsymbol{s}$ *is linearly independent.*

§4c The Replacement Lemma

We turn now to the proofs of the results stated in the previous section. In the interests of rigour, the proofs are detailed. This makes them look more complicated than they are, but for the most part the ideas are simple enough.

The key fact is that the number of terms in a linearly independent sequence of vectors cannot exceed the number of terms in a spanning sequence, and the strategy of the proof is to replace terms of the spanning sequence by

terms of the linearly independent sequence and keep track of what happens. More exactly, if a sequence $\boldsymbol{s}$ of vectors is linearly independent and another sequence $\boldsymbol{t}$ spans V then it is possible to use the vectors in $\boldsymbol{s}$ to replace an equal number of vectors in $\boldsymbol{t}$, always preserving the spanning property. The statement of the lemma is rather technical, since it is designed specifically for use in the proof of the next theorem.

4.13 The Replacement Lemma *Suppose that r, s are nonnegative integers, and v_1, v_2, ..., v_r, v_{r+1} and x_1, x_2, ..., x_s elements of V such that $(v_1, v_2, \ldots, v_r, v_{r+1})$ is linearly independent and $(v_1, v_2, \ldots, v_r, x_1, x_2, \ldots, x_s)$ spans V. Then another spanning sequence can be obtained from this by inserting v_{r+1} and deleting a suitable x_j. That is, there exists a j with $1 \leq j \leq s$ such that the sequence $(v_1, \ldots, v_r, v_{r+1}, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_s)$ spans V.*

Comments ▷▷▷

4.13.1 If $r = 0$ the assumption that $(v_1, v_2, \ldots, v_{r+1})$ is linearly independent reduces to $v_1 \neq \underset{\sim}{0}$. The other assumption is that $(x_1, \ldots, x_s)$ spans V, and the conclusion that some x_j can be replaced by v_1 without losing the spanning property.

4.13.2 One conclusion of the Lemma is that there is an x_j to replace; so the hypotheses of the Lemma cannot be satisfied if $s = 0$. In other words, in the case $s = 0$ the Lemma says that it is impossible for $(v_1, \ldots, v_{r+1})$ to be linearly independent if $(v_1, \ldots, v_r)$ spans V. ▷▷▷

Proof of 4.13. Since $v_{r+1} \in V = \mathrm{Span}(v_1, v_2, \ldots, v_r, x_1, x_2, \ldots, x_s)$ there exist scalars λ_i and μ_k with

$$v_{r+1} = \Big(\sum_{i=1}^{r} \lambda_i v_i\Big) + \Big(\sum_{k=1}^{s} \mu_k x_k\Big).$$

Writing $\lambda_{r+1} = -1$ we have

$$\lambda_1 v_1 + \cdots + \lambda_r v_r + \lambda_{r+1} v_{r+1} + \mu_1 x_1 + \cdots + \mu_s x_s = \underset{\sim}{0},$$

which shows that $(v_1, \ldots, v_r, v_{r+1}, x_1, \ldots, x_s)$ is linearly dependent, since the coefficient of λ_{r+1} is nonzero. (Observe that this gives a contradiction if

$s = 0$, justifying the remarks in 4.13.2 above.) Now consider the sequences

$$\begin{gathered}(v_1, v_2, \ldots, v_{r+1}) \\ (v_1, v_2, \ldots, v_{r+1}, x_1) \\ (v_1, v_2, \ldots, v_{r+1}, x_1, x_2) \\ \vdots \\ (v_1, v_2, \ldots, v_{r+1}, x_1, x_2, \ldots, x_s).\end{gathered}$$

The first of these is linearly independent, and the last is linearly dependent. We can therefore find the first linearly dependent sequence in the list: let j be the least positive integer for which $(v_1, v_2, \ldots, v_{r+1}, x_1, x_2, \ldots, x_j)$ is linearly dependent. Then $(v_1, v_2, \ldots, v_{r+1}, x_1, x_2, \ldots, x_{j-1})$ is linearly independent, and by 4.4,

$$\begin{aligned}x_j &\in \mathrm{Span}(v_1, v_2, \ldots, v_{r+1}, x_1, \ldots, x_{j-1}) \\ &\subseteq \mathrm{Span}(v_1, v_2, \ldots, v_{r+1}, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_s) \quad \text{(by 4.2 (i))}.\end{aligned}$$

Hence, by 4.2 (ii),

$$\begin{aligned}&\mathrm{Span}(v_1, \ldots, v_{r+1}, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_s) \\ &\qquad = \mathrm{Span}(v_1, \ldots, v_{r+1}, x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_s).\end{aligned}$$

Let us call this last space S. Obviously then $S \subseteq V$. But (by 4.2 (i)) we know that $\mathrm{Span}(v_1, \ldots, v_r, x_1, \ldots, x_s) \subseteq S$, while $\mathrm{Span}(v_1, \ldots, v_r, x_1, \ldots, x_s) = V$ by hypothesis. So

$$\mathrm{Span}(v_1, \ldots, v_{r+1}, x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_s) = V,$$

as required. □

We can now prove the key theorem, by repeated application of the Replacement Lemma.

4.14 THEOREM *Let $(w_1, w_2, \ldots, w_m)$ be a sequence of elements of V which spans V, and let $(v_1, v_2, \ldots, v_n)$ be a linearly independent sequence in V. Then $n \leq m$.*

Proof. Suppose that $n > m$. We will use induction on i to prove the following statement for all $i \in \{1, 2, \ldots, m\}$:

$$(*) \qquad \begin{gathered}\text{There exists a subsequence } (w_1^{(i)}, w_2^{(i)}, \ldots, w_{m-i}^{(i)}) \\ \text{of } (w_1, w_2, \ldots, w_m) \text{ such that} \\ (v_1, v_2, \ldots, v_i, w_1^{(i)}, w_2^{(i)}, \ldots, w_{m-i}^{(i)}) \text{ spans } V.\end{gathered}$$

In other words, what this says is that i of the terms of $(w_1, w_2, \ldots, w_m)$ can be replaced by v_1, v_2, …, v_i without losing the spanning property.

The fact that $(w_1, w_2, \ldots, w_m)$ spans V proves $(*)$ in the case $i = 0$: in this case the subsequence involved is the whole sequence $(w_1, w_2, \ldots, w_m)$ and there is no replacement of terms at all. Now assume that $1 \leq k \leq m$ and that $(*)$ holds when $i = k - 1$. We will prove that $(*)$ holds for $i = k$, and this will complete our induction.

By our hypothesis there is a subsequence $(w_1^{(k-1)}, w_2^{(k-1)}, \ldots, w_{m-k+1}^{(k-1)})$ of $(w_1, w_2, \ldots, w_m)$ such that $(v_1, v_2, \ldots, v_{k-1}, w_1^{(k-1)}, w_2^{(k-1)}, \ldots, w_{m-k+1}^{(k-1)})$ spans V. Repeated application of 4.2 (iii) shows that any subsequence of a linearly independent sequence is linearly independent; so since $(v_1, v_2, \ldots, v_n)$ is linearly independent and $n > m \geq k$ it follows that $(v_1, v_2, \ldots, v_k)$ is linearly independent. Now we can apply the Replacement Lemma to conclude that $(v_1, \ldots, v_{k-1}, v_k, w_1^{(k)}, w_2^{(k)}, \ldots, w_{m-k}^{(k)})$ spans V, $(w_1^{(k)}, w_2^{(k)}, \ldots, w_{m-k}^{(k)})$ being obtained by deleting one term of $(w_1^{(k-1)}, w_2^{(k-1)}, \ldots, w_{m-k+1}^{(k-1)})$. Hence $(*)$ holds for $i = k$, as required.

Since $(*)$ has been proved for all i with $0 \leq i \leq m$, it holds in particular for $i = m$, and in this case it says that $(v_1, v_2, \ldots, v_m)$ spans V. Since $m + 1 \leq n$ we have that v_{m+1} exists; so $v_{m+1} \in \mathrm{Span}(v_1, v_2, \ldots, v_m)$, giving a solution of $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{m+1} v_{m+1} = \underset{\sim}{0}$ with $\lambda_{m+1} = -1 \neq 0$. This contradicts the fact that the sequence of v_j is linearly independent, showing that the assumption that $n > m$ is false, and completing the proof. □

It is now straightforward to deal with the theorems and propositions stated in the previous section.

Proof of 4.6. Since $(w_1, w_2, \ldots, w_m)$ spans and $(v_1, v_2, \ldots, v_n)$ is linearly independent, it follows from 4.14 that $n \leq m$. Dually, since $(v_1, v_2, \ldots, v_n)$ spans and $(w_1, w_2, \ldots, w_m)$ is linearly independent, it follows that $m \leq n$. □

Proof of 4.7. Suppose that the sequence $(v_1, v_2, \ldots, v_n)$ is linearly dependent. Then there exist $\lambda_i \in F$ with

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = \underset{\sim}{0}$$

and $\lambda_r \neq 0$ for some r. For such an r we have

$$\begin{aligned} v_r &= -\lambda_r^{-1}(\lambda_1 v_1 + \cdots + \lambda_{r-1} v_{r-1} + \lambda_{r+1} v_{r+1} + \cdots + \lambda_n v_n) \\ &\in \mathrm{Span}(v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n), \end{aligned}$$

and, by 4.2 (ii),

$$\mathrm{Span}(v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n) = \mathrm{Span}(v_1, v_2, \ldots, v_n).$$

This contradicts the assumption that $(v_1, v_2, \ldots, v_n)$ spans V whilst proper subsequences of it do not. Hence $(v_1, v_2, \ldots, v_n)$ is linearly independent, and, since it also spans, it is therefore a basis. □

Proof of 4.8. Let $v \in V$. By our hypotheses the sequence $(v_1, v_2, \ldots, v_n, v)$ is not linearly independent, but the sequence $(v_1, v_2, \ldots, v_n)$ is. Hence, by 4.4, $v \in \mathrm{Span}(v_1, v_2, \ldots, v_n)$. Since this holds for all $v \in V$ it follows that $V \subseteq \mathrm{Span}(v_1, v_2, \ldots, v_n)$. Since the reverse inclusion is obvious we deduce that $(v_1, v_2, \ldots, v_n)$ spans V, and, since it is also linearly independent, is therefore a basis. □

Proof of 4.9. Given that $V = \mathrm{Span}(v_1, v_2, \ldots, v_n)$, let $\mathcal{S}$ be the set of all subsequences of $(v_1, v_2, \ldots, v_n)$ which span V. Observe that the set $\mathcal{S}$ has at least one element, namely $(v_1, \ldots, v_n)$ itself. Start with this sequence, and if it is possible to delete a term and still be left with a sequence which spans V, do so. Repeat this for as long as possible, and eventually (in at most n steps) we will obtain a sequence $(u_1, u_2, \ldots, u_s)$ in $\mathcal{S}$ with the property that no proper subsequence of $(u_1, u_2, \ldots, u_s)$ is in $\mathcal{S}$. By 4.7 above, such a sequence is necessarily a basis. □

Observe that Theorem 4.5 follows immediately from 4.9.

Proof of 4.10. Let $S = \mathrm{Span}(v_1, v_2, \ldots, v_n)$. If S is not equal to V then it must be a proper subset of V, and we may choose $v_{n+1} \in V$ with $v_{n+1} \notin S$. If the sequence $(v_1, v_2, \ldots, v_n, v_{n+1})$ were linearly dependent 4.4 would give $v_{n+1} \in \mathrm{Span}(v_1, v_2, \ldots, v_n)$, a contradiction. So we have obtained a longer linearly independent sequence, and if this also fails to span V we may choose $v_{n+2} \in V$ which is not in $\mathrm{Span}(v_1, v_2, \ldots, v_n, v_{n+1})$ and increase the length again. Repeat this process for as long as possible.

Since V is finitely generated there is a finite sequence $(w_1, w_2, \ldots, w_m)$ which spans V, and by 4.14 it follows that a linearly independent sequence in V can have at most m elements. Hence the process described in the above paragraph cannot continue indefinitely. Thus at some stage we obtain a linearly independent sequence $(v_1, v_2, \ldots, v_n, \ldots, v_d)$ which cannot be extended, and which therefore spans V. □

The proofs of 4.11 and 4.12 are left as exercises. Our final result in this section is little more than a rephrasing of the definition of a basis; however, it is useful from time to time:

4.15 Proposition *Let V be a vector space over the field F. A sequence $(v_1, v_2, \ldots, v_n)$ is a basis for V if and only if for each $v \in V$ there exist unique $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$ with*

$$(\heartsuit) \qquad v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n.$$

Proof. Clearly $(v_1, v_2, \ldots, v_n)$ spans V if and only if for each $v \in V$ the equation $(\heartsuit)$ has a solution for the scalars λ_i. Hence it will be sufficient to prove that $(v_1, v_2, \ldots, v_n)$ is linearly independent if and only if $(\heartsuit)$ has at most one solution for each $v \in V$.

Suppose that $(v_1, v_2, \ldots, v_n)$ is linearly independent, and suppose that $\lambda_i, \lambda_i' \in F$ $(i = 1, 2, \ldots, n)$ are such that

$$\sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} \lambda_i' v_i = v$$

for some $v \in V$. Collecting terms gives $\sum_{i=1}^{n} (\lambda_i - \lambda_i') v_i = \underset{\sim}{0}$, and linear independence of the v_i gives $\lambda_i - \lambda_i' = 0$ for each i. Thus $\lambda_i = \lambda_i'$, and it follows that $(\heartsuit)$ cannot have more than one solution.

Conversely, suppose that $(\heartsuit)$ has at most one solution for each $v \in V$. Then in particular $\sum_{i=1}^{n} \lambda_i v_i = \underset{\sim}{0}$ has at most one solution, and so $\lambda_i = 0$ is the unique solution to this. That is, $(v_1, v_2, \ldots, v_n)$ is linearly independent. □

§4d Two properties of linear transformations

Since linear transformations are of central importance in this subject, it is natural to investigate their relationships with bases. This section contains two theorems in this direction.

4.16 Theorem *Let V and W be vector spaces over the same field F. Let $(v_1, v_2, \ldots, v_n)$ be a basis for V and let $w_1, w_2, \ldots, w_n$ be arbitrary elements*

of W. Then there is a unique linear transformation $\theta: V \to W$ such that $\theta(v_i) = w_i$ for $i = 1, 2, \ldots, n$.

Proof. We prove first that there is at most one such linear transformation. To do this, assume that θ and φ are both linear transformations from V to W and that $\theta(v_i) = \varphi(v_i) = w_i$ for all i. Let $v \in V$. Since $(v_1, v_2, \ldots, v_n)$ spans V there exist $\lambda_i \in F$ with $v = \sum_{i=1}^{n} \lambda_i v_i$, and we find

$$\begin{aligned}
\theta(v) &= \theta\Big(\sum_{i=1}^{n} \lambda_i v_i\Big) \\
&= \sum_{i=1}^{n} \lambda_i \theta(v_i) && \text{(by linearity of } \theta) \\
&= \sum_{i=1}^{n} \lambda_i \varphi(v_i) && \text{(since } \theta(v_i) = \varphi(v_i)) \\
&= \varphi\Big(\sum_{i=1}^{n} \lambda_i v_i\Big) && \text{(by linearity of } \varphi) \\
&= \varphi(v).
\end{aligned}$$

Thus $\theta = \varphi$, as required.

We must now prove the existence of a linear transformation with the required properties. Let $v \in V$, and write $v = \sum_{i=1}^{n} \lambda_i v_i$ as above. By 4.15 the scalars λ_i are uniquely determined by v, and therefore $\sum_{i=1}^{n} \lambda_i w_i$ is a uniquely determined element of W. This gives us a well defined rule for obtaining an element of W for each element of V; that is, a function from V to W. Thus there is a function $\theta: V \to W$ satisfying

$$\theta\Big(\sum_{i=1}^{n} \lambda_i v_i\Big) = \sum_{i=1}^{n} \lambda_i w_i$$

for all $\lambda_i \in F$, and it remains for us to prove that it is linear.

Let $u, v \in V$ and $\alpha, \beta \in F$. Let $u = \sum_{i=1}^{n} \lambda_i v_i$ and $v = \sum_{i=1}^{n} \mu_i v_i$. Then

$$\alpha u + \beta v = \sum_{i=1}^{n} (\alpha\lambda_i + \beta\mu_i) v_i,$$

and the definition of θ gives

$$\begin{aligned}\theta(\alpha u + \beta v) &= \sum_{i=1}^{n} (\alpha\lambda_i + \beta\mu_i) w_i \\ &= \alpha \sum_{i=1}^{n} \lambda_i w_i + \beta \sum_{i=1}^{n} \mu_i w_i \\ &= \alpha\theta(u) + \beta\theta(v).\end{aligned}$$

Hence θ is linear. □

Comment ▷▷▷

4.16.1 Theorem 4.16 says that a linearly transformation can be defined in an arbitrary fashion on a basis; moreover, once its values on the basis elements have been specified its values everywhere else are uniquely determined. ▷▷▷

Our second theorem of this section, the proof of which is left as an exercise, examines what injective and surjective linear transformations do to a basis of a space.

4.17 THEOREM *Let $(v_1, v_2, \ldots, v_n)$ be a basis of a vector space V and let $\theta: V \to W$ be a linear transformation. Then*

(i) θ is injective if and only if $(\theta(v_1), \theta(v_2), \ldots, \theta(v_n))$ is linearly independent,

(ii) θ is surjective if and only if $(\theta(v_1), \theta(v_2), \ldots, \theta(v_n))$ spans W.

Comment ▷▷▷

4.17.1 If $\theta: V \to W$ is bijective and $(v_1, v_2, \ldots, v_n)$ is a basis of V then it follows from 4.17 that $(\theta(v_1), \theta(v_2), \ldots, \theta(v_n)$ is a basis of W. Hence the existence of a bijective linear transformation from one space to another guarantees that the spaces must have the same dimension. ▷▷▷

§4e Coordinates relative to a basis

In this final section of this chapter we show that choosing a basis in a vector space enables one to coordinatize the space, in the sense that each element of the space is associated with a uniquely determined n-tuple, where n is the dimension of the space. Thus it turns out that an arbitrary n-dimensional vector space over the field F is, after all, essentially the the same as F^n.

4.18 THEOREM *Let V be a vector space over F and let $v_1, v_2, \ldots, v_n$ be arbitrary elements of V. Then the function $T\colon F^n \to V$ defined by*

$$T\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix} = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

is a linear transformation. Moreover, T is surjective if and only if the sequence $(v_1, v_2, \ldots, v_n)$ spans V and injective if and only if $(v_1, v_2, \ldots, v_n)$ is linearly independent.

Proof. Let $\alpha, \beta \in F^n$ and $\lambda, \mu \in F$. Let α_i, β_i be the i^{th} entries of α, β respectively. Then we have

$$T(\lambda\alpha + \mu\beta) = T\left(\begin{pmatrix}\lambda\alpha_1\\ \lambda\alpha_2\\ \vdots\\ \lambda\alpha_n\end{pmatrix} + \begin{pmatrix}\mu\beta_1\\ \mu\beta_2\\ \vdots\\ \mu\beta_n\end{pmatrix}\right) = T\begin{pmatrix}\lambda\alpha_1 + \mu\beta_1\\ \lambda\alpha_2 + \mu\beta_2\\ \vdots\\ \lambda\alpha_n + \mu\beta_n\end{pmatrix}$$

$$= \sum_{i=1}^{n}(\lambda\alpha_i + \mu\beta_i)v_i = \lambda\sum_{i=1}^{n}\alpha_i v_i + \mu\sum_{i=1}^{n}\beta_i v_i = \lambda T(\alpha) + \mu T(\beta).$$

Hence T is linear.

By the definition of the image of a function, we have

$$\operatorname{im} T = \left\{ T\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_n\end{pmatrix} \;\middle|\; \lambda_i \in F \right\}$$

$$= \{\, \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \mid \lambda_i \in F \,\}$$

$$= \operatorname{Span}(v_1, v_2, \ldots, v_n).$$

By definition, T is surjective if and only if $\operatorname{im} T = W$; hence T is surjective if and only if $(v_1, v_2, \ldots, v_n)$ spans W.

By 3.15 we know that T is injective if and only if the unique solution of $T(\alpha) = \underset{\sim}{0}$ is $\alpha = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$. Since $T(\alpha) = \sum_{i=1}^{n}\alpha_i v_i$ (where α_i is the i^{th} entry of α) this can be restated as follows: T is injective if and only if $\alpha_i = 0$ (for all i) is the unique solution of $\sum_{i=1}^{n}\alpha_i v_i = \underset{\sim}{0}$. That is, T is injective if and only if $(v_1, v_2, \ldots, v_n)$ is linearly independent. □

Comment ▷▷▷

4.18.1 The above proof can be shortened by using 4.16, 4.17 and the standard basis of F^n. ▷▷▷

Assume now that $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ is a basis of V and let $T\colon F^n \to V$ be as defined in 4.18 above. By 4.18 we have that T is bijective, and so it follows that there is an inverse function $T^{-1}\colon V \to F^n$ which associates to every $v \in V$ a column $T^{-1}(v)$; we call this column the *coordinate vector* of v relative to the basis $\boldsymbol{b}$, and we denote it by '$\mathrm{cv}_{\boldsymbol{b}}(v)$'. That is,

4.19 Definition The *coordinate vector* of $v \in V$ relative to the basis $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ is the unique column vector

$$\mathrm{cv}_{\boldsymbol{b}}(v) = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \in F^n$$

such that $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$.

Comment ▷▷▷

4.19.1 Observe that this bijective correspondence between elements of V and n-tuples also follows immediately from 4.15. We have, however, also proved that the corresponding mapping $F^n \to V$, satisfying $\mathrm{cv}_{\boldsymbol{b}}(v) \mapsto v$ for all $v \in V$, is linear. ▷▷▷

—Examples—

#1 Let $\boldsymbol{s} = (e_1, e_2, \ldots, e_n)$, the standard basis of F^n. If $v = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in F^n$ then clearly $v = \lambda_1 e_1 + \cdots + \lambda_n e_n$, and so the coordinate vector of v relative to $\boldsymbol{s}$ is the column with λ_i as its i^{th} entry; that is, the coordinate vector of v is just the same as v:

(4.19.2) *If $\boldsymbol{s}$ is the standard basis of F^n then $\mathrm{cv}_{\boldsymbol{s}}(v) = v$ for all $v \in F^n$.*

#2 Prove that $\boldsymbol{b} = \left(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right)$ is a basis for $\mathbb{R}^3$ and calculate the coordinate vectors of $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ relative to $\boldsymbol{b}$.

$\gg\!\!\rightarrow$ By 4.15 we know that $\boldsymbol{b}$ is a basis of $\mathbb{R}^3$ if and only if each element of $\mathbb{R}^3$ is uniquely expressible as a linear combination of the elements of $\boldsymbol{b}$. That is, $\boldsymbol{b}$ is a basis if and only if the equations

$$x \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + z \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

have a unique solution for all a, b, $c \in \mathbb{R}$. We may rewrite these equations as

$$\begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \end{pmatrix},$$

and we know that there is a unique solution for all a, b, c if and only if the coefficient matrix has an inverse. It has an inverse if and only if the reduced echelon matrix obtained from it by row operations is the identity matrix. We are also asked to calculate x, y and z in three particular cases, and again this involves finding the reduced echelon matrices for the corresponding augmented matrices. We can do all these things at once by applying row operations to the augmented matrix

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right).$$

If the left hand half reduces to the identity it means that $\boldsymbol{b}$ is a basis, and the three columns in the right hand half will be the coordinate vectors we seek.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_3 := R_3 - R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 \end{array} \right)$$

$$\xrightarrow[R_3:=R_3+R_2]{R_1:=R_1-2R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & 1 & -2 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 & 1 \end{array}\right)$$

$$\xrightarrow[R_2:=R_2-R_3]{R_1:=R_1+R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 1 & 1 \end{array}\right).$$

Hence we have shown that $\boldsymbol{b}$ is indeed a basis, and, furthermore,

$$\mathrm{cv}_{\boldsymbol{b}}\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\-1\end{pmatrix}, \quad \mathrm{cv}_{\boldsymbol{b}}\begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}-1\\0\\1\end{pmatrix}, \quad \mathrm{cv}_{\boldsymbol{b}}\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}1\\-1\\1\end{pmatrix}. \quad \lhd\!\ll$$

#3 Let V be the set of all polynomials over $\mathbb{R}$ of degree at most three. Let p_0, p_1, p_2, $p_3 \in V$ be defined by $p_i(x) = x^i$ (for $i = 0, 1, 2, 3$). For each $f \in V$ there exist unique coefficients $a_i \in \mathbb{R}$ such that

$$\begin{aligned} f(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 \\ &= a_0 p_0(x) + a_1 p_1(x) + a_2 p_2(x) + a_3 p_3(x). \end{aligned}$$

Hence we see that $\boldsymbol{b} = (p_0, p_1, p_2, p_3)$ is a basis of V, and if $f(x) = \sum a_i x^i$ as above then $\mathrm{cv}_{\boldsymbol{b}}(f) = {}^t(\, a_0 \quad a_1 \quad a_2 \quad a_3\,)$.

Exercises

1. In each of the following examples the set S has a natural vector space structure over the field F. In each case decide whether S is finitely generated, and, if it is, find its dimension.

(i) $S = \mathbb{C}$ (complex numbers), $F = \mathbb{R}$.

(ii) $S = \mathbb{C}$, $F = \mathbb{C}$.

(iii) $S = \mathbb{R}$, $F = \mathbb{Q}$ (rational numbers).

(iv) $S = \mathbb{R}[X]$ (polynomials over $\mathbb{R}$ in the variable X), $F = \mathbb{R}$.

(v) $S = \mathrm{Mat}(n, \mathbb{C})$ ($n \times n$ matrices over $\mathbb{C}$), $F = \mathbb{R}$.

2. Determine whether or not the following two subspaces of $\mathbb{R}^3$ are the same:

$$\text{Span}\left(\begin{pmatrix}1\\2\\-1\end{pmatrix},\begin{pmatrix}2\\4\\1\end{pmatrix}\right) \text{ and } \quad \text{Span}\left(\begin{pmatrix}1\\2\\4\end{pmatrix},\begin{pmatrix}2\\4\\-5\end{pmatrix}\right).$$

3. Suppose that (v_1, v_2, v_3) is a basis for a vector space V, and define elements $w_1, w_2, w_3 \in V$ by $w_1 = v_1 - 2v_2 + 3v_3$, $w_2 = -v_1 + v_3$, $w_3 = v_2 - v_3$.

(*i*) Express v_1, v_2, v_3 in terms of w_1, w_2, w_3.

(*ii*) Prove that w_1, w_2, w_3 are linearly independent.

(*iii*) Prove that w_1, w_2, w_3 span V.

4. Let V be a vector space and $(v_1, v_2, \ldots, v_n)$ a sequence of vectors in V. Prove that $\text{Span}(v_1, v_2, \ldots, v_n)$ is a subspace of V.

5. Prove Proposition 4.11.

6. Prove Proposition 4.12.

7. Prove Theorem 4.17.

8. Let $(v_1, v_2, \ldots, v_n)$ be a basis of a vector space V and let

$$\begin{aligned} w_1 &= \alpha_{11}v_1 + \alpha_{21}v_2 + \cdots + \alpha_{n1}v_n \\ w_2 &= \alpha_{12}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{n2}v_n \\ &\vdots \\ w_n &= \alpha_{1n}v_1 + \alpha_{2n}v_2 + \cdots + \alpha_{nn}v_n \end{aligned}$$

where the α_{ij} are scalars. Let A be the matrix with (i, j)-entry α_{ij}.

Prove that $(w_1, w_2, \ldots, w_n)$ is a basis for V if and only if A is invertible.

5
Inner Product Spaces

To regard $\mathbb{R}^2$ and $\mathbb{R}^3$ merely as vector spaces is to ignore two basic concepts of Euclidean geometry: the length of a line segment and the angle between two lines. Thus it is desirable to give these vector spaces some additional structure which will enable us to talk of the length of a vector and the angle between two vectors. To do so is the aim of this chapter.

§5a The inner product axioms

If v and w are n-tuples over $\mathbb{R}$ we define the *dot product* of v and w to be the scalar $v \cdot w = \sum_{i=1}^{n} v_i w_i$ where v_i is the i^{th} entry of v and w_i the i^{th} entry of w. That is, $v \cdot w = v({}^{\text{t}}w)$ if v and w are rows, $v \cdot w = ({}^{\text{t}}v)w$ if v and w are columns.

Suppose that a Cartesian coordinate system is chosen for 3-dimensional Euclidean space in the usual manner. If O is the origin and P and Q are points with coordinates $v = (x_1, y_1, z_1)$ and $w = (x_2, y_2, z_2)$ respectively, then by Pythagoras's Theorem the lengths of OP, OQ and PQ are as follows:

$$\begin{aligned} OP &= \sqrt{x_1^2 + y_1^2 + z_1^2} \\ OQ &= \sqrt{x_2^2 + y_2^2 + z_2^2} \\ PQ &= \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}. \end{aligned}$$

By the cosine rule the cosine of the angle POQ is

$$\begin{aligned} &\frac{(x_1^2 + y_1^2 + z_1^2) + (x_2^2 + y_2^2 + z_2^2) - ((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2)}{2\sqrt{x_1^2 + y_1^2 + z_1^2}\sqrt{x_2^2 + y_2^2 + z_2^2}} \\ &\qquad = \frac{x_1 x_2 + y_1 y_2 + z_1 z_2}{\sqrt{x_1^2 + y_1^2 + z_1^2}\sqrt{x_2^2 + y_2^2 + z_2^2}} \\ &\qquad = (v.w)/(\sqrt{v.v}\sqrt{w.w}). \end{aligned}$$

Thus we see that the dot product is closely allied with the concepts of 'length' and 'angle'. Note also the following properties:

(a) The dot product is *bilinear*. That is,

$$(\lambda u + \mu v) \cdot w = \lambda(u \cdot w) + \mu(v \cdot w)$$

and

$$u \cdot (\lambda v + \mu w) = \lambda(u \cdot v) + \mu(u \cdot w)$$

for all n-tuples u, v, w, and all λ, $\mu \in \mathbb{R}$.

(b) The dot product is *symmetric*. That is,

$$v \cdot w = w \cdot v \qquad \text{for all } n\text{-tuples } v,\ w.$$

(c) The dot product is *positive definite*. That is,

$$v \cdot v \geq 0 \qquad \text{for every } n\text{-tuple } v$$

and

$$v \cdot v = 0 \qquad \text{if and only if } v = 0.$$

The proofs of these properties are straightforward and are omitted. It turns out that all important properties of the dot product are consequences of these three basic properties. Furthermore, these same properties arise in other, slightly different, contexts. Accordingly, we use them as the basis of a new axiomatic system.

5.1 Definition A *real inner product space* is a vector space over $\mathbb{R}$ which is equipped with a scalar valued product which is bilinear, symmetric and positive definite. That is, writing $\langle v, w\rangle$ for the scalar product of v and w, we must have $\langle v, w\rangle \in \mathbb{R}$ and

(i) $\langle \lambda u + \mu v, w\rangle = \lambda\langle u, w\rangle + \mu\langle v, w\rangle$,

(ii) $\langle v, w\rangle = \langle w, v\rangle$,

(iii) $\langle v, v\rangle > 0$ if $v \neq 0$,

for all vectors u, v, w and scalars λ, μ.

Comment ▷▷▷

5.1.1 Since the inner product is assumed to be symmetric, linearity in the second variable is a consequence of linearity in the first. It also follows from bilinearity that $\langle v, w\rangle = 0$ if either v or w is zero. To see this, suppose that w is fixed and define a function f_w from the vector space to $\mathbb{R}$ by $f_w(v) = \langle v, w\rangle$ for all vectors v. By (i) above we have that f_w is linear, and hence $f_w(0) = 0$ (by 3.12). ◁◁◁

Apart from $\mathbb{R}^n$ with the dot product, the most important example of an inner product space is the set $\mathcal{C}[a,b]$ of all continuous real valued functions on a closed interval $[a,b]$, with the inner product of functions f and g defined by the formula

$$\langle f, g\rangle = \int_a^b f(x)g(x)\,dx.$$

We leave it as an exercise to check that this gives a symmetric bilinear scalar product. It is a theorem of calculus that if f is continuous and $\int_a^b f(x)^2\,dx = 0$ then $f(x) = 0$ for all $x \in [a,b]$, from which it follows that the scalar product as defined is positive definite.

—***Examples***—

#1 For all u, $v \in \mathbb{R}^3$, let $\langle u, v\rangle \in \mathbb{R}$ be defined by the formula

$$\langle u, v\rangle = {}^{\mathrm{t}}u \begin{pmatrix} 1 & 1 & 2 \\ 1 & 3 & 2 \\ 2 & 2 & 7 \end{pmatrix} v.$$

Prove that $\langle\ ,\ \rangle$ is an inner product on $\mathbb{R}^3$.

$\gg\!\!\rightarrow$ Let A be the 3×3 matrix appearing in the definition of $\langle\ ,\ \rangle$ above. Let u, v, $w \in \mathbb{R}^3$ and λ, $\mu \in \mathbb{R}$. Then using the distributive property of matrix multiplication and linearity of the "transpose" map from $\mathbb{R}^3$ to ${}^{\mathrm{t}}\mathbb{R}^3$, we have

$$\begin{aligned} \langle \lambda u + \mu v, w\rangle &= {}^{\mathrm{t}}(\lambda u + \mu v)Aw \\ &= (\lambda({}^{\mathrm{t}}u) + \mu({}^{\mathrm{t}}v))Aw \\ &= \lambda({}^{\mathrm{t}}u)Aw + \mu({}^{\mathrm{t}}v)Aw \\ &= \lambda\langle u, w\rangle + \mu\langle v, w\rangle, \end{aligned}$$

and it follows that (i) of the definition is satisfied. Part (ii) follows since A is symmetric: for all v, $w \in \mathbb{R}^3$

$$\langle v, w\rangle = ({}^{\mathrm{t}}v)Aw = ({}^{\mathrm{t}}v)({}^{\mathrm{t}}A)w = {}^{\mathrm{t}}(({}^{\mathrm{t}}w)Av) = {}^{\mathrm{t}}(\langle w, v\rangle) = \langle w, v\rangle$$

(the second of these equalities follows since $A = {}^{\mathrm{t}}A$, the third since transposing reverses the order of factors in a product, and the last because $\langle w, v\rangle$ is a 1×1 matrix—that is, a scalar—and hence symmetric).

Now let $v = {}^{\mathrm{t}}(\,x \quad y \quad z\,) \in \mathbb{R}^3$ be arbitrary. We find that

$$\langle v, v\rangle = (\,x \quad y \quad z\,)\begin{pmatrix}1&1&2\\1&3&2\\2&2&7\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}$$
$$= (x^2 + xy + 2xz) + (yx + 3y^2 + 2yz) + (2zx + 2zy + 7z^2).$$

Applying completion of the square techniques we deduce that

$$\langle v, v\rangle = (x + y + 2z)^2 + 2y^2 + 4yz + 3z^2 = (x + y + 2z)^2 + 2(y + z)^2 + z^2,$$

which is nonnegative, and can only be zero if z, $y + z$ and $x + y + 2z$ are all zero. This only occurs if $x = y = z = 0$. So we have shown that $\langle v, v\rangle > 0$ whenever $v \neq 0$, which is the third and last requirement in Definition 5.1.

⊲⊲

#2 Show that if the matrix A in #1 above is replaced by either

$$\begin{pmatrix}1&2&3\\0&3&1\\1&3&7\end{pmatrix} \quad \text{or} \quad \begin{pmatrix}1&1&2\\1&3&2\\2&2&1\end{pmatrix}$$

then the resulting scalar valued product on $\mathbb{R}^3$ does not satisfy the inner product axioms.

⊳⊳ In the first case the fact that the matrix is not symmetric means that the resulting product would not satisfy (ii) of Definition 5.1. For example, we would have

$$\langle\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}\rangle = (\,1 \quad 0 \quad 0\,)\begin{pmatrix}1&2&3\\0&3&1\\1&3&7\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix} = 2$$

while on the other hand

$$\langle\begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}\rangle = (\,0 \quad 1 \quad 0\,)\begin{pmatrix}1&2&3\\0&3&1\\1&3&7\end{pmatrix}\begin{pmatrix}1\\0\\0\end{pmatrix} = 0.$$

In the second case Part (iii) of Definition 5.1 would fail. For example, we would have

$$\langle\begin{pmatrix}-1\\-1\\1\end{pmatrix}, \begin{pmatrix}-1\\-1\\1\end{pmatrix}\rangle = (\,-1 \quad -1 \quad 1\,)\begin{pmatrix}1&1&2\\1&3&2\\2&2&1\end{pmatrix}\begin{pmatrix}-1\\-1\\1\end{pmatrix} = -1,$$

contrary to the requirement that $\langle v, v\rangle \geq 0$ for all v. ⊲⊲

#3 The *trace* $\mathrm{Tr}(A)$ of an $n \times n$ matrix A is defined to be the sum of the diagonal entries of A; that is, $\mathrm{Tr}(A) = \sum_{i=1}^{n} A_{ii}$. Show that

$$\langle M, N \rangle = \mathrm{Tr}({}^{\mathrm{t}}M)N)$$

defines an inner product on the space of all $m \times n$ matrices over $\mathbb{R}$.

$\gg\!\!\rightarrow$ The (i,i)-entry of $({}^{\mathrm{t}}M)N$ is

$$(({}^{\mathrm{t}}M)N)_{ii} = \sum_{j=1}^{m} ({}^{\mathrm{t}}M)_{ij} N_{ji} = \sum_{j=1}^{m} M_{ji} N_{ji}$$

since the (i,j)-entry of ${}^{\mathrm{t}}M$ is the (j,i)-entry of M. Thus the trace of $({}^{\mathrm{t}}M)N$ is $\sum_{i=1}^{n}(({}^{\mathrm{t}}M)N)_{ii} = \sum_{i=1}^{n}\sum_{j=1}^{m} M_{ji}N_{ji}$. Thus, if we think of an $m \times n$ matrix as an mn-tuple which is simply written as a rectangular array instead of as a row or column, then the given formula for $\langle M, N \rangle$ is just the standard dot product formula: the sum of the products of each entry of M by the corresponding entry of N. So the verification that $\langle\ ,\ \rangle$ as defined is an inner product involves almost exactly the same calculations as involved in proving bilinearity, symmetry and positive definiteness of the dot product on R^n.

Thus, let M, N, P be $m \times n$ matrices, and let λ, $\mu \in \mathbb{R}$. Then

$$\begin{aligned}\langle \lambda M + \mu N, P \rangle &= \sum_{i,j} (\lambda M + \mu N)_{ji} P_{ji} = \sum_{i,j} (\lambda M_{ji} + \mu N_{ji}) P_{ji} \\ &= \sum_{i,j} (\lambda M_{ji} P_{ji} + \mu N_{ji} P_{ji}) = \lambda \sum_{i,j} M_{ji} P_{ji} + \mu \sum_{i,j} N_{ji} P_{ji} \\ &= \lambda \langle M, P \rangle + \mu \langle N, P \rangle,\end{aligned}$$

verifying Property (i) of 5.1. Furthermore,

$$\langle M, N \rangle = \sum_{i,j} M_{ji} N_{ji} = \sum_{i,j} N_{ji} M_{ji} = \langle N, M \rangle,$$

verifying Property (ii). Finally, $\langle M, M \rangle = \sum_{i,j} (M_{ji})^2$ is clearly nonnegative in all cases, and can only be zero if $M_{ji} = 0$ for all i and j. That is, $\langle M, M \rangle \geq 0$, with equality only if $M = 0$. Hence Property (iii) holds as well. $\ll\!\!\leftarrow$

It is also possible to define a dot product on $\mathbb{C}^n$. In this case the definition is

$$v \cdot w = ({}^{\mathrm{t}}\overline{v})w = \sum_{i=1}^{n} \overline{v_i} w_i$$

where the overline indicates complex conjugation. This apparent complication is introduced to preserve positive definiteness. If z is an arbitrary complex number then $\overline{z}z$ is real and nonnegative, and zero only if z is zero. It follows easily that if v is an arbitrary complex column vector then $v \cdot v$ as defined above is real and nonnegative, and is zero only if $v = 0$.

The price to be paid for making the complex dot product positive definite is that it is no longer bilinear. It is still linear in the second variable, but *semilinear* or *conjugate linear* in the first:

$$(\lambda u + \mu v) \cdot w = \overline{\lambda}(u \cdot w) + \overline{\mu}(v \cdot w)$$

and

$$u \cdot (\lambda v + \mu w) = \lambda(u \cdot v) + \mu(u \cdot w)$$

for all u, v, $w \in \mathbb{C}^n$ and λ, $\mu \in \mathbb{C}$. Likewise, the complex dot product is not quite symmetric; instead, it satisfies

$$v \cdot w = \overline{w \cdot v} \qquad \text{for all } v,\ w \in \mathbb{C}^n.$$

Analogy with the real case leads to the following definition.

5.2 Definition A *complex inner product space* is a complex vector space V which is equipped with a scalar product $\langle\ ,\ \rangle : V \times V \to \mathbb{C}$ satisfying

(i) $\langle u, \lambda v + \mu w\rangle = \lambda\langle u, v\rangle + \mu\langle u, w\rangle$,

(ii) $\langle v, w\rangle = \overline{\langle w, v\rangle}$,

(iii) $\langle v, v\rangle \in \mathbb{R}$ and $\langle v, v\rangle > 0$ if $v \neq 0$,

for all u, v, $w \in V$ and λ, $\mu \in \mathbb{C}$.

Comments ▷▷▷

5.2.1 Note that $\langle v, v\rangle \in \mathbb{R}$ is in fact a consequence of $\langle v, w\rangle = \overline{\langle w, v\rangle}$

5.2.2 Complex inner product spaces are often called *unitary* spaces, and real inner product spaces are often called *Euclidean* spaces. ▷▷▷

If V is any inner product space (real or complex) we define the *length* or *norm* of a vector $v \in V$ to be the nonnegative real number $\|v\| = \sqrt{\langle v, v\rangle}$. (This definition is suggested by the fact, noted above, that the distance from the origin of the point with coordinates $v = (\ x \quad y \quad z\ )$ is $\sqrt{v.v}$.) It is an easy

exercise to prove that if $v \in V$ and λ is a scalar then $\|\lambda v\| = |\lambda|\,\|v\|$. (Recall that the absolute value of a complex number λ is given by $|\lambda| = \sqrt{\lambda\overline{\lambda}}$.) In particular, if $\lambda = (1/\|v\|)$ then $\|\lambda v\| = 1$.

Having defined the length of a vector it is natural now to say that the *distance* between two vectors x and y is the length of $x - y$; thus we define

$$d(x, y) = \|x - y\|.$$

It is customary in mathematics to reserve the term 'distance' for a function d satisfying the following properties:

(i) $d(x, y) = d(y, x)$,

(ii) $d(x, y) \geq 0$, and $d(x, y) = 0$ only if $x = y$,

(iii) $d(x, z) \leq d(x, y) + d(y, z)$ (the *triangle inequality*),

for all x, y and z. It is easily seen that our definition meets the first two of these requirements; the proof that it also meets the third is deferred for a while.

Analogy with the dot product suggests also that for real inner product spaces the angle θ between two nonzero vectors v and w should be defined by the formula

$$\cos\theta = \langle v, w\rangle / (\|v\|\,\|w\|).$$

Obviously we want $-1 \leq \cos\theta \leq 1$; so to justify the definition we must prove that $|\langle v, w\rangle| \leq \|v\|\,\|w\|$ (the *Cauchy-Schwarz inequality*). We will do this later.

5.3 Definition Let V be an inner product space. Vectors $v, w \in V$ are said to be *orthogonal* if $\langle v, w\rangle = 0$. A set X of vectors is said to be *orthonormal* if $\langle v, v\rangle = 1$ for all v in X and $\langle v, w\rangle = 0$ for all $v, w \in X$ such that $v \neq w$.

Comments ▷▷▷

5.3.1 In view of our intended definition of the angle between two vectors, this definition will say that two nonzero vectors in a real inner product space are orthogonal if and only if they are at rightangles to each other.

5.3.2 Observe that orthogonality is a symmetric relation, since if $\langle v, w\rangle$ is zero then $\langle w, v\rangle = \overline{\langle v, w\rangle}$ is too. Observe also that if v is orthogonal to w then all scalar multiples of v are orthogonal to w. In particular, if $v_1, v_2, \ldots, v_n$ are nonzero vectors satisfying $\langle v_i, v_j\rangle = 0$ whenever $i \neq j$, then an othonormal set of vectors can be obtained by replacing v_i by $\|v_i\|^{-1}v_i$ for each i. ▷▷▷

§5b Orthogonal projection

Note that the standard bases of $\mathbb{R}^n$ and $\mathbb{C}^n$ are orthonormal bases. As we shall see below, such bases are of particular importance. It is easily shown that orthonormal vectors are always linearly independent.

5.4 PROPOSITION *Let $v_1, v_2, \ldots, v_n$ be nonzero elements of V (an inner product space) and suppose that $\langle v_i, v_j\rangle = 0$ whenever $i \neq j$. Then the v_i are linearly independent.*

Proof. Suppose that $\sum_{i=1}^n \lambda_i v_i = 0$, where the λ_i are scalars. By 5.1.1 above we see that for all j,

$$\begin{aligned} 0 &= \langle v_j, \sum_{i=1}^n \lambda_i v_i\rangle \\ &= \sum_{i=1}^n \lambda_i \langle v_j, v_i\rangle \qquad \text{(by linearity in the second variable)} \\ &= \lambda_j \langle v_j, v_j\rangle \qquad \text{(since the other terms are zero)} \end{aligned}$$

and since $\langle v_j, v_j\rangle \neq 0$ it follows that $\lambda_j = 0$. □

Under the hypotheses of 5.4 the v_i form a basis of the subspace they span. Such a basis is called an *orthogonal basis* of the subspace.

—***Example***—

#4 The space $\mathcal{C}[-1,1]$ has a subspace of dimension 3 consisting of polynomial functions on $[-1,1]$ of degree at most two. It can be checked that f_0, f_1 and f_2 defined by $f_0(x) = 1$, $f_1(x) = x$ and $f_2(x) = 3x^2 - 1$ form an orthogonal basis of this subspace. Indeed, since $f_0(x)f_1(x)$ and $f_1(x)f_2(x)$ are both odd functions it is immediate that $\int_{-1}^1 f_0(x)f_1(x)\,dx$ and $\int_{-1}^1 f_1(x)f_2(x)\,dx$ are both zero, while

$$\int_{-1}^1 f_0(x)f_2(x)\,dx = \int_{-1}^1 3x^2 - 1\,dx = (x^3 - x)\big]_{-1}^1 = 0.$$

5.5 LEMMA *Let $(u_1, u_2, \dots, u_n)$ be an orthogonal basis of a subspace U of V, and let $v \in V$. There is a unique element $u \in U$ such that $\langle x, u\rangle = \langle x, v\rangle$ for all $x \in U$, and it is given by the formula $u = \sum_{i=1}^{n} \big(\langle u_i, v\rangle / \langle u_i, u_i\rangle\big) u_i$.*

Proof. The elements of a basis must be nonzero; so we have that $\langle u_i, u_i\rangle \neq 0$ for all i. Write $\lambda_i = \langle u_i, v\rangle / \langle u_i, u_i\rangle$ and $u = \sum_{i=1}^{n} \lambda_i u_i$. Then for each j from 1 to n we have

$$\begin{aligned}\langle u_j, u\rangle &= \langle u_j, \sum_{i=1}^{n} \lambda_i u_i\rangle \\ &= \sum_{i=1}^{n} \lambda_i \langle u_j, u_i\rangle \\ &= \lambda_j \langle u_j, u_j\rangle \qquad \text{(since the other terms are zero)} \\ &= \langle u_j, v\rangle.\end{aligned}$$

If $x \in U$ is arbitrary then $x = \sum_{j=1}^{n} \mu_j u_j$ for some scalars μ_j, and we have

$$\langle x, u\rangle = \sum_j \overline{\mu_j} \langle u_j, u\rangle = \sum_j \overline{\mu_j} \langle u_j, v\rangle = \langle x, v\rangle$$

showing that u has the required property. If $u' \in U$ also has this property then for all $x \in U$,

$$\langle x, u - u'\rangle = \langle x, u\rangle - \langle x, u'\rangle = \langle x, v\rangle - \langle x, v\rangle = 0.$$

Since $u - u' \in U$ this gives, in particular, that $\langle u - u', u - u'\rangle = 0$, and hence $u - u' = 0$. So u is uniquely determined. □

Our first consequence of 5.5 is the *Gram-Schmidt orthogonalization process*, by which an arbitrary finite dimensional subspace of an inner product space is shown to have an orthogonal basis.

5.6 THEOREM *Let $(v_1, v_2, v_3, \dots)$ be a sequence (finite or infinite) of vectors in an inner product space, such that $\boldsymbol{b}_r = (v_1, v_2, \dots, v_r)$ is linearly independent for all r. Let V_r be the subspace spanned by $\boldsymbol{b}_r$. Then there exist vectors u_1, u_2, u_3, … in V such that $\boldsymbol{c}_r = (u_1, u_2, \dots, u_r)$ is an orthogonal basis of V_r for each r.*

Proof. This is proved by induction. The case $r = 1$ is easily settled by defining $u_1 = v_1$; the statement that $\boldsymbol{c}_1$ is orthogonal is vacuously true.

Assume now that $r > 1$ and that u_1 to u_{r-1} have been found with the required properties. By 5.5 there exists $u \in V_{r-1}$ such that $\langle u_i, u\rangle = \langle u_i, v_r\rangle$ for all i from 1 to $r-1$. We define $u_r = v_r - u$, noting that this is nonzero since, by linear independence of $\boldsymbol{b}_r$, the vector v_r is not in the subspace V_{r-1}. To complete the proof it remains to check that $\langle u_i, u_j\rangle = 0$ for all $i, j \leq r$ with $i \neq j$. If $i, j \leq r-1$ this is immediate from our inductive hypothesis, and the remaining case is clear too, since for all $i < r$,

$$\langle u_i, u_r\rangle = \langle u_i, v_r - u\rangle = \langle u_i, v_r\rangle - \langle u_i, u\rangle = 0$$

by the definition of u. □

In view of this we see from 5.5 that if U is any finite dimensional subspace of an inner product space V then there is a unique mapping $P\colon V \to U$ such that $\langle u, P(v)\rangle = \langle u, v\rangle$ for all $v \in V$ and $u \in U$. Furthermore, if $(u_1, u_2, \ldots, u_n)$ is any orthogonal basis of U then we have the formula

$$P(v) = \sum_{i=1}^{n} \big(\langle u_i, v\rangle / \langle u_i, u_i\rangle\big) u_i. \tag{5.6.1}$$

5.7 Definition The transformation $P\colon V \to U$ defined above is called the *orthogonal projection* of V onto U.

Comments ▷▷▷

5.7.1 It follows easily from the formula 5.6.1 that orthogonal projections are linear transformations; this is left as an exercise for the reader.

5.7.2 The Gram-Schmidt process, given in the proof of Theorem 5.6 above, is an algorithm for which the input is a linearly independent sequence of vectors $v_1, v_2, v_3, \ldots$ and the output an orthogonal sequence of vectors $u_1, u_2, u_3, \ldots$ which are linear combinations of the v_i. The proof gives the following formulae for the u_i:

$$\begin{aligned}
u_1 &= v_1 \\
u_2 &= v_2 - \frac{\langle u_1, v_2\rangle}{\langle u_1, u_1\rangle} u_1 \\
u_3 &= v_3 - \frac{\langle u_1, v_3\rangle}{\langle u_1, u_1\rangle} u_1 - \frac{\langle u_2, v_3\rangle}{\langle u_2, u_2\rangle} u_2 \\
&\vdots \\
u_r &= v_r - \frac{\langle u_1, v_r\rangle}{\langle u_1, u_1\rangle} u_1 - \cdots - \frac{\langle u_{r-1}, v_r\rangle}{\langle u_{r-1}, u_{r-1}\rangle} u_{r-1}.
\end{aligned}$$

In practice it is not necessary to remember the formulae for the coefficients of the u_i on the right hand side. Instead, if one remembers merely that

$$u_r = v_r + \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_{r-1} u_{r-1}$$

then it is easy to find λ_i for each $i < r$ by taking inner products with u_i. Indeed, since $\langle u_i, u_j \rangle = 0$ for $i \neq j$, we get

$$0 = \langle u_i, u_r \rangle = \langle u_i, v_r \rangle + \lambda_i \langle u_i, u_i \rangle$$

since the terms $\lambda_j \langle u_i, u_j \rangle$ are zero for $i \neq j$, and this yields the stated formula for λ_i. ▷▷▷

—Examples—

#5 Let $V = \mathbb{R}^4$ considered as an inner product space via the dot product, and let U be the subspace of V spanned by the vectors

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 2 \\ 3 \\ 2 \\ -4 \end{pmatrix} \quad \text{and} \quad v_3 = \begin{pmatrix} -1 \\ 5 \\ -2 \\ -1 \end{pmatrix}.$$

Use the Gram-Schmidt process to find an orthonormal basis of U.

≫▷ Using the formulae given in 5.7.2 above, if we define

$$u_1 = v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$u_2 = v_2 - \frac{u_1 \cdot v_2}{u_1 \cdot u_1} u_1 = \begin{pmatrix} 2 \\ 3 \\ 2 \\ -4 \end{pmatrix} - \frac{3}{4} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5/4 \\ 9/4 \\ 5/4 \\ -19/4 \end{pmatrix}$$

and

$$\begin{aligned} u_3 &= v_3 - \frac{u_1 \cdot v_3}{u_1 \cdot u_1} u_1 - \frac{u_2 \cdot v_3}{u_2 \cdot u_2} u_2 \\ &= \begin{pmatrix} -1 \\ 5 \\ -2 \\ -1 \end{pmatrix} - \frac{1}{4} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \frac{(49/4)}{(492/16)} \begin{pmatrix} 5/4 \\ 9/4 \\ 5/4 \\ -19/4 \end{pmatrix} \\ &= \begin{pmatrix} -1 \\ 5 \\ -2 \\ -1 \end{pmatrix} - \frac{123}{492} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} - \frac{49}{492} \begin{pmatrix} 5 \\ 9 \\ 5 \\ -19 \end{pmatrix} = \begin{pmatrix} -860/492 \\ 1896/492 \\ -1352/492 \\ 316/492 \end{pmatrix} \end{aligned}$$

then u_1, u_2 and u_3 are mutually orthogonal and span U. It remains to "normalize" the basis vectors; that is, replace each u_i by a vector of length 1 which is a scalar multiple of u_i. This is achieved by the formula $u_i' = \dfrac{1}{\sqrt{u_i \cdot u_i}} u_i$. We obtain

$$u_1' = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix}, \qquad u_2' = \begin{pmatrix} 5/\sqrt{492} \\ 9/\sqrt{492} \\ 5/\sqrt{492} \\ -19/\sqrt{492} \end{pmatrix}, \qquad u_3' = \begin{pmatrix} -215/\sqrt{391386} \\ 474/\sqrt{391386} \\ -338/\sqrt{391386} \\ 79/\sqrt{391386} \end{pmatrix}$$

as a suitable orthonormal basis for the given subspace. ⋘⊣

#6 With U and V as in #5 above, let $P: V \to U$ be the orthogonal projection, and let $v = \begin{pmatrix} -20 \\ 8 \\ 19 \\ -1 \end{pmatrix}$. Calculate $P(v)$.

⊢≫ Using the formula 5.6.1 and the orthonormal basis (u_1', u_2', u_3') found in #5 gives

$$\begin{aligned} P\begin{pmatrix} -20 \\ 8 \\ 19 \\ -1 \end{pmatrix} &= (u_1' \cdot v)u_1' + (u_2' \cdot v)u_2' + (u_3' \cdot v)u_3' \\ &= 3\begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{pmatrix} + \frac{86}{\sqrt{492}}\begin{pmatrix} 5/\sqrt{492} \\ 9/\sqrt{492} \\ 5/\sqrt{492} \\ -19/\sqrt{492} \end{pmatrix} + \frac{1591}{\sqrt{391386}}\begin{pmatrix} -215/\sqrt{391386} \\ 474/\sqrt{391386} \\ -338/\sqrt{391386} \\ 79/\sqrt{391386} \end{pmatrix} \\ &= \frac{3}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \frac{43}{246}\begin{pmatrix} 5 \\ 9 \\ 5 \\ -19 \end{pmatrix} + \frac{1}{246}\begin{pmatrix} -215 \\ 474 \\ -338 \\ 79 \end{pmatrix} = \begin{pmatrix} 3/2 \\ 5 \\ 1 \\ -3/2 \end{pmatrix} \end{aligned}$$

⋘⊣

Suppose that $V = \mathbb{R}^3$, with the dot product, and let U be a subspace of V of dimension 2. Geometrically, U is a plane through the origin. The geometrical process corresponding to the orthogonal projection is "dropping

a perpendicular" to U from a given point v. Then $P(v)$ is the point of U which is the foot of the perpendicular. It is geometrically clear that $u = P(v)$ is the unique $u \in U$ such that $v - u$ is perpendicular to everything in U; this corresponds to the algebraic statement that $\langle x, v - P(v)\rangle = 0$ for all $x \in U$. It is also geometrically clear that $P(v)$ is the point of U which is closest to v. We ought to prove this algebraically.

5.8 THEOREM *Let U be a finite dimensional subspace of an inner product space V, and let P be the orthogonal projection of V onto U. If v is any element of V then $\|v - u\| \geq \|v - P(v)\|$ for all $u \in U$, with equality only if $u = P(v)$.*

Proof. Given $u \in U$ we have $v - u = (v - P(v)) + x$ where $x = P(v) - u$ is an element of U. Since $v - P(v)$ is orthogonal to all elements of U we see that

$$\begin{aligned}\|v-u\|^2 &= \langle v-u, v-u\rangle \\ &= \langle v-P(v)+x, v-P(v)+x\rangle \\ &= \langle v-P(v), v-P(v)\rangle + \langle v-P(v), x\rangle + \langle x, v-P(v)\rangle + \langle x, x\rangle \\ &= \langle v-P(v), v-P(v)\rangle + \langle x, x\rangle \\ &\geq \langle v-P(v), v-P(v)\rangle\end{aligned}$$

with equality if and only if $x = 0$. □

An extremely important application of this method of finding the point of a subspace which is closest to a given point, is the approximate solution of inconsistent systems of equations. The equations $Ax = b$ have a solution if and only if b is contained in the column space of the matrix A (see 3.20.1). If b is not in the column space then it is reasonable to find that point b_0 of the column space which is closest to b, and solve the equations $Ax = b_0$ instead. Inconsistent systems commonly arise in practice in cases where we can obtain as many (approximate) equations as we like by simply taking more measurements.

—Examples—

#7 Three measurable variables A, B and C are known to be related by a formula of the form $xA + yB = C$, and an experiment is performed to find the values x and y. In four cases measurement yields the results tabulated

below, in which, no doubt, there are some experimental errors. What are the values of x and y which best fit this data?

	A	B	C
1^{st} case:	1.0	2.0	3.8
2^{nd} case:	1.0	3.0	5.1
3^{rd} case:	1.0	4.0	5.9
4^{th} case:	1.0	5.0	6.8

$\gg\!\!\rightarrow$ We have a system of four equations in two unknowns:

$$\begin{pmatrix} A_1 & B_1 \\ A_2 & B_2 \\ A_3 & B_3 \\ A_4 & B_4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix}$$

which is bound to be inconsistent. Viewing these equations as $x\underset{\sim}{A} + y\underset{\sim}{B} = \underset{\sim}{C}$ (where $\underset{\sim}{A} \in \mathbb{R}^4$ has i^{th} entry A_i, and so on) we see that a reasonable choice for x and y comes from the point in $U = \text{Span}(\underset{\sim}{A}, \underset{\sim}{B})$ which is closest to $\underset{\sim}{C}$; that is, the point $P(\underset{\sim}{C})$ where P is the projection of $\mathbb{R}^4$ onto the subspace U. To compute the projection we first need to find an orthogonal basis for U, which we do by means of the Gram-Schmidt process applied to $\underset{\sim}{A}$ and $\underset{\sim}{B}$. This gives the orthogonal basis $(\underset{\sim}{A}', \underset{\sim}{B}')$ where $\underset{\sim}{A}' = \underset{\sim}{A}$ and

$$\begin{aligned} \underset{\sim}{B}' &= \underset{\sim}{B} - (\langle \underset{\sim}{A}, \underset{\sim}{B} \rangle / \langle \underset{\sim}{A}, \underset{\sim}{A} \rangle)\underset{\sim}{A} \\ &= \underset{\sim}{B} - (7/2)\underset{\sim}{A} \\ &= {}^{\text{t}}(\,-1.5 \quad -0.5 \quad 0.5 \quad 1.5\,)\,. \end{aligned}$$

Now $P(\underset{\sim}{C})$ is given by the formula

$$P(\underset{\sim}{C}) = (\langle \underset{\sim}{A}', \underset{\sim}{C} \rangle / \langle \underset{\sim}{A}', \underset{\sim}{A}' \rangle)\underset{\sim}{A}' + (\langle \underset{\sim}{B}', \underset{\sim}{C} \rangle / \langle \underset{\sim}{B}', \underset{\sim}{B}' \rangle)\underset{\sim}{B}'$$

and calculation gives the coefficients of $\underset{\sim}{A}'$ and $\underset{\sim}{B}'$ as 5.4 and 0.98. Expressing this combination of $\underset{\sim}{A}'$ and $\underset{\sim}{B}'$ back in terms of $\underset{\sim}{A}$ and $\underset{\sim}{B}$ gives the coefficient of $\underset{\sim}{B}$ as $y = 0.98$ and the coefficient of $\underset{\sim}{A}$ as $x = 5.4 - 3.5 \times 0.98 = 1.97$. (If these are the correct values of x and y then the values of C for the given values of A and B should be, in the four cases, 3.93, 4.91, 5.89 and 6.87)

$\ll\!\!\leftarrow$

#8 Find the parabola $y = ax^2 + bx + c$ which most closely fits the graph of $y = e^x$ on the interval $[-1, 1]$, in the sense that $\int_{-1}^{1}(f(x) - e^x)^2\,dx$ is minimized.

⋙▷ Let P be the orthogonal projection of $\mathcal{C}[a, b]$ onto the subspace of polynomial functions of degree at most 2. We seek to calculate $P(\exp)$, where exp is the exponential function. Using the orthogonal basis (f_0, f_1, f_2) from #4 above we find that $P(\exp) = \lambda f_0 + \mu f_1 + \nu f_2$ where

$$\lambda = \int_{-1}^{1} e^x\,dx \Big/ \int_{-1}^{1} 1\,dx$$
$$\mu = \int_{-1}^{1} xe^x\,dx \Big/ \int_{-1}^{1} x^2\,dx$$
$$\nu = \int_{-1}^{1} (3x^2 - 1)e^x\,dx \Big/ \int_{-1}^{1} (3x^2 - 1)^2\,dx.$$

That is, the sought after function is $f(x) = \lambda + \mu x + \nu(3x^2 - 1)$ for the above values of λ, μ and ν. ◁⋘

#9 Define functions c_0, c_1, s_1, c_2, s_2, ... on the interval $[-\pi, \pi]$ by

$$c_n(x) = \cos(nx) \qquad (\text{for } n = 0, 1, 2, \dots)$$
$$s_n(x) = \sin(nx) \qquad (\text{for } n = 1, 2, 3, \dots).$$

Show that the c_n for $0 \le n \le k$ and the s_m for $1 \le m \le k$ together form an orthogonal basis of a subspace of $\mathcal{C}[-\pi, \pi]$, and determine the formula for the element of this subspace closest to a given f.

⋙▷ Recall the trigonometric formulae

$$2\sin(nx)\cos(mx) = \sin((n + m)x) - \sin((n - m)x)$$
$$2\cos(nx)\cos(mx) = \cos((n + m)x) + \cos((n - m)x)$$
$$2\sin(nx)\sin(mx) = \cos((n - m)x) - \cos((n + m)x).$$

Since $\int_{-\pi}^{\pi}\sin(kx)\,dx = 0$ for all k and

$$\int_{-\pi}^{\pi}\cos(kx)\,dx = \begin{cases} 0 & \text{if } k \neq 0 \\ 2\pi & \text{if } k = 0 \end{cases}$$

we deduce that

(i) $\langle s_n, c_m\rangle = 0$ for all n and m,
(ii) $\langle s_n, s_m\rangle = \langle c_n, c_m\rangle = 0$ if $n \neq m$,
(iii) $\langle s_n, s_n\rangle = \langle c_n, c_n\rangle = \pi$ if $n \neq 0$,
(iv) $\langle c_0, c_0\rangle = 2\pi$.

Hence if P is the orthogonal projection onto the subspace spanned by the c_n and s_m then for an arbitrary $f \in \mathcal{C}[-\pi, \pi]$,

$$\big(P(f)\big)(x) = (1/2\pi)a_0 + (1/\pi)\sum_{n=1}^{k}(a_n\cos(nx) + b_n\sin(nx))$$

where

$$a_n = \langle c_n, f\rangle = \int_{-\pi}^{\pi} f(x)\cos(nx)\,dx$$

and

$$b_n = \langle s_n, f\rangle = \int_{-\pi}^{\pi} f(x)\sin(nx)\,dx.$$

We know from 5.8 that $g = P(f)$ is the element of the subspace for which $\int_{-\pi}^{\pi}(f-g)^2$ is minimized. ⊲⊢≪

We have been happily talking about orthogonal projections onto subspaces and ignoring the fact that the word 'onto' should only be applied to functions that are surjective. Fortunately, it is easy to see that the image of the projection of V onto U is indeed the whole of U. In fact, if P is the projection then $P(u) = u$ for all $u \in U$. (A consequence of this is that P is an *idempotent* transformation: it satisfies $P^2 = P$.) It is natural at this stage to ask about the kernel of P.

5.9 Definition If U is a finite dimensional subspace of an inner product space V and P the projection of V onto U then the subspace $U^{\perp} = \ker P$ is called the *orthogonal complement* of U.

Comment ▷▷▷

5.9.1 If $\langle x, v\rangle = 0$ for all $x \in U$ then $u = 0$ is clearly an element of U satisfying $\langle x, u\rangle = \langle x, v\rangle$ for all $x \in U$. Hence $P(v) = 0$. Conversely, if $P(v) = 0$ we must have $\langle x, v\rangle = \langle x, P(v)\rangle = 0$ for all $x \in U$. Hence the orthogonal complement of U consists of all $v \in V$ which are orthogonal to all elements of U. ▷▷▷

Our final task in this section is to prove the triangle and Cauchy-Schwarz inequalities, and some related matters.

5.10 Proposition *Assume that $(u_1, u_2, \dots, u_n)$ is an orthogonal basis of a subspace U of V.*

(i) Let $v \in V$ and for all i let $\alpha_i = \langle u_i, v\rangle$. Then $\|v\|^2 \geq \sum_i |\alpha_i|^2/\|u_i\|^2$.

(ii) If $u \in U$ then $u = \sum_{i=1}^{n} \big(\langle u_i, u\rangle/\langle u_i, u_i\rangle\big)u_i$.

(iii) If $x, y \in U$ then $\langle x, y\rangle = \sum_i (\langle x, u_i\rangle\langle u_i, y\rangle)/\langle u_i, u_i\rangle$.

Proof. (i) If $P\colon V \to U$ is the orthogonal projection then 5.6.1 above gives $P(v) = \sum_i \lambda_i u_i$, where

$$\lambda_i = \langle u_i, v\rangle/\langle u_i, u_i\rangle = \alpha_i/\|u_i\|^2.$$

Since $\langle u_i, u_j\rangle = 0$ for $i \neq j$ we have

$$\langle P(v), P(v)\rangle = \sum_{i,j} \overline{\lambda}_i \lambda_j \langle u_i, u_j\rangle = \sum_i |\lambda_i|^2 \langle u_i, u_i\rangle = \sum_i |\alpha_i|^2/\|u_i\|^2,$$

so that our task is to prove that $\langle v, v\rangle \geq \langle P(v), P(v)\rangle$.

Writing $x = v - P(v)$ we have

$$\begin{aligned}
\langle v, v\rangle &= \langle x + P(v), x + P(v)\rangle \\
&= \langle x, x\rangle + \langle x, P(v)\rangle + \langle P(v), x\rangle + \langle P(v), P(v)\rangle \\
&= \langle x, x\rangle + \langle P(v), P(v)\rangle \qquad (\text{since } P(v) \in U \text{ and } x \in U^{\perp}) \\
&\geq \langle P(v), P(v)\rangle,
\end{aligned}$$

as required.

(ii) This amounts to the statement that $P(u) = u$ for $u \in U$, and it is immediate from 5.8 above, since the element of U which is closest to u is obviously u itself. A direct proof is also trivial: we may write $u = \sum_i \lambda_i u_i$ for some scalars λ_i (since the u_i span U), and now for all j,

$$\langle u_j, u\rangle = \sum_i \lambda_i \langle u_j, u_i\rangle = \lambda_j \langle u_j, u_j\rangle$$

whence the result.

(iii) This is follows easily from (ii) and is left as an exercise. □

5.11 THEOREM *If V is an inner product space (complex or real) then*
(i) $|\langle v, w\rangle| \leq \|v\|\,\|w\|$, *and*
(ii) $\|v + w\| \leq \|v\| + \|w\|$
for all v, $w \in V$.

Proof. (i) If $v = 0$ then both sides are zero. If $v \neq 0$ then v by itself forms an orthogonal basis for a 1-dimensional subspace of V, and by part (i) of 5.10 we have for all w,

$$\|w\|^2 \geq |\langle v, w\rangle|^2 / \|v\|^2$$

so that the result follows.

(ii) If $z = x + iy$ is any complex number then

$$z + \overline{z} = 2x \leq 2\sqrt{x^2 + y^2} = 2|z|.$$

Hence for all v, $w \in V$,

$$\begin{aligned}(\|v\| + \|w\|)^2 - \|v + w\|^2 &= (\langle v, v\rangle + \langle w, w\rangle + 2\|v\|\,\|w\|) - \langle v + w, v + w\rangle \\ &= (\langle v, v\rangle + \langle w, w\rangle + 2\|v\|\,\|w\|) - (\langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle) \\ &= 2\|v\|\,\|w\| - 2(\langle v, w\rangle + \overline{\langle v, w\rangle}) \\ &\geq 2\|v\|\,\|w\| - 2|\langle v, w\rangle|\end{aligned}$$

which is nonnegative by the first part. Hence $(\|v\| + \|w\|)^2 \geq \|v + w\|^2$, and the result follows. □

§5c Orthogonal and unitary transformations

As always in mathematics, we are particularly interested in functions which preserve the mathematical structure. Hence if V and W are inner product spaces it is of interest to investigate functions $T: V \to W$ which are linear and preserve the inner product, in the sense that $\langle T(u), T(v)\rangle = \langle u, v\rangle$ for all u, $v \in V$. Such a transformation is called an *orthogonal* transformation (for real inner product spaces) or a *unitary* transformation (in the complex case). It turns out that preservation of length is an equivalent condition; hence these transformations are sometimes called *isometries*.

5.12 PROPOSITION *If V and W are inner product spaces then a linear transformation $T: V \to W$ preserves inner products if and only if it preserves lengths.*

Proof. Since by definition the length of v is $\sqrt{\langle v, v\rangle}$ it is trivial that a transformation which preserves inner products preserves lengths. For the converse, we assume that $\|T(v)\| = \|v\|$ for all $v \in V$; we must prove that $\langle T(u), T(v)\rangle = \langle u, v\rangle$ for all u, $v \in V$.

Let u, $v \in V$. Note that (as in the proof of 5.11 above)

$$\|u + v\|^2 - \|u\|^2 - \|v\|^2 = \langle u, v\rangle + \overline{\langle u, v\rangle},$$

and similarly

$$\|T(u) + T(v)\|^2 - \|T(u)\|^2 - \|T(v)\|^2 = \langle T(u), T(v)\rangle + \overline{\langle T(u), T(v)\rangle},$$

so that the real parts of $\langle u, v\rangle$ and $\langle T(u), T(v)\rangle$ are equal. By exactly the same argument the real parts of $\langle iu, v\rangle$ and $\langle T(iu), T(v)\rangle$ are equal too. But writing $\langle u, v\rangle = x + iy$ with x, $y \in \mathbb{R}$ we see that

$$\langle iu, v\rangle = \bar{i}\langle u, v\rangle = (-i)\langle u, v\rangle = (-i)(x + iy) = y - ix$$

so that the real part of $\langle iu, v\rangle$ is the imaginary part of $\langle u, v\rangle$. Likewise, the real part of $\langle T(iu), T(v)\rangle = \langle iT(u), T(v)\rangle$ equals the imaginary part of $\langle T(u), T(v)\rangle$, and we conclude, as required, that $\langle u, v\rangle$ and $\langle T(u), T(v)\rangle$ have the same imaginary part as well as the same real part. □

We know from §3b#11 that if $T \in \mathrm{Mat}(n \times n, \mathbb{C})$ then the function $\phi: \mathbb{C}^n \to \mathbb{C}^n$ defined by $\phi(x) = Tx$ is linear, and, furthermore, it is easily shown (see Exercise 14 of Chapter Three) that every linear transformation from $\mathbb{C}^n$ to $\mathbb{C}^n$ has this form for some matrix T. Our next task is to describe those matrices T for which the corresponding linear transformation is an isometry. We need the following two definitions.

5.13 DEFINITION If A is a matrix with complex entries we define the *conjugate* of A to be the matrix $\overline{A}$ whose (i, j)-entry is the conjugate of the (i, j)-entry of A. The transpose of the conjugate of A will be denoted by 'A^*'.†

By Exercise 6 of Chapter Two we deduce that $(AB)^* = B^*A^*$ whenever AB is defined.

† Some people call A^* the *adjoint* of A, in conflict with the definition of "adjoint" given in Chapter 1.

5.14 DEFINITION An $n \times n$ complex matrix T is said to be *unitary* if $T^* = T^{-1}$. If T has real entries this becomes ${}^{\mathrm{t}}T = T^{-1}$, and T is said to be *orthogonal*.

5.15 PROPOSITION *Let $T \in \mathrm{Mat}(n \times n, \mathbb{C})$. The linear transformation $\phi\colon \mathbb{C}^n \to C^n$ defined by $\phi(x) = Tx$ is an isometry if and only if T is unitary.*

Proof. Suppose first that ϕ is an isometry, and let $(e_1, e_2, \ldots, e_n)$ be the standard basis of $\mathbb{C}^n$. Note that $e_i \cdot e_j = \delta_{ij}$. Since Te_i is the i^{th} column of T we see that $(Te_i)^*$ is the i^{th} row of T^*, and $(Te_i)^*(Te_j)$ is the (i,j)-entry of T^*T. However,

$$(Te_i)^*(Te_j) = Te_i \cdot Te_j = \phi(e_i) \cdot \phi(e_j) = e_i \cdot e_j = \delta_{ij}$$

since ϕ preserves the dot product, whence T^*T is the identity matrix. By 2.9 it follows that T is unitary.

Conversely, if T is unitary then $T^*T = I$, and for all u, $v \in \mathbb{C}^n$ we have

$$\phi(u) \cdot \phi(v) = Tu \cdot Tv = (Tu)^*(Tv) = u^*T^*Tv = u^*v = u \cdot v.$$

Thus ϕ preserves the dot product, and is therefore an isometry. □

Comment ▷▷▷

5.15.1 Since the (i,j)-entry of T^*T is the dot product of the i^{th} and j^{th} columns of T, we see that T is unitary if and only if the columns of T form an orthonormal basis of $\mathbb{C}^n$. Furthermore, the (i,j)-entry of TT^* is the conjugate of the dot product of the i^{th} and j^{th} rows of T; so it is also true that T is unitary if and only if its rows form an orthonormal basis of ${}^{\mathrm{t}}\mathbb{C}^n$.

5.15.2 Of course, corresponding things are true in the real case, where the complication due to complex conjugation is absent. Premultiplication by a real $n \times n$ matrix is an isometry of $\mathbb{R}^n$ if and only if the matrix is orthogonal; a real $n \times n$ matrix is orthogonal if and only if its columns form an orthonormal basis of $\mathbb{R}^n$; a real $n \times n$ matrix is orthogonal if and only if its rows form an orthonormal basis of ${}^{\mathrm{t}}\mathbb{R}^n$.

5.15.3 It is easy to prove, and we leave it as an exercise, that the product of two unitary matrices is unitary and the inverse of a unitary matrix is unitary. The same is true in the real case, of course, with the word 'orthogonal' replacing the word 'unitary'. ▷▷▷

—Examples—

#10 Find an orthogonal matrix P and an upper triangular matrix U such that

$$PU = \begin{pmatrix} 1 & 4 & 5 \\ 2 & 5 & 1 \\ 2 & 2 & 1 \end{pmatrix}.$$

≫⊳ Let the columns of P be $\underset{\sim}{v}_1$, $\underset{\sim}{v}_2$ and $\underset{\sim}{v}_3$, and let $U = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$. Then the columns of PU are $a\underset{\sim}{v}_1$, $b\underset{\sim}{v}_1 + d\underset{\sim}{v}_2$ and $c\underset{\sim}{v}_1 + e\underset{\sim}{v}_2 + f\underset{\sim}{v}_3$. Thus we wish to find a, b, c, d, e and f such that

$$a\underset{\sim}{v}_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \quad b\underset{\sim}{v}_1 + d\underset{\sim}{v}_2 = \begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix}, \quad c\underset{\sim}{v}_1 + e\underset{\sim}{v}_2 + f\underset{\sim}{v}_3 = \begin{pmatrix} 5 \\ 1 \\ 1 \end{pmatrix},$$

and $(\underset{\sim}{v}_1, \underset{\sim}{v}_2, \underset{\sim}{v}_3)$ is an orthonormal basis of $\mathbb{R}^3$. Now since we require $\|\underset{\sim}{v}_1\| = 1$, the first equation gives $a = 3$ and $\underset{\sim}{v}_1 = {}^{\mathrm{t}}(\,1/3 \quad 2/3 \quad 2/3\,)$. Taking the dot product of both sides of the second equation with $\underset{\sim}{v}_1$ now gives $b = 6$ (since we require $\underset{\sim}{v}_2 \cdot \underset{\sim}{v}_1 = 0$), and similarly taking the dot product of both sides of the third equation with $\underset{\sim}{v}_1$ gives $c = 3$. Substituting these values into the equations gives

$$d\underset{\sim}{v}_2 = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, \qquad e\underset{\sim}{v}_2 + f\underset{\sim}{v}_3 = \begin{pmatrix} 4 \\ -1 \\ -1 \end{pmatrix}.$$

The first of these equations gives $d = 3$ and $\underset{\sim}{v}_2 = {}^{\mathrm{t}}(\,2/3 \quad 1/3 \quad -2/3\,)$, and then taking the dot product of $\underset{\sim}{v}_2$ with the other equation gives $e = 3$. After substituting these values the remaining equation becomes

$$f\underset{\sim}{v}_3 = \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix},$$

and we see that $f = 3$ and $\underset{\sim}{v}_3 = {}^{\mathrm{t}}(\,2/3 \quad -2/3 \quad 1/3\,)$. Thus the only possible solution to the given problem is

$$P = \begin{pmatrix} 1/3 & 2/3 & 2/3 \\ 2/3 & 1/3 & -2/3 \\ 2/3 & -2/3 & 1/3 \end{pmatrix}, \qquad U = \begin{pmatrix} 3 & 6 & 3 \\ 0 & 3 & 3 \\ 0 & 0 & 3 \end{pmatrix}.$$

It is easily checked that ${}^{\mathrm{t}}PP = I$ and that PU has the correct value. (Note that the method we used to calculate the columns of P was essentially just the Gram-Schmidt process.) ⊲≪

#11 Let u_1, u_2 and u_3 be real numbers satisfying $u_1^2+u_2^2+u_3^2=1$, and let u be the 3×1 column with i^{th} entry u_i. Define

$$X=\begin{pmatrix} u_1^2 & u_1u_2 & u_1u_3\\ u_2u_1 & u_2^2 & u_2u_3\\ u_3u_1 & u_3u_2 & u_3^2\end{pmatrix},\qquad Y=\begin{pmatrix} 0 & u_3 & -u_2\\ -u_3 & 0 & u_1\\ u_2 & -u_1 & 0\end{pmatrix}.$$

Show that $X^2=X$ and $Y^2=I-X$, and $XY=YX=0$. Furthermore, show that for all θ, the matrix $R(u,\theta)=\cos\theta I+(1-\cos\theta)X+\sin\theta Y$ is orthogonal.

⋙▷ Observe that $X=u({}^{\mathrm{t}}u)$, and so

$$X^2=\big(u({}^{\mathrm{t}}u)\big)\big(u({}^{\mathrm{t}}u)\big)=u\big(({}^{\mathrm{t}}u)u\big)({}^{\mathrm{t}}u)=u(u\cdot u)({}^{\mathrm{t}}u)=X$$

since $u\cdot u=1$. By direct calculation we find that

$$Yu=\begin{pmatrix} 0 & u_3 & -u_2\\ -u_3 & 0 & u_1\\ u_2 & -u_1 & 0\end{pmatrix}\begin{pmatrix} u_1\\ u_2\\ u_3\end{pmatrix}=\begin{pmatrix} 0\\ 0\\ 0\end{pmatrix},$$

and hence $YX=Yu({}^{\mathrm{t}}u)=0$. Since ${}^{\mathrm{t}}X=X$ and ${}^{\mathrm{t}}Y=-Y$ it follows that $YX=-({}^{\mathrm{t}}Y)({}^{\mathrm{t}}X)=-{}^{\mathrm{t}}(XY)=-{}^{\mathrm{t}}0=0$. And an easy calculation yields

$$Y^2=\begin{pmatrix} u_2^2+u_3^2 & -u_1u_2 & -u_1u_3\\ -u_2u_1 & u_1^2+u_3^2 & -u_2u_3\\ -u_3u_1 & -u_3u_2 & u_1^2+u_2^2\end{pmatrix}=\begin{pmatrix} 1-u_1^2 & -u_1u_2 & -u_1u_3\\ -u_2u_1 & 1-u_2^2 & -u_2u_3\\ -u_3u_1 & -u_3u_2 & 1-u_3^2\end{pmatrix}=I-X.$$

To check that $R=R(u,\theta)$ is orthogonal we show that $({}^{\mathrm{t}}R)R=I$. Now

$${}^{\mathrm{t}}R=\cos\theta I+(1-\cos\theta)X-\sin\theta Y,$$

since ${}^{\mathrm{t}}X=X$ and ${}^{\mathrm{t}}Y=-Y$. So

$$\begin{aligned}({}^{\mathrm{t}}R)R&=\cos^2\theta I^2+(1-\cos\theta)^2X^2+\sin^2\theta Y^2\\ &\qquad+2\cos\theta(1-\cos\theta)IX+(1-\cos\theta)\sin\theta(XY-YX)\\ &=\cos^2\theta I+(1-\cos\theta)^2X+\sin^2\theta(I-X)+2\cos\theta(1-\cos\theta)X\\ &=(\cos^2\theta+\sin^2\theta)I+((1-\cos\theta)(1+\cos\theta)-\sin^2\theta)X\\ &=I\qquad\text{as required.}\end{aligned}$$

◁⋘

It can be shown that the matrix $R(u,\theta)$ defined in #11 above corresponds geometrically to a rotation through the angle θ about an axis in the direction of the vector u.

§5d Quadratic forms

When using Cartesian coordinates to investigate geometrical problems, it invariably simplifies matters if one can choose coordinate axes which are in some sense natural for the problem concerned. It therefore becomes important to be able keep track of what happens when a new coordinate system is chosen.

If $T \in \mathrm{Mat}(n \times n, \mathbb{R})$ is an orthogonal matrix then, as we have seen, the transformation ϕ defined by $\phi(\underset{\sim}{x}) = T\underset{\sim}{x}$ preserves lengths and angles. Hence if S is any set of points in $\mathbb{R}^n$ then the set $\phi(S) = \{\, T\underset{\sim}{x} \mid \underset{\sim}{x} \in S \,\}$ is congruent to S (in the sense of Euclidean geometry). Clearly such transformations will be important in geometrical situations. Observe now that if

$$T\underset{\sim}{x} = \mu_1 e_1 + \mu_2 e_2 + \cdots + \mu_n e_n$$

where $(e_1, e_2, \ldots, e_n)$ is the standard basis of $\mathbb{R}^n$, then

$$\underset{\sim}{x} = \mu_1(T^{-1}e_1) + \mu_2(T^{-1}e_2) + \cdots + \mu_n(T^{-1}e_n),$$

whence the coordinates of $T\underset{\sim}{x}$ relative to the standard basis are the same as the coordinates of $\underset{\sim}{x}$ relative to the basis $(T^{-1}e_1, T^{-1}e_2, \ldots, T^{-1}e_n)$. Note that these vectors are the columns of T^{-1}, and they form an orthonormal basis of $\mathbb{R}^n$ since T^{-1} is an orthogonal matrix. So choosing a new orthonormal basis is effectively the same as applying an orthogonal transformation, and doing so leaves all lengths and angles unchanged. We comment that in the three-dimensional case the only length preserving linear transformations are rotations and reflections.

A *quadratic form* over $\mathbb{R}$ in variables x_1, x_2, …, x_n is an expression of the form $\sum_i a_{ii}x_i^2 + 2\sum_{i<j} a_{ij}x_ix_j$ where the coefficients are real numbers. If A is the matrix with diagonal entries $A_{ii} = a_{ii}$ and off-diagonal entries $A_{ij} = A_{ji} = a_{ij}$ (for $i < j$) then the quadratic form can be written as $Q(\underset{\sim}{x}) = {}^{\mathrm{t}}\underset{\sim}{x}A\underset{\sim}{x}$, where x is the column with x_i as its i^{th} entry. For example, multiplying out

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a & p & q \\ p & b & r \\ q & r & c \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

gives $ax^2 + by^2 + cz^2 + 2pxy + 2qxz + 2ryz$.

In the above situation we call A the matrix of the quadratic form Q. Since $A_{ij} = A_{ji}$ for all i and j we have that A is a symmetric matrix, in the sense of the following definition.

5.16 DEFINITION A real $n \times n$ matrix A is said to be *symmetric* if ${}^tA = A$, and a complex $n \times n$ matrix A is said to be *Hermitian* if $A^* = A$.

The following remarkable facts concerning eigenvalues and eigenvectors of Hermitian matrices are very important, and not hard to prove.

5.17 THEOREM *Let A be an Hermitian matrix. Then*

(i) All eigenvalues of A are real, and

(ii) if λ and μ are two distinct eigenvalues of A, and if u and v are corresponding eigenvectors, then $u \cdot v = 0$

The proof is left as an exercise (although a hint is given). Of course the theorem applies to Hermitian matrices which happen to be real; that is, the same results hold for real symmetric matrices.

If f is an arbitrary smooth real valued function on $\mathbb{R}^n$, and if we choose a critical point of f as the origin of our coordinate system, then the terms of degree one in the Taylor series for f vanish. Ignoring the terms of degree three and higher then gives an approximation to f of the form $c + Q(\underset{\sim}{x})$, where $c = f(0)$ is a constant and Q is a quadratic form, the coefficients of the corresponding symmetric matrix being the second order partial derivatives of f at the critical point. We would now like to be able to rotate the axes so as to simplify the expression for $Q(\underset{\sim}{x})$ as much as possible, and hence determine the behaviour of f near the critical point.

From our discussion above we know that introducing a new coordinate system corresponding to an orthonormal basis of $\mathbb{R}^n$ amounts to introducing new variables $\underset{\sim}{x}'$ which are related to the old variables $\underset{\sim}{x}$ by $x = Tx'$, where T is the orthogonal matrix whose columns are the new basis vectors.† In terms of the new variables the quadratic form $Q(\underset{\sim}{x}) = {}^t\underset{\sim}{x}A\underset{\sim}{x}$ becomes

$$Q'(\underset{\sim}{x}') = {}^t(T\underset{\sim}{x}')A(T\underset{\sim}{x}') = {}^t\underset{\sim}{x}'({}^tTAT)\underset{\sim}{x}' = {}^t\underset{\sim}{x}'A'\underset{\sim}{x}'$$

where $A' = {}^tTAT$.

† The T in this paragraph corresponds to the T^{-1} above.

5.18 DEFINITION Two $n \times n$ real matrices A and A' are said to be *orthogonally similar* if there exists an orthogonal matrix T such that $A' = {}^tTAT$. Two $n \times n$ complex matrices A and A' are said to be unitarily similar if there exists a unitary matrix T such that $A' = T^*AT$.

Comment ▷▷▷
5.18.1 In both parts of the above definition we could alternatively have written $A' = T^{-1}AT$, since $T^{-1} = {}^tT$ in the real case and $T^{-1} = T^*$ in the complex case. ▷▷▷

We have shown that the change of coordinates corresponding to choosing a new orthonormal basis for $\mathbb{R}^n$ induces an orthogonal similarity transformation on the matrix of a quadratic form. The main theorem of this section says that it is always possible to diagonalize a symmetric matrix by an orthogonal similarity transformation. Unfortunately, we have to make use of the following fact, whose proof is beyond the scope of this book:

5.18.2 *Every square complex matrix has at least one complex eigenvalue.*

(In fact 5.18.2 is a trivial consequence of the "Fundamental Theorem of Algebra", which asserts that the field $\mathbb{C}$ is algebraically closed. See also §9c.)

5.19 THEOREM *(i) If A is an $n \times n$ real symmetric matrix then there exists an orthogonal matrix T such that ${}^tTAT$ is a diagonal matrix.*

(ii) If A is an $n \times n$ Hermitian matrix then there exists a unitary matrix U such that U^*AU is a real diagonal matrix.

Proof. We prove only part (i) since the proof of part (ii) is virtually identical. The proof is by induction on n. The case $n = 1$ is vacuously true, since every 1×1 matrix is diagonal.

Assume then that all $k \times k$ symmetric matrices over $\mathbb{R}$ are orthogonally similar to diagonal matrices, and let A be a $(k+1) \times (k+1)$ real symmetric matrix. By 5.18.2 we know that A has at least one complex eigenvalue λ, and by 5.17 we know that $\lambda \in \mathbb{R}$. Let $v \in \mathbb{R}^n$ be an eigenvector corresponding to the eigenvalue λ.

Since v constitutes a basis for a one-dimensional subspace of $\mathbb{R}^n$, we can apply the Gram-Schmidt process to find an orthogonal basis $(v_1, v_2, \ldots, v_n)$ of $\mathbb{R}^n$ with $v_1 = v$. Replacing each v_i by $\|v_i\|^{-1}v_i$ makes this into an orthonormal basis, with v_1 still a λ-eigenvector for A. Now define P to be the

(real) matrix which has v_i as its i^{th} column (for each i). By the comments in 5.15.1 above we see that P is orthogonal.

The first column of $P^{-1}AP$ is $P^{-1}Av$, since v is the first column of P, and since v is a λ-eigenvector of A this simplifies to $P^{-1}(\lambda v) = \lambda P^{-1}v$. But the same reasoning shows that $P^{-1}v$ is the first column of $P^{-1}P = I$, and so we deduce that the first entry of the first column of $P^{-1}AP$ is λ, all the other entries in the first column are zero. That is

$$P^{-1}AP = \begin{pmatrix} \lambda & \underset{\sim}{z} \\ \underset{\sim}{0} & B \end{pmatrix}$$

for some k-component row $\underset{\sim}{z}$ and some $k \times k$ matrix B, with $\underset{\sim}{0}$ being the k-component zero column.

Since P is orthogonal and A is symmetric we have that

$$P^{-1}AP = {}^{\mathrm{t}}P{}^{\mathrm{t}}AP = {}^{\mathrm{t}}({}^{\mathrm{t}}PAP) = {}^{\mathrm{t}}(P^{-1}AP),$$

so that $P^{-1}AP$ is symmetric. It follows that $z = 0$ and B is symmetric: we have

$$P^{-1}AP = \begin{pmatrix} \lambda & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & B \end{pmatrix}.$$

By the inductive hypothesis there exists a real orthogonal matrix Q such that $Q^{-1}BQ$ is diagonal. By multiplication of partitioned matrices we find that

$$\begin{aligned} \begin{pmatrix} 1 & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & Q \end{pmatrix}^{-1} \begin{pmatrix} \lambda & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & B \end{pmatrix} \begin{pmatrix} 1 & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & Q \end{pmatrix} &= \begin{pmatrix} 1 & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & Q^{-1} \end{pmatrix} \begin{pmatrix} \lambda & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & BQ \end{pmatrix} \\ &= \begin{pmatrix} \lambda & {}^{\mathrm{t}}\underset{\sim}{0} \\ \underset{\sim}{0} & Q^{-1}BQ \end{pmatrix} \end{aligned}$$

which is diagonal since $Q^{-1}BQ$ is. Thus $(PQ')^{-1}A(PQ')$ is diagonal, where $Q' = \begin{pmatrix} 1 & \underset{\sim}{0} \\ \underset{\sim}{0} & Q \end{pmatrix}$.

It remains to prove that PQ' is orthogonal. It is clear by multiplication of block matrices and the fact that $({}^{\mathrm{t}}Q)Q = I$ that $({}^{\mathrm{t}}Q')Q' = I$. Hence Q' is orthogonal, and since the product of two orthogonal matrices is orthogonal (see 5.15.3) it follows that PQ' is orthogonal too. □

Comments ▷▷▷

5.19.1 Given a $n \times n$ symmetric (or Hermitian) matrix the problem of finding an orthogonal (or unitary) matrix which diagonalizes it amounts to finding an orthonormal basis of $\mathbb{R}^n$ (or $\mathbb{C}^n$) consisting of eigenvectors of the matrix. To do this, proceed in the same way as for any matrix: find the characteristic equation and solve it. If there are n distinct eigenvalues then the eigenvectors are uniquely determined up to a scalar factor, and the theory above guarantees that they will be a right angles to each other. So if the eigenvectors you find for two different eigenvalues do not have the property that their dot product is zero, it means that you have made a mistake. If the characteristic equation has a repeated root λ then you will have to find more than one eigenvector corresponding to λ. In this case, when you solve the linear equations $(A-\lambda I)x = 0$ you will find that the number of arbitrary parameters in the general solution is equal to the multiplicity of λ as a root of the characteristic polynomial. You must find an orthonormal basis for this solution space (by using the Gram-Schmidt process, for instance).

5.19.2 Let A be a Hermitian matrix and let U be a Unitary matrix which diagonalizes A. It is clear from the above discussion that the diagonal entries of $U^{-1}AU$ are exactly the eigenvalues of A. Note also that $\det U^{-1}AU = \det U^{-1} \det A \det U = \det A$, and since the determinant of the diagonal matrix $U^{-1}AU$ is just the product of the diagonal entries we conclude that the determinant of A is just the product of its eigenvalues. (This can also be proved by observing that the determinant and the product of the eigenvalues are both equal to the constant term of the characteristic polynomial.) ▷▷▷

The quadratic form $Q(x) = {}^{\mathrm{t}}xAx$ and the symmetric matrix A are both said to be *positive definite* if $Q(x) > 0$ for all nonzero $x \in \mathbb{R}^n$. If A is positive definite and T is an invertible matrix then certainly ${}^{\mathrm{t}}(Tx)A(Tx) > 0$ for all nonzero $x \in \mathbb{R}^n$, and it follows that ${}^{\mathrm{t}}TAT$ is positive definite also. Note that ${}^{\mathrm{t}}TAT$ is also symmetric. The matrices A and ${}^{\mathrm{t}}TAT$ are said to be *congruent*. Obviously, symmetric matrices which are orthogonally similar are congruent; the reverse is not true. It is easily checked that a diagonal matrix is positive definite if and only if the diagonal entries are all positive. It follows that an arbitrary real symmetric matrix is positive definite if and only if all its eigenvalues are positive. The following proposition can be used as a test for positive definiteness.

5.20 Proposition *A real symmetric $n \times n$ matrix A is positive definite if*

and only if for all k from 1 to n the $k \times k$ matrix A_k with (i,j)-entry A_{ij} (obtained by deleting the last $n-k$ rows and columns of A) has positive determinant.

Proof. Assume that A is positive definite. Then the eigenvalues of A are all positive, and so the determinant, being the product of the eigenvalues, is positive also. Now if x is any nonzero k-component column and y the n-component column obtained from x by appending $n-k$ zeros then, since A is positive definite,

$$0 < {}^{\mathrm{t}}yAy = \begin{pmatrix} {}^{\mathrm{t}}x & 0 \end{pmatrix} \begin{pmatrix} A_k & * \\ * & * \end{pmatrix} \begin{pmatrix} x \\ 0 \end{pmatrix} = {}^{\mathrm{t}}xA_kx$$

and it follows that A_k is positive definite. Thus the determinant of each A_k is positive too.

We must prove, conversely, that if all the A_k have positive determinants then A is positive definite. We use induction on n, the case $n = 1$ being trivial. For the case $n > 1$ the inductive hypothesis gives that A_{n-1} is positive definite, and it immediately follows that the $n \times n$ matrix A' defined by

$$A' = \begin{pmatrix} A_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$$

is positive definite whenever λ is a positive number. Note that since the determinant of A_{n-1} is positive, λ is positive if and only if $\det A'$ is positive.

We now prove that A is congruent to A' for an appropriate choice of λ. We have

$$A = \begin{pmatrix} A_{n-1} & v \\ {}^{\mathrm{t}}v & \mu \end{pmatrix}$$

for some $(n-1)$-component column v and some real number μ. Defining $\lambda = \mu - {}^{\mathrm{t}}vA_{n-1}^{-1}v$ and

$$X = \begin{pmatrix} I_{n-1} & A_{n-1}^{-1}v \\ 0 & 1 \end{pmatrix}$$

an easy calculation gives ${}^{\mathrm{t}}XA'X = A$. Furthermore, we have that $\det X = 1$, and hence $\det A' = \det A > 0$. So A' is positive definite, and hence A is too. $\square$

Suppose that a surface in three dimensional Euclidean space is defined by an equation of the form $Q(x, y, z) = \text{constant}$, where Q is a quadratic form. We can find an orthogonal matrix to diagonalize the symmetric matrix associated with Q. It is easily seen that an orthogonal matrix necessarily has determinant either equal to 1 or -1, and by multiplying a column by -1 if necessary we can make sure that our diagonalizing matrix has determinant 1. Orthogonal transition matrices of determinant 1 correspond simply to rotations of the coordinate axes, and so we deduce that a suitable rotation transforms the equation of the surface to

$$\lambda(x')^2 + \mu(y')^2 + \nu(z')^2 = \text{constant}$$

where the coefficients λ, μ and ν are the eigenvalues of the matrix we started with. The nature of these surfaces depends on the signs of the coefficients, and the separate cases are easily enumerated.

Exercises

1. Prove that the dot product is an inner product on $\mathbb{R}^n$.

2. Prove that $\langle f, g\rangle = \int_a^b f(x)g(x)\,dx$ defines an inner product on $\mathcal{C}[a, b]$. Assume any theorems of calculus you need.

3. Define the distance between two elements v and w of an inner product space by $d(v, w) = \|v - w\|$. Prove that

(i) $d(v, w) = d(w, v)$,

(ii) $d(v, w) \geq 0$, with $d(v, w) = 0$ only if $v = w$,

(iii) $d(u, w) \leq d(u, v) + d(v, w)$,

(iv) $d(u + v, u + w) = d(v, w)$,

for all u, v, $w \in V$.

4. Prove that orthogonal projections are linear transformations.

5. Prove part (iii) of Proposition 5.10.

6. (i) Let V be a real inner product space and v, $w \in V$. Use calculus to prove that the minimum value of $\langle v - \lambda w, v - \lambda w\rangle$ occurs at $\lambda = \langle v, w\rangle / \langle w, w\rangle$.

(ii) Put $\lambda = \langle v, w\rangle / \langle w, w\rangle$ and use $\langle v - \lambda w, v - \lambda w\rangle \geq 0$ to prove the Cauchy-Schwarz inequality in any inner product space.

7. Prove that $(AB)^* = (B^*)(A^*)$ for all complex matrices A and B such that AB is defined. Hence prove that the product of two unitary matrices is unitary. Prove also that the inverse of a unitary matrix is unitary.

8. (*i*) Let A be a Hermitian matrix and λ an eigenvalue of A. Prove that λ is real.

(Hint: Let v be a nonzero column satisfying $Av = \lambda v$. Prove that $v^*A^* = \overline{\lambda}v^*$, and then calculate v^*Av in two different ways.)

(*ii*) Let λ and μ be two distinct eigenvalues of the Hermitian matrix A, and let u and v be corresponding eigenvectors. Prove that u and v are orthogonal to each other.

(Hint: Consider u^*Av.)

6

Relationships between spaces

In this chapter we return to the general theory of vector spaces over an arbitrary field. Our first task is to investigate isomorphism, the "sameness" of vector spaces. We then consider various ways of constructing spaces from others.

§6a Isomorphism

Let $V = \mathrm{Mat}(2 \times 2, \mathbb{R})$, the set of all 2×2 matrices over $\mathbb{R}$, and let $W = \mathbb{R}^4$, the set of all 4-component columns over $\mathbb{R}$. Then V and W are both vector spaces over $\mathbb{R}$, relative the usual addition and scalar multiplication for matrices and columns. Furthermore, there is an obvious one-to-one correspondence between V and W: the function f from V to W defined by

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

is bijective. It is clear also that f interacts in the best possible way with the addition and scalar multiplication functions corresponding to V and W: the column which corresponds to the sum of two given matrices A and B is the sum of the column corresponding to A and the column corresponding to B, and the column corresponding to a scalar multiple of A is the same scalar times the column corresponding to A. One might even like to say that V and W are really the same space; after all, whether one chooses to write four real numbers in a column or a rectangular array is surely a notational matter of no great substance. In fact we say that V and W are *isomorphic* vector spaces, and the function f is called an *isomorphism*. Intuitively, to say that V and W are isomorphic, is to say that, as vector spaces, they are the same.

The property of the one-to-one correspondence f which was written out in words in the last paragraph, becomes, when written symbolically,

$$f(A+B) = f(A) + f(B)$$
$$f(\lambda A) = \lambda f(A)$$

for all A, $B \in V$ and $\lambda \in \mathbb{R}$. That is, f is a linear transformation.

6.1 DEFINITION Let V and W be vector spaces over the same field F. A function $f: V \to W$ which is bijective and linear is called an *isomorphism* of vector spaces. If there is an isomorphism from V to W then V and W are said to be *isomorphic*, and we write $V \cong W$.

Comments ▷▷▷

6.1.1 Rephrasing the definition, an isomorphism is a one-to-one correspondence which preserves addition and scalar multiplication. Alternatively, an isomorphism is a linear transformation which is one-to-one and onto.

6.1.2 Every vector space is obviously isomorphic to itself: the identity function `i` (defined by $\mathtt{i}(x) = x$ for all x) is an isomorphism. This says that isomorphism is a reflexive relation.

6.1.3 Since isomorphisms are bijective functions they have inverses. We leave it as an exercise to prove that the inverse of an isomorphism is also an isomorphism. Thus if V is isomorphic to W then W is isomorphic to V; in other words, isomorphism is a symmetric relation.

6.1.4 If $f: U \to W$ and $g: V \to U$ are isomorphisms then the composite function $fg: V \to W$ is also an isomorphism. Thus if V is isomorphic to U and U is isomorphic to W then V is isomorphic to W—isomorphism is a transitive relation. This proof is also left as an exercise. ▷▷▷

The above comments show that isomorphism is an equivalence relation (see §1e), and it follows that vector spaces can be separated into mutually nonoverlapping classes—which are known as *isomorphism classes*—such that spaces in the same class are isomorphic to one another. Restricting attention to finitely generated vector spaces, the next proposition shows that (for a given field F) there is exactly one equivalence class for each nonnegative integer: there is, essentially, only one vector space of each dimension.

6.2 PROPOSITION *If U and V are finitely generated vector spaces over F of the same dimension d then they are isomorphic.*

Proof. Let $\boldsymbol{b}$ be a basis of V. We have seen (see 4.19.1 and 6.1.3) that $v \mapsto \mathrm{cv}_{\boldsymbol{b}}(v)$ defines a bijective linear transformation from F^d to V; that is, V and F^d are isomorphic. By the same argument, so are U and F^d. □

—Examples—

#1 Prove that the function f from $\mathrm{Mat}(2,\mathbb{R})$ to $\mathbb{R}^4$ defined at the start of this section is an isomorphism.

⋙▷ Let A, $B \in \mathrm{Mat}(2,\mathbb{R})$ and $\lambda \in \mathbb{R}$. Then

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad B = \begin{pmatrix} e & k \\ g & h \end{pmatrix}$$

for some a, b, …, $h \in \mathbb{R}$, and we find

$$f(A+B) = f\begin{pmatrix} a+e & b+k \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} a+e \\ b+k \\ c+g \\ d+h \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} + \begin{pmatrix} e \\ k \\ g \\ h \end{pmatrix}$$
$$= f\begin{pmatrix} a & b \\ c & d \end{pmatrix} + f\begin{pmatrix} e & k \\ g & h \end{pmatrix} = f(A) + f(B)$$

and

$$f(\lambda A) = f\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} = \begin{pmatrix} \lambda a \\ \lambda b \\ \lambda c \\ \lambda d \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \lambda f(A).$$

Hence f is a linear transformation.

Let $\underset{\sim}{v} \in \mathbb{R}^4$ be arbitrary. Then $\underset{\sim}{v} = \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$ for some x, y, z, $w \in \mathbb{R}$, and

$$f\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \underset{\sim}{v}.$$

Hence f is surjective.

Suppose that A, $B \in \mathrm{Mat}(2,\mathbb{R})$ are such that $f(A) = f(B)$. Writing $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & k \\ g & h \end{pmatrix}$ we have

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = f(A) = f(B) = \begin{pmatrix} e \\ k \\ g \\ h \end{pmatrix},$$

whence $a = e$, $b = k$, $c = g$ and $d = h$, showing that $A = B$. Thus f is injective. Since it is also surjective and linear, f is an isomorphism. ⊲⊢≪

#2 Let $\mathcal{P}$ be set of all polynomial functions from $\mathbb{R}$ to $\mathbb{R}$ of degree two or less, and let $\mathcal{F}$ be the set of all functions from the set $\{1,2,3\}$ to $\mathbb{R}$. Show that $\mathcal{P}$ and $\mathcal{F}$ are isomorphic vector spaces over $\mathbb{R}$.

≫⊢⊳ Observe that $\mathcal{P}$ is a subset of the set of all functions from $\mathbb{R}$ to $\mathbb{R}$, which we know to be a vector space over $\mathbb{R}$ (by §3b#6). A function $f\colon \mathbb{R} \to \mathbb{R}$ is in the subset $\mathcal{P}$ if and only if there exist a, b, $c \in \mathbb{R}$ such that $f(x) = ax^2 + bx + c$ for all $x \in \mathbb{R}$. Now let f, $g \in \mathcal{P}$ and $\lambda \in \mathbb{R}$ be arbitrary. We have

$$f(x) = ax^2 + bx + c, \qquad g(x) = a'x^2 + b'x + c'$$

for some a, a', b, b', c, $c' \in \mathbb{R}$. Now by the definitions of addition and scalar multiplication for functions we have for all $x \in \mathbb{R}$

$$\begin{aligned}(f+g)(x) &= f(x) + g(x) \\ &= (ax^2 + bx + c) + (a'x^2 + b'x + c') \\ &= (a + a')x^2 + (b + b') + (c + c')\end{aligned}$$

and similarly

$$\begin{aligned}(\lambda f)(x) &= \lambda\big(f(x)\big) \\ &= \lambda(ax^2 + bx + c) \\ &= (\lambda a)x^2 + (\lambda b)x + (\lambda c),\end{aligned}$$

so that $f + g$ and λf are both in $\mathcal{P}$. Hence $\mathcal{P}$ is closed under addition and scalar multiplication, and is therefore a subspace.

Since §3b#6 also gives that $\mathcal{F}$ is a vector space over $\mathbb{R}$, it remains to find an isomorphism $\phi\colon \mathcal{P} \to \mathcal{S}$. There are many ways to do this. One is as

follows: if $f \in \mathcal{P}$ let $\phi(f)$ be the restriction of f to $\{1, 2, 3\}$. That is, if $f \in \mathcal{P}$ then $\phi(f) \in \mathcal{F}$ is defined by

$$(\phi(f))(1) = f(1), \qquad (\phi(f))(2) = f(2), \qquad (\phi(f))(3) = f(3).$$

We prove first that ϕ as defined above is linear. Let $f, g \in \mathcal{P}$ and $\lambda, \mu \in \mathbb{R}$. Then for each $i \in \{1, 2, 3\}$ we have

$$\begin{aligned}\phi(\lambda f + \mu g)(i) &= (\lambda f + \mu g)(i) = (\lambda f)(i) + (\mu g)(i) = \lambda f(i) + \mu g(i) \\ &= \lambda\big(\phi(f)(i)\big) + \mu\big(\phi(g)(i)\big) = \big(\lambda\phi(f)\big)(i) + \big(\mu\phi(g)\big)(i) = \big(\lambda\phi(f) + \mu\phi(g)\big)(i),\end{aligned}$$

and so $\phi(\lambda f + \mu g) = \lambda\phi(f) + \mu\phi(g)$. Thus ϕ preserves addition and scalar multiplication.

To prove that ϕ is injective we must prove that if f and g are polynomials of degree at most two such that $\phi(f) = \phi(g)$ then $f = g$. The assumption that $\phi(f) = \phi(g)$ gives $f(i) = g(i)$, and hence $(f - g)(i) = 0$, for $i = 1, 2, 3$. Thus $x - 1$, $x - 2$ and $x - 3$ are all factors of $(f - g)(x)$, and so

$$(f - g)(x) = q(x)(x - 1)(x - 2)(x - 3)$$

for some polynomial q. Now since $f - g$ cannot have degree greater than two we see that the only possibility is $q = 0$, and it follows that $f = g$, as required.

Finally, we must prove that ϕ is surjective, and this involves showing that for every $\alpha\colon \{1, 2, 3\} \to \mathbb{R}$ there is a polynomial f of degree at most two with $f(i) = \alpha(i)$ for $i = 1, 2, 3$. In fact one can immediately write down a suitable f:

$$f(x) = \tfrac{1}{2}(x - 2)(x - 3)\alpha(1) - (x - 1)(x - 3)\alpha(2) + \tfrac{1}{2}(x - 1)(x - 2)\alpha(3).$$

(This formula is an instance of *Lagrange's interpolation formula*.) ⊲⊢≪

There is an alternative and possibly shorter proof using (instead of ϕ) an isomorphism which maps the polynomial $ax^2 + bx + c$ to $\alpha \in \mathcal{F}$ given by $\alpha(1) = a$, $\alpha(2) = b$ and $\alpha(3) = c$.

§6b Direct sums

Let F be a field, and consider the space F^6, consisting of all 6-component columns over F. The subset

$$S_1 = \left\{ \left(\begin{array}{c} \alpha \\ \beta \\ 0 \\ 0 \\ 0 \\ 0 \end{array} \right) \middle| \, \alpha, \beta \in F \right\}$$

is a subspace of F^6 isomorphic to F^2; the map which appends four zero components to the bottom of a 2-component column is an isomorphism from F^2 to S_1. Likewise,

$$S_2 = \left\{ \left(\begin{array}{c} 0 \\ 0 \\ \gamma \\ \delta \\ 0 \\ 0 \end{array} \right) \middle| \, \gamma, \delta \in F \right\} \quad \text{and} \quad S_3 = \left\{ \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ \varepsilon \\ \zeta \end{array} \right) \middle| \, \varepsilon, \zeta \in F \right\}$$

are also subspaces of F^6. It is easy to see that for an arbitrary $v \in F^6$ there exist uniquely determined v_1, v_2 and v_3 such that $v = v_1 + v_2 + v_3$ and $v_i \in S_i$; specifically, we have

$$\left(\begin{array}{c} \alpha \\ \beta \\ \gamma \\ \delta \\ \varepsilon \\ \zeta \end{array} \right) = \left(\begin{array}{c} \alpha \\ \beta \\ 0 \\ 0 \\ 0 \\ 0 \end{array} \right) + \left(\begin{array}{c} 0 \\ 0 \\ \gamma \\ \delta \\ 0 \\ 0 \end{array} \right) + \left(\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ \varepsilon \\ \zeta \end{array} \right).$$

We say that F^6 is the "direct sum" of its subspaces S_1, S_2 and S_3.

More generally, suppose that $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ is a basis for the vector space V, and suppose that we split $\boldsymbol{b}$ into k parts:

$$\begin{aligned} \boldsymbol{b}_1 &= (v_1, v_2, \ldots, v_{r_1}) \\ \boldsymbol{b}_2 &= (v_{r_1+1}, v_{r_1+2}, \ldots, v_{r_2}) \\ \boldsymbol{b}_3 &= (v_{r_2+1}, v_{r_2+2}, \ldots, v_{r_3}) \\ &\vdots \\ \boldsymbol{b}_k &= (v_{r_{k-1}+1}, v_{r_{k-1}+2}, \ldots, v_n) \end{aligned}$$

where the r_j are integers with $0 = r_0 < r_1 < r_2 < \cdots < r_{k-1} < r_k = n$. For each $j = 1, 2, \ldots, k$ let U_j be the subspace of V spanned by $\boldsymbol{b}_j$. It is not hard to see that $\boldsymbol{b}_j$ is a basis of U_j, for each j. Furthermore,

6.3 PROPOSITION *In the situation described above, for each $v \in V$ there exist uniquely determined $u_1, u_2, \ldots, u_k$ such that $v = u_1 + u_2 + \cdots + u_k$ and $u_j \in U_j$ for each j.*

Proof. Let $v \in V$. Since $\boldsymbol{b}$ spans V there exist scalars λ_i with

$$\begin{aligned} v &= \sum_{i=1}^{n} \lambda_i v_i \\ &= \sum_{i=1}^{r_1} \lambda_i v_i + \sum_{i=r_1+1}^{r_2} \lambda_i v_i + \cdots + \sum_{i=r_{k-1}+1}^{n} \lambda_i v_i. \end{aligned}$$

Defining for each j

$$u_j = \sum_{i=r_{j-1}}^{r_j} \lambda_i v_i$$

we see that $u_j \in \operatorname{Span} \boldsymbol{b}_j = U_j$ and $v = \sum_{j=1}^{k} u_j$, so that each v can be expressed in the required form.

To prove that the expression is unique we must show that if $u_j, u'_j \in U_j$ and $\sum_{j=1}^{k} u_j = \sum_{j=1}^{k} u'_j$ then $u_j = u'_j$ for each j. Since $U_j = \operatorname{Span} \boldsymbol{b}_j$ we may write (for each j)

$$u_j = \sum_{i=r_{j-1}+1}^{r_j} \lambda_i v_i \quad \text{and} \quad u'_j = \sum_{i=r_{j-1}+1}^{r_j} \lambda'_i v_i$$

for some scalars λ_i and λ'_i. Now we have

$$\begin{aligned} \sum_{i=1}^{n} \lambda_i v_i = \sum_{j=1}^{k} \sum_{i=r_{j-1}+1}^{r_j} \lambda_i v_i &= \sum_{j=1}^{k} u_j \\ = \sum_{j=1}^{k} u'_j = \sum_{j=1}^{k} \sum_{i=r_{j-1}+1}^{r_j} \lambda'_i v_i &= \sum_{i=1}^{n} \lambda'_i v_i \end{aligned}$$

and since $\boldsymbol{b}$ is a basis for V it follows from 4.15 that $\lambda_i = \lambda'_i$ for each i. Hence for each j,

$$u_j = \sum_{i=r_{j-1}+1}^{r_j} \lambda_i v_i = \sum_{i=r_{j-1}+1}^{r_j} \lambda'_i v_i = u'_j$$

as required. □

6.4 DEFINITION A vector space V is said to be the *direct sum* of subspaces $U_1, U_2, \ldots, U_k$ if every element of V is uniquely expressible in the form $u_1 + u_2 + \cdots + u_k$ with $u_j \in U_j$ for each j. To signify that V is the direct sum of the U_j we write

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_k.$$

Example

#3 Let $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ be a basis of V and for each i let U_i be the one-dimensional space spanned by v_i. Prove that $V = U_1 \oplus U_2 \oplus \cdots \oplus U_n$.

≫⟶ Let v be an arbitrary element of V. Since $\boldsymbol{b}$ spans V there exist $\lambda_i \in F$ such that $v = \sum_{i=1}^{n} \lambda_i v_i$. Now since $u_i = \lambda_i v_i$ is an element of U_i this shows that v can be expressed in the required form $\sum_{i=1}^{n} u_i$. It remains to prove that the expression is unique, and this follows directly from 4.15. For suppose that we also have $v = \sum_{i=1}^{n} u_i'$ with $u_i' \in U_i$. Letting $u_i' = \lambda_i' v_i$ we find that $v = \sum_{i=1}^{n} \lambda_i' v_i$, whence 4.15 gives $\lambda_i' = \lambda_i$, and it follows that $u_i' = u_i$, as required. ⟵≪

Observe that this corresponds to the particular case of 6.3 for which the parts into which the basis is split have one element each.

The case of two direct summands is the most important:

6.5 DEFINITION If $V = U_1 \oplus U_2$ then U_1 and U_2 are called *complementary subspaces.*

6.6 THEOREM *If U_1 and U_2 are subspaces of the vector space V then $V = U_1 \oplus U_2$ if and only if $V = U_1 + U_2$ and $U_1 \cap U_2 = \{0\}$.*

Proof. Recall that, by definition, $U_1 + U_2$ consists of all elements of V of the form $u_1 + u_2$ with $u_1 \in U_1$, $u_2 \in U_2$. (See Exercise 9 of Chapter Three.) Thus $V = U_1 + U_2$ if and only if each element of V is expressible as $u_1 + u_2$.

Assume that $V = U_1 + U_2$ and $U_1 \cap U_2 = \{0\}$. Then each element of V can be expressed in the form $u_1 + u_2$, and to show that $V = U_1 \oplus U_2$ it suffices to prove that these expressions are unique. So, assume that $u_1 + u_2 = u_1' + u_2'$

with u_i, $u_i' \in U_i$ for $i = 1, 2$. Then $u_1 - u_1' = u_2' - u_2$; let us call this element v. By closure properties for the subspace U_1 we have

$$v = u_1 - u_1' \in U_1 \qquad (\text{since } u_1,\, u_1' \in U_1),$$

and similarly closure of U_2 gives

$$v = u_2' - u_2 \in U_2 \qquad (\text{since } u_2,\, u_2 \in U_2).$$

Hence $v \in U_1 \cap U_2 = \{\underset{\sim}{0}\}$, and we have shown that

$$u_1 - u_1' = \underset{\sim}{0} = u_2' - u_2.$$

Thus $u_i = u_i'$ for each i, and uniqueness is proved.

Conversely, assume that $V = U_1 \oplus U_2$. Then certainly each element of V can be expressed as $u_1 + u_2$ with $u_i \in U_i$; so $V = U_1 + U_2$. It remains to prove that $U_1 \cap U_2 = \{\underset{\sim}{0}\}$. Subspaces always contain the zero vector; so $\{\underset{\sim}{0}\} \subseteq U_1 \cap U_2$. Now let $v \in U_1 \cap U_2$ be arbitrary. If we define

$$\begin{matrix} u_1 = \underset{\sim}{0} \\ u_2 = v \end{matrix} \qquad \text{and} \qquad \begin{matrix} u_1' = v \\ u_2' = \underset{\sim}{0} \end{matrix}$$

then we see that u_1, $u_1' \in U_1$ and u_2, $u_2' \in U_2$ and also $u_1 + u_2 = v = u_1' + u_2'$. Since each element of V is uniquely expressible as the sum of an element of U_1 and an element of U_2 this equation implies that $u_1 = u_1'$ and $u_2 = u_2'$; that is, $v = \underset{\sim}{0}$. □

The above theorem can be generalized to deal with the case of more than two direct summands. If $U_1, U_2, \ldots, U_k$ are subspaces of V it is natural to define their sum to be

$$U_1 + U_2 + \cdots + U_k = \{\, u_1 + u_2 + \cdots + u_k \mid u_i \in U_i \,\}$$

and it is easy to prove that this is always a subspace of V. One might hope that V is the direct sum of the U_i if the U_i generate V, in the sense that V is the sum of the U_i, and we also have that $U_i \cap U_j = \{0\}$ whenever $i \neq j$. However, consideration of #3 above shows that this condition will not be sufficient even in the case of one-dimensional summands, since to prove that $(v_1, v_2, \ldots, v_n)$ is a basis it is not sufficient to prove that v_i is not a scalar multiple of v_j for $i \neq j$. What we really need, then, is a generalization of the notion of linear independence.

6.7 DEFINITION The subspaces $U_1, U_2, \ldots, U_k$ of V are said to be *independent* if the only solution of

$$u_1 + u_2 + \cdots + u_k = \underset{\sim}{0}, \qquad u_i \in U_i \text{ for each } i$$

is given by $u_1 = u_2 = \cdots = u_k = \underset{\sim}{0}$.

We can now state the correct generalization of 6.6:

6.8 THEOREM *Let $U_1, \ldots, U_k$ be subspaces of the vector space V. Then $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ if and only if the U_i are independent and generate V.*

We omit the proof of this since it is a straightforward adaption of the proof of 6.6. Note in particular that the uniqueness part of the definition corresponds to the independence part of 6.8.

We have proved in 6.3 that a direct sum decomposition of a space is obtained by splitting a basis into parts, the summands being the subspaces spanned by the various parts. Conversely, given a direct sum decomposition of V one can obtain a basis of V by combining bases of the summands.

6.9 THEOREM *Let $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$, and for each $j = 1, 2, \ldots, k$ let $\boldsymbol{b}_j = (v_1^{(j)}, v_2^{(j)}, \ldots, v_{d_j}^{(j)})$ be a basis of the subspace U_j. Then*

$$\boldsymbol{b} = (v_1^{(1)}, \ldots, v_{d_1}^{(1)}, v_1^{(2)}, \ldots, v_{d_2}^{(2)}, \ldots \ldots \ldots, v_1^{(k)}, \ldots, v_{d_k}^{(k)})$$

is a basis of V and $\dim V = \sum_{j=1}^{k} \dim U_j$.

Proof. Let $v \in V$. Then $v = \sum_{j=1}^{k} u_j$ for some $u_j \in U_j$, and since $\boldsymbol{b}_j$ spans U_j we have $u_j = \sum_{i=1}^{d_j} \lambda_{ij} v_i^{(j)}$ for some scalars λ_{ij}. Thus

$$v = \sum_{i=1}^{d_1} \lambda_{i1} v_i^{(1)} + \sum_{i=1}^{d_2} \lambda_{i2} v_i^{(2)} + \cdots + \sum_{i=1}^{d_k} \lambda_{ik} v_i^{(k)},$$

a linear combination of the elements of $\boldsymbol{b}$. Hence $\boldsymbol{b}$ spans V.

Suppose we have an expression for $\underset{\sim}{0}$ as a linear combination of the elements of $\boldsymbol{b}$. That is, assume that

$$\underset{\sim}{0} = \sum_{i=1}^{d_1} \lambda_{i1} v_i^{(1)} + \sum_{i=1}^{d_2} \lambda_{i2} v_i^{(2)} + \cdots + \sum_{i=1}^{d_k} \lambda_{ik} v_i^{(k)}$$

for some scalars λ_{ij}. If we define $u_j = \sum_{i=1}^{d_j} \lambda_{ij} v_i^{(j)}$ for each j then we have $u_j \in U_j$ and

$$u_1 + u_2 + \cdots + u_k = \underset{\sim}{0}.$$

Since V is the direct sum of the U_j we know from 6.8 that the U_i are independent, and it follows that $u_j = \underset{\sim}{0}$ for each j. So $\sum_{i=1}^{d_j} \lambda_{ij} v_i^{(j)} = u_j = \underset{\sim}{0}$, and since $\boldsymbol{b}_j = (v_1^{(j)}, \ldots, v_{d_j}^{(j)})$ is linearly independent it follows that $\lambda_{ij} = 0$ for all i and j. We have shown that the only way to write $\underset{\sim}{0}$ as a linear combination of the elements of $\boldsymbol{b}$ is to make all the coefficients zero; thus $\boldsymbol{b}$ is linearly independent.

Since $\boldsymbol{b}$ is linearly independent and spans, it is a basis for V. The number of elements in $\boldsymbol{b}$ is $\sum_{j=1}^{k} d_j = \sum_{j=1}^{k} \dim U_j$; hence the statement about dimensions follows. □

As a corollary of the above we obtain:

6.10 Proposition *Any subspace of a finite dimensional space has a complement.*

Proof. Let U be a subspace of V and let d be the dimension of V. By 4.11 we know that U is finitely generated and has dimension less than d. Assume then that $(u_1, u_2, \ldots, u_r)$ is a basis for U. By 4.10 we may choose $w_1, w_2, \ldots, w_{d-r} \in V$ such that $(u_1, \ldots, u_r, w_1, \ldots, w_{d-r})$ is a basis of V. Now by 6.3 we have

$$V = \mathrm{Span}(u_1, \ldots, u_r) \oplus \mathrm{Span}(w_1, \ldots, w_{d-r}).$$

That is, $W = \mathrm{Span}(w_1, \ldots, w_{d-r})$ is a complement to U. □

§6c Quotient spaces

Let U be a subspace of the vector space V. If v is an arbitrary element of V we define the *coset* of U containing v to be the subset $v + U$ of V defined by

$$v + U = \{\, v + u \mid u \in U \,\}.$$

We have seen that subspaces arise naturally as solution sets of linear equations of the form $T(x) = 0$. Cosets arise naturally as solution sets of linear equations when the right hand side is nonzero.

6.11 PROPOSITION *Suppose that $T: V \to W$ is a linear transformation. Let $w \in W$ and let S be the set of solutions of the equation $T(x) = w$; that is, $S = \{\, x \in V \mid T(x) = w \,\}$. If $w \notin \operatorname{im} T$ then S is empty. If $w \in \operatorname{im} T$ then S is a coset of the kernel of T:*

$$S = x_0 + K$$

where x_0 is a particular solution of $T(x) = w$ and K is the set of all solutions of $T(x) = 0$.

Proof. By definition $\operatorname{im} T$ is the set of all $w \in W$ such that $w = T(x)$ for some $x \in V$; so if $w \notin \operatorname{im} T$ then S is certainly empty.

Suppose that $w \in \operatorname{im} T$ and let x_0 be any element of V such that $T(x_0) = w$. If $x \in S$ then $x - x_0 \in K$, since linearity of T gives

$$T(x - x_0) = T(x) - T(x_0) = w - w = 0,$$

and it follows that

$$x = x_0 + (x - x_0) \in x_0 + K.$$

Thus $S \subseteq x_0 + K$. Conversely, if x is an element of $x_0 + K$ then we have $x = x_0 + v$ with $v \in K$, and now

$$T(x) = T(x_0 + v) = T(x_0) + T(v) = w + 0 = w$$

shows that $x \in S$. Hence $x_0 + K \subseteq S$, and therefore $x_0 + K = S$. □

Cosets can also be described as equivalence classes, in the following way. Given that U is a subspace of V, define a relation $\equiv$ on V by

$(*)$ $$x \equiv y \text{ if and only if } x - y \in U.$$

It is straightforward to check that $\equiv$ is reflexive, symmetric and transitive, and that the resulting equivalence classes are precisely the cosets of U.

The set of all cosets of U in V can be made into a vector space in a manner totally analogous to that used in Chapter Two to construct a field with three elements. It is easily checked that if $x + U$ and $y + U$ are cosets of U then the sum of any element of $x + U$ and any element of $y + U$ will lie in the coset $(x + y) + U$. Thus it is natural to define addition of cosets by the rule

6.11.1 $$(x + U) + (y + U) = (x + y) + U.$$

Similarly, if λ is a scalar and $x+U$ a coset then multiplying any element of $x+U$ by λ gives an element of $(\lambda x)+U$, and so we define

6.11.2 $$\lambda(x+U) = (\lambda x)+U.$$

It is routine to check that addition and scalar multiplication of cosets as defined above satisfy the vector space axioms. (Note in particular that the coset $0+U$, which is just U itself, plays the role of zero.)

6.12 THEOREM *Let U be a subspace of the vector space V and let V/U be the set of all cosets of U in V. Then V/U is a vector space over F relative to the addition and scalar multiplication defined in 6.11.1 and 6.11.2 above.*

Comments ▷▷▷

6.12.1 The vector space defined above is called the *quotient* of V by U. Note that it is precisely the quotient, as defined in §1e, of V by the equivalence relation $\equiv$ (see $(*)$ above).

6.12.2 Note that it is possible to have $x+U = x'+U$ and $y+U = y'+U$ without having $x = x'$ or $y = y'$. However, it is necessarily true in these circumstances that $(x+y)+U = (x'+y')+U$, so that addition of cosets is well-defined. A similar remark is valid for scalar multiplication. ▷▷▷

The quotient space V/U can be thought of as the space obtained from V by identifying things which differ by an element of U, or, equivalently, pretending that all the elements of U are zero. Thus it is reasonable to regard V as being in some sense made up of U and V/U. The next proposition reinforces this idea.

6.13 PROPOSITION *Let U be a subspace of V and let W be any complement to U. Then W is isomorphic to V/U.*

Proof. Define $T\colon W \to V/U$ by $T(w) = w+U$. We will prove that T is linear and bijective.

By the definitions of addition and scalar multiplication of cosets we have

$$T(\lambda x+\mu y) = (\lambda x+\mu y)+U = \lambda(x+U)+\mu(y+U) = \lambda T(x)+\mu T(y)$$

for all x, $y \in W$ and all λ, $\mu \in F$. Hence T is linear.

Let $w \in \ker T$. Then $T(w) = w + U$ is the zero element of V/U; that is, $w + U = U$. Since $w = w + 0 \in w + U$ it follows that $w \in U$, and hence that $w \in U \cap W$. But W and U are complementary, and so it follows from 6.6 that $U \cap W = \{0\}$, and we deduce that $w = 0$. So $\ker T = \{0\}$, and therefore (by 3.15) T is injective.

Finally, an arbitrary element of V/U has the form $v + U$ for some $v \in V$, and since V is the sum of U and W there exist $u \in U$ and $w \in W$ with $v = w + u$. We see from this that $v \equiv w$ in the sense of $(*)$ above, and hence

$$v + U = w + U = T(w) \in \operatorname{im} T.$$

Since $v + U$ was an arbitrary element of V/U this shows that T is surjective. □

Comment ▷▷▷

6.13.1 In the situation of 6.13 suppose that $(u_1, \ldots, u_r)$ is a basis for U and $(w_1, \ldots, w_s)$ a basis for W. Since $w \mapsto w + U$ is an isomorphism $W \to V/U$ we must have that the elements $w_1 + U$, …, $w_s + U$ form a basis for V/U. This can also be seen directly. For instance, to see that they span observe that since each element v of $V = W \oplus U$ is expressible in the form

$$v = \sum_{j=1}^{s} \mu_j w_j + \sum_{i=1}^{r} \lambda_i u_i,$$

it follows that

$$v + U = \left(\sum_{j=1}^{s} \mu_j w_j \right) + U = \sum_{j=1}^{s} \mu_j (w_j + U).$$

▷▷▷

§6d The dual space

Let V and W be vector spaces over F. It is easily checked, by arguments almost identical to those used in §3b#6, that the set of all functions from V to W becomes a vector space if addition and scalar multiplication are defined in the natural way. We have also seen in Exercise 11 of Chapter Three that the sum of two linear transformations from V to W is also a linear transformation from V to W, and the product of a linear transformation by a scalar also gives a linear transformation. The set $\mathrm{L}(V, W)$ of all linear transformations from V to W is nonempty (the zero function is linear) and so it follows from 3.10 that $\mathrm{L}(V, W)$ is a vector space. The special case $W = F$ is of particular importance.

6.14 DEFINITION Let V be a vector space over F. The space of all linear transformations from V to F is called the *dual space* of V, and it is commonly denoted 'V^*'.

Comment ▷▷▷
6.14.1 In another strange tradition, elements of the dual space are commonly called *linear functionals*. ▷▷▷

6.15 THEOREM *Let $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ be a basis for the vector space V. For each $i = 1, 2, \ldots, n$ there exists a unique linear functional f_i such that $f_i(v_j) = \delta_{ij}$ (Kronecker delta) for all j. Furthermore, $(f_1, f_2, \ldots, f_n)$ is a basis of V^*.*

Proof. Existence and uniqueness of the f_i is immediate from 4.16. If $\sum_{i=1}^n \lambda_i f_i$ is the zero function then for all j we have

$$0 = \left(\sum_{i=1}^n \lambda_i f_i\right)(v_j) = \sum_{i=1}^n \lambda_i f_i(v_j) = \sum_{i=1}^n \lambda_i \delta_{ij} = \lambda_j$$

and so it follows that the f_i are linearly independent. It remains to show that they span.

Let $f \in V^*$ be arbitrary, and for each i define $\lambda_i = f(v_i)$. We will show that $f = \sum_{i=1}^n \lambda_i f_i$. By 4.16 it suffices to show that f and $\sum_{i=1}^n \lambda_i f_i$ take the same value on all elements of the basis $\boldsymbol{b}$. This is indeed satisfied, since

$$\left(\sum_{i=1}^n \lambda_i f_i\right)(v_j) = \sum_{i=1}^n \lambda_i f_i(v_j) = \sum_{i=1}^n \lambda_i \delta_{ij} = \lambda_j = f(v_j).$$

□

Comment ▷▷▷
6.15.1 The basis of V^* described in the theorem is called the *dual basis* of V^* corresponding to the basis $\boldsymbol{b}$ of V. ▷▷▷

To accord with the normal use of the word 'dual' it ought to be true that the dual of the dual space is the space itself. This cannot strictly be satisfied: elements of $(V^*)^*$ are linear functionals on the space V^*, whereas elements of V need not be functions at all. Our final result in this chapter shows that, nevertheless, there is a natural isomorphism between V and $(V^*)^*$.

6.16 THEOREM *Let V be a finite dimensional vector space over the field F. For each $v \in V$ define $e_v : V^* \to F$ by*

$$e_v(f) = f(v) \qquad \text{for all } f \in V^*.$$

Then e_v is an element of $(V^*)^*$, and furthermore the mapping $V \to (V^*)^*$ defined by $v \mapsto e_v$ is an isomorphism.

We omit the proof. All parts are in fact easy, except for the proof that $v \mapsto e_v$ is surjective, which requires the use of a dimension argument. This will also be easy once we have proved the Main Theorem on Linear Transformations, which we will do in the next chapter. It is important to note, however, that Theorem 6.16 becomes false if the assumption of finite dimensionality is omitted.

Exercises

1. Prove that isomorphic spaces have the same dimension.

2. Let U and V be finite dimensional vector spaces over the field F and let $f : U \to V$ be a linear transformation which is injective. Prove that U is isomorphic to a subspace of V, and hence prove that $\dim U \leq \dim V$.

3. Prove that the inverse of a vector space isomorphism is a vector space isomorphism, and that the composite of two vector space isomorphisms is a vector space isomorphism.

4. In each case determine (giving reasons) whether the given linear transformation is a vector space isomorphism. If it is, give a formula for its inverse.

(*i*) $\rho : \mathbb{R}^2 \to \mathbb{R}^3$ defined by $\rho \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

(*ii*) $\sigma : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $\sigma \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$

5. Let $\phi: V \to V$ be a linear transformation such that $\phi^2 = \phi$. (Note that multiplication of linear transformations is always defined to be composition; thus $\phi^2(v) = \phi\big(\phi(v)\big)$. Let $\mathtt{i}$ denote the identity transformation $V \to V$; that is, $\mathtt{i}(v) = v$ for all $v \in V$.

(*i*) Prove that $\mathtt{i} - \phi: V \to V$ (defined by $(\mathtt{i} - \phi)(v) = v - \phi(v)$) satisfies

$$(\mathtt{i} - \phi)^2 = \mathtt{i} - \phi.$$

(*ii*) Prove that $\operatorname{im}\phi = \ker(\mathtt{i} - \phi)$ and $\ker\phi = \operatorname{im}(id - \phi)$.

(*iii*) Prove that for each element $v \in V$ there exist unique $x \in \operatorname{im}\phi$ and $y \in \ker\phi$ with $v = x + y$.

6. Let W be the space of all twice differentiable functions $f: \mathbb{R} \to \mathbb{R}$ satisfying $d^2f/dt^2 = 0$. For all $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{R}^2$ let $\phi\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ be the function from $\mathbb{R}$ to $\mathbb{R}$ given by

$$\phi\begin{pmatrix}\alpha\\ \beta\end{pmatrix}(t) = \alpha t + (\beta - \alpha).$$

Prove that $\phi(v) \in W$ for all $v \in \mathbb{R}^2$, and that $\phi: v \mapsto \phi(v)$ is an isomorphism from $\mathbb{R}^2$ to W. Give a formula for the inverse isomorphism ϕ^{-1}.

7. Let V be a vector space and S and T subspaces of V such that $V = S \oplus T$. Prove or disprove the following assertion:

If U is any subspace of V then $U = (U \cap S) \oplus (U \cap T)$.

8. Express $\mathbb{R}^2$ as the sum of two one dimensional subspaces in two different ways.

9. Is it possible to find subspaces U, V and W of $\mathbb{R}^4$ such that

$$\mathbb{R}^4 = U \oplus V = V \oplus W = W \oplus U\,?$$

10. Let $U_1, U_2, \ldots, U_k$ be subspaces of V. Prove that the U_i are independent if and only if each element of $U_1 + U_2 + \cdots + U_k$ (the subspace generated by the U_i) is uniquely expressible in the form $\sum_{i=1}^{k} u_i$ with $u_i \in U_i$ for each i.

11. Let $U_1, U_2, \ldots, U_k$ be subspaces of V. Prove that the U_i are independent if and only if

$$U_j \cap (U_1 + \cdots + U_{j-1} + U_{j+1} + \cdots + U_k) = \{0\}$$

for all $j = 1, 2, \ldots, k$.

12. (*i*) Let V be a vector space over F and let $v \in V$. Prove that the function $e_v: V^* \to F$ defined by $e_v(f) = f(v)$ (for all $f \in V^*$) is linear.

(*ii*) With e_v as defined above, prove that the function $e: V \to (V^*)^*$ defined by

$$e(v) = e_v \quad \text{for all } v \text{ in } V$$

is a linear transformation.

(*iii*) Prove that the function e defined above is injective.

13. (*i*) Let V and W be vector spaces over F. Show that the Cartesian product of V and W becomes a vector space if addition and scalar multiplication are defined in the natural way. (This space is called the *external direct sum* of V and W, and is sometimes denoted by '$V \dotplus W$'.)

(*ii*) Show that $V' = \{\,(v, 0) \mid v \in V\,\}$ and $W' = \{\,(0, w) \mid w \in W\,\}$ are subspaces of $V \dotplus W$ with $V' \cong V$ and $W' \cong W$, and that $V \dotplus W = V' \oplus W'$.

(*iii*) Prove that $\dim(V \dotplus W) = \dim V + \dim W$.

14. Let S and T be subspaces of a vector space V. Prove that $(s, t) \mapsto s + t$ defines a linear transformation from $S \dotplus T$ to V which has image $S + T$.

15. Suppose that V is the direct sum of subspaces V_i (for $i = 1, 2, \ldots, n$) and each V_i is the direct sum of subspaces V_{ij} (for $j = 1, 2, \ldots, m_i$). Prove that V is the direct sum of all the subspaces V_{ij}.

16. Let V be a real inner product space, and for all $w \in V$ define $f_w: V \to \mathbb{R}$ by $f_w(v) = \langle v, w \rangle$ for all $v \in V$.

(*i*) Prove that for each element $w \in V$ the function $f_w: V \to \mathbb{R}$ is linear.

(*ii*) By (*i*) each f_w is an element of the dual space V^* of V. Prove that $f: V \to V^*$ defined by $f(w) = f_w$ is a linear transformation.

(*iii*) By considering $f_w(w)$ prove that $f_w = 0$ only if $w = 0$. Hence prove that the kernel of the linear transformation f in (*ii*) is $\{0\}$.

(*iv*) Assume that V is finite dimensional. Use Exercise 2 above and the fact that V and V^* have the same dimension to prove that the linear transformation f in (*ii*) is an isomorphism.

7

Matrices and Linear Transformations

We have seen in Chapter Four that an arbitrary finite dimensional vector space is isomorphic to a space of n-tuples. Since an n-tuple of numbers is (in the context of pure mathematics!) a fairly concrete sort of thing, it is useful to use these isomorphisms to translate questions about abstract vector spaces into questions about n-tuples. And since we introduced vector spaces to provide a context in which to discuss linear transformations, our first task is, surely, to investigate how this passage from abstract spaces to n-tuples interacts with linear transformations. For instance, is there some concrete thing, like an n-tuple, which can be associated with a linear transformation?

§7a The matrix of a linear transformation

We have shown in 4.16 that the action of a linear transformation on a basis of a space determines it uniquely. Suppose then that $T\colon V \to W$ is a linear transformation, and let $\boldsymbol{b} = (v_1, \dots, v_n)$ be a basis for the space V and $\boldsymbol{c} = (w_1, \dots, w_m)$ a basis for W. If we know expressions for each Tv_i in terms of the w_j then for any scalars λ_i we can calculate $T\left(\sum_{i=1}^n \lambda_i v_i\right)$ in terms of the w_j. Thus there should be a formula expressing $\mathrm{cv}_{\boldsymbol{c}}(Tv)$ (for any $v \in V$) in terms of the $\mathrm{cv}_{\boldsymbol{c}}(Tv_i)$ and $\mathrm{cv}_{\boldsymbol{b}}(v)$.

7.1 Theorem *Let V and W be vector spaces over the field F with bases $\boldsymbol{b} = (v_1, v_2, \dots, v_n)$ and $\boldsymbol{c} = (w_1, w_2, \dots, w_m)$, and let $T\colon V \to W$ be a linear transformation. Define $\mathrm{M}_{\boldsymbol{cb}}(T)$ to be the $m \times n$ matrix whose i^{th} column is $\mathrm{cv}_{\boldsymbol{c}}(Tv_i)$. Then for all $v \in V$,*

$$\mathrm{cv}_{\boldsymbol{c}}(Tv) = \mathrm{M}_{\boldsymbol{cb}}(T)\,\mathrm{cv}_{\boldsymbol{b}}(v).$$

Proof. Let $v \in V$ and let $v = \sum_{i=1}^n \lambda_i v_i$, so that $\mathrm{cv}_{\boldsymbol{b}}(v)$ is the column with λ_i as its i^{th} entry. For each v_j in the basis $\boldsymbol{b}$ let $T(v_j) = \sum_{i=1}^m \alpha_{ij} w_i$. Then

α_{ij} is the i^{th} entry of the column $\mathrm{cv}_{\boldsymbol{c}}(Tv_j)$, and by the definition of $\mathrm{M}_{\boldsymbol{cb}}(T)$ this gives

$$\mathrm{M}_{\boldsymbol{cb}}(T) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}.$$

We obtain

$$\begin{aligned} Tv &= T(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n) \\ &= \lambda_1 Tv_1 + \lambda_2 Tv_2 + \cdots + \lambda_n Tv_n \\ &= \lambda_1 \left(\sum_{i=1}^{m} \alpha_{i1} w_i \right) + \lambda_2 \left(\sum_{i=1}^{m} \alpha_{i2} w_i \right) + \cdots + \lambda_n \left(\sum_{i=1}^{m} \alpha_{in} w_i \right) \\ &= \sum_{i=1}^{m} (\alpha_{i1}\lambda_1 + \alpha_{i2}\lambda_2 + \cdots + \alpha_{in}\lambda_n) w_i, \end{aligned}$$

and since the coefficient of w_i in this expression is the i^{th} entry of $\mathrm{cv}_{\boldsymbol{c}}(Tv)$ it follows that

$$\begin{aligned} \mathrm{cv}_{\boldsymbol{c}}(Tv) &= \begin{pmatrix} \alpha_{11}\lambda_1 + \alpha_{12}\lambda_2 + \cdots + \alpha_{1n}\lambda_n \\ \alpha_{21}\lambda_1 + \alpha_{22}\lambda_2 + \cdots + \alpha_{2n}\lambda_n \\ \vdots \\ \alpha_{m1}\lambda_1 + \alpha_{m2}\lambda_2 + \cdots + \alpha_{mn}\lambda_n \end{pmatrix} \\ &= \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \\ &= \mathrm{M}_{\boldsymbol{cb}}(T)\, \mathrm{cv}_{\boldsymbol{b}}(v). \end{aligned}$$

□

Comments ▷▷▷

7.1.1 The matrix $\mathrm{M}_{\boldsymbol{cb}}(T)$ is called *the matrix of T relative to the bases $\boldsymbol{c}$ and $\boldsymbol{b}$*. The theorem says that in terms of coordinates relative to bases $\boldsymbol{c}$ and $\boldsymbol{b}$ the effect of a linear transformation T is multiplication by the matrix of T relative to these bases.

7.1.2 The matrix of a transformation from an m-dimensional space to an n-dimensional space is an $n \times m$ matrix. (One column for each element of the basis of the domain.) ▷▷▷

—Examples—

#1 Let V be the space considered in §4e#3, consisting of all polynomials over $\mathbb{R}$ of degree at most three, and define a transformation $D\colon V \to V$ by $(Df)(x) = \frac{d}{dx}f(x)$. That is, Df is the derivative of f. Since the derivative of a polynomial of degree at most three is a polynomial of degree at most two, it is certainly true that $Df \in V$ if $f \in V$, and hence D is a well-defined transformation from V to V. Moreover, elementary calculus gives

$$D(\lambda f + \mu g) = \lambda(Df) + \mu(Dg)$$

for all f, $g \in V$ and all λ, $\mu \in \mathbb{R}$; hence D is a linear transformation. Now, if $\boldsymbol{b} = (p_0, p_1, p_2, p_3)$ is the basis defined in §4e#3, we have

$$Dp_0 = 0, \quad Dp_1 = p_0, \quad Dp_2 = 2p_1, \quad Dp_3 = 3p_2,$$

and therefore

$$\mathrm{cv}_{\boldsymbol{b}}(Dp_0) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathrm{cv}_{\boldsymbol{b}}(Dp_1) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

$$\mathrm{cv}_{\boldsymbol{b}}(Dp_2) = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \qquad \mathrm{cv}_{\boldsymbol{b}}(Dp_3) = \begin{pmatrix} 0 \\ 0 \\ 3 \\ 0 \end{pmatrix}.$$

Thus the matrix of D relative to $\boldsymbol{b}$ and $\boldsymbol{b}$ is

$$\mathrm{M}_{\boldsymbol{b}\boldsymbol{b}}(D) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

(Note that the domain and codomain are equal in this example; so we may use the same basis for each. We could have, if we had wished, used a basis for V considered as the codomain of D different from the basis used for V considered as the domain of D. Of course, this would result in a different matrix.)

By linearity of D we have, for all $a_i \in \mathbb{R}$,

$$\begin{aligned} D(a_0p_0 + a_1p_1 + a_2p_2 + a_3p_3) &= a_0Dp_0 + a_1Dp_1 + a_2Dp_2 + a_3Dp_3 \\ &= a_1p_0 + 2a_2p_1 + 3a_3p_2. \end{aligned}$$

so that if $\mathrm{cv}_{\boldsymbol{c}}(p) = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$ then $\mathrm{cv}_{\boldsymbol{b}}(Dp) = \begin{pmatrix} a_1 \\ 2a_2 \\ 3a_3 \\ 0 \end{pmatrix}$. To verify the assertion of the theorem in this case it remains to observe that

$$\begin{pmatrix} a_1 \\ 2a_2 \\ 3a_3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

#2 Let $\boldsymbol{b} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$, a basis of $\mathbb{R}^3$, and let $\boldsymbol{s}$ be the standard basis of $\mathbb{R}^3$. Let $\mathtt{i}\colon \mathbb{R}^3 \to \mathbb{R}^3$ be the identity transformation, defined by $\mathtt{i}(v) = v$ for all $v \in \mathbb{R}^3$. Calculate $\mathrm{M}_{\boldsymbol{sb}}(\mathtt{i})$ and $\mathrm{M}_{\boldsymbol{bs}}(\mathtt{i})$. Calculate also the coordinate vector of $\begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix}$ relative to $\boldsymbol{b}$.

⋙▷ We proved in §4e#2 that $\boldsymbol{b}$ is a basis. The i^{th} column of $\mathrm{M}_{\boldsymbol{sb}}(\mathtt{i})$ is the coordinate vector $\mathrm{cv}_{\boldsymbol{s}}(\mathtt{i}(v_i))$, where $\boldsymbol{b} = (v_1, v_2, v_3)$. But, by 4.19.2 and the definition of $\mathtt{i}$,

$$\mathrm{cv}_{\boldsymbol{s}}(\mathtt{i}(v)) = \mathrm{cv}_{\boldsymbol{s}}(v) = v \qquad (\text{for all } v \in \mathbb{R}^3)$$

and it follows that

$$\mathrm{M}_{\boldsymbol{sb}}(\mathtt{i}) = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The i^{th} column of $\mathrm{M}_{\boldsymbol{bs}}(\mathtt{i})$ is $\mathrm{cv}_{\boldsymbol{b}}(\mathtt{i}(e_i)) = \mathrm{cv}_{\boldsymbol{b}}(e_i)$, where e_1, e_2 and e_3 are the vectors of $\boldsymbol{s}$. Hence we must solve the equations

$$(*) \qquad \begin{aligned} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} &= x_{11} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_{21} \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + x_{31} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} &= x_{12} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_{22} \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + x_{32} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} &= x_{13} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_{23} \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + x_{33} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}. \end{aligned}$$

The solution $\begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix}$ of the first of these equations gives the first column of $\mathrm{M}_{\boldsymbol{bs}}(\mathtt{i})$, the solution of the second equation gives the second column, and likewise for the third. In matrix notation the equations can be rewritten as

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{21} \\ x_{31} \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{12} \\ x_{22} \\ x_{32} \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{13} \\ x_{23} \\ x_{33} \end{pmatrix},$$

or, more succinctly still,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix}$$

in which the matrix (x_{ij}) is $\mathrm{M}_{\boldsymbol{bs}}(\mathtt{i})$. Thus

$$\mathrm{M}_{\boldsymbol{bs}}(\mathtt{i}) = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{pmatrix}$$

as calculated in §4e#2. (This is an instance of the general fact that if $T\colon V \to W$ is a vector space isomorphism and $\boldsymbol{b}$, $\boldsymbol{c}$ are bases for V, W then $\mathrm{M}_{\boldsymbol{bc}}(T^{-1}) = \mathrm{M}_{\boldsymbol{cb}}(T)^{-1}$. The present example is slightly degenerate since $\mathtt{i}^{-1} = \mathtt{i}$. Note also that if we had not already proved that $\boldsymbol{b}$ is a basis, the fact that the equations $(*)$ have a solution proves it. For, once the e_i have been expressed as linear combinations of $\boldsymbol{b}$ it is immediate that $\boldsymbol{b}$ spans $\mathbb{R}^3$, and since $\mathbb{R}^3$ has dimension three it then follows from 4.12 that $\boldsymbol{b}$ is a basis.)

Finally, with $v = \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix}$, 7.1 yields that

$$\mathrm{cv}_{\boldsymbol{b}}(v) = \mathrm{cv}_{\boldsymbol{b}}\big(\mathtt{i}(v)\big) = \mathrm{M}_{\boldsymbol{bs}}(\mathtt{i})\,\mathrm{cv}_{\boldsymbol{S}}\big(\mathtt{i}(v)\big) = \mathrm{M}_{\boldsymbol{BS}}(\mathtt{i})\,v$$

$$= \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ -4 \\ 3 \end{pmatrix}$$

⇦≪

Let $T: F^n \to F^m$ be an arbitrary linear transformation, and let $\boldsymbol{b}$ and $\boldsymbol{c}$ be the standard bases of F^n and F^m respectively. If M is the matrix of T relative to $\boldsymbol{c}$ and $\boldsymbol{b}$ then by 4.19.2 we have, for all $v \in F^n$,

$$T(v) = \mathrm{cv}_{\boldsymbol{c}}\big(T(v)\big) = \mathrm{M}_{\boldsymbol{cb}}(T)\,\mathrm{cv}_{\boldsymbol{b}}(v) = Mv.$$

Thus we have proved

7.2 Proposition *Every linear transformation from F^n to F^m is given by multiplication by an $m \times n$ matrix; furthermore, the matrix involved is the matrix of the transformation relative to the standard bases.*

7.3 Definition Let $\boldsymbol{b}$ and $\boldsymbol{c}$ be bases for the vector space V. Let $\mathtt{i}$ be the identity transformation from V to V and let $\mathrm{M}_{\boldsymbol{cb}} = \mathrm{M}_{\boldsymbol{cb}}(\mathtt{i})$, the matrix of $\mathtt{i}$ relative to $\boldsymbol{c}$ and $\boldsymbol{b}$. We call $\mathrm{M}_{\boldsymbol{cb}}$ the *transition matrix* from $\boldsymbol{b}$-coordinates to $\boldsymbol{c}$-coordinates.

The reason for this terminology is clear: if the coordinate vector of v relative to $\boldsymbol{b}$ is multiplied by $\mathrm{M}_{\boldsymbol{cb}}$ the result is the coordinate vector of v relative to $\boldsymbol{c}$.

7.4 Proposition *In the notation of 7.3 we have*

$$\mathrm{cv}_{\boldsymbol{c}}(v) = \mathrm{M}_{\boldsymbol{cb}}\,\mathrm{cv}_{\boldsymbol{b}}(v) \qquad \textit{for all } v \in V.$$

The proof of this is trivial. (See #2 above.)

§7b Multiplication of transformations and matrices

We saw in Exercise 10 of Chapter Three that if $\phi: U \to V$ and $\psi: V \to W$ are linear transformations then their product is also a linear transformation. (Remember that multiplication of linear transformations is composition; $\psi\phi: U \to W$ is ϕ followed by ψ.) In view of the correspondence between matrices and linear transformations given in the previous section it is natural to seek a formula for the matrix of $\psi\phi$ in terms of the matrices of ψ and ϕ. The answer is natural too: the matrix of a product is the product the matrices. Of course this is no fluke: matrix multiplication is defined the way it is just so that it corresponds like this to composition of linear transformations.

7.5 THEOREM *Let U, V, W be vector spaces with bases $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$ respectively, and let $\phi\colon U \to V$ and $\psi\colon V \to W$ be linear transformations. Then* $\mathrm{M}_{\boldsymbol{db}}(\psi\phi) = \mathrm{M}_{\boldsymbol{dc}}(\psi)\,\mathrm{M}_{\boldsymbol{cb}}(\phi)$.

Proof. Let $\boldsymbol{b} = (u_1, \ldots, u_m)$, $\boldsymbol{c} = (v_1, \ldots, v_n)$ and $\boldsymbol{d} = (w_1, \ldots, w_p)$. Let the $(i,j)^{\text{th}}$ entries of $\mathrm{M}_{\boldsymbol{dc}}(\psi)$, $\mathrm{M}_{\boldsymbol{cb}}(\phi)$ and $\mathrm{M}_{\boldsymbol{db}}(\psi\phi)$ be (respectively) α_{ij}, β_{ij} and γ_{ij}. Thus, by the definition of the matrix of a transformation,

$$\text{(a)} \qquad \psi(v_k) = \sum_{i=1}^{p} \alpha_{ik} w_i \qquad (\text{for } k = 1, 2, \ldots, n),$$

$$\text{(b)} \qquad \phi(u_j) = \sum_{k=1}^{n} \beta_{kj} v_k \qquad (\text{for } j = 1, 2, \ldots, m),$$

and

$$\text{(c)} \qquad (\psi\phi)(u_j) = \sum_{i=1}^{p} \gamma_{ij} w_i \qquad (\text{for } j = 1, 2, \ldots, m).$$

But, by the definition of the product of linear transformations,

$$\begin{aligned}
(\psi\phi)(u_j) &= \psi\big(\phi(u_j)\big) \\
&= \psi\left(\sum_{k=1}^{n} \beta_{kj} v_k\right) && \text{(by (b))} \\
&= \sum_{k=1}^{n} \beta_{kj}\, \psi(v_k) && \text{(by linearity of } \psi) \\
&= \sum_{k=1}^{n} \beta_{kj} \sum_{i=1}^{p} \alpha_{ik} w_i && \text{(by (a))} \\
&= \sum_{i=1}^{p} \left(\sum_{k=1}^{n} \alpha_{ik}\beta_{kj}\right) w_i,
\end{aligned}$$

and comparing with (c) we have (by 4.15 and the fact that the w_i form a basis) that

$$\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}$$

for all $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, m$. Since the right hand side of this equation is precisely the formula for the $(i,j)^{\text{th}}$ entry of the product of the matrices $\mathrm{M}_{\boldsymbol{dc}}(\psi) = (\alpha_{ij})$ and $\mathrm{M}_{\boldsymbol{cb}}(\phi) = (\beta_{ij})$ it follows that $\mathrm{M}_{\boldsymbol{db}}(\psi\phi) = \mathrm{M}_{\boldsymbol{dc}}(\psi)\,\mathrm{M}_{\boldsymbol{cb}}(\phi)$. □

Comments ▷▷▷

7.5.1 Here is a shorter proof of 7.5. The j^{th} column of $\mathrm{M}_{\boldsymbol{dc}}(\psi)\,\mathrm{M}_{\boldsymbol{cb}}(\phi)$ is, by the definition of matrix multiplication, the product of $\mathrm{M}_{\boldsymbol{dc}}(\psi)$ and the j^{th} column of $\mathrm{M}_{\boldsymbol{cb}}(\phi)$. Hence, by the definition of $\mathrm{M}_{\boldsymbol{cb}}(\phi)$, it equals

$$\mathrm{M}_{\boldsymbol{dc}}(\psi)\,\mathrm{cv}_{\boldsymbol{c}}\big(\phi(u_j)\big),$$

which in turn equals $\mathrm{cv}_{\boldsymbol{d}}\big(\psi(\phi(u_j))\big)$ (by 7.1). But this is just $\mathrm{cv}_{\boldsymbol{d}}\big((\psi\phi)(u_j)\big)$, the j^{th} column of $\mathrm{M}_{\boldsymbol{db}}(\psi\phi)$.

7.5.2 Observe that the shapes of the matrices are right. Since the dimension of V is n and the dimension of W is p the matrix $\mathrm{M}_{\boldsymbol{dc}}(\psi)$ has n columns and p rows; that is, it is a $p\times n$ matrix. Similarly $\mathrm{M}_{\boldsymbol{cb}}(\phi)$ is an $n\times m$ matrix. Hence the product $\mathrm{M}_{\boldsymbol{dc}}(\psi)\,\mathrm{M}_{\boldsymbol{cb}}(\phi)$ exists and is a $p\times m$ matrix—the right shape to be the matrix of a transformation from an m-dimensional space to a p-dimensional space. ▷▷▷

It is trivial that if $\boldsymbol{b}$ is a basis of V and $\mathtt{i}\colon V\to V$ the identity then $\mathrm{M}_{\boldsymbol{bb}}(\mathtt{i})$ is the identity matrix (of the appropriate size). Hence,

7.6 Corollary *If $f\colon V\to W$ is an isomorphism then*

$$\mathrm{M}_{\boldsymbol{bc}}(f^{-1}) = (\mathrm{M}_{\boldsymbol{cb}}(f))^{-1}$$

for any bases $\boldsymbol{b}$, $\boldsymbol{c}$ of V, W.

Proof. Let I be the $d\times d$ identity matrix, where $d=\dim V=\dim W$ (see Exercise 1 of Chapter Six). Then by 7.5 we have

$$\mathrm{M}_{\boldsymbol{bc}}(f^{-1})\,\mathrm{M}_{\boldsymbol{cb}}(f) = \mathrm{M}_{\boldsymbol{bb}}(f^{-1}f) = \mathrm{M}_{\boldsymbol{bb}}(\mathtt{i}) = I$$

and

$$\mathrm{M}_{\boldsymbol{cb}}(f)\,\mathrm{M}_{\boldsymbol{bc}}(f^{-1}) = \mathrm{M}_{\boldsymbol{cc}}(ff^{-1}) = \mathrm{M}_{\boldsymbol{cc}}(\mathtt{i}) = I$$

whence the result. □

As another corollary we discover how changing the bases alters the matrix of a transformation:

7.7 COROLLARY *Let $T: V \to W$ be a linear transformation. Let $\boldsymbol{b}_1$, $\boldsymbol{b}_2$ be bases for V and let $\boldsymbol{c}_1$, $\boldsymbol{c}_2$ be bases for W. Then*

$$\mathrm{M}_{\boldsymbol{c}_2\boldsymbol{b}_2}(T) = \mathrm{M}_{\boldsymbol{c}_2\boldsymbol{c}_1}\,\mathrm{M}_{\boldsymbol{c}_1\boldsymbol{b}_1}(T)\,\mathrm{M}_{\boldsymbol{b}_1\boldsymbol{b}_2}\,.$$

Proof. By their definitions $\mathrm{M}_{\boldsymbol{c}_2\boldsymbol{c}_1} = \mathrm{M}_{\boldsymbol{c}_2\boldsymbol{c}_1}(\mathtt{i}_W)$ and $\mathrm{M}_{\boldsymbol{b}_2\boldsymbol{b}_1} = \mathrm{M}_{\boldsymbol{b}_2\boldsymbol{b}_1}(\mathtt{i}_V)$ (where $\mathtt{i}_V$ and $\mathtt{i}_W$ are the identity transformations); so 7.5 gives

$$\mathrm{M}_{\boldsymbol{c}_2\boldsymbol{c}_1}\,\mathrm{M}_{\boldsymbol{c}_1\boldsymbol{b}_1}(T)\,\mathrm{M}_{\boldsymbol{b}_1\boldsymbol{b}_2} = \mathrm{M}_{\boldsymbol{c}_2\boldsymbol{b}_2}(\mathtt{i}_W T \mathtt{i}_V),$$

and since $\mathtt{i}_W T \mathtt{i}_V = T$ the result follows. □

Our next corollary is a special case of the last; it will be of particular importance later.

7.8 COROLLARY *Let $\boldsymbol{b}$ and $\boldsymbol{c}$ be bases of V and let $T: V \to V$ be linear. Let $X = \mathrm{M}_{\boldsymbol{b}\boldsymbol{c}}$ be the transition matrix from $\boldsymbol{c}$-coordinates to $\boldsymbol{b}$-coordinates. Then*

$$\mathrm{M}_{\boldsymbol{c}\boldsymbol{c}}(T) = X^{-1}\,\mathrm{M}_{\boldsymbol{b}\boldsymbol{b}}(T)X.$$

Proof. By 7.6 we see that $X^{-1} = \mathrm{M}_{\boldsymbol{c}\boldsymbol{b}}$, so that the result follows immediately from 7.7. □

—Example—

#3 Let $f: \mathbb{R}^3 \to \mathbb{R}^3$ be defined by

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 8 & 85 & -9 \\ 0 & -2 & 0 \\ 6 & 49 & -7 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

and let $\boldsymbol{b} = \left(\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -4 \\ 1 \\ 5 \end{pmatrix}\right)$. Prove that $\boldsymbol{b}$ is a basis for $\mathbb{R}^3$ and calculate $\mathrm{M}_{\boldsymbol{b}\boldsymbol{b}}(f)$.

≫→ As in previous examples, $\boldsymbol{b}$ will be a basis if and only if the matrix with the elements of $\boldsymbol{b}$ as its columns is invertible. If it is invertible it is the

transition matrix $\mathrm{M}_{\boldsymbol{sb}}$, and its inverse is $\mathrm{M}_{\boldsymbol{bs}}$. Now

$$\left(\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 2 & 5 & 0 & 0 & 1 \end{array}\right) \xrightarrow{R_3:=R_3-R_1} \left(\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 9 & -1 & 0 & 1 \end{array}\right)$$

$$\xrightarrow[R_2:=-1R_2]{R_2\leftrightarrow R_3} \left(\begin{array}{ccc|ccc} 1 & 3 & -4 & 1 & 0 & 0 \\ 0 & 1 & -9 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow[R_1:=R_1-R_2]{\substack{R_2:=R_2+9R_3 \\ R_1:=R_1+4R_3}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -2 & -23 & 3 \\ 0 & 1 & 0 & 1 & 9 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right),$$

so that $\boldsymbol{b}$ is a basis. Moreover, by 7.8,

$$\begin{aligned} \mathrm{M}_{\boldsymbol{bb}}(f) &= \begin{pmatrix} -2 & -23 & 3 \\ 1 & 9 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 8 & 85 & -9 \\ 0 & -2 & 0 \\ 6 & 49 & -7 \end{pmatrix} \begin{pmatrix} 1 & 3 & -4 \\ 0 & 0 & 1 \\ 1 & 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} -2 & -23 & 3 \\ 1 & 9 & -1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 6 & 8 \\ 0 & 0 & -2 \\ -1 & 4 & -10 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix}. \end{aligned}$$

⇦≪

---

§7c The Main Theorem on Linear Transformations

If A and B are finite sets with the same number of elements then a function from A to B which is one-to-one is necessarily onto as well, and, likewise, a function from A to B which is onto is necessarily one-to-one. There is an analogous result for linear transformations between finite dimensional vector spaces: if V and U are spaces of the same finite dimension then a linear transformation from V to U is one-to-one if and only if it is onto. More generally, if V and U are arbitrary finite dimensional vector spaces and $\phi\colon V \to U$ a linear transformation then the dimension of the image of ϕ equals the dimension of V minus the dimension of the kernel of ϕ. This is one of the assertions of the principal result of this section:

7.9 The Main Theorem on Linear Transformations *Let V and U be vector spaces over the field F and $\phi\colon V \to U$ a linear transformation. Let W be a subspace of V complementing* $\ker\phi$. *Then*

(i) W is isomorphic to $\operatorname{im}\phi$,

(ii) if V is finite dimensional then

$$\dim V = \dim(\operatorname{im}\phi) + \dim(\ker\phi).$$

Comments ▷▷▷

7.9.1 Recall that 'W complements $\ker\phi$' means that $V = W \oplus \ker\phi$. We have proved in 6.10 that if V is finite dimensional then there always exists such a W. In fact it is also true in the infinite dimensional case, but the proof (using Zorn's Lemma) is beyond the scope of this course.

7.9.2 In physical examples the dimension of the space V can be thought of intuitively as the number of degrees of freedom of the system. Then the dimension of $\ker\phi$ is the number of degrees of freedom which are killed by ϕ and the dimension of $\operatorname{im}\phi$ the number which survive ϕ. ▷▷▷

Proof. (i) Define $\psi\colon W \to \operatorname{im}\phi$ by

$$\psi(v) = \phi(v) \qquad \text{for all } v \in W.$$

Thus ψ is simply ϕ with the domain restricted to W and the codomain restricted to $\operatorname{im}\phi$. Note that it is legitimate to restrict the codomain like this since $\phi(v) \in \operatorname{im}\phi$ for all $v \in W$. We prove that ψ is an isomorphism.

Since ϕ is linear, ψ is certainly linear also:

$$\psi(\lambda x + \mu y) = \phi(\lambda x + \mu y) = \lambda\phi(x) + \mu\phi(y) = \lambda\psi(x) + \mu\psi(y)$$

for all x, $y \in W$ and λ, $\mu \in F$. We have

$$\ker\psi = \{\, x \in W \mid \psi(x) = 0 \,\} = \{\, x \in W \mid \phi(x) = 0 \,\} = W \cap \ker\phi = \{0\}$$

by 6.6, since the sum of W and $\ker\phi$ is direct. Hence ψ is injective, by 3.15, and it remains to prove that ψ is surjective.

Let $u \in \operatorname{im}\phi$. Then $u = \phi(v)$ for some $v \in V$, and since $V = W + \ker\phi$ we may write $v = w + z$ with $w \in W$ and $z \in \ker\phi$. Then we have

$$u = \phi(v) = \phi(w + z) = \phi(w) + \phi(z) = \phi(w) + 0$$

since $z \in \ker\phi$, and so $u = \phi(w) = \psi(w)$. This holds for all $u \in \operatorname{im}\phi$; so we have shown that $\psi\colon W \to \operatorname{im}\phi$ is surjective, as required. Hence W is isomorphic to $\operatorname{im}\phi$.

(ii) Let $(x_1, x_2, \ldots, x_r)$ be a basis for W. Since ψ is an isomorphism it follows from 4.17 that $(\psi(x_1), \psi(x_2), \ldots, \psi(x_r))$ is a basis for $\operatorname{im}\phi$, and so $\dim(\operatorname{im}\phi) = \dim W$. Hence 6.9 yields

$$\dim V = \dim W + \dim(\ker\phi) = \dim(\operatorname{im}\phi) + \dim(\ker\phi).$$

□

—Example—

#4 Let $\phi\colon \mathbb{R}^3 \to \mathbb{R}^3$ be defined by

$$\phi\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

It is easily seen that the image of ϕ consists of all scalar multiples of the column $\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, and is therefore a space of dimension 1. By the Main Theorem the kernel of ϕ must have dimension 2, and, indeed, it is easily checked that

$$\left(\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}\right)$$

is a basis for $\ker\phi$.

In our treatment of the Main Theorem we have avoided mentioning quotient spaces, so that §6c would not be a prerequisite. This does, however, distort the picture somewhat; a more natural version of the theorem is as follows:

7.10 Theorem *Let V and U be vector spaces and $\phi\colon V \to U$ a linear transformation. Then the image of ϕ is isomorphic to the quotient of V by the kernel of ϕ. That is, symbolically,* $\operatorname{im}\phi \cong (V/\ker\phi)$.

Proof. Let $I = \operatorname{im}\phi$ and $K = \ker\phi$. Elements of V/K are cosets, of the form $v + K$ where $v \in V$. Now if $x \in K$ then

$$\phi(v + x) = \phi(v) + \phi(x) = \phi(v) + 0 = \phi(v)$$

and so it follows that ϕ maps all elements of the coset $x + K$ to the same element $u = \phi(v)$ in the subspace I of U. Hence there is a well-defined mapping $\psi\colon (V/K) \to I$ satisfying

$$\psi(v + K) = \phi(v) \qquad \text{for all } v \in V.$$

Linearity of ψ follows easily from linearity of ϕ and the definitions of addition and scalar multiplication for cosets:

$$\begin{aligned}\psi(\lambda(x + K) + \mu(y + K)) &= \psi((\lambda x + \mu y) + K) = \phi(\lambda x + \mu y)\\ &= \lambda\phi(x) + \mu\phi(y) = \lambda\psi(x + K) + \mu\psi(y + K)\end{aligned}$$

for all x, $y \in V$ and λ, $\mu \in F$.

Since every element of I has the form $\phi(v) = \psi(v + K)$ it is immediate that ψ is surjective. Moreover, if $v+K \in \ker\psi$ then since $\phi(v) = \psi(v+K) = 0$ it follows that $v \in K$, whence $v + K = K$, the zero element of V/K. Hence the kernel of ψ consists of the zero element alone, and therefore ψ is injective. □

We leave to the exercises the proof of the following consequence of the Main Theorem.

7.11 Proposition *If S and T are subspaces of V then*

$$\dim(S + T) + \dim(S \cap T) = \dim S + \dim T.$$

Another consequence of the Main Theorem is that it is possible to choose bases of the domain and codomain so that the matrix of a linear transformation has a particularly simple form.

7.12 Theorem *Let V, U be vector spaces of dimensions n, m respectively, and $\phi\colon V \to U$ a linear transformation. Then there exist bases $\boldsymbol{b}$, $\boldsymbol{c}$ of V, U and a positive integer r such that*

$$\mathrm{M}_{\boldsymbol{cb}}(\phi) = \begin{pmatrix} I_{r\times r} & 0_{r\times(n-r)} \\ 0_{(m-r)\times r} & 0_{(m-r)\times(n-r)} \end{pmatrix}$$

where $I_{r\times r}$ is an $r\times r$ identity matrix, and the other blocks are zero matrices of the sizes indicated. Thus, the (i,j)-entry of $\mathrm{M}_{\boldsymbol{cb}}(\phi)$ is zero unless $i=j\le r$, in which case it is one.

Proof. By 6.10 we may write $V = W \oplus \ker\phi$, and, as in the proof of the Main Theorem, let $(x_1, x_2, \dots, x_r)$ be a basis of W. Choose any basis of $\ker\phi$; by 6.9 it will have $n-r$ elements, and combining it with the basis of W will give a basis of V. Let $(x_{r+1}, \dots, x_n)$ be the chosen basis of $\ker\phi$, and let $\boldsymbol{b} = (x_1, x_2, \dots, x_n)$ the resulting basis of V.

As in the proof of the Main Theorem, $(\phi(x_1), \dots, \phi(x_r))$ is a basis for the subspace $\operatorname{im}\phi$ of U. By 4.10 we may choose u_{r+1}, u_{r+2}, …, $u_m \in U$ so that

$$\boldsymbol{c} = (\phi(x_1), \phi(x_2), \dots, \phi(x_r), u_{r+1}, u_{r+2}, \dots, u_m)$$

is a basis for U.

The bases $\boldsymbol{b}$ and $\boldsymbol{c}$ having been defined, it remains to calculate the matrix of ϕ and check that it is as claimed. By definition the i^{th} column of $\mathrm{M}_{\boldsymbol{cb}}(\phi)$ is the coordinate vector of $\phi(x_i)$ relative to $\boldsymbol{c}$. If $r+1 \le i \le n$ then $x_i \in \ker\phi$ and so $\phi(x_i) = 0$. So the last $n-r$ columns of the matrix are zero. If $1 \le i \le r$ then $\phi(x_i)$ is actually in the basis c; in this case the solution of

$$\phi(x_i) = \lambda_1\phi(x_1) + \cdots + \lambda_r\phi(x_r) + \lambda_{r+1}u_{r+1} + \cdots + \lambda_m u_m$$

is $\lambda_i = 1$ and $\lambda_j = 0$ for $j \ne i$. Thus for $1 \le i \le r$ the i^{th} column of the matrix has a 1 in the i^{th} position and zeros elsewhere. □

Comment ▷▷▷

7.12.1 The number r which appears in 7.12 is called the *rank* of ϕ. Note that r is an *invariant* of ϕ, in the sense that it depends only on ϕ and not on the bases $\boldsymbol{b}$ and $\boldsymbol{c}$. Indeed, r is just the dimension of the image of ϕ. ▷▷▷

§7d Rank and nullity of matrices

Because of the connection between matrices and linear transformations, the Main Theorem on Linear Transformations ought to have an analogue for matrices. This section is devoted to the relevant concepts. Our first aim is to prove the following important theorem:

7.13 Theorem *Let A be any rectangular matrix over the field F. The dimension of the column space of A is equal to the dimension of the row space of A.*

7.14 DEFINITION The *rank* of A, $\operatorname{rank}(A)$, is defined to be the dimension of the row space of A.

In view of 7.13 we could equally well define the rank to be the dimension of the column space. However, we are not yet ready to prove 7.13; there are some preliminary results we need first. The following is trivial:

7.15 PROPOSITION *The dimension of* $\mathrm{RS}(A)$ *does not exceed the number of rows of* A*, and the dimension of* $\mathrm{CS}(A)$ *does not exceed the number of columns.*

Proof. Immediate from 4.12 (i), since the rows span the row space and the columns span the column space. □

We proved in Chapter Three (see 3.21) that if A and B are matrices such that AB exists then the row space of AB is contained in the row space of B, and the two are equal if A is invertible. It is natural to ask whether there is any relationship between the column space of AB and the column space of B.

7.16 PROPOSITION *If* $A \in \mathrm{Mat}(m \times n, F)$ *and* $B \in \mathrm{Mat}(n \times p, F)$ *then* $\phi(x) = Ax$ *defines a surjective linear transformation from* $\mathrm{CS}(B)$ *to* $\mathrm{CS}(AB)$.

Proof. Let the columns of B be $x_1, x_2, \ldots, x_p$. Then the columns of AB are $Ax_1, Ax_2, \ldots, Ax_m$. Now if $v \in \mathrm{CS}(B)$ then $v = \sum_{i=1}^{m} \lambda_i x_i$ for some $\lambda_i \in F$, and so

$$\phi(v) = Av = A\Big(\sum_{i=1}^{p} \lambda_i x_i\Big) = \sum_{i=1}^{p} \lambda_i A x_i \in \mathrm{CS}(AB).$$

Thus ϕ is a function from $\mathrm{CS}(B)$ to $\mathrm{CS}(AB)$. It is trivial that ϕ is linear:

$$\phi(\lambda x + \mu y) = A(\lambda x + \mu y) = \lambda(Ax) + \mu(Ay) = \lambda\phi(x) + \mu\phi(y).$$

It remains to prove that ϕ is surjective. If $y \in \mathrm{CS}(AB)$ is arbitrary then y must be a linear combination of the Ax_i (the columns of AB); so for some scalars λ_i

$$y = \sum_{i=1}^{p} \lambda_i A x_i = A\Big(\sum_{i=1}^{p} \lambda_i x_i\Big).$$

Defining $x = \sum_{i=1}^{n} \lambda_i x_i$ we have that $x \in \mathrm{CS}(B)$, and $y = Ax = \phi(x) \in \operatorname{im}\phi$, as required. □

7.17 Corollary *The dimension of* $\mathrm{CS}(AB)$ *is less than or equal to the dimension of* $\mathrm{CS}(B)$.

Proof. This follows from the Main Theorem on Linear Transformations: since ϕ is surjective we have

$$\dim \mathrm{CS}(B) = \dim(\mathrm{CS}(AB)) + \dim(\ker \phi),$$

and since $\dim(\ker \phi)$ is certainly nonnegative the result follows. □

If the matrix A is invertible then we may apply 7.17 with B replaced by AB and A replaced by A^{-1} to deduce that $\dim(\mathrm{CS}(A^{-1}AB) \leq \dim(\mathrm{CS}(AB)$, and combining this with 7.17 itself gives

7.18 Corollary *If* A *is invertible then* $\mathrm{CS}(B)$ *and* $\mathrm{CS}(AB)$ *have the same dimension.*

We have already seen that elementary row operations do not change the row space at all; so they certainly do not change the dimension of the row space. In 7.18 we have shown that they do not change the dimension of the column space either. Note, however, that the column space itself is changed by row operations, it is only the dimension of the column space which is unchanged.

The next three results are completely analogous to 7.16, 7.17 and 7.18, and so we omit the proofs.

7.19 Proposition *If* A *and* B *are matrices such that* AB *exists then* $x \mapsto xB$ *is a surjective linear transformation from* $\mathrm{RS}(A)$ *to* $\mathrm{RS}(AB)$.

7.20 Corollary *The dimension of* $\mathrm{RS}(AB)$ *is less than or equal to the dimension of* $\mathrm{RS}(A)$.

7.21 Corollary *If* B *is invertible then* $\dim(\mathrm{RS}(AB)) = \dim(\mathrm{RS}(A))$.

By 7.18 and 7.21 we see that premultiplying and postmultiplying by invertible matrices both leave unchanged the dimensions of the row space and column space. Given a matrix A, then, it is natural to look for invertible matrices P and Q for which PAQ is as simple as possible. Then, with any luck, it may be obvious that $\dim(\mathrm{RS}(PAQ)) = \dim(\mathrm{CS}(PAQ))$. If so we will have achieved our aim of proving that $\dim(\mathrm{RS}(A)) = \dim(\mathrm{CS}(A))$. Theorem 7.12 readily provides the result we seek:

7.22 THEOREM *Let $A \in \mathrm{Mat}(m \times n, F)$. Then there exist invertible matrices $P \in \mathrm{Mat}(m \times m, F)$ and $Q \in \mathrm{Mat}(n \times n, F)$ such that*

$$PAQ = \begin{pmatrix} I_{r\times r} & 0_{r\times(n-r)} \\ 0_{(m-r)\times r} & 0_{(m-r)\times(n-r)} \end{pmatrix}$$

where the integer r equals both the dimension of the row space of A and the dimension of the column space of A.

Proof. Let $\phi\colon F^n \to F^m$ be given by $\phi(x) = Ax$. Then ϕ is a linear transformation, and $A = \mathrm{M}_{\boldsymbol{s_2 s_1}}(\phi)$, where s_1, s_2 are the standard bases of F^n, F^m. (See 7.2 above.) By 7.12 there exist bases $\boldsymbol{b}$, $\boldsymbol{c}$ of F^n, F^m such that $\mathrm{M}_{\boldsymbol{cb}}(\phi) = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$, and if we let P and Q be the transition matrices $\mathrm{M}_{\boldsymbol{cs_2}}$ and $\mathrm{M}_{\boldsymbol{s_1 b}}$ (respectively) then 7.7 gives

$$PAQ = \mathrm{M}_{\boldsymbol{cs_2}}\ \mathrm{M}_{\boldsymbol{s_2 s_1}}(\phi)\ \mathrm{M}_{\boldsymbol{s_1 b}} = \mathrm{M}_{\boldsymbol{cb}}(\phi) = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}.$$

Note that since P and Q are transition matrices they are invertible (by 7.6); hence it remains to prove that if the identity matrix I in the above equation is of shape $r \times r$, then the row space of A and the column space of A both have dimension r.

By 7.21 and 3.22 we know that $\mathrm{RS}(PAQ)$ and $\mathrm{RS}(A)$ have the same dimension. But the row space of $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$ consists of all n-component rows of the form $(\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$, and is clearly an r-dimensional space isomorphic to ${}^{\mathrm{t}}F^r$. Indeed, the nonzero rows of $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$—that is, the first r rows—are linearly independent, and therefore form a basis for the row space. Hence $r = \dim(\mathrm{RS}(PAQ)) = \dim(\mathrm{RS}(A))$, and by totally analogous reasoning we also obtain that $r = \dim(\mathrm{CS}(PAQ)) = \dim(\mathrm{CS}(A))$. □

Comments ▷▷▷

7.22.1 We have now proved 7.13.

7.22.2 The proof of 7.22 also shows that the rank of a linear transformation (see 7.12.1) is the same as the rank of the matrix of that linear transformation, independent of which bases are used.

7.22.3 There is a more direct computational proof of 7.22, as follows. Apply row operations to A to obtain a reduced echelon matrix. As we have

seen in Chapter One, row operations are performed by premultiplying by invertible matrices; so the echelon matrix obtained has the form PA with P invertible. Now apply column operations to PA; this amounts to postmultiplying by an invertible matrix. It can be seen that a suitable choice of column operations will transform an echelon matrix to the desired form. ▷▷▷

As an easy consequence of the above results we can deduce the following important fact:

7.23 THEOREM *An $n \times n$ matrix has an inverse if and only if its rank is n.*

Proof. Let $A \in \mathrm{Mat}(n \times n, F)$ and suppose that $\mathrm{rank}(A) = n$. By 7.22 there exist $n \times n$ invertible P and Q with $PAQ = I$. Multiplying this equation on the left by P^{-1} and on the right by P gives $P^{-1}PAQP = P^{-1}P$, and hence $A(QP) = I$. We conclude that A is invertible (QP being the inverse).

Conversely, suppose that A is invertible, and let $B = A^{-1}$. By 7.20 we know that $\mathrm{rank}(AB) \leq \mathrm{rank}(A)$, and by 7.15 the number of rows of A is an upper bound on the rank of A. So $n \geq \mathrm{rank}(A) \geq \mathrm{rank}(AB) = \mathrm{rank}(I) = n$ since (reasoning as in the proof of 7.22) it is easily shown that the $n \times n$ identity has rank n. Hence $\mathrm{rank}(A) = n$. □

Let A be an $m \times n$ matrix over F and let $\phi\colon F^n \to F^m$ be the linear transformation given by multiplication by A. Since

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{pmatrix} x_i$$

we see that for every $v \in F^n$ the column $\phi(v)$ is a linear combination of the columns of A, and, conversely, every linear combination of the columns of A is $\phi(v)$ for some $v \in F^n$. In other words, the image of ϕ is just the column space of A. The kernel of ϕ involves us with a new concept:

7.24 DEFINITION The *right null space* of a matrix $A \in \mathrm{Mat}(m \times n, F)$ is the set $\mathrm{RN}(A)$ consisting of all $v \in F^n$ such that $Av = 0$. The dimension of $\mathrm{RN}(A)$ is called the *right nullity*, $\mathrm{rn}(A)$, of A. Similarly, the *left null space* $\mathrm{LN}(A)$ is the set of all $w \in {}^{\mathrm{t}}F^m$ such that $wA = 0$, and its dimension is called the *left nullity*, $\mathrm{ln}(A)$, of A.

It is obvious that if A and ϕ are as in the above discussion, the kernel of ϕ is the right null space of A. The domain of ϕ is F^n, which has dimension equal to n, the number of columns of A. Hence the Main Theorem on Linear Transformations applied to ϕ gives:

7.25 THEOREM *For any rectangular matrix A over the field F, the rank of A plus the right nullity of A equals the number of columns of A. That is,*

$$\operatorname{rank}(A) + \operatorname{rn}(A) = n$$

for all $A \in \operatorname{Mat}(m \times n, F)$.

Comment ▷▷▷

7.25.1 Similarly, the linear transformation $x \mapsto xA$ has kernel equal to the left null space of A and image equal to the row space of A, and it follows that $\operatorname{rank}(A)+\operatorname{ln}(A) = m$, the number of rows of A. Combining this equation with the one in 7.25 gives $\operatorname{ln}(A) - \operatorname{rn}(A) = m - n$. ▷▷▷

Exercises

1. Let U be the vector space consisting of all functions $f\colon \mathbb{R} \to \mathbb{R}$ which satisfy the differential equation $f''(t) - f(t) = 0$, and assume that that $\boldsymbol{b}_1 = (u_1, u_2)$ and $\boldsymbol{b}_2 = (v_1, v_2)$ are two different bases of U, where u_1, u_2, v_1, v_2 are defined as follows:

$$u_1(t) = e^t \qquad v_1(t) = \cosh(t)$$
$$u_2(t) = e^{-t} \qquad v_2(t) = \sinh(t)$$

for all $t \in \mathbb{R}$. Find the $(\boldsymbol{b}_1, \boldsymbol{b}_2)$-transition matrix.

2. Let f, g, h be the functions from $\mathbb{R}$ to $\mathbb{R}$ defined by

$$f(t) = \sin(t), \quad g(t) = \sin(t + \frac{\pi}{4}), \quad h(t) = \sin(t + \frac{\pi}{2}).$$

(*i*) What is the dimension of the vector space V (over $\mathbb{R}$) spanned by (f, g, h)? Determine two different bases $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ of V.

(*ii*) Show that differentiation yields a linear transformation from V to V, and calculate the matrix of this transformation relative to the bases $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ found in (*i*). (That is, use $\boldsymbol{b}_1$ as the basis of V considered as the domain, $\boldsymbol{b}_2$ as the basis of V considered as the codomain.)

3. Regard $\mathbb{C}$ as a vector space over $\mathbb{R}$. Show that the function $\theta\colon \mathbb{C} \to \mathbb{C}$ defined by $\theta(z) = \bar{z}$ (complex conjugate of z) is a linear transformation, and calculate the matrix of θ relative to the basis $(1, \boldsymbol{i})$ (for both the domain and codomain).

4. Let $\boldsymbol{b}_1 = (v_1, v_2, \ldots, v_n)$, $\boldsymbol{b}_2 = (w_1, w_2, \ldots w_n)$ be two bases of a vector space V. Prove that $\mathrm{M}_{\boldsymbol{b}_1\boldsymbol{b}_2} = \mathrm{M}_{\boldsymbol{b}_2\boldsymbol{b}_1}^{-1}$.

5. Let $\theta\colon \mathbb{R}^3 \to \mathbb{R}^2$ be defined by

$$\theta\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Calculate the matrix of θ relative to the bases

$$\left(\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ -2 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 4 \\ -3 \end{pmatrix}\right) \quad \text{and} \quad \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$$

of $\mathbb{R}^3$ and $\mathbb{R}^2$.

6. (*i*) Let $\phi\colon \mathbb{R}^2 \to \mathbb{R}$ be defined by $\phi\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$. Calculate the matrix of ϕ relative to the bases $\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$ and (-1) of $\mathbb{R}^2$ and $\mathbb{R}$.

(*ii*) With ϕ as in (*i*) and θ as in Exercise 5, calculate $\phi\theta$ and its matrix relative the two given bases. Hence verify Theorem 7.5 in this case.

7. Let S and T be subspaces of a vector space V and let U be a subspace of T such that $T = (S \cap T) \oplus U$. Prove that $S + T = S \oplus U$, and hence deduce that $\dim(S + T) = \dim S + \dim T - \dim(S \cap T)$.

8. Give an alternative proof of the result of the previous exercise by use of the Main Theorem and Exercise 14 of Chapter Six.

9. Prove that the rank of a linear transformation is an invariant. (See 7.12.1.)

10. Let $S = \text{span}(v_1, v_2, \ldots, v_s)$, $T = \text{span}(w_1, w_2, \ldots, w_t)$ where the v_i and w_j are n-component rows over F. Form the matrix

$$\left(\begin{array}{c|c} v_1 & v_1 \\ v_2 & v_2 \\ \vdots & \vdots \\ v_s & v_s \\ w_1 & 0 \\ w_2 & 0 \\ \vdots & \vdots \\ w_t & 0 \end{array}\right)$$

and use row operations to reduce it to echelon form. If the result is

$$\left(\begin{array}{c|c} x_1 & * \\ \vdots & \vdots \\ x_l & * \\ 0 & y_1 \\ \vdots & \vdots \\ 0 & y_k \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{array}\right)$$

then $(x_1, x_2, \ldots, x_l)$ is a basis for $S+T$ and $(y_1, y_2, \ldots, y_k)$ is a basis for $S \cap T$.

Do this for the following example:

$$\begin{array}{llll} v_1 = (1 & 1 & 1 & 1) \\ v_2 = (2 & 0 & -2 & 3) \\ v_3 = (1 & 3 & 5 & 0) \\ v_4 = (7 & -3 & 8 & -1) \end{array} \qquad \begin{array}{llll} w_1 = (0 & -2 & -4 & 1) \\ w_2 = (1 & 5 & 9 & -1) \\ w_3 = (3 & -3 & -9 & 6) \\ w_4 = (1 & 1 & 0 & 0). \end{array}$$

Think about why it works.

11. Let V, W be vector spaces over the field F and let $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$, $\boldsymbol{c} = (w_1, w_2, \ldots, w_m)$ be bases of V, W respectively. Let $\mathrm{L}(V, W)$ be the set of all linear transformations from V to W, and let $\mathrm{Mat}(m \times n, F)$ be the set of all $m \times n$ matrices over F.

Prove that the function $\Omega\colon \mathrm{L}(V, W) \to \mathrm{Mat}(m \times n, F)$ defined by $\Omega(\theta) = \mathrm{M}_{\boldsymbol{bc}}(\theta)$ is a vector space isomorphism. Find a basis for $\mathrm{L}(V, W)$.

(Hint: Elements of the basis must be linear transformations from V to W, and to describe a linear transformation θ from V to W it suffices to specify $\theta(v_i)$ for each i. First find a basis for $\mathrm{Mat}(m \times n, F)$ and use the isomorphism above to get the required basis of $\mathrm{L}(V, W)$.)

12. For each of the following linear transformations calculate the dimensions of the kernel and image, and check that your answers are in agreement with the Main Theorem on Linear Transformations.

(*i*) $\theta\colon \mathbb{R}^4 \to \mathbb{R}^2$ given by $\theta \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} 2 & -1 & 3 & 5 \\ 1 & -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$.

(*ii*) $\theta\colon \mathbb{R}^2 \to \mathbb{R}^3$ given by $\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 & -2 \\ -2 & 1 \\ -6 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$.

(*iii*) $\theta\colon V \to V$ given by $\theta(p(x)) = p'(x)$, where V is the space of all polynomials over $\mathbb{R}$ of degree less than or equal to 3.

13. Suppose that $\theta\colon \mathbb{R}^6 \to \mathbb{R}^4$ is a linear transformation with kernel of dimension 2. Is θ surjective?

14. Let $\theta\colon \mathbb{R}^3 \to \mathbb{R}^3$ be defined by $\theta \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & -4 & 2 \\ -1 & -2 & 2 \\ 1 & -5 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, and let $\boldsymbol{b}$ be the basis of $\mathbb{R}^3$ given by $\boldsymbol{b} = \left(\begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix} \right)$. Calculate $\mathrm{M}_{\boldsymbol{bb}}(\theta)$ and find a matrix X such that

$$X^{-1} \begin{pmatrix} 1 & -4 & 2 \\ -1 & -2 & 2 \\ 1 & -5 & 3 \end{pmatrix} X = \mathrm{M}_{\boldsymbol{bb}}(\theta).$$

15. Let $\theta\colon \mathbb{R}^3 \to \mathbb{R}^4$ be defined by

$$\theta\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & -1 & 3 \\ 2 & -1 & -2 \\ 1 & -1 & 1 \\ 4 & -2 & -4 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Find bases $\boldsymbol{b} = (u_1, u_2, u_3)$ of $\mathbb{R}^3$ and $\boldsymbol{c} = (v_1, v_2, v_3, v_4)$ of $\mathbb{R}^4$ such that the matrix of θ relative to $\boldsymbol{b}$ and $\boldsymbol{c}$ is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

16. Let V and W be finitely generated vector spaces of the same dimension, and let $\theta\colon V \to W$ be a linear transformation. Prove that θ is injective if and only if it is surjective.

17. Give an example, or prove that no example can exist, for each of the following.

(*i*) A surjective linear transformation $\theta\colon \mathbb{R}^8 \to \mathbb{R}^5$ with kernel of dimension 4.

(*ii*) $A \in \mathrm{Mat}(3 \times 2, \mathbb{R})$, $B \in \mathrm{Mat}(2 \times 2, \mathbb{R})$, $C \in \mathrm{Mat}(2 \times 3, \mathbb{R})$ with

$$ABC = \begin{pmatrix} 2 & 2 & 2 \\ 3 & 3 & 0 \\ 4 & 0 & 0 \end{pmatrix}.$$

18. Let A be the 50×100 matrix with $(i, j)^{\text{th}}$ entry $100(i-1) + j$. (Thus the first row consists of the numbers from 1 to 100, the second consists of the numbers from 101 to 200, and so on.) Let V be the space of all 50-component rows v over $\mathbb{R}$ such that $vA = 0$ and W the space of 100-component columns w over $\mathbb{R}$ such that $Aw = 0$. (That is, V and W are the left null space and right null space of A.) Calculate $\dim W - \dim V$.

(Hint: You do not really have to do any calculation!)

19. Let U and V be vector spaces over F and $\phi\colon U \to V$ a linear transformation. Let $\boldsymbol{b}$, $\boldsymbol{b}'$ be bases for U and $\boldsymbol{d}$, $\boldsymbol{d}'$ bases for V. Prove that the matrices $\mathrm{M}_{\boldsymbol{bd}}(\phi)$ and $\mathrm{M}_{\boldsymbol{b}'\boldsymbol{d}'}(\phi)$ have the same rank.

8

Permutations and determinants

This chapter is devoted to studying determinants, and in particular to proving the properties which were stated without proof in Chapter Two. Since a proper understanding of determinants necessitates some knowledge of permutations, we investigate these first.

§8a Permutations

Our discussion of this topic will be brief since all we really need is the definition of the parity of a permutation (see Definition 8.3 below), and some of its basic properties.

8.1 Definition A *permutation* of the set $\{1, 2, \ldots, n\}$ is a bijective function $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. The set of all permutations of $\{1, 2, \ldots, n\}$ will be denoted by 'S_n'.

For example, the function $\sigma\colon \{1, 2, 3\} \to \{1, 2, 3\}$ defined by

$$\sigma(1) = 2, \qquad \sigma(2) = 3, \qquad \sigma(3) = 1$$

is a permutation. In a notation which is commonly used one would write

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

for this permutation. In general, the notation

$$\tau = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ r_1 & r_2 & r_3 & \cdots & r_n \end{bmatrix}$$

means

$$\tau(1) = r_1, \quad \tau(2) = r_2, \quad \ldots, \quad \tau(n) = r_n.$$

Comments ▷▷▷

8.1.1 Altogether there are six permutations of $\{1, 2, 3\}$, namely

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

8.1.2 It is usual to give a more general definition than 8.1 above: a permutation of any set S is a bijective function from S to itself. However, we will only need permutations of $\{1, 2, \ldots, n\}$. ▷▷▷

Multiplication of permutations is defined to be composition of functions. That is,

8.2 Definition For $\sigma, \tau \in S_n$ define $\sigma\tau : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ by $(\sigma\tau)(i) = \sigma(\tau(i))$.

Comments ▷▷▷

8.2.1 We proved in Chapter One that the composite of two bijections is a bijection; hence the product of two permutations is a permutation. Furthermore, for each permutation σ there is an inverse permutation σ^{-1} such that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \mathtt{i}$ (the identity permutation).

In fact, permutations form an algebraic system known as a *group*. We leave the study of groups to another course.

8.2.2 Unfortunately, there are two conflicting conventions within the mathematical community, both widespread, concerning multiplication of permutations. Some people, perhaps most people, write permutations as *right* operators, rather than *left* operators (which is the convention that we will follow). If $\sigma \in S_n$ and $i \in \{1, 2, \ldots, n\}$ our convention is to write '$\sigma(i)$' for the image of of i under the action of σ; the permutation is written to the left of the the thing on which it acts. The right operator convention is to write either 'i^σ' or '$i\sigma$' instead of $\sigma(i)$. This seems at first to be merely a notational matter of no mathematical consequence. But, naturally enough, right operator people define the product $\sigma\tau$ of two permutations σ and τ by the rule $i^{\sigma\tau} = (i^\sigma)^\tau$, instead of by the rule given in 8.2 above. Thus for right operators, '$\sigma\tau$' means 'apply σ first, then apply τ', while for left operators it means 'apply τ first, then apply σ' (since '$(\sigma\tau)(i)$' means 'σ applied to (τ applied to i)'). The upshot is that we multiply permutations from right to left, others go from left to right. ▷▷▷

—Example—

#1 Compute the following product of permutations:

$$\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}\begin{bmatrix}1&2&3&4\\3&2&4&1\end{bmatrix}.$$

$\gg\!\!\rightarrow$ Let $\sigma = \begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}$ and $\tau = \begin{bmatrix}1&2&3&4\\3&2&4&1\end{bmatrix}$. Then

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 4.$$

The procedure is immediately clear: to find what the product does to 1, first find the number underneath 1 in the right hand factor—it is 3 in this case—then look under this number in the next factor to get the answer. Repeat this process to find what the product does to 2, 3 and 4. We find that

$$\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}\begin{bmatrix}1&2&3&4\\3&2&4&1\end{bmatrix} = \begin{bmatrix}1&2&3&4\\4&3&1&2\end{bmatrix}.$$

$\ll\!\!\leftarrow$

Note that the right operator convention leads to exactly the same method for computing products, but starting with the left hand factor and proceeding to the right. This would give $\begin{bmatrix}1&2&3&4\\2&4&1&3\end{bmatrix}$ as the answer.

#2 It is equally easy to compute a product of more than two factors. Thus, for instance

$$\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix} = \begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}.$$

Starting from the right one finds, for example, that 3 goes to 1, then to 3, then 2, then 1, then 3.

The notation adopted above is good, but can be somewhat cumbersome. The trouble is that each number in $\{1, 2, \ldots, n\}$ must written down twice. There is a shorter notation which writes each number down at most once. In this notation the permutation

$$\sigma = \begin{bmatrix}1&2&3&4&5&6&7&8&9&10&11\\8&6&3&2&1&9&7&5&4&11&10\end{bmatrix}$$

would be written as $\sigma = (1,8,5)(2,6,9,4)(10,11)$. The idea is that the permutation is made up of disjoint "cycles". Here the cycle $(2,6,9,4)$ means that 6 is the image of 2, 9 the image of 6, 4 the image of 9 and 2 the image of 4 under the action of σ. Similarly $(1,8,5)$ indicates that σ maps 1 to 8, 8 to 5 and 5 to 1. Cycles of length one (like (3) and (7) in the above example) are usually omitted, and the cycles can be written in any order. The computation of products is equally quick, or quicker, in the disjoint cycle notation, and (fortunately) the cycles of length one have no effect in such computations. The reader can check, for example, that if $\sigma = (1)(2,3)(4)$ and $\tau = (1,4)(2)(3)$ then $\sigma\tau$ and $\tau\sigma$ are both equal to $(1,4)(2,3)$.

8.3 DEFINITION For each $\sigma \in S_n$ define $l(\sigma)$ to be the number of ordered pairs (i,j) such that $1 \le i < j \le n$ and $\sigma(i) > \sigma(j)$. If $l(\sigma)$ is an odd number we say that σ is an *odd* permutation; if $l(\sigma)$ is even we say that σ is an *even* permutation. We define $\varepsilon\colon S_n \to \{+1,-1\}$ by

$$\varepsilon(\sigma) = (-1)^{l(\sigma)} = \begin{cases} +1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

for each $\sigma \in S_n$, and call $\varepsilon(\sigma)$ the *parity* or *sign* of σ.

The reason for this definition becomes apparent (after a while!) when one considers the polynomial E in n variables $x_1, x_2, \ldots, x_n$ defined by $E = \Pi_{i<j}(x_i - x_j)$. That is, E is the product of all factors $(x_i - x_j)$ with $i < j$. In the case $n = 4$ we would have

$$E = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Now take a permutation σ and in the expression for E replace each subscript i by $\sigma(i)$. For instance, if $\sigma = (4,2,1,3)$ then applying σ to E in this way gives

$$\sigma(E) = (x_3 - x_1)(x_3 - x_4)(x_3 - x_2)(x_1 - x_4)(x_1 - x_2)(x_4 - x_2).$$

Note that one gets exactly the same factors, except that some of the signs are changed. With some thought it can be seen that this will always be the case. Indeed, the factor $(x_i - x_j)$ in E is transformed into the factor $(x_{\sigma(i)} - x_{\sigma(j)})$ in $\sigma(E)$, and $(x_{\sigma(i)} - x_{\sigma(j)})$ appears explicitly in the expression for E if $\sigma(i) < \sigma(j)$, while $(x_{\sigma(j)} - x_{\sigma(i)})$ appears there if $\sigma(i) > \sigma(j)$. Thus the number of sign changes is exactly the number of pairs (i,j) with $i < j$ such that $\sigma(i) > \sigma(j)$; that is, the number of sign changes is $l(\sigma)$. It follows that $\sigma(E)$ equals E if σ is even and $-E$ if σ is odd; that is, $\sigma E = \varepsilon(\sigma)E$.

The following definition was implicitly used in the above argument:

8.4 DEFINITION Let $\sigma \in S_n$ and let f be a real-valued function of n real variables $x_1, x_2, \ldots, x_n$. Then σf is the function defined by

$$(\sigma f)(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

If f and g are two real valued functions of n variables it is usual to define their product fg by

$$(fg)(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n)g(x_1, x_2, \ldots, x_n).$$

(Note that this is the *pointwise* product, not to be confused with the composite, given by $f(g(x))$, which is the only kind of product of functions previously encountered in this book. In fact, since f is a function of n variables, $f(g(x))$ cannot make sense unless $n = 1$. Thus confusion is unlikely.)

We leave it for the reader to check that, for the pointwise product, $\sigma(fg) = (\sigma f)(\sigma g)$ for all $\sigma \in S_n$ and all functions f and g. In particular if c is a constant this gives $\sigma(cf) = c(\sigma f)$. Furthermore

8.5 PROPOSITION *For all $\sigma, \tau \in S_n$ and any function f of n variables we have $(\sigma\tau)f = \sigma(\tau f)$.*

Proof. Let $\sigma, \tau \in S_n$. Let $x_1, x_2, \ldots, x_n$ be variables and define $y_i = x_{\sigma(i)}$ for each i. Then by definition

$$(\sigma(\tau f))(x_1, x_2, \ldots, x_n) = (\tau f)(y_1, y_2, \ldots, y_n)$$

and

$$\begin{aligned}(\tau f)(y_1, y_2, \ldots, y_n) &= f(y_{\tau(1)}, y_{\tau(2)}, \ldots, y_{\tau(n)}) \\ &= f(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}).\end{aligned}$$

Thus we have shown that

$$(\sigma(\tau f))(x_1, x_2, \ldots, x_n) = f(x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \ldots, x_{(\sigma\tau)(n)})$$

for all values of the x_i, and so $\sigma(\tau f) = (\sigma\tau)f$, as claimed. □

It can now be seen that for all σ, $\tau \in S_n$, with E as above,

$$\varepsilon(\sigma\tau)E = (\sigma\tau)E = \sigma(\tau E) = \sigma(\varepsilon(\tau)E) = \varepsilon(\tau)\sigma E = \varepsilon(\tau)\varepsilon(\sigma)E$$

and we deduce that $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Since the proof of this fact is the chief reason for including a section on permutations we give another proof, based on properties of cycles of length two.

8.6 Definition A permutation in S_n which is of the form (i, j) for some i, $j \in I = \{1, 2, \ldots, n\}$ is called a *transposition*. That is, if τ is a transposition then there exist i, $j \in I$ such that $\tau(i) = j$ and $\tau(j) = i$, and $\tau(k) = k$ for all other $k \in I$. A transposition of the form $(i, i+1)$ is called *simple*.

8.7 Lemma *Suppose that $\tau = (i, i+1)$ is a simple transposition in S_n. If $\sigma \in S_n$ and $\sigma' = \sigma\tau$ then*

$$l(\sigma') = \begin{cases} l(\sigma) + 1 & \text{if } \sigma(i) < \sigma(i+1) \\ l(\sigma) - 1 & \text{if } \sigma(i) > \sigma(i+1). \end{cases}$$

Proof. Observe that $\sigma'(i) = \sigma(i+1)$ and $\sigma'(i+1) = \sigma(i)$, while for other values of j we have $\sigma'(j) = \sigma(j)$. In our original notation for permutations, σ' is obtained from σ by swapping the numbers in the i^{th} and $(i+1)^{\text{th}}$ positions in the second row. The point is now that if $r > s$ and r occurs to the left of s in the second row of σ then the same is true in the second row of σ', except in the case of the two numbers we have swapped. Hence the number of such pairs is one more for σ' than it is for σ if $\sigma(i) < \sigma(i+1)$, one less if $\sigma(i) > \sigma(i+1)$, as required.

At the risk of making an easy argument seem complicated, let us spell this out in more detail. Define

$$N = \{\, (j,k) \mid j < k \text{ and } \sigma(j) > \sigma(k) \,\}$$

and

$$N' = \{\, (j,k) \mid j < k \text{ and } \sigma'(j) > \sigma'(k) \,\}$$

so that by definition the number of elements of N is $l(\sigma)$ and the number of elements of N' is $l(\sigma')$. We split N into four pieces as follows:

$$\begin{aligned} N_1 &= \{\, (j,k) \in N \mid j \notin \{i, i+1\} \text{ and } k \notin \{i, i+1\} \,\} \\ N_2 &= \{\, (j,k) \in N \mid j \in \{i, i+1\} \text{ and } k \notin \{i, i+1\} \,\} \\ N_3 &= \{\, (j,k) \in N \mid j \notin \{i, i+1\} \text{ and } k \in \{i, i+1\} \,\} \\ N_4 &= \{\, (j,k) \in N \mid j \in \{i, i+1\} \text{ and } k \in \{i, i+1\} \,\}. \end{aligned}$$

Define also N_1', N_2', N_3' and N_4' by exactly the same formulae with N replaced by N'. Every element of N lies in exactly one of the N_i, and every element of N' lies in exactly one of the N_i'.

If neither j nor k is in $\{i, i+1\}$ then $\sigma'(j)$ and $\sigma'(k)$ are the same as $\sigma(j)$ and $\sigma(k)$, and so (j,k) is in N' if and only if it is in N. Thus $N_1 = N_1'$.

Consider now pairs (i,k) and $(i+1,k)$, where $k \notin \{i, i+1\}$. We show that $(i,k) \in N$ if and only if $(i+1,k) \in N'$. Obviously $i < k$ if and only if $i+1 < k$, and since $\sigma(i) = \sigma'(i+1)$ and $\sigma(k) = \sigma'(k)$ we see that $\sigma(i) > \sigma(k)$ if and only if $\sigma'(i+1) > \sigma'(k)$; hence $i < k$ and $\sigma(i) > \sigma(k)$ if and only if $i+1 < k$ and $\sigma'(i+1) > \sigma'(k)$, as required. Furthermore, since $\sigma(i+1) = \sigma'(i)$, exactly the same argument gives that $i+1 < k$ and $\sigma(i+1) > \sigma(k)$ if and only if $i < k$ and $\sigma'(i) > \sigma'(k)$. Thus $(i,k) \mapsto (i+1,k)$ and $(i+1,k) \mapsto (i,k)$ gives a one to one correspondence between N_2 and N_2'.

Moving on now to pairs of the form (j,i) and $(j,i+1)$ where $j \notin \{i, i+1\}$, we have that $\sigma(j) > \sigma(i)$ if and only if $\sigma'(j) > \sigma'(i+1)$ and $\sigma(j) > \sigma(i+1)$ if and only if $\sigma'(j) > \sigma'(i)$. Since also $j < i$ if and only if $j < i+1$ we see that $(j,i) \in N$ if and only if $(j,i+1) \in N'$ and $(j,i+1) \in N$ if and only if $(j,i) \in N'$. Thus $(j,i) \mapsto (j,i+1)$ and $(j,i+1) \mapsto (j,i)$ gives a one to one correspondence between N_3 and N_3'.

We have now shown that the number of elements in N and not in N_4 equals the number of elements in N' and not in N_4'. But N_4 and N_4' each have at most one element, namely $(i,i+1)$, which is in N_4 and not in N_4' if $\sigma(i) > \sigma(i+1)$, and in N_4' and not N_4 if $\sigma(i) < \sigma(i+1)$. Hence N has one more element than N' in the former case, one less in the latter. □

8.8 Proposition *(i) If $\sigma = \tau_1\tau_2\ldots\tau_r$ where the τ_i are simple transpositions, then $l(\sigma)$ is odd is r is odd and even if r is even.*

(ii) Every permutation $\sigma \in S_n$ can be expressed as a product of simple transpositions.

Proof. The first part is proved by an easy induction on r, using 8.7. The point is that

$$l((\tau_1\tau_2\ldots\tau_{r-1})\tau_r) = l(\tau_1\tau_2\ldots\tau_{r-1}) \pm 1$$

and in either case the parity of $\tau_1\tau_2\ldots\tau_r$ is opposite that of $\tau_1\tau_2\ldots\tau_{r-1}$. The details are left as an exercise.

The second part is proved by induction on $l(\sigma)$. If $l(\sigma) = 0$ then $\sigma(i) < \sigma(j)$ whenever $i < j$. Hence

$$1 \leq \sigma(1) < \sigma(2) < \cdots < \sigma(n) \leq n$$

and it follows that $\sigma(i) = i$ for all i. Hence the only permutation σ with $l(\sigma) = 0$ is the identity permutation. This is trivially a product of simple transpositions—an empty product. (Just as empty sums are always defined to be 0, empty products are always defined to be 1. But if you don't like empty products, observe that $\tau^2 = \mathtt{i}$ for any simple transposition τ.)

Suppose now that $l(\sigma) = l > 1$ and that all permutations σ' with $l(\sigma') < l$ can be expressed as products of simple transpositions. There must exist some i such that $\sigma(i) > \sigma(i+1)$, or else the same argument as used above would prove that $\sigma = \mathtt{i}$. Choosing such an i, let $\tau = (i, i+1)$ and $\sigma' = \sigma\tau$.

By 8.7 we have $l(\sigma') = l-1$, and by the inductive hypothesis there exist simple transpositions τ_i with $\sigma' = \tau_1\tau_2 \dots \tau_r$. This gives $\sigma = \tau_1\tau_2 \dots \tau_r\tau$, a product of simple transpositions. □

8.9 Corollary *If $\sigma, \tau \in S_n$ then $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.*

Proof. Write σ and τ as products of simple transpositions, and suppose that there are s factors in the expression for σ and t in the expression for τ. Multiplying these expressions expresses $\sigma\tau$ as a product of $r+s$ simple transpositions. By 8.8 (i),

$$\varepsilon(\sigma\tau) = (-1)^{r+s} = (-1)^r(-1)^s = \varepsilon(\sigma)\varepsilon(\tau).$$

□

Our next proposition shows that if the disjoint cycle notation is employed then calculation of the parity of a permutation is a triviality.

8.10 Proposition *Transpositions are odd permutations. More generally, any cycle with an even number of terms is an odd permutation, and any cycle with an odd number of terms is an even permutation.*

Proof. It is easily seen (by 8.7 with $\sigma = \mathtt{i}$ or directly) that if $\tau = (m, m+1)$ is a simple transposition then $l(\tau) = 1$, and so τ is odd: $\varepsilon(\tau) = (-1)^1 = -1$.

Consider next an arbitrary transposition $\sigma = (i, j) \in S_n$, where $i < j$. A short calculation yields $(i+1, i+2, \dots, j)(i, j) = (i, i+1)(i+1, i+2, \dots, j)$, with both sides equal to $(i, i+1, \dots, j)$. That is, $\rho\sigma = \tau\rho$, where $\tau = (i, i+1)$ and $\rho = (i+1, i+2, \dots, j)$. By 8.5 we obtain

$$\varepsilon(\rho)\varepsilon(\sigma) = \varepsilon(\rho\sigma) = \varepsilon(\tau\rho) = \varepsilon(\tau)\varepsilon(\rho),$$

and cancelling $\varepsilon(\rho)$ gives $\varepsilon(\sigma) = \varepsilon(\tau) = -1$ by the first case. (It is also easy to directly calculate $l(\sigma)$ in this case; in fact, $l(\sigma) = 2(j-i)-1$.)

Finally, let $\varphi = (r_1, r_2, \ldots, r_k)$ be an arbitrary cycle of k terms. Another short calculation shows that $\varphi = (r_1, r_2)(r_2, r_3)\ldots(r_{k-1}, r_k)$, a product of $k-1$ transpositions. So 8.9 gives $\varepsilon(\tau) = (-1)^{k-1}$, which is -1 if k is even and $+1$ if k is odd. □

Comment ▷▷▷

8.10.1 Proposition 8.10 shows that a permutation is even if and only if, when it is expressed as a product of cycles, the number of even-term cycles is even. ▷▷▷

The proof of the final result of this section is left as an exercise.

8.11 Proposition *(i) The number of elements of S_n is $n!$.*
(ii) The identity $\mathtt{i} \in S_n$, defined by $\mathtt{i}(i) = i$ for all i, is an even permutation.
(iii) The parity of σ^{-1} equals that of σ (for any $\sigma \in S_n$).
(iv) If σ, τ, $\tau' \in S_n$ are such that $\sigma\tau = \sigma\tau'$ then $\tau = \tau'$. Thus if σ is fixed then as τ varies over all elements of S_n so too does $\sigma\tau$.

§8b Determinants

8.12 Definition Let F be a field and $A \in \mathrm{Mat}(n \times n, F)$. Let the entry in i^{th} row and j^{th} column of A be a_{ij}. The *determinant* of A is the element of F given by

$$\begin{aligned}\det A &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}.\end{aligned}$$

Comments ▷▷▷

8.12.1 Determinants are only defined for square matrices.

8.12.2 Let us examine the definition first in the case $n = 3$. That is, we seek to calculate the determinant of a matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

The definition involves a sum over all permutations in S_3. There are six, listed in 8.1.1 above. Using the disjoint cycle notation we find that there are two 3-cycles ($(1,2,3)$ and $(1,3,2)$), three transpositions ($(1,2)$, $(1,3)$ and $(2,3)$) and the identity $\mathtt{i} = (1)$. The 3-cycles and the identity are even and the transpositions are odd. So, for example, if $\sigma = (1,2,3)$ then $\varepsilon(\sigma) = +1$, $\sigma(1) = 2$, $\sigma(2) = 3$ and $\sigma(3) = 1$, so that $\varepsilon(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}a_{3\sigma(3)} = (+1)a_{12}a_{23}a_{31}$. The results of similar calculations for all the permutations in S_3 are listed in the following table, in which the matrix entries $a_{i\sigma(i)}$ are also indicated in each case.

Permutation	Matrix entries $a_{i\sigma(i)}$	$\varepsilon(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}a_{3\sigma(3)}$
(1)	$\begin{pmatrix} \boxed{a_{11}} & a_{12} & a_{13} \\ a_{21} & \boxed{a_{22}} & a_{23} \\ a_{31} & a_{32} & \boxed{a_{33}} \end{pmatrix}$	$(+1)a_{11}a_{22}a_{33}$
$(2,3)$	$\begin{pmatrix} \boxed{a_{11}} & a_{12} & a_{13} \\ a_{21} & a_{22} & \boxed{a_{23}} \\ a_{31} & \boxed{a_{32}} & a_{33} \end{pmatrix}$	$(-1)a_{11}a_{23}a_{32}$
$(1,2)$	$\begin{pmatrix} a_{11} & \boxed{a_{12}} & a_{13} \\ \boxed{a_{21}} & a_{22} & a_{23} \\ a_{31} & a_{32} & \boxed{a_{33}} \end{pmatrix}$	$(-1)a_{12}a_{21}a_{33}$
$(1,2,3)$	$\begin{pmatrix} a_{11} & \boxed{a_{12}} & a_{13} \\ a_{21} & a_{22} & \boxed{a_{23}} \\ \boxed{a_{31}} & a_{32} & a_{33} \end{pmatrix}$	$(+1)a_{12}a_{23}a_{31}$
$(1,3,2)$	$\begin{pmatrix} a_{11} & a_{12} & \boxed{a_{13}} \\ \boxed{a_{21}} & a_{22} & a_{23} \\ a_{31} & \boxed{a_{32}} & a_{33} \end{pmatrix}$	$(+1)a_{13}a_{21}a_{32}$
$(1,3)$	$\begin{pmatrix} a_{11} & a_{12} & \boxed{a_{13}} \\ a_{21} & \boxed{a_{22}} & a_{23} \\ \boxed{a_{31}} & a_{32} & a_{33} \end{pmatrix}$	$(-1)a_{13}a_{22}a_{31}$

The determinant is the sum of the six terms in the third column. So, the determinant of the 3×3 matrix $A = (a_{ij})$ is given by

$$a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

8.12.3 Notice that in each of the matrices in the middle column of the above table there three boxed entries, each of the three rows contains exactly one boxed entry, and each of the three columns contains exactly one boxed

entry. Furthermore, the above six examples of such a boxing of entries are the only ones possible. So the determinant of a 3×3 matrix is a sum, with appropriate signs, of all possible terms obtained by multiplying three factors with the property that every row contains exactly one of the factors and every column contains exactly one of the factors.

Of course, there is nothing special about the 3×3 case. The determinant of a general $n \times n$ matrix is obtained by the natural generalization of the above method, as follows. Choose n matrix positions in such a way that no row contains more than one of the chosen positions and no column contains more than one of the chosen positions. Then it will necessarily be true that each row contains exactly one of the chosen positions and each column contains exactly one of the chosen positions. There are exactly $n!$ ways of doing this. In each case multiply the entries in the n chosen positions, and then multiply by the sign of the corresponding permutation. The determinant is the sum of the $n!$ terms so obtained.

We give an example to illustrate the rule for finding the permutation corresponding to a choice of matrix positions of the above kind. Suppose that $n = 4$. If one chooses the 4^{th} entry in row 1, the 2^{nd} in row 2, the 1^{st} in row 3 and the 3^{rd} in row 4, then the permutation is $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix} = (1, 4, 3)$. That is, if the j^{th} entry in row i is chosen then the permutation maps i to j. (In our example the term would be multiplied by $+1$ since $(1, 4, 3)$ is an even permutation.)

8.12.4 So far in this section we have merely been describing what the determinant is; we have not addressed the question of how best in practice to calculate the determinant of a given matrix. We will come to this question later; for now, suffice it to say that the definition does not provide a good method itself, except in the case $n = 3$. It is too tiresome to compute and add up the 24 terms arising in the definition of a 4×4 determinant or the 120 for a 5×5, and things rapidly get worse still. ▷▷▷

We start now to investigate properties of determinants. Several are listed in the next theorem.

8.13 Theorem *Let F be a field and $A \in \mathrm{Mat}(n \times n, F)$, and let the rows of A be $\underset{\sim}{a}_1, \underset{\sim}{a}_2, \ldots, \underset{\sim}{a}_n \in {}^{\mathrm{t}}F^n$.*

(i) Suppose that $1 \leq k \leq n$ and that $\underset{\sim}{a}_k = \lambda \underset{\sim}{a}'_k + \mu \underset{\sim}{a}''_k$. Then

$$\det A = \lambda \det A' + \mu \det A''$$

where A' is the matrix with a'_k as k^{th} row and all other rows the same as A, and, likewise, A'' has a''_k as its k^{th} row and other rows the same as A.

(ii) Suppose that B is the matrix obtained from A by permuting the rows by a permutation $\tau \in S_n$. That is, suppose that the first row of B is $a_{\tau(1)}$, the second $a_{\tau(2)}$, and so on. Then $\det B = \varepsilon(\tau) \det A$.

(iii) The determinant of the transpose of A is the same as the determinant of A.

(iv) If two rows of A are equal then $\det A = 0$.

(v) If A has a zero row then $\det A = 0$.

(vi) If $A = I$, the identity matrix, then $\det A = 1$.

Proof. (i) Let the $(i,j)^{\text{th}}$ entries of A, A' and A'' be (respectively) a_{ij}, a'_{ij} and a''_{ij}. Then we have $a_{ij} = a'_{ij} = a''_{ij}$ if $i \neq k$, and

$$a_{kj} = \lambda a'_{kj} + \mu a''_{kj}$$

for all j. Now by definition $\det A$ is the sum over all $\sigma \in S_n$ of the terms $\varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$. In each of these terms we may replace $a_{k\sigma(k)}$ by $\lambda a'_{k\sigma(k)} + \mu a''_{k\sigma(k)}$, so that the term then becomes the sum of the two terms

$$\lambda \varepsilon(\sigma) a_{1\sigma(1)} \dots a_{(k-1)\sigma(k-1)} a'_{k\sigma(k)} a_{(k+1)\sigma(k+1)} \dots a_{n\sigma(n)}$$

and

$$\mu \varepsilon(\sigma) a_{1\sigma(1)} \dots a_{(k-1)\sigma(k-1)} a''_{k\sigma(k)} a_{(k+1)\sigma(k+1)} \dots a_{n\sigma(n)}$$

In the first of these we replace $a_{i\sigma(i)}$ by $a'_{i\sigma(i)}$ (for all $i \neq k$) and in the second we likewise replace $a_{i\sigma(i)}$ by $a''_{i\sigma(i)}$. This shows that $\det A$ is equal to

$$\lambda\Big(\sum_{\sigma\in S_n} \varepsilon(\sigma) a'_{1\sigma(1)} a'_{2\sigma(2)} \dots a'_{n\sigma(n)}\Big) + \mu\Big(\sum_{\sigma\in S_n} \varepsilon(\sigma) a''_{1\sigma(1)} a''_{2\sigma(2)} \dots a''_{n\sigma(n)}\Big)$$

which is $\lambda \det A' + \mu \det A''$.

(ii) Let a_{ij} and b_{ij} be the $(i,j)^{\text{th}}$ entries of A and B respectively. We are given that if $\underset{\sim}{b}_i$ is the i^{th} row of B then $\underset{\sim}{b}_i = \underset{\sim}{a}_{\tau(i)}$; so $b_{ij} = a_{\tau(i)j}$ for all i and j. Now

$$\begin{aligned}\det B &= \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_{i\sigma(i)} \\ &= \sum_{\sigma\in S_n} \varepsilon(\sigma\tau) \prod_{i=1}^{n} b_{i(\sigma\tau)(i)} \\ &\qquad \text{(since } \sigma\tau \text{ runs through all of } S_n \text{ as } \sigma \text{ does—see 8.11)}\end{aligned}$$

$$= \sum_{\sigma\in S_n} \varepsilon(\tau)\varepsilon(\sigma) \prod_{i=1}^{n} b_{i\sigma(\tau(i))} \qquad \text{(by 8.5)}$$

$$= \varepsilon(\tau) \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\tau(i)\sigma(\tau(i))}$$

$$= \varepsilon(\tau) \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j\sigma(j)}$$

since $j = \tau(i)$ runs through all of the set $\{1, 2, \ldots, n\}$ as i does. Thus $\det B = \varepsilon(\tau) \det A$.

(iii) Let C be the transpose of A and let the $(i, j)^{\text{th}}$ entry of C be c_{ij}. Then $c_{ij} = a_{ji}$, and

$$\det C = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} c_{i\sigma(i)} = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}.$$

For a fixed σ, if $j = \sigma(i)$ then $i = \sigma^{-1}(j)$, and j runs through all of $\{1, 2, \ldots, n\}$ as i does. Hence

$$\det C = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j\sigma^{-1}(j)}.$$

But if we let $\rho = \sigma^{-1}$ then ρ runs through all of S_n as σ does, and since $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ our expression for $\det C$ becomes $\sum_{\rho\in S_n} \varepsilon(\rho) \prod_{j=1}^{n} a_{j\rho(j)}$, which equals $\det A$.

(iv) Suppose that $\underset{\sim}{a}_i = \underset{\sim}{a}_j$ where $i \neq j$. Let τ be the transposition (i, j), and let B be the matrix obtained from A by permuting the rows by τ, as in part (ii). Since we have just swapped two equal rows we in fact have that $B = A$, but by (ii) we know that $\det B = \varepsilon(\tau) \det A = -\det A$ since transpositions are odd permutations. We have proved that $\det A = -\det A$; so $\det A = 0$.

(v) Suppose that $\underset{\sim}{a}_k = \underset{\sim}{0}$. Then $\underset{\sim}{a}_k = \underset{\sim}{a}_k + \underset{\sim}{a}_k$, and applying part (i) with $\underset{\sim}{a}'_k = \underset{\sim}{a}''_k = \underset{\sim}{a}_k$ and $\lambda = \mu = 1$ we obtain $\det A = \det A + \det A$. Hence $\det A = 0$.

(vi) We know that $\det A$ is the sum of terms $\varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$, and obviously such a term is zero if $a_{i\sigma(i)} = 0$ for any value of i. Now if $A = I$ the

only nonzero entries are the diagonal entries; $a_{ij} = 0$ if $i \neq j$. So the term in the expression for $\det A$ corresponding to the permutation σ is zero unless $\sigma(i) = i$ for all i. Thus all $n!$ terms are zero except the one corresponding to the identity permutation. And that term is 1 since all the diagonal entries are 1 and the identity permutation is even. □

Comment ▷▷▷

8.13.1 The first part of 8.13 says that if all but one of the rows of A are kept fixed, then $\det A$ is a linear function of the remaining row. In other words, given $\underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_{k-1}$ and $\underset{\sim}{a}_{k+1}, \ldots, \underset{\sim}{a}_n \in {}^{\mathrm{t}}F^n$ the function $\phi\colon {}^{\mathrm{t}}F^n \to F$ defined by

$$\phi(\underset{\sim}{x}) = \det \begin{pmatrix} \underset{\sim}{a}_1 \\ \vdots \\ \underset{\sim}{a}_{k-1} \\ \underset{\sim}{x} \\ \underset{\sim}{a}_{k+1} \\ \vdots \\ \underset{\sim}{a}_n \end{pmatrix}$$

is a linear transformation. Moreover, since $\det A = \det {}^{\mathrm{t}}A$ it follows that the determinant function is also linear in each of the columns. ▷▷▷

8.14 Proposition *Suppose that $E \in \mathrm{Mat}(n \times n, F)$ is any elementary matrix. Then $\det(EA) = \det E \det A$ for all $A \in \mathrm{Mat}(n \times n, F)$.*

Proof. We consider the three kinds of elementary matrices separately. First of all, suppose that $E = E_{ij}$, the matrix obtained by swapping rows i and j of I. By 2.6, $B = EA$ is the matrix obtained from A by swapping rows i and j. By 8.13 (ii) we know that $\det B = \varepsilon(\tau) \det A$, where $\tau = (i, j)$. Thus, in this case, $\det(EA) = -\det A$ for all A.

Next, consider the case $E = E_{ij}^{(\lambda)}$, the matrix obtained by adding λ times row i to row j. In this case 2.6 says that row j of EA is $\lambda \underset{\sim}{a}_i + \underset{\sim}{a}_j$ (where $\underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n$ are the rows of A), and all other rows of EA are the same as the corresponding rows of A. So by 8.13 (i) we see that $\det(EA)$ is $\lambda \det A' + \det A$, where A' has the same rows as A, except that row j of A' is $\underset{\sim}{a}_i$. In particular, A' has row j equal to row i. By 8.13 (iv) this gives $\det A' = 0$, and so in this case we have $\det(EA) = \det A$.

The third possibility is $E = E_i^{(\lambda)}$. In this case the rows of EA are the same as the rows of A except for the i^{th}, which gets multiplied by λ. Writing $\lambda \underset{\sim}{a}_i$ as $\lambda \underset{\sim}{a}_i + 0\underset{\sim}{a}_i$ we may again apply 8.13 (i), and conclude that in this case $\det(EA) = \lambda \det A + 0 \det A = \lambda \det A$ for all matrices A.

In every case we have that $\det(EA) = c \det A$ for all A, where c is independent of A; explicitly, $c = -1$ in the first case, 1 in the second, and λ in the third. Putting $A = I$ this gives

$$\det E = \det(EI) = c \det I = c$$

since $\det I = 1$. So we may replace c by $\det E$ in the formula for $\det(EA)$, giving the desired result. □

As a corollary of the above proof we have

8.15 Corollary *The determinants of the three kinds of elementary matrices are as follows:* $\det E_{ij} = -1$ *for all* i *and* j; $\det E_{ij}^{(\lambda)} = 1$ *for all* i, j *and* λ; $\det E_i^{(\lambda)} = \lambda$ *for all* i *and* λ.

As an easy consequence of 8.14 we deduce

8.16 Proposition *If* B, $A \in \mathrm{Mat}(n \times n, F)$ *and* B *can be written as a product of elementary matrices, then* $\det(BA) = \det B \det A$.

Proof. Let $B = E_1 E_2 \dots E_r$ where the E_i are elementary. We proceed by induction on r; the case $r = 1$ is 8.14 itself. Now let $r = k + 1$, and assume the result for k. By 8.14 we have

$$\det(BA) = \det(E_1(B'A)) = \det E_1 \det(B'A)$$

where $B' = E_2 \dots E_{k+1}$ is a product of k elementary matrices, so that the inductive hypothesis gives

$$\det E_1 \det(B'A) = \det E_1 \det B' \det A = \det(E_1 B') \det A$$

by 8.14 again. Since $E_1 B' = B$ these equations combine to give the desired result. □

In fact the formula $\det(BA) = \det B \det A$ for square matrices A and B is valid for all A and B without restriction, and we will prove this shortly.

As we observed in Chapter 2 (see 2.8) it is possible to obtain a reduced echelon matrix from an arbitrary matrix by premultiplying by a suitable sequence of elementary matrices. Hence

8.17 LEMMA *For any $A \in \mathrm{Mat}(n \times n, F)$ there exist B, $R \in \mathrm{Mat}(n \times n, F)$ such that B is a product of elementary matrices and R is a reduced echelon matrix, and $BA = R$.*

Furthermore, as in the proof of 2.9, it is easily shown that the reduced echelon matrix R obtained in this way from a square matrix A is either equal to the identity or else has a zero row. Since the rank of A is just the number of nonzero rows in R (since the rows of R are linearly independent and span $\mathrm{RS}(R) = \mathrm{RS}(A)$) this can be reformulated as follows:

8.18 LEMMA *In the situation of 8.17, if the rank of A is n then $R = I$, and if the rank of A is not n then R has at least one zero row.*

An important consequence of this is

8.19 THEOREM *The determinant of any $n \times n$ matrix of rank less than n is zero.*

Proof. Let $A \in \mathrm{Mat}(n \times n, F)$ have rank less than n. By 8.17 there exist elementary matrices $E_1, E_2, \ldots, E_k$ and a reduced echelon matrix R with $E_1 E_2 \ldots E_k A = R$. By 8.18 R has a zero row. By 2.5 elementary matrices have inverses which are themselves elementary matrices, and we deduce that $A = E_k^{-1} \ldots E_2^{-1} E_1^{-1} R$. Now 8.16 gives $\det A = \det(E_k^{-1} \ldots E_1^{-1}) \det R = 0$ since $\det R = 0$ (by 8.13 (v)). □

8.20 THEOREM *If A, $B \in \mathrm{Mat}(n \times n, F)$ then $\det(AB) = \det A \det B$.*

Proof. Suppose first that the rank of A is n. As in the proof of 8.19 we have $\det A = \det(E_k^{-1} \ldots E_1^{-1}) \det R$ where the E_i^{-1} are elementary and R is reduced echelon. In this case, however, 8.18 yields that $R = I$, whence A is a product of elementary matrices and our conclusion comes at once from 8.16.

The other possibility is that the rank of A is less than n. Then by 3.21 (ii) and 7.13 it follows that the rank of AB is also less than n, so that $\det(AB) = \det A = 0$ (by 8.19). So $\det(AB) = \det A \det B$, both sides being zero. □

Comment ▷▷▷

8.20.1 Let A be a $n \times n$ matrix over the field F. From the theory above and in the preceding chapters it can be seen that the following conditions are equivalent:

(i) A is expressible as a product of elementary matrices.
(ii) The rank of A is n.
(iii) The nullity of A is zero.
(iv) $\det A \neq 0$.
(v) A has an inverse.
(vi) The rows of A are linearly independent.
(vii) The rows of A span ${}^{\mathrm{t}}F^n$.
(viii) The columns of A are linearly independent.
(ix) The columns of A span F^n.
(x) The right null space of A is zero. (That is, the only solution of $Av = 0$ is $v = 0$.)
(xi) The left null space of A is zero.

◁◁◁

8.21 DEFINITION A matrix $A \in \mathrm{Mat}(n \times n, F)$ possessing the properties listed in 8.20.1 is said to be *nonsingular*. Other matrices in $\mathrm{Mat}(n \times n, F)$ are said to be *singular*.

We promised above to present a good practical method for calculating determinants, and we now address this matter. Let $A \in \mathrm{Mat}(n \times n, F)$. As we have seen, there exist elementary matrices E_i such that $(E_1 \dots E_k)A = R$, with R reduced echelon. Furthermore, if R is not the identity matrix then $\det A = 0$, and if R is the identity matrix then $\det A$ is the product of the determinants of the inverses of $E_1, \dots, E_k$. We also know the determinants of all elementary matrices. This gives a good method. Apply elementary row operations to A and at each step write down the determinant of the inverse of the corresponding elementary matrix. Stop when the identity matrix, or a matrix with a zero row, is reached. In the zero row case tha determinant is 0, otherwise it is the product of the numbers written down. Effectively, all one is doing is simplifying the matrix by row operations and keeping track of how the determinant is changed. There is a refinement worth noting: column operations are as good as row operations for calculating determinants; so one can use either, or a combination of both.

—***Example***—

#3 Calculate the determinant of

$$\begin{pmatrix} 2 & 6 & 14 & -4 \\ 2 & 5 & 10 & 1 \\ 0 & -1 & 2 & 1 \\ 2 & 7 & 11 & -3 \end{pmatrix}.$$

≫▷ Apply row operations, keeping a record.

$$\begin{pmatrix} 2 & 6 & 14 & -4 \\ 2 & 5 & 10 & 1 \\ 0 & -1 & 2 & 1 \\ 2 & 7 & 11 & -3 \end{pmatrix} \xrightarrow[R_4:=R_4-2R_1]{R_1:=\frac{1}{2}R_1, \; R_2:=R_2-2R_1} \begin{pmatrix} 1 & 3 & 7 & -2 \\ 0 & -1 & -4 & 5 \\ 0 & -1 & 2 & 1 \\ 0 & 1 & -3 & 1 \end{pmatrix} \begin{matrix} 2 \\ 1 \\ 1 \end{matrix}$$

$$\xrightarrow[R_4:=R_4-R_2]{R_2:=-1R_2, \; R_3:=R_3+R_2} \begin{pmatrix} 1 & 3 & 7 & -2 \\ 0 & 1 & 4 & -5 \\ 0 & 0 & 6 & -4 \\ 0 & 0 & -7 & 6 \end{pmatrix} \begin{matrix} -1 \\ 1 \\ 1 \end{matrix}$$

$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 6 & -4 \\ 0 & 0 & -7 & 6 \end{pmatrix}$$

where in the last step we applied column operations, first adding suitable multiples of the first column to all the others, then suitable multiples of column 2 to columns 3 and 4. For our first row operation the determinant of the inverse of the elementary matrix was 2, and later when we multiplied a row by -1 the number we recorded was -1. The determinant of the original matrix is therefore equal to 2 times -1 times the determinant of the simplified matrix we have obtained. We could easily go on with row and column operations and obtain the identity, but there is no need since the determinant of the last matrix above is obviously 8—all but two of the terms in its expansion are zero. Hence the original matrix had determinant -16.

◁≪

---

§8c Expansion along a row

We should show that the definition of the determinant that we have given is consistent with the formula we gave in Chapter Two. We start with some elementary propositions.

8.22 PROPOSITION *Let A be an $r \times r$ matrix. Then for any $n > r$,*

$$\det \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} = \det A$$

where I is the $(n-r) \times (n-r)$ identity.

Proof. If A is an elementary matrix then it is clear that $\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$ is an elementary matrix of the same type, and the result is immediate from 8.15. If $A = E_1 E_2 \dots E_k$ is a product of elementary matrices then, by multiplication of partitioned matrices,

$$\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} = \begin{pmatrix} E_1 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} E_2 & 0 \\ 0 & I \end{pmatrix} \cdots \begin{pmatrix} E_k & 0 \\ 0 & I \end{pmatrix}$$

and by 8.20,

$$\det \begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix} = \prod_{i=1}^{k} \det \begin{pmatrix} E_i & 0 \\ 0 & I \end{pmatrix} = \prod_{i=1}^{k} \det E_i = \det A.$$

Finally, if A is not a product of elementary matrices then it is singular. We leave it as an exercise to prove that $\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$ is also singular and conclude that both determinants are zero. □

Comments ▷▷▷

8.22.1 This result is also easy to derive directly from the definition.

8.22.2 It is clear that exactly the same proof applies for matrices of the form $\begin{pmatrix} I & 0 \\ 0 & A \end{pmatrix}$. ▷▷▷

8.23 PROPOSITION *If C is any $s \times r$ matrix then the $(r+s) \times (r+s)$ matrix*

$$T = \begin{pmatrix} I_r & 0 \\ C & I_s \end{pmatrix}$$

has determinant equal to 1.

Proof. Observe that T is obtainable from the $(r+s) \times (r+s)$ identity by adding appropriate multiples of the first r rows to the last s rows. To be precise, T is the product (in any order) of the elementary matrices $E_{i,r+j}^{(C_{ij})}$ (for $i = 1, 2, \dots, r$ and $j = 1, 2, \dots, s$). Since these elementary matrices all have determinant 1 the result follows. □

8.24 PROPOSITION *For any square matrices A and B and any C of appropriate shape,*

$$\det \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = \det A \det B.$$

The proof of this is left as an exercise.

Using the above propositions we can now give a straightforward proof of the first row expansion formula. If A has (i,j)-entry a_{ij} then the first row of A can be expressed as a linear combination of standard basis rows as follows:

$$\begin{aligned}(\, a_{11} \quad a_{12} \quad \dots \quad a_{1n}\,) = a_{11}\,(\,1 \quad 0 \quad \dots \quad 0\,) + a_{12}\,(\,0 \quad 1 \quad \dots \quad 0\,) + \cdots \\ \cdots + a_{1n}\,(\,0 \quad 0 \quad \dots \quad 1\,).\end{aligned}$$

Since the determinant is a linear function of the first row

$$\begin{aligned}\det A = a_{11} \det \begin{pmatrix} 1 & 0 & \dots & 0 \\ & & A' & \end{pmatrix} + a_{12} \det \begin{pmatrix} 0 & 1 & \dots & 0 \\ & & A' & \end{pmatrix} + \cdots \\ \cdots + a_{1n} \det \begin{pmatrix} 0 & 0 & \dots & 1 \\ & & A' & \end{pmatrix}\end{aligned} \tag{\$}$$

where A' is the matrix obtained from A by deleting the first row. We apply column operations to the matrices on the right hand side to bring the 1's in the first row to the $(1,1)$ position. If e_i is the i^{th} row of the standard basis (having j^{th} entry δ_{ij}) then

$$\begin{pmatrix} e_i \\ A' \end{pmatrix} E_{i,i-1} E_{i-1,i-2} \dots E_{21} = \begin{pmatrix} 1 & 0 \\ * & \tilde{A}_i \end{pmatrix}$$

where A_i is the matrix obtained from A by deleting the 1^{st} row and i^{th} column. (The entries designated by the asterisk are irrelevant, but in fact come from the i^{th} column of A.) Taking determinants now gives

$$\det \begin{pmatrix} e_i \\ A' \end{pmatrix} = (-1)^{i-1} \det A_i = \operatorname{cof}_{1i}(A)$$

by definition of the cofactor. Substituting back in (\$) gives

$$\det A = \sum_{i=1}^{n} a_{1i} \operatorname{cof}_{1i}(A)$$

as required.

We remark that it follows trivially by permuting the rows that one can expand along any row: $\det A = \sum_{k=1}^{n} a_{jk} \operatorname{cof}_{jk}(A)$ is valid for all j. Furthermore, since the determinant of a matrix equals the determinant of its transpose, one can also expand along columns.

Our final result for the chapter deals with the adjoint matrix, and immediately yields the formula for the inverse mentioned in Chapter Two.

8.25 THEOREM *If A is an $n \times n$ matrix then $A(\operatorname{adj} A) = (\det A)I$.*

Proof. Let a_{ij} be the (i,j)-entry of A. The (i,j)-entry of $A(\operatorname{adj} A)$ is

$$\sum_{k=1}^{n} a_{ik} \operatorname{cof}_{jk}(A)$$

(since $\operatorname{adj} A$ is the transpose of the matrix of cofactors). If $i = j$ this is just the determinant of A, by the i^{th} row expansion. So all diagonal entries of $A(\operatorname{adj} A)$ are equal to the determinant.

If the j^{th} row of A is changed to be made equal to the i^{th} row ($i \neq j$) then the cofactors $\operatorname{cof}_{jk}(A)$ are unchanged for all k, but the determinant of the new matrix is zero since it has two equal rows. The j^{th} row expansion for the determinant of this new matrix gives

$$0 = \sum_{k=1}^{n} a_{ik} \operatorname{cof}_{jk}(A)$$

(since the (j,k)-entry of the new matrix is a_{ik}), and we conclude that the off-diagonal entries of $A(\operatorname{adj} A)$ are zero. □

Exercises

1. Compute the given products of permutations.

(i) $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$

(ii) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{bmatrix}$

(*iii*) $\left(\begin{bmatrix}1&2&3&4\\2&1&4&3\end{bmatrix}\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}\right)\begin{bmatrix}1&2&3&4\\4&3&1&2\end{bmatrix}$

(*iv*) $\begin{bmatrix}1&2&3&4\\2&1&4&3\end{bmatrix}\left(\begin{bmatrix}1&2&3&4\\2&3&4&1\end{bmatrix}\begin{bmatrix}1&2&3&4\\4&3&1&2\end{bmatrix}\right)$

2. Calculate the parity of each permutation appearing in Exercise 1.

3. Let σ and τ be permutations of $\{1, 2, \ldots, n\}$. Let S be the matrix with $(i,j)^{\text{th}}$ entry equal to 1 if $i = \sigma(j)$ and 0 if $i \neq \sigma(j)$, and similarly let T be the matrix with $(i,j)^{\text{th}}$ entry 1 if $i = \tau(j)$ and 0 otherwise. Prove that the $(i,j)^{\text{th}}$ entry of ST is 1 if $i = \sigma\tau(j)$ and 0 otherwise.

4. Prove Proposition 8.11.

5. Use row and column operations to calculate the determinant of

$$\begin{pmatrix}1&5&11&2\\2&11&-6&8\\-3&0&-452&6\\-3&-16&-4&13\end{pmatrix}$$

6. Consider the determinant

$$\det\begin{vmatrix}1&x_1&x_1^2&\ldots&x_1^{n-1}\\1&x_2&x_2^2&\ldots&x_2^{n-1}\\\vdots&\vdots&\vdots&&\vdots\\1&x_n&x_n^2&\ldots&x_n^{n-1}\end{vmatrix}.$$

Use row and column operations to evaluate this in the case $n = 3$. Then do the case $n = 4$. Then do the general case. (The answer is $\prod_{i>j}(x_i - x_j)$.)

7. Let $p(x) = a_0 + a_1x + a_2x^2$, $q(x) = b_0 + b_1x + b_2x^2$, $r(x) = c_0 + c_1x + c_2x^2$. Prove that

$$\det\begin{vmatrix}p(x_1)&q(x_1)&r(x_1)\\p(x_2)&q(x_2)&r(x_2)\\p(x_3)&q(x_3)&r(x_3)\end{vmatrix} = (x_2-x_1)(x_3-x_1)(x_3-x_2)\det\begin{vmatrix}a_0&b_0&c_0\\a_1&b_1&c_1\\a_2&b_2&c_2\end{vmatrix}.$$

8. Prove that if A is singular then so is $\begin{pmatrix} A & 0 \\ 0 & I \end{pmatrix}$.

9. Use 8.22 and 8.23 to prove that

$$\det \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} = \det A \det B.$$

(Hint: Factorize the matrix on the left hand side.)

10. (*i*) Write out the details of the proof of the first part of Proposition 8.8.

(*ii*) Modify the proof of the second part of 8.8 to show that any $\sigma \in S_n$ can be written as a product of $l(\sigma)$ simple transpositions.

(*iii*) Use 8.7 to prove that $\sigma \in S_n$ cannot be written as a product of fewer than $l(\sigma)$ simple transpositions.

(Because of these last two properties, $l(\sigma)$ may be termed the *length* of σ.)

9

Classification of linear operators

A *linear operator* on a vector space V is a linear transformation from V to V. We have already seen that if $T\colon V \to W$ is linear then there exist bases of V and W for which the matrix of T has a simple form. However, for an operator T the domain V and codomain W are the same, and it is natural to insist on using the same basis for each when calculating the matrix. Accordingly, if $T\colon V \to V$ is a linear operator on V and $\boldsymbol{b}$ is a basis of V, we call $\mathrm{M}_{\boldsymbol{bb}}(T)$ the *matrix of T relative to $\boldsymbol{b}$*; the problem is to find a basis of V for which the matrix of T is as simple as possible.

Tackling this problem naturally involves us with more eigenvalue theory.

§9a Similarity of matrices

9.1 Definition Square matrices A and B are said to be *similar* if there exists a nonsingular matrix X with $A = X^{-1}BX$.

It is an easy exercise to show that similarity is an equivalence relation on $\mathrm{Mat}(n \times n, F)$.

We proved in 7.8 that if $\boldsymbol{b}$ and $\boldsymbol{c}$ are two bases of a space V and T is a linear operator on V then the matrix of T relative to $\boldsymbol{b}$ and the matrix of T relative to $\boldsymbol{c}$ are similar. Specifically, if $A = \mathrm{M}_{\boldsymbol{bb}}(T)$ and $B = \mathrm{M}_{\boldsymbol{cc}}(T)$ then $B = X^{-1}AX$ where $X = \mathrm{M}_{\boldsymbol{bc}}$, the $\boldsymbol{c}$ to $\boldsymbol{b}$ transition matrix. Moreover, since any invertible matrix can be a transition matrix (see Exercise 8 of Chapter Four), finding a simple matrix for a given linear operator corresponds exactly to finding a simple matrix similar to a given one.

In this context, 'simple' means 'as near to diagonal as possible'. We investigated diagonalizing real matrices in Chapter One, but failed to mention the fact that not all matrices are diagonalizable. It is true, however, that many—and over some fields most—matrices are are diagonalizable; for

instance, we will show that if an $n \times n$ matrix has n distinct eigenvalues then it is diagonalizable.

The following definition provides a natural extension of concepts previously introduced.

9.2 DEFINITION Let $A \in \mathrm{Mat}(n \times n, F)$ and $\lambda \in F$. The set of all $v \in F^n$ such that $Av = \lambda v$ is called the λ-*eigenspace* of A.

Comments ▷▷▷

9.2.1 Observe that λ is an eigenvalue if and only if the λ-eigenspace is nonzero.

9.2.2 The λ-eigenspace of A contains zero and is closed under addition and scalar multiplication. Hence it is a subspace of F^n.

9.2.3 Since $Av = \lambda v$ if and only if $(A - \lambda I)v = 0$ we see that the λ-eigenspace of A is exactly the right null space of $A - \lambda I$. This is nonzero if and only if $A - \lambda I$ is singular.

9.2.4 We can equally well use rows instead of columns, defining the *left eigenspace* to be the set of all $v \in {}^{\mathrm{t}}F^n$ satisfying $vA = \lambda v$. For square matrices the left and right null spaces have the same dimension; hence the eigenvalues are the same whether one uses rows or columns. However, there is no easy way to calculate the left (row) eigenvectors from the right (column) eigenvectors, or vice versa. ▷▷▷

The same terminology is also applied to linear operators. The λ-eigenspace of $T\colon V \to V$ is the set of all $v \in V$ such that $T(v) = \lambda v$. That is, it is the kernel of the linear operator $T - \lambda\mathtt{i}$, where $\mathtt{i}$ is the identity operator on V. And λ is an eigenvalue of T if and only if the λ-eigenspace of T is nonzero. If $\boldsymbol{b}$ is any basis of V then the eigenvalues of T are the same as the eigenvalues of $\mathrm{M}_{\boldsymbol{bb}}(T)$, and v is in the λ-eigenspace of T if and only if $\mathrm{cv}_{\boldsymbol{b}}(v)$ is in the λ-eigenspace of $\mathrm{M}_{\boldsymbol{bb}}(T)$.

Since choosing a different basis for V replaces the matrix of T by a similar matrix, the above remarks indicate that similar matrices must have the same eigenvalues. In fact, more is true: similar matrices have the same characteristic polynomial. This enables us to define the characteristic polynomial $c_T(x)$ of a linear operator T to be the characteristic polynomial of $\mathrm{M}_{\boldsymbol{bb}}(T)$, for arbitrarily chosen $\boldsymbol{b}$. That is, $c_T(x) = \det(\mathrm{M}_{\boldsymbol{bb}}(T) - xI)$.

9.3 PROPOSITION *Similar matrices have the same characteristic polynomial.*

Proof. Suppose that A and B are similar matrices. Then there exists a nonsingular P with $A = P^{-1}BP$. Now

$$\begin{aligned}\det(A - xI) &= \det(P^{-1}BP - xP^{-1}P) \\ &= \det\big((P^{-1}B - xP^{-1})P\big) \\ &= \det\big(P^{-1}(B - xI)P\big) \\ &= \det P^{-1} \det(B - xI) \det P,\end{aligned}$$

where we have used the fact that the scalar x commutes with the matrix P^{-1}, and the multiplicative property of determinants. In the last line above we have the product of three scalars, and since multiplication of scalars is commutative this last line equals

$$\det P^{-1} \det P \det(B - xI) = \det(P^{-1}P) \det(B - xI) = \det(B - xI)$$

since $\det I = 1$. Hence $\det(A - xI) = \det(B - xI)$, as required. □

The next proposition gives the precise criterion for diagonalizability of a matrix.

9.4 PROPOSITION *(i) If $A \in \mathrm{Mat}(n \times n, F)$ then A is diagonalizable if and only if there is a basis of F^n consisting entirely of eigenvectors for A.*

(ii) If A, $X \in \mathrm{Mat}(n \times n, F)$ and X is nonsingular then $X^{-1}AX$ is diagonal if and only if the columns of X are all eigenvectors of A.

Proof. Since a matrix $X \in \mathrm{Mat}(n \times n, F)$ is nonsingular if and only if its columns are a basis for F^n the first part is a consequence of the second. If the columns of X are $\underset{\sim}{t}_1, \underset{\sim}{t}_2, \ldots, \underset{\sim}{t}_n$ then the i^{th} column of AX is $A\underset{\sim}{t}_i$, while the i^{th} column of $X \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is $\lambda_i \underset{\sim}{t}_i$. So $AX = X \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ if and only if for each i the column $\underset{\sim}{t}_i$ is in the λ_i-eigenspace of A, and the result follows. □

It is perhaps more natural to state the above criterion for operators rather than matrices. A linear operator $T: V \to V$ is said to be *diagonalizable* if there is a basis $\boldsymbol{b}$ of V such that $\mathrm{M}_{\boldsymbol{bb}}(T)$ is a diagonal matrix. Now if $\boldsymbol{b} = (v_1, v_2, \ldots, v_n)$ then

$$\mathrm{M}_{\boldsymbol{bb}}(T) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

if and only if $T(v_i) = \lambda_i v_i$ for all i. Hence we have proved the following:

9.5 Proposition *A linear operator T on a vector space V is diagonalizable if and only if there is a basis of V consisting entirely of eigenvectors of T. If T is diagonalizable and $\boldsymbol{b}$ is such a basis of eigenvectors, then $\mathrm{M}_{\boldsymbol{bb}}(T)$, the matrix of T relative to $\boldsymbol{b}$, is $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, where λ_i is the eigenvalue corresponding to the i^{th} basis vector.*

Of course, if $\boldsymbol{c}$ is an arbitrary basis of V then T is diagonalizable if and only if $\mathrm{M}_{\boldsymbol{cc}}(T)$ is.

When one wishes to diagonalize a matrix $A \in \mathrm{Mat}(n \times n, F)$ the procedure is to first solve the characteristic equation to find the eigenvalues, and then for each eigenvalue λ find a basis for the λ-eigenspace by solving the simultaneous linear equations $(A - \lambda I)\underset{\sim}{x} = \underset{\sim}{0}$. Then one combines all the elements from the bases for all the different eigenspaces into a single sequence, hoping thereby to obtain a basis for F^n. Two questions naturally arise: does this combined sequence necessarily span F^n, and is it necessarily linearly independent? The answer to the first of these questions is no, as we will soon see by examples, but the answer to the second is yes. This follows from our next theorem.

9.6 Theorem *Let $T: V \to V$ be a linear operator, and let the distinct eigenvalues of T be $\lambda_1, \lambda_2, \ldots, \lambda_k$. For each i let V_i be the λ_i-eigenspace. Then the spaces V_i are independent. That is, if U is the subspace defined by*

$$U = V_1 + V_2 + \cdots + V_k = \{\, v_1 + v_2 + \cdots + v_k \mid v_i \in V_i \text{ for all } i \,\}$$

then $U = V_1 \oplus V_2 \oplus \cdots \oplus V_k$.

Proof. We use induction on r to prove that for all $r \in \{1, 2, \ldots, n\}$ the spaces $V_1, V_2, \ldots, V_r$ are independent. This is trivially true in the case $r = 1$.

Suppose then that $r > 1$ and that $V_1, V_2, \ldots, V_{r-1}$ are independent; we seek to prove that $V_1, V_2, \ldots, V_r$ are independent. According to Definition 6.7, our task is to prove the following statement:

($) If $u_i \in V_i$ for $i = 1, 2, \ldots, r$ and $\sum_{i=1}^{r} u_i = 0$ then each $u_i = 0$.

Assume that we have elements u_i satisfying the hypotheses of ($). Since T is linear we have

$$0 = T(0) = T\big(\sum_{i=1}^{r} u_i\big) = \sum_{i=1}^{r} T(u_i) = \sum_{i=1}^{r} \lambda_i u_i$$

since u_i is in the λ_i-eigenspace of T. Multiplying the equation $\sum_{i=1}^{r} u_i = 0$ by λ_r and combining with the above allows us to eliminate u_r, and we obtain

$$\sum_{i=1}^{r-1} (\lambda_i - \lambda_r) u_i = 0.$$

Since the i^{th} term in this sum is in the space V_i and our inductive hypothesis is that $V_1, V_2, \ldots, V_{r-1}$ are independent, it follows that $(\lambda_i - \lambda_r)u_i = 0$ for $i = 1, 2, \ldots, r-1$. Since the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$ were assumed to be all distinct we have that each $\lambda_i - \lambda_r$ above is nonzero, and multiplying through by $(\lambda_i - \lambda_r)^{-1}$ gives $u_i = 0$ for $i = 1, 2, \ldots, r-1$. Since $\sum_{i=1}^{r} u_i = 0$ it follows that $u_r = 0$ also. This proves ($) and completes our induction. □

As an immediate consequence of this we may rephrase our diagonalizability criterion:

9.7 Corollary *A linear operator $T: V \to V$ is diagonalizable if and only V is the direct sum of eigenspaces of T.*

Proof. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of T and let $V_1, \ldots, V_k$ be the corresponding eigenspaces. If V is the direct sum of the V_i then by 6.9 a basis of V can be obtained by concatenating bases of $V_1, \ldots, V_k$, which results in a basis of V consisting of eigenvectors of T and shows that T is diagonalizable. Conversely, assume that T is diagonalizable, and let $\boldsymbol{b} = (x_1, x_2, \ldots, x_n)$ be a basis of V consisting of eigenvectors of T. Let $I = \{1, 2, \ldots, n\}$, and for each $j = 1, 2, \ldots, k$ let $I_j = \{\, i \in I \mid x_i \in V_j \}$.

Each x_i lies in some eigenspace; so I is the union of the I_j. Since B spans V, for each $v \in V$ there exist scalars λ_i such that

$$v = \sum_{i\in I} \lambda_i v_i = \sum_{i\in I_1} \lambda_i x_i + \sum_{i\in I_2} \lambda_i x_i + \cdots + \sum_{i\in I_k} \lambda_i x_i.$$

Writing $u_j = \sum_{i\in I_j} \lambda_i x_i$ we have that $u_j \in V_j$, and

$$v = u_1 + u_2 + \cdots + u_k \in V_1 + V_2 + \cdots + V_k.$$

Since the sum $\sum_{j=1}^{k} V_j$ is direct (by 9.6) and since we have shown that every element of V lies in this subspace, we have shown that V is the direct sum of eigenspaces of T, as required. □

The implication of the above for the practical problem of diagonalizing an $n \times n$ matrix is that if the sum of the dimensions of the eigenspaces is n then the matrix is diagonalizable, otherwise the sum of the dimensions is less than n and it is not diagonalizable.

—Example—

#1 Is the the following matrix A diagonalizable?

$$A = \begin{pmatrix} -2 & 1 & -1 \\ 2 & -1 & 2 \\ 4 & -1 & 3 \end{pmatrix}$$

⋙▷ Expanding the determinant

$$\det \begin{pmatrix} -2-x & 1 & -1 \\ 2 & -1-x & 2 \\ 4 & -1 & 3-x \end{pmatrix}$$

we find that

$$(-2-x)(-1-x)(3-x) - (-2-x)(-1)(2) - (1)(2)(3-x) \\ +(1)(2)(4) + (-1)(2)(-1) - (-1)(-1-x)(4)$$

is the characteristic polynomial of A. (Note that for calculating characteristic polynomials it seems to be easier to work with the first row expansion

technique, rather than attempt to do row operations with polynomials.) Simplifying the above expression and factorizing it gives $-(x+1)^2(x-2)$, so that the eigenvalues are -1 and 2. When, as here, the characteristic equation has a repeated root, one must hope that the dimension of the corresponding eigenspace is equal to the multiplicity of the root; it cannot be more, and if it is less then the matrix is not diagonalizable.

Alas, in this case it is less. Solving

$$\begin{pmatrix} -1 & 1 & -1 \\ 2 & 0 & 2 \\ 4 & -1 & 4 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

we find that the solution space has dimension one, $\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$ being a basis. For the other eigenspace (for the eigenvalue 2) one must solve

$$\begin{pmatrix} -4 & 1 & -1 \\ 2 & -3 & 2 \\ 4 & -1 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

and we obtain solution space of dimension one with $\begin{pmatrix} -1 \\ 6 \\ 10 \end{pmatrix}$ as basis. The sum of the dimensions of the eigenspaces is not sufficient; the matrix is not diagonalizable. ⊲⋘

Here is a practical point which deserves some emphasis. If when calculating the eigenspace corresponding to some eigenvalue λ you find that the equations have only the trivial solution zero, then you have made a mistake. Either λ was not an eigenvalue at all and you made a mistake when solving the characteristic equation, or else you have made a mistake solving the linear equations for the eigenspace. By definition, an eigenvalue of A is a λ for which the equations $(A - \lambda I)v = 0$ have a nontrivial solution v.

§9b Invariant subspaces

9.8 Definition If T is an operator on V and U is a subspace of V then U is said to be *invariant* under T if $T(u) \in U$ for all $u \in U$.

Observe that the 1-dimensional subspace spanned by an eigenvector of T is invariant under T. Conversely, if a 1-dimensional subspace is T-invariant then it must be contained in an eigenspace.

—***Example***—

#2 Let A be a $n \times n$ matrix. Prove that the column space of A is invariant under left multiplication by $A^3 + 5A - 2I$.

⋙▷ We know that the column space of A equals $\{\, Av \mid v \in F^n \,\}$. Multiplying an arbitrary element of this on the left by $A^3+5A-2I$ yields another element of the same space:

$$(A^3 + 5A - 2I)Av = (A^4 + 5A^2 - 2A)v = A(A^3 + 5A - 2I)v = Av'$$

where $v' = (A^3 + 5A - 2I)v$. ◁⋘

Discovering T-invariant subspaces aids one's understanding of the operator T, since it enables T to be described in terms of operators on lower dimensional subspaces.

9.9 THEOREM *Let T be an operator on V and suppose that $V = U \oplus W$ for some T-invariant subspaces U and W. If $\boldsymbol{b}$ and $\boldsymbol{c}$ are bases of U and W then the matrix of T relative to the basis $(\boldsymbol{b}, \boldsymbol{c})$ of V is*

$$\begin{pmatrix} \mathrm{M}_{\boldsymbol{bb}}(T_U) & 0 \\ 0 & \mathrm{M}_{\boldsymbol{cc}}(T_W) \end{pmatrix}$$

where T_U and T_W are the operators on U and W given by restricting T to these subspaces.

Proof. Let $\boldsymbol{b} = (v_1, v_2, \ldots, v_r)$ and $\boldsymbol{c} = (v_{r+1}, v_{r+2}, \ldots, v_n)$, and write $B = \mathrm{M}_{\boldsymbol{bb}}(T_U)$, $C = \mathrm{M}_{\boldsymbol{cc}}(T_W)$. Let A be the matrix of T relative to the combined basis $(v_1, v_2, \ldots, v_n)$. If $j \le r$ then $v_j \in U$ and so

$$\sum_{i=1}^{n} A_{ij} v_i = T(v_j) = T_U(v_j) = \sum_{i=1}^{r} B_{ij} v_i$$

and by linear independence of the v_i we deduce that $A_{ij} = B_{ij}$ for $i \le r$ and $A_{ij} = 0$ for $i > r$. This gives

$$A = \begin{pmatrix} B & * \\ 0 & * \end{pmatrix}$$

and a similar argument for the remaining basis vectors v_j completes the proof. □

Comment ▷▷▷

9.9.1 In the situation of this theorem it is common to say that T is the direct sum of T_U and T_W, and to write $T = T_U \oplus T_W$. The matrix in the theorem statement can be called the *diagonal sum* of $\mathrm{M}_{\boldsymbol{bb}}(T_U)$ and $\mathrm{M}_{\boldsymbol{cc}}(T_W)$. ▷▷▷

—***Example***—

#3 Describe geometrically the effect on 3-dimensional Euclidean space of the operator T defined by

$$(\star) \qquad T\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -2 & 1 & -2 \\ 4 & 1 & 2 \\ 2 & -3 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

≫▷ Let A be the 3×3 matrix in $(\star)$. We look first for eigenvectors of A (corresponding to 1-dimensional T-invariant subspaces). Since

$$\det\begin{pmatrix} -2-x & 1 & -2 \\ 4 & 1-x & 2 \\ 2 & -3 & 3-x \end{pmatrix} = x^3 - 2x^2 + x - 2 = (x^2+1)(x-2)$$

we find that 2 is an eigenvalue, and solving

$$\begin{pmatrix} -4 & 1 & -2 \\ 4 & -1 & 2 \\ 2 & -3 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

we find that $v_1 = {}^{\mathrm{t}}(\,-1 \quad 0 \quad 2\,)$ spans the 2-eigenspace.

The other eigenvalues of A are complex. However, since $\ker(T - 2\mathtt{i})$ has dimension 1, we deduce that $\mathrm{im}(T - 2\mathtt{i})$ is a 2-dimensional T-invariant subspace. Indeed, $\mathrm{im}(T - 2\mathtt{i})$ is the column space of $A - 2I$, which is clearly of dimension 2 since the first column is twice the third. We may choose a basis (v_2, v_3) of this subspace by choosing v_2 arbitrarily (for instance, let v_2 be the third column of $A - 2I$) and letting $v_3 = T(v_2)$. (We make this choice simply so that it is easy to express $T(v_2)$ in terms of v_2 and v_3.) A quick calculation in fact gives that $v_3 = {}^{\mathrm{t}}(\,4 \quad -4 \quad -7\,)$ and $T(v_3) = -v_2$. It is easily checked that v_1, v_2 and v_3 are linearly independent and hence form a basis of $\mathbb{R}^3$, and the action of T is given by the equations $T(v_1) = 2v_1$,

$T(v_2) = v_3$ and $T(v_3) = -v_2$. In matrix terms, the matrix of T relative to this basis is

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

On the one-dimensional subspace spanned by v_1 the action of T is just multiplication by 2. Its action on the two dimensional subspace spanned by v_2 and v_3 is also easy to visualize. If v_2 and v_3 were orthogonal to each other and of equal lengths then $v_2 \mapsto v_3$ and $v_3 \mapsto -v_2$ would give a rotation through 90°. Although they are not orthogonal and equal in length the action of T on the plane spanned by v_2 and v_3 is nonetheless rather like a rotation through 90°: it is what the rotation would become if the plane were "squashed" so that the axes are no longer perpendicular. Finally, an arbitrary point is easily expressed (using the parallelogram law) as a sum of a multiple of v_1 and something in the plane of v_2 and v_3. The action of T is to double the v_1 component and "rotate" the (v_2, v_3) part. ⊲⊣≪

If U is an invariant subspace which does not have an invariant complement W it is still possible to obtain some simplification. Choose a basis $\boldsymbol{b} = (v_1, v_2, \ldots, v_r)$ of U and extend it to a basis $(v_1, v_2, \ldots, v_n)$ of V. Exactly as in the proof of 9.9 above we see that the matrix of T relative to this basis has the form $\begin{pmatrix} B & D \\ 0 & C \end{pmatrix}$, for $B = \mathrm{M}_{\boldsymbol{bb}}(T_U)$ and some matrices C and D. A little thought shows that

$$T_{V/U}\colon v + U \mapsto T(v) + U$$

defines an operator $T_{V/U}$ on the quotient space V/U, and that C is the matrix of $T_{V/U}$ relative to the basis $(v_{r+1} + U, v_{r+2} + U, \ldots, v_n + U)$. It is less easy to describe the significance of the matrix D.

The characteristic polynomial also simplifies when invariant subspaces are found.

9.10 Theorem *Suppose that $V = U \oplus W$ where U and W are T-invariant, and let T_1, T_2 be the operators on U and W given by restricting T. If $f_1(x)$, $f_2(x)$ are the characteristic polynomials of T_1, T_2 then the characteristic polynomial of T is the product $f_1(x)f_2(x)$.*

Proof. Choose bases $\boldsymbol{b}$ and $\boldsymbol{c}$ of U and W, and let B and C be the corresponding matrices of T_1 and T_2. Using 9.9 we find that the characteristic polynomial of T is

$$c_T(x) = \det \begin{pmatrix} B - xI & 0 \\ 0 & C - xI \end{pmatrix} = \det(B - xI) \det(C - xI) = f_1(x) f_2(x)$$

(where we have used 8.24) as required. □

In fact we do not need a direct decomposition for this. If U is a T-invariant subspace then the characteristic polynomial of T is the product of the characteristic polynomials of T_U and $T_{V/U}$, the operators on U and V/U induced by T. As a corollary it follows that the dimension of the λ-eigenspace of an operator T is at most the multiplicity of $x - \lambda I$ as a factor of the characteristic polynomial $c_T(x)$.

9.11 Proposition *Let U be the λ-eigenspace of T and let $r = \dim U$. Then $c_T(x)$ is divisible by $(x - \lambda)^r$.*

Proof. Relative to a basis $(v_1, v_2, \ldots, v_n)$ of V such that $(v_1, v_2, \ldots, v_r)$ is a basis of U, the matrix of T has the form $\begin{pmatrix} \lambda I_r & D \\ 0 & C \end{pmatrix}$. By 8.24 we deduce that $c_T(x) = (\lambda - x)^r \det(C - xI)$. □

§9c Algebraically closed fields

Up to now the field F has played only a background role, and which field it is has been irrelevant. But it is not true that all fields are equivalent, and differences between fields are soon encountered when solving polynomial equations. For instance, over the field $\mathbb{R}$ of real numbers the polynomial $x^2 + 1$ has no roots (and so the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ has no eigenvalues), but over the field $\mathbb{C}$ of complex numbers it has two roots, i and $-i$. So which field one is working over has a big bearing on questions of diagonalizability. (For example, the above matrix is not diagonalizable over $\mathbb{R}$ but is diagonalizable over $\mathbb{C}$.)

9.12 Definition A field F is said to be *algebraically closed* if every polynomial of degree greater than zero with coefficients in F has a zero in F.

A trivial induction based on the definition shows that over an algebraically closed field every polynomial of degree greater than zero can be expressed as a product of factors of degree one. In particular

9.13 Proposition *If F is an algebraically closed field then for every matrix $A \in \mathrm{Mat}(n \times n, F)$ there exist $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$ (not necessarily distinct) such that*

$$c_A(x) = (\lambda_1 - x)(\lambda_2 - x) \ldots (\lambda_n - x)$$

(where $c_A(x)$ is the characteristic polynomial of A).

As a consequence of 9.13 the analysis of linear operators is significantly simpler if the ground field is algebraically closed. Because of this it is convenient to make use of complex numbers when studying linear operators on real vector spaces.

9.14 The Fundamental Theorem of Algebra *The complex field $\mathbb{C}$ is algebraically closed.*

The traditional name of this theorem is somewhat inappropriate, since it is proved by methods of complex analysis. We will not prove it here. There is an important theorem, which really is a theorem of algebra, which asserts that for every field F there is an algebraically closed field containing F as a subfield. The proof of this is also beyond the scope of this book, but it proceeds by "adjoining" new elements to F, in much the same way as $\sqrt{-1}$ is adjoined to $\mathbb{R}$ in the construction of $\mathbb{C}$.

§9d Generalized eigenspaces

Let T be a linear operator on an n-dimensional vector space V and suppose that the characteristic polynomial of T can be factorized into factors of degree one:

$$c_T(x) = (\lambda_1 - x)^{m_1}(\lambda_2 - x)^{m_2} \ldots (\lambda_k - x)^{m_k}$$

where $\lambda_i \neq \lambda_j$ for $i \neq j$. (If the field F is algebraically closed this will always be the case.) Let V_i be the λ_i-eigenspace and let $n_i = \dim V_i$. Certainly $n_i \geq 1$ for each i, since λ_i is an eigenvalue of T; so, by 9.11,

9.14.1 $$1 \leq n_i \leq m_i \text{ for all } i = 1, 2, \ldots, k.$$

If $m_i = 1$ for all i then since c_T has degree n (by Exercise 12 of Chapter Two) it follows that $k = n$ and

$$\dim(V_1 \oplus V_2 \oplus \cdots \oplus V_k) = \sum_{i=1}^{n} \dim V_i = n = \dim V$$

so that V is the direct sum of the eigenspaces.

If the m_i are not all equal to 1 then, as we have seen by example, V need not be the sum of the eigenspaces $V_i = \ker(T - \lambda_i \mathtt{i})$. A question immediately suggests itself: instead of V_i, should we perhaps use $W_i = \ker(T - \lambda_i \mathtt{i})^{m_i}$?

9.15 Definition Let λ be an eigenvalue of the operator T and let m be the multiplicity of $\lambda - x$ as a factor of the characteristic polynomial $c_T(x)$. Then $\ker(T - \lambda\mathtt{i})^m$ is called the *generalized λ-eigenspace* of T.

9.16 Proposition *Let T be a linear operator on V. The generalized eigenspaces of T are T-invariant subspaces of V.*

Proof. It is immediate from Definition 9.15 and Theorem 3.13 that generalized eigenspaces are subspaces; hence invariance is all that needs to be proved.

Let λ be an eigenvalue of T and m the multiplicity of $x-\lambda$ in $c_T(x)$, and let W be the generalized λ-eigenspace of T. By definition, $v \in W$ if and only if $(T-\lambda\mathtt{i})^m(v) = 0$; let v be such an element. Since $(T-\lambda\mathtt{i})^m T = T(T-\lambda\mathtt{i})^m$ we see that

$$(T - \lambda\mathtt{i})^m(T(v)) = T((T - \lambda\mathtt{i})^m(v)) = T(0) = 0,$$

and it follows that $T(v) \in W$. Thus $T(v) \in W$ for all $v \in W$, as required. □

If $(T-\lambda\mathtt{i})^i(x) = 0$ then clearly $(T-\lambda\mathtt{i})^j(x) = 0$ whenever $j \geq i$. Hence

9.16.1 $$\ker(T - \lambda\mathtt{i}) \subseteq \ker(T - \lambda\mathtt{i})^2 \subseteq \ker(T - \lambda\mathtt{i})^3 \subseteq \cdots$$

and in particular the λ-eigenspace of T is contained in the generalized λ-eigenspace. Because our space V is finite dimensional the subspaces in the chain 9.16.1 cannot get arbitrarily large. We will show below that in fact the generalized eigenspace is the largest, the subsequent terms in the chain all being equal:

$$\ker(T - \lambda\mathtt{i})^m = \ker(T - \lambda\mathtt{i})^{m+1} = \ker(T - \lambda\mathtt{i})^{m+2} = \cdots$$

where m is the multiplicity of $x - \lambda$ in $c_T(x)$.

9.17 LEMMA *Let $S: V \to V$ be a linear operator and $x \in V$. If r is a positive integer such that $S^r(x) = 0$ but $S^{r-1}(x) \neq 0$ then the elements $x, S(x), \ldots, S^{r-1}(x)$ are linearly independent.*

Proof. Suppose that $\lambda_0 x + \lambda_1 S(x) + \cdots + \lambda_{r-1} S^{r-1}(x) = 0$ and suppose that the scalars λ_i are not all zero. Choose k minimal such that $\lambda_k \neq 0$. Then the above equation can be written as

$$\lambda_k S^k(x) + \lambda_{k+1} S^{k+1}(x) + \cdots + \lambda_{r-1} S^{r-1}(x) = 0.$$

Applying S^{r-k-1} to both sides gives

$$\lambda_k S^{r-1}(x) + \lambda_{k+1} S^r(x) + \cdots + \lambda_{r-1} S^{2r-k-2}(x) = 0$$

and this reduces to $\lambda_k S^{r-1}(x) = 0$ since $S^i(x) = 0$ for $i \geq r$. This contradicts 3.7 since both λ_k and $S^{r-1}(x)$ are nonzero. □

9.18 PROPOSITION *Let $T: V \to V$ be a linear operator, and let λ and m be as in Definition 9.15. If r is an integer such that $\ker(T-\lambda\mathtt{i})^r \neq \ker(T-\lambda\mathtt{i})^{r-1}$ then $r \leq m$.*

Proof. By 9.16.1 we have $\ker(T-\lambda\mathtt{i})^{r-1} \subseteq \ker(T-\lambda\mathtt{i})^r$; so if they are not equal there must be an x in $\ker(T-\lambda\mathtt{i})^r$ and not in $\ker(T-\lambda\mathtt{i})^{r-1}$. Given such an x, define $x_i = (T-\lambda\mathtt{i})^i(x)$ for i from 1 to r, noting that this gives

9.18.1 $$T(x_i) = \begin{cases} \lambda x_i + x_{i+1} & (\text{for } i = 1, 2, \ldots, r-1) \\ \lambda x_i & (\text{for } i = r). \end{cases}$$

Lemma 9.17, applied with $S = T - \lambda\mathtt{i}$, shows that $x_1, x_2, \ldots, x_r$ are linearly independent, and by 4.10 there exist $x_{r+1}, x_{r+2} \ldots, x_n \in V$ such that $\boldsymbol{b} = (x_1, x_2, \ldots, x_n)$ is a basis.

The first r columns of $\mathrm{M}_{\boldsymbol{bb}}(T)$ can be calculated using 9.18.1, and we find that

$$\mathrm{M}_{\boldsymbol{bb}}(T) = \begin{pmatrix} J_r(\lambda) & C \\ 0 & D \end{pmatrix}$$

for some $D \in \mathrm{Mat}((n-r) \times (n-r), F)$ and $C \in \mathrm{Mat}(r \times (n-r), F)$, where $J_r(\lambda) \in \mathrm{Mat}(r \times r, F)$ is the matrix

9.18.2 $$J_r(\lambda) = \begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & 0 \\ 0 & 0 & 0 & \ldots & 1 & \lambda \end{pmatrix}$$

(having diagonal entries equal to λ, entries immediately below the diagonal equal to 1, and all other entries zero).

Since $J_r(\lambda) - xI$ is lower triangular with all diagonal entries equal to $\lambda - x$ we see that

$$\det(J_r(\lambda) - xI) = (\lambda - x)^r$$

and hence the characteristic polynomial of $\mathrm{M}_{\boldsymbol{bb}}(T)$ is $(\lambda - x)^r f(x)$, where $f(x)$ is the characteristic polynomial of D. So $c_T(x)$ is divisible by $(x - \lambda)^r$. But by definition the multiplicity of $x - \lambda$ in $c_T(x)$ is m; so we must have $r \leq m$. □

It follows from Proposition 9.18 that the intersection of $\ker(T - \lambda\mathtt{i})^m$ and $\mathrm{im}(T - \lambda\mathtt{i})^m$ is $\{0\}$. For if $x \in \mathrm{im}(T - \lambda\mathtt{i})^m \cap \ker(T - \lambda\mathtt{i})^m$ then $x = (T - \lambda\mathtt{i})^m(y)$ for some y, and $(T - \lambda\mathtt{i})^m(x) = 0$. But from this we deduce that $(T - \lambda\mathtt{i})^{2m}(y) = 0$, whence

$$y \in \ker(T - \lambda\mathtt{i})^{2m} = \ker(T - \lambda\mathtt{i})^m \qquad \text{(by 9.18)}$$

and it follows that $x = (T - \lambda\mathtt{i})^m(y) = 0$.

9.19 Theorem *In the above situation,*

$$V = \ker(T - \lambda\mathtt{i})^m \oplus \mathrm{im}(T - \lambda\mathtt{i})^m.$$

Proof. We have seen that $\ker(T - \lambda\mathtt{i})^m$ and $\mathrm{im}(T - \lambda\mathtt{i})^m$ have trivial intersection, and hence their sum is direct. Now by Theorem 6.9 the dimension of $\ker(T - \lambda\mathtt{i})^m \oplus \mathrm{im}(T - \lambda\mathtt{i})^m$ equals $\dim(\ker(T - \lambda\mathtt{i})^m) + \dim(\mathrm{im}(T - \lambda\mathtt{i})^m)$, which equals the dimension of V by the Main Theorem on Linear Transformations. Since $\ker(T - \lambda\mathtt{i})^m \oplus \mathrm{im}(T - \lambda\mathtt{i})^m \subseteq V$ the result follows. □

Let $U = \ker(T - \lambda\mathtt{i})^m$ (the generalized eigenspace) and let W be the image of $(T - \lambda\mathtt{i})^m$. We have seen that U is T-invariant, and it is equally easy to see that W is T-invariant. Indeed, if $x \in W$ then $x = (T - \lambda\mathtt{i})^m(y)$ for some y, and hence

$$T(x) = T((T - \lambda\mathtt{i})^m(y) = (T - \lambda\mathtt{i})^m(T(y)) \in \mathrm{im}(T - \lambda\mathtt{i})^m = W.$$

By 9.10 we have that $c_T(x) = f(x)g(x)$ where $f(x)$ and $g(x)$ are the characteristic polynomials of T_U and T_W, the restrictions of T to U and W.

Let μ be an eigenvalue of T_U. Then $T(x) = \mu x$ for some nonzero $x \in U$, and this gives $(T - \lambda\mathtt{i})(x) = (\mu - \lambda)x$. It follows easily by induction that $(T - \lambda\mathtt{i})^m(x) = (\mu - \lambda)^m x$, and therefore $(\mu - \lambda)^m x = 0$ since $x \in U = \ker(T - \lambda\mathtt{i})^m$. But $x \neq 0$; so we must have $\mu = \lambda$. We have proved that λ is the only eigenvalue of T_U.

On the other hand, λ is not an eigenvalue of T_W, since if it were then we would have $(T - \lambda\mathtt{i})(x) = 0$ for some nonzero $x \in W$, a contradiction since $\ker(T - \lambda\mathtt{i}) \subseteq U$ and $U \cap W = \{0\}$.

We are now able to prove the main theorem of this section:

9.20 Theorem *Suppose that $T: V \to V$ is a linear operator whose characteristic polynomial factorizes into factors of degree 1. Then V is a direct sum of the generalized eigenspaces of T. Furthermore, the dimension of each generalized eigenspace equals the multiplicity of the corresponding factor of the characteristic polynomial.*

Proof. Let $c_T(x) = (x - \lambda_1)^{m_1}(x - \lambda_2)^{m_2} \dots (x - \lambda_k)^{m_k}$ and let U_1 be the generalized λ_1-eigenspace, W_1 the image of $(T - \lambda\mathtt{i})^{m_1}$.

As noted above we have a factorization $c_T(x) = f_1(x)g_1(x)$, where $f_1(x)$ and $g_1(x)$ are the characteristic polynomials of T_{U_1} and T_{W_1}, and since $c_T(x)$ can be expressed as a product of factors of degree 1 the same is true of $f_1(x)$ and $g_1(x)$. Moreover, since λ_1 is the only eigenvalue of T restricted to U_1 and λ_1 is not an eigenvalue of T restricted to W_1, we must have

$$f(x) = (x - \lambda_1)^{m_1}$$

and

$$g(x) = (x - \lambda_2)^{m_2} \dots (x - \lambda_k)^{m_k}.$$

One consequence of this is that $\dim U_1 = m_1$; similarly for each i the generalized λ_i-eigenspace has dimension m_i.

Applying the same argument to the restriction of T to W_1 and the eigenvalue λ_2 gives $W_1 = U_2 \oplus W_2$ where U_2 is contained in $\ker(T - \lambda_2\mathtt{i})^{m_2}$ and the characteristic polynomial of T restricted to U_2 is $(x - \lambda_2)^{m_2}$. Since the dimension of U_2 is m_2 it must be the whole generalized λ_2-eigenspace. Repeating the process we eventually obtain

$$V = U_1 \oplus U_2 \oplus \dots \oplus U_k$$

where U_i is the generalized λ_i-eigenspace of T. □

Comments ▷▷▷

9.20.1 Theorem 9.20 is a good start in our quest to understand an arbitrary linear operator; however, generalized eigenspaces are not as simple as eigenspaces, and we need further investigation to understand the action of T on each of its generalized eigenspaces. Observe that the restriction of $(T - \lambda\mathtt{i})^m$ to the kernel of $(T - \lambda\mathtt{i})^m$ is just the zero operator; so if λ is an eigenvalue of T and N the restriction of $T - \lambda\mathtt{i}$ to the generalized λ-eigenspace, then $N^m = 0$ for some m. We investigate operators satisfying this condition in the next section.

9.20.2 Let A be an $n \times n$ matrix over an algebraically closed field F. Theorem 9.20 shows that there exists a nonsingular $T \in \mathrm{Mat}(n \times n, F)$ such that the first m_1 columns of T are in the null space of $(A - \lambda_1 I)^{m_1}$, the next m_2 are in the null space of $(A - \lambda_2 I)^{m_2}$, and so on, and that $T^{-1}AT$ is a diagonal sum of blocks $A_i \in \mathrm{Mat}(m_i \times m_i, F)$. Furthermore, each block A_i satisfies $(A_i - \lambda_i I)^{m_i} = 0$ (since the matrix $A - \lambda_i I$ corresponds to the operator N in 9.20.1 above).

9.20.3 We will say that an operator T is λ-*primary* if its characteristic polynomial $c_T(x)$ is a power of $x - \lambda$. An equivalent condition is that some power of $T - \lambda\mathtt{i}$ is zero. ▷▷▷

§9e Nilpotent operators

9.21 Definition A linear operator N on a space V is said to be *nilpotent* if there exists a positive integer q such that $N^q(v) = 0$ for all $v \in V$. The least such q is called the *index of nilpotence* of N.

As we commented in 9.20.1, an understanding of nilpotent operators is crucial for an understanding of operators in general. The present section is devoted to a thorough investigation of nilpotent operators. We start by considering a special case.

9.22 Proposition *Let $\boldsymbol{b} = (v_1, v_2, \ldots, v_q)$ be a basis of the space V, and $T\colon V \to V$ a linear operator satisfying $T(v_i) = v_{i+1}$ for i from 1 to $q - 1$, and $T(v_q) = 0$. Then T is nilpotent of index q. Moreover, for each l with $1 \le l \le q$ the l elements v_{q-l+1}, …, v_{q-1}, v_q form a basis for the kernel of T^l.*

The proof of this is left as an exercise. Note that the matrix of T relative to $\boldsymbol{b}$ is the $q \times q$ matrix

$$J_q(0) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

(where the entries immediately below the main diagonal are 1 and all other entries are 0.)

We consider now an operator which is a direct sum of operators like T in 9.22. Thus we suppose that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ with $\dim V_j = q_j$, and that $T_j : V_j \to V_j$ is an operator with matrix $J_{q_j}(0)$ relative to some basis $\boldsymbol{b}_j$ of V_j. Let $N : V \to V$ be the direct sum of the T_j. We may write

$$\boldsymbol{b}_j = (x_j, N(x_j), N^2(x_j), \dots, N^{q_j-1}(x_j))$$

and combine the $\boldsymbol{b}_j$ to give a basis $\boldsymbol{b} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \dots, \boldsymbol{b}_k)$ of V; the elements of $\boldsymbol{b}$ are all the elements $N^i(x_j)$ for $j = 1$ to k and $i = 0$ to $q_j - 1$. We see that the matrix of N relative to $\boldsymbol{b}$ is the diagonal sum of the $J_{q_j}(0)$ for $j = 1$ to k.

For each $i = 1, 2, 3, \dots$ let k_i be the number of j for which $q_j \geq i$. Thus k_1 is just k, the total number of summands V_j, while k_2 is the number of summands of dimension 2 or more, k_3 the number of dimension 3 or more, and so on.

9.23 Proposition *For each l $(= 1, 2, 3, \dots)$ the dimension of the kernel of N^l is $k_1 + k_2 + \cdots + k_l$.*

Proof. In the basis $\boldsymbol{b}$ there are k_1 elements $N^i(x_j)$ for which $i = q_j - 1$, there are k_2 for which $i = q_j - 2$, and so on. Hence the total number of elements $N^i(x_j)$ in $\boldsymbol{b}$ such that $i \geq q_j - l$ is $\sum_{i=1}^{l} k_i$. So to prove the proposition it suffices to show that these elements form a basis for the kernel of N^l.

Let $v \in V$ be arbitrary. Expressing v as a linear combination of the elements of the basis $\boldsymbol{b}$ we have

9.23.1
$$v = \sum_{j=1}^{k} \sum_{i=0}^{q_j-1} \lambda_{ij} N^i(x_j)$$

for some scalars λ_{ij}. Now

$$\begin{aligned} N^l(v) &= \sum_{j=1}^{k} \sum_{i=0}^{q_j-1} \lambda_{ij} N^{i+l}(x_j) \\ &= \sum_{j=1}^{k} \sum_{i=l}^{q_j+l-1} \lambda_{i-l,j} N^i(x_j) \\ &= \sum_{j=1}^{k} \sum_{i=l}^{q_j-1} \lambda_{i-l,j} N^i(x_j) \end{aligned}$$

since $N^i(x_j) = 0$ for $i > q_j - 1$. Since the above expresses $N^l(v)$ in terms of the basis $\boldsymbol{b}$ we see that $N^l(v)$ is zero if and only if the coefficients $\lambda_{i-l,j}$ are zero for all $j = 1, 2, \ldots, k$ and i such that $l \leq i \leq q_j - 1$. That is, $v \in \ker N^l$ if and only if $\lambda_{ij} = 0$ for all i and j satisfying $0 \leq i < q_j - l$. So $\ker N^l$ consists of arbitrary linear combinations of the $N^i(x_j)$ for which $i \geq q_j - l$. Since these elements are linearly independent they form a basis of $\ker N^l$, as required. □

Our main theorem asserts that every nilpotent operator has the above form.

9.24 Theorem *Let N be a nilpotent linear operator on the finite dimensional space V. Then V has a direct decomposition $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ in which each V_j has a basis $\boldsymbol{b}_j = (x_j, N(x_j), \ldots, N^{q_j-1}(x_j))$ with $N^{q_j}(x_j) = 0$. Furthermore, in any such decomposition the number of summands V_j of dimension l equals $2(\dim \ker N^l) - \dim \ker N^{l-1} - \dim \ker N^{l+1}$.*

The construction of the subspaces V_j is somewhat tedious, and occupies the rest of this section. Note, however, that once this has been done the second assertion of the theorem follows from Proposition 9.23; if k_i is the number of j with $q_j \geq i$ then the number of summands V_j of dimension l is $k_l - k_{l+1}$, while 9.23 gives that $2(\dim \ker N^l) - \dim \ker N^{l-1} - \dim \ker N^{l+1}$ is equal to $2\left(\sum_{i=1}^{l} k_i\right) - \left(\sum_{i=1}^{l-1} k_i\right) - \left(\sum_{i=1}^{l+1} k_i\right)$, which is $k_l - k_{l+1}$.

Before beginning the construction of the V_j we state a lemma which can be easily proved using 6.10.

9.25 LEMMA *Let W be a subspace of the vector space V. If Y is a subspace of V such that $Y \cap W = \{0\}$ then there exists a subspace X of V which contains Y and is complementary to W.*

The proof proceeds by noting first that the sum $Y + W$ is direct, then choosing Y' complementing $Y \oplus W$, and defining $X = Y' \oplus Y$.

We return now to the proof of 9.24. Assume then that $N: V \to V$ is a nilpotent operator on the finite dimensional space V. It is in fact convenient for us to prove slightly more than was stated in 9.24. Specifically, we will prove the following:

9.26 THEOREM *Let q be the index of nilpotence of N and let $z_1, z_2, \ldots, z_r$ be any elements of V which form a basis for a complement to the kernel of N^{q-1}. Then the elements $x_1, x_2, \ldots, x_k$ in 9.24 can be chosen so that $x_i = z_i$ for $i = 1, 2, \ldots, r$.*

The proof uses induction on q. If $q = 1$ then N is the zero operator and $\ker N^{q-1} = \ker \mathtt{i} = \{0\}$; if $(x_1, x_2, \ldots, x_k)$ is any basis of V and we define V_j to be the 1-dimensional space spanned by x_j then it is trivial to check that the assertions of Theorem 9.24 are satisfied.

Assume then that $q > 1$ and that the assertions of 9.26 hold for nilpotent operators of lesser index. Suppose that $(x_1, x_2, \ldots, x_r)$ is a basis of a subspace X of V which is complementary to the kernel of N^{q-1}; observe that 6.10 guarantees the existence of at least one such.

9.27 LEMMA *The qr vectors $N^i(x_j)$ (for i from 0 to $q-1$ and j from 1 to r) are linearly independent.*

Proof. Suppose that

$$\sum_{i=0}^{q-1} \sum_{j=1}^{r} \lambda_{ij} N^i(x_j) = 0 \tag{9.27.1}$$

and suppose that the coefficients λ_{ij} are not all zero. Choose k minimal such that $\lambda_{kj} \neq 0$ for some j, so that the equation 9.27.1 may be written as

$$\sum_{j=1}^{r} \sum_{i=k}^{q-1} \lambda_{ij} N^i(x_j) = 0,$$

and apply the operator N^{q-1-k} to both sides. This gives

$$\sum_{j=1}^{r}\sum_{i=k}^{q-1}\lambda_{ij}N^{i+q-1-k}(x_j) = N^{q-1-k}(0) = 0$$

and since $N^h(x_j) = 0$ for all $h \geq q$ we obtain

$$0 = \sum_{j=1}^{r}\sum_{i=k}^{q-1}\lambda_{ij}N^{i+q-1-k}(x_j) = \sum_{j=1}^{r}\lambda_{kj}N^{q-1}(x_j) = N^{q-1}\left(\sum_{j=1}^{r}\lambda_{kj}x_j\right)$$

giving $\sum_{j=1}^{r}\lambda_{kj}x_j \in \ker N^{q-1}$. But the x_j lie in X, and $X \cap \ker N^{q-1} = \{0\}$. Hence $\sum_{j=1}^{r}\lambda_{kj}x_j = 0$, and by linear independence of the x_j we deduce that $\lambda_{kj} = 0$ for all j, a contradiction. We conclude that the λ_{ij} must all be zero. □

For $j = 1, 2, \ldots, r$ we set $\boldsymbol{b}_j = (x_j, N(x_j), \ldots, N^{q-1}(x_j))$; by Lemma 9.27 these are bases of independent subspaces V_j, so that $V_1 \oplus V_2 \oplus \cdots \oplus V_r$ is a subspace of V. We need to find further summands $V_{r+1}, V_{r+2}, \ldots, V_k$ to make this into a direct decomposition of V, and the inductive hypothesis (that 9.24 holds for nilpotent operators of index less than q) will enable us to do this.

Observe that $V' = \ker N^{q-1}$ is an N-invariant subspace of V, and if N' is the restriction of N to V' then N' is nilpotent of index $q-1$. It is to N' that the inductive hypothesis will be applied. Before doing so we need a basis of a subspace X' of V' complementary to $\ker(N')^{q-2}$. This basis will consist of the $N(x_j)$ (for $j = 1$ to r) and (possibly) some extra elements. (Note that N'-invariant subspaces of V' are exactly the same as N-invariant subspaces of V', since N' is simply the restriction of N. Similarly, since $\ker N^{q-2} \subseteq \ker N^{q-1} = V'$ it follows that $\ker N^{q-2}$ and $\ker(N')^{q-2}$ coincide.)

9.28 Lemma *The elements $N(x_j)$ (for $j = 1, 2, \ldots, r$) form a basis of a subspace Y of V' for which $Y \cap (\ker N^{q-2}) = \{0\}$.*

Proof. By 9.27 the elements $N(x_j)$ are linearly independent, and they lie in $V' = \ker N^{q-1}$ since $N^{q-1}(N(x_j)) = N^q(x_j) = 0$. Let Y be the space they span, and suppose that $v \in Y \cap \ker N^{q-2}$. Writing $v = \sum_{j=1}^{r}\lambda_j N(x_j)$ we see that $v = N(x)$ with $x = \sum_{j=1}^{j}\lambda_j x_j \in X$. Now

$$N^{q-1}(x) = N^{q-2}(N(x)) = N^{q-2}(v) = 0$$

shows that $x \in X \cap \ker N^{q-1} = \{0\}$, whence $x = 0$ and $v = N(x) = 0$. □

By 9.25 we may choose a subspace X' of V' containing Y and complementary to $\ker N^{q-2}$, and by 4.10 we may choose a basis $(z'_1, z'_2, \ldots, z'_s)$ of X' such that $z'_j = N(x_j)$ for j from 1 to r. Now applying the inductive hypothesis we conclude that V' contains elements $x'_1, x'_2, \ldots, x'_k$ such that:

(i) $x'_j = z'_j$ for $j = 1, 2, \ldots, s$; in particular, $x'_j = N(x_j)$ for $j = 1, 2, \ldots, r$.

(ii) $\boldsymbol{b}'_j = (x'_j, N(x'_j), \ldots, N^{t_j-1}(x'_j))$ is a basis of a subspace V'_j of V', where t_j is the least integer such that $N^{t_j}(x'_j) = 0$ (for all $j = 1, 2, \ldots, k$).

(iii) $V' = V'_1 \oplus V'_2 \oplus \ldots \oplus V'_k$.

For j from $r+1$ to k we define $V_j = V'_j$ and $\boldsymbol{b}_j = \boldsymbol{b}'_j$; in particular, $x_j = x'_j$ and $q_j = t_j$. For j from 1 to r let $q_j = q$. Then for all j (from 1 to k) we have that $\boldsymbol{b}_j = (x_j, N(x_j), \ldots, N^{q_j-1}(x_j))$ is a basis for V_j and q_j is the least integer with $N^{q_j}(x_j) = 0$. For j from 1 to r we see that the basis $\boldsymbol{b}'_j$ of V'_j is obtained from the basis $\boldsymbol{b}_j$ of V_j by deleting x_j. Thus

$$V_j = X_j \oplus V'_j \qquad \text{for } j = 1, 2, \ldots, r$$

where X_j is the 1-dimensional space spanned by x_j.

To complete the proofs of 9.24 and 9.26 it remains only to prove that V is the direct sum of the V_j.

Since $(x_1, x_2, \ldots, x_r)$ is a basis of X we have

$$X = X_1 \oplus X_2 \oplus \cdots \oplus X_r$$

and since X complements V' this gives

$$V = X_1 \oplus X_2 \oplus \cdots \oplus X_r \oplus V'.$$

Combining this with the direct decomposition of V' above and rearranging the order of summands gives

$$\begin{aligned} V &= (X_1 \oplus V'_1) \oplus (X_2 \oplus V'_2) \oplus \cdots \oplus (X_r \oplus V'_r) \oplus V'_{r+1} \oplus V'_{r+2} \oplus \cdots \oplus V'_k \\ &= V_1 \oplus V_2 \oplus \cdots \oplus V_k \end{aligned}$$

as required.

Comments ▷▷▷

9.28.1 We have not formally proved anywhere that it is legitimate to rearrange the terms in a direct sum as in the above proof. But it is a trivial task. Note also that we have used Exercise 15 of Chapter Six.

9.28.2 It is clear that we may choose the ordering of the summands V_j in 9.24 so that $q_1 \geq q_2 \geq \cdots \geq q_k$. (Indeed, this is the ordering which our proof gives.) The matrix of N relative to $\boldsymbol{b}$ is the diagonal sum of the matrices $J_{q_j}(0)$ (for j from 1 to k); that is, if $A = \mathrm{M}_{\boldsymbol{bb}}(N)$ then

$$A = \operatorname{diag}(J_{q_1}(0), J_{q_2}(0), \ldots, J_{q_k}(0)) \qquad q_1 \geq q_2 \geq \cdots \geq q_k.$$

We call such a matrix a *canonical nilpotent matrix*, and it is a corollary of 9.24 that every nilpotent matrix is similar to a unique canonical nilpotent matrix. ▷▷▷

§9f The Jordan canonical form

Let V be a finite dimensional vector space $T: V \to V$ a linear operator. If λ is an eigenvalue of T and U the corresponding generalized eigenspace then T_U is λ-primary, and so there is a basis $\boldsymbol{b}$ of U such that the matrix of $T_U - \lambda\mathtt{i}$ is a canonical nilpotent matrix. Now since

$$\mathrm{M}_{\boldsymbol{bb}}(T_U - \lambda\mathtt{i}) = \mathrm{M}_{\boldsymbol{bb}}(T_U) - \lambda\,\mathrm{M}_{\boldsymbol{bb}}(\mathtt{i}) = \mathrm{M}_{\boldsymbol{bb}}(T_U) - \lambda I$$

we see that the matrix of T_U is a canonical nilpotent matrix plus λI. Since $J_r(0) + \lambda I = J_r(\lambda)$ (defined in 9.18.2 above) it follows that the matrix of T_U is a diagonal sum of blocks of the form $J_r(\lambda)$.

9.29 Definition Matrices of the form $J_r(\lambda)$ are called *Jordan blocks*. A matrix of the form $\operatorname{diag}(J_{r_1}(\lambda), J_{r_2}(\lambda), \ldots, J_{r_k}(\lambda))$ with $r_1 \geq r_2 \geq \cdots \geq r_k$ (a diagonal sum of Jordan blocks in order of nonincreasing size) is called a *canonical λ-primary matrix*. A diagonal sum of canonical primary matrices for different eigenvalues is called a *Jordan matrix*, or a matrix in *Jordan canonical form*.

Comment ▷▷▷

9.29.1 Different books use different terminology. In particular, some authors use bases which are essentially the same as ours taken in the reverse order. This has the effect of making Jordan blocks upper triangular rather than lower triangular; in fact, their Jordan blocks are the transpose of ours. ▷▷▷

Combining the main theorems of the previous two sections gives our final verdict on linear operators.

9.30 THEOREM *Let V be a finite dimensional vector space over an algebraically closed field F, and let T be a linear operator on V. Then there exists a basis $\boldsymbol{b}$ of V such that the matrix of T relative to $\boldsymbol{b}$ is a Jordan matrix. Moreover, the Jordan matrix is unique apart from reordering the eigenvalues.*

Equivalently, every square matrix over an algebraically closed field is similar to a Jordan matrix, the primary components of which are uniquely determined.

—Examples—

#4 Find a nonsingular matrix T such that $T^{-1}AT$ is in Jordan canonical form, where

$$A = \begin{pmatrix} 1 & 1 & 0 & -2 \\ 1 & 5 & 3 & -10 \\ 0 & 1 & 1 & -2 \\ 1 & 2 & 1 & -4 \end{pmatrix}.$$

⋙▷ Using expansion along the first row we find that the determinant of $A - xI$ is equal to

$$(1-x)\det\begin{pmatrix} 5-x & 3 & -10 \\ 1 & 1-x & -2 \\ 2 & 1 & -4-x \end{pmatrix} - \det\begin{pmatrix} 1 & 3 & -10 \\ 0 & 1-x & -2 \\ 1 & 1 & -4-x \end{pmatrix}$$
$$+2\det\begin{pmatrix} 1 & 5-x & 3 \\ 0 & 1 & 1-x \\ 1 & 2 & 1 \end{pmatrix}$$
$$= (1-x)(-x^3+2x^2) - (x^2-7x+2) + 2(x^2-4x+1) = x^4 - 3x^3 + 3x^2 - x$$

so that the eigenvalues are 0 and 1, with the corresponding generalized eigenspaces having dimensions 1 and 3 respectively. We find a basis for the 0-eigenspace by solving $Ax = 0$ as usual. Solving $(A - I)x = 0$ we find that the 1-eigenspace has dimension equal to 1, and it follows that there will be only one Jordan block corresponding to this eigenvalue. Thus the Jordan canonical form will be $\mathrm{diag}(J_3(1), J_1(0))$. We could find a basis for the generalized 1-eigenspace by solving $(A - I)^3 x = 0$, but it is easier to use

Theorem 9.19. The generalized 1-eigenspace is the unique invariant complement to the generalized 0-eigenspace, and by 9.19 it is simply the column space of $A - 0I$. Choose x_1 to be any column of A. Certainly x_1 will lie in the kernel of $(A - I)^3$; we will be unlucky if it lies in the kernel of $(A - I)^2$, but if it does we will just choose a different column of A instead. Then set $x_2 = Ax_1 - x_1$ and $x_3 = Ax_2 - x_2$ (and hope that $x_3 \neq 0$). Finally, let x_4 be an eigenvector for the eigenvalue 0. The matrix T that we seek has the x_i as its columns. We find

$$T = \begin{pmatrix} 1 & -1 & -1 & 0 \\ 1 & -5 & -4 & 2 \\ 0 & -1 & -1 & 0 \\ 1 & -2 & -2 & 1 \end{pmatrix}$$

and it is easily checked that

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

The theory we have developed guarantees that T is nonsingular; there is no point calculating T^{-1}. ⊲⊣≪

#5 Given that the matrix A below is nilpotent, find a nonsingular T such that $T^{-1}AT$ is a canonical nilpotent matrix.

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

≫⊣▷ We first solve $Ax = 0$, and we find that the null space has dimension 2. Hence the canonical form will have two blocks. At this stage there are two possibilities: either $\mathrm{diag}(J_2(0), J_2(0))$ or $\mathrm{diag}(J_3(0), J_1(0))$. Finding the dimension of the null space of A^2 will settle the issue. In fact we see immediately that $A^2 = 0$, which rules out the latter of our possibilities. Our task now is simply to find two linearly independent columns x and y which lie outside the null space of A. Then we can let T be the matrix with columns x, Ax, y and Ay. The theory guarantees that T will be nonsingular.

Practically any two columns you care to choose for x and y will do. For instance, a suitable matrix is

$$T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & -1 \\ 0 & -2 & 0 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix}$$

and it is easily checked that $AT = T\,\mathrm{diag}(J_2(0), J_2(0))$. ⊲⋘

We will not investigate the question of how best to compute the Jordan canonical form in general. Note, however, the following points.

(a) Once the characteristic polynomial has been factorized, it is simply a matter of solving simultaneous equations to find the dimensions of the null spaces of the matrices $(A - \lambda I)^m$ for all eigenvalues λ and the relevant values of m. Knowing these dimensions determines the Jordan canonical form (by the last sentence of Theorem 9.24).

(b) Knowing what the Jordan canonical form for A has to be, it is in principle a routine task to calculate a matrix T such that $AT = TJ$ (where J is the Jordan matrix). Let the columns of T be $v_1, v_2, \ldots, v_n$. If the first Jordan block in J is $J_r(\lambda)$ then the first r columns of T must satisfy $T(v_i) = \lambda v_i + v_{i+1}$ (for i from 1 to $r-1$) and $T(v_r) = \lambda v_r$. The next batch of columns of T satisfy a similar condition determined by the second Jordan block in J. Finding suitable columns for T is then a matter of solving simultaneous equations.

Let T be a linear operator on V, and assume that the field is algabraically closed. Let $U_1, U_2, \ldots, U_k$ be the generalized eigenspaces of T, and for each i let T_i be the restriction of T to U_i. Thus T is the direct sum of the T_i, in the sense of 9.9.1. For each i let $S_i : U_i \to U_i$ be given by $S_i(u) = \lambda_i u$, where λ_i is the eigenvalue of T associated with the space U_i, and let S be the direct sum of the operators S_i. It can be seen that S is the unique linear operator on V having the same eigenvalues as T and such that for each i the generalized λ_i-eigenspace of T is the λ_i-eigenspace of S. Because S_i is simply $\lambda_i \mathtt{i}$, it is clear that $S_i T_i = T_i S_i$ for each i, and from this it follows that $ST = TS$. Furthermore, if we write $N = T - S$ then the restriction of N to U_i is equal to the nilpotent operator $T - \lambda_i \mathtt{i}$, and it follows that N, being a direct sum of nilpotent operators, is itself nilpotent.

The operator S is called the *semisimple part* of T, and the operator N is called the *nilpotent part* of T. They are uniquely determined by the properties that S is diagonalizable, N is nilpotent, $SN = NS$ and $S+N = T$.

If $A \in \mathrm{Mat}(n \times n, \mathbb{C})$ we define the *exponential* of A by

$$\exp(A) = e^A = I + A + \frac{1}{2}A^2 + \frac{1}{6}A^3 + \cdots = \sum_{i=0}^{\infty} \frac{1}{n!}A^n.$$

It can be proved that this infinite series converges. Furthermore, if T is any nonsingular matrix then

$$\exp(T^{-1}AT) = T^{-1}\exp(A)T.$$

For a Jordan matrix the calculation of its exponential is relatively easy; so for an arbitrary matrix A it is reasonable to proceed by first finding T so that $T^{-1}AT$ is in Jordan form. If A is diagonalizable this works out particularly well since

$$\exp(\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)) = \mathrm{diag}(e^{\lambda_1}, e^{\lambda_2}, \ldots, e^{\lambda_n}).$$

It is unfortunately not true that $\exp(A + B) = \exp(A)\exp(B)$ for all A and B; however, this property is valid if $AB = BA$, and so, in particular, if S and N are the semisimple and nilpotent parts of A then $\exp(A) = \exp(S)\exp(N)$. Calculation of the exponential of a nilpotent matrix is easy, since the infinite series in the definition becomes a finite series. For example,

$$\exp\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = I + \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}.$$

Matrix exponentials occur naturally in the solution of simultaneous differential equations of the kind we have already considered. Specifically, the solution of the system

$$\frac{d}{dt}\begin{pmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{pmatrix} = A\begin{pmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{pmatrix} \quad \text{subject to} \quad \begin{pmatrix} x_1(0) \\ \vdots \\ x_n(0) \end{pmatrix} = \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$$

(where A is an $n \times n$ matrix) can be written as

$$\begin{pmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{pmatrix} = \exp(tA)\begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix},$$

a formula which is completely analogous to the familiar one-variable case.

—***Example***—

#6 Solve

$$\frac{d}{dt}\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix}$$

subject to $x(0) = 1$ and $y(0) = z(0) = 0$.

≫—▷ Since A is (conveniently) already in Jordan form we can immediately write down the semisimple and nilpotent parts of tA. The semisimple part is $S = tI$ and the nilpotent part is

$$N = \begin{pmatrix} 0 & 0 & 0 \\ t & 0 & 0 \\ 0 & t & 0 \end{pmatrix}.$$

Calculation of the exponential of N is easy since $N^3 = 0$, and, even easier, $\exp(S) = e^t I$. Hence the solution is

$$\begin{aligned}\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} &= e^t \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ \frac{t^2}{2} & t & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} e^t \\ te^t \\ \frac{1}{2}t^2 e^t \end{pmatrix}.\end{aligned}$$

◁—≪

§9g Polynomials

Our behaviour concerning polynomials has, up to now, been somewhat reprehensible. We have not even defined them, and we have used, without proof, several important properties. Let us therefore, belatedly, rectify this situation a little.

9.31 Definition A *polynomial* in the *indeterminate* x over the field F is an expression of the form $a_0 + a_1 x + \cdots + a_n x^n$, where n is a nonnegative integer and the a_i are elements of F.

9.32 Definition Let $a(x)$ be a nonzero polynomial over the field F, and let $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ with $a_n \neq 0$. Then n is called the *degree*

of $a(x)$, and a_n the *leading coefficient*. If the leading coefficient is 1 then the polynomial is said to be *monic*.

Let $F[x]$ be the set of all polynomials over F in the indeterminate x. Addition and scalar multiplication of polynomials is definable in the obvious way, and it is easily seen that the polynomials of degree less than or equal to n form a vector space of dimension $n+1$. The set $F[x]$ itself is an infinite dimensional vector space. However, $F[x]$ has more algebraic structure than this, since one can also multiply polynomials (by the usual rule: $(\sum_i a_i x^i)(\sum_j b_j x^j) = \sum_r (\sum_i a_i b_{r-i}) x^r$).

The set of all integers and the set $F[x]$ of all polynomials in x over the field F enjoy many similar properties. Notably, in each case there is a *division algorithm*:

If n and m are integers and $n \neq 0$ then there exist unique integers q and r with $m = qn + r$ and $0 \leq r < n$.

For polynomials:

If $n(x)$ and $m(x)$ are polynomials over F and $n(x) \neq 0$ then there exist unique polynomials $q(x)$ and $r(x)$ with $m(x) = q(x)n(x) + r(x)$ and the degree of $r(x)$ less than that of $n(x)$.

A minor technical point: the degree of the zero polynomial is undefined. For the purposes of the division algorithm, however, the zero polynomial should be considered to have degree less than that of any other polynomial. Note also that for nonzero polynomials the degree of a product is the sum of the degrees of the factors; thus if the degree of the zero polynomial is to be defined at all it should be set equal to $-\infty$.

If n and m are integers which are not both zero then one can use the division algorithm to find an integer d such that

(i) d is a factor of both n and m, and

(ii) $d = rn + sm$ for some integers r and s.

(Obviously, if n and m are both positive then either $r < 0$ or $s < 0$.) The process by which one finds d is known as *the Euclidean algorithm*, and it goes as follows. Assuming that $m > n$, replace m by the remainder on dividing m by n. Now we have a smaller pair of integers, and we repeat the process. When one of the integers is replaced by 0, the other is the sought after integer d. For example, starting with $m = 1001$ and $n = 35$, divide m by n. The remainder is 21. Divide 35 by 21; the remainder is 14. Divide 21 by 14;

the remainder is 7. Now 14 is divisible by 7, and we conclude that $d = 7$. It is easily checked that 7 is a factor of both 1001 and 35, and furthermore

$$7 = 21 - 14 = 21 - (35 - 21) = 2 \times 21 - 35 = 2 \times (1001 - 28 \times 35) - 35$$
$$= 2 \times 1001 - 57 \times 35.$$

Properties (i) and (ii) above determine d uniquely up to sign. The positive d satisfying (i) and (ii) is called the *greatest common divisor* of m and n, denoted by '$\gcd(m, n)$'. Using the gcd theorem and induction one can prove the unique factorization theorem for integers: each nonzero integer is expressible in the form $(\pm 1)p_1 p_2 \dots p_k$ where each p_i is positive and has no divisors other than ± 1 and $\pm p_i$, and the expression is unique except for reordering the factors.

All of the above works for $F[x]$. Given two polynomials $m(x)$ and $n(x)$ which are not both zero there exists a polynomial $d(x)$ which is a divisor of each and which can be expressed in the form $r(x)n(x) + s(x)m(x)$; the Euclidean algorithm can be used to find one. The polynomial $d(x)$ is unique up to multiplication by a scalar, and multiplying by a suitable scalar ensures that $d(x)$ is monic; the resulting $d(x)$ is the greatest common divisor of $m(x)$ and $n(x)$. There is a unique factorization theorem which states that every nonzero polynomial is expressible uniquely (up to order of the factors) in the form $cp_1(x)p_2(x) \dots p_k(x)$ where c is a scalar and the $p_i(x)$ are monic polynomials all of which have no divisors other than scalars and scalar multiples of themselves. Note that if the field F is algebraically closed then the $p_i(x)$ are all necessarily of the form $x - \lambda$.

If two integers n and m have no common divisors (other than ± 1) then the Euclidean algorithm shows that there exist integers r and s such that $rn + sm = 1$. A double application can be used to show that if three integers n, m and p have no common divisors then there exist r, s and t with $rn + sm + tp = 1$. For example, starting with 6, 10 and 15 we first find that $2 = 2 \times 6 - 10$ and then that $1 = 15 - 7 \times 2$, and combining these gives $1 = 15 - 14 \times 6 + 7 \times 10$. The result clearly generalizes to any number of integers.

The same is also true for polynomials. For instance, it is possible to find polynomials $r(x)$, $s(x)$ and $t(x)$ such that

$$x(x-1)r(x) + (x-1)(x+1)s(x) + x(x+1)t(x) = 1.$$

We have a linear algebra application of this:

9.33 THEOREM *Let T be a linear operator on V and suppose that the characteristic polynomial factorizes as $\prod_{i=1}^{k}(x-\lambda_i)^{m_i}$. If for each i from 1 to k we define $f_i(x) = \prod_{j\neq i}(x-\lambda_j)^{m_j}$, then the image of the operator $f_i(T)$ is equal to the generalized λ_i-eigenspace.*

Proof. Since the only polynomials which are divisors of all the $f_i(x)$ are scalars, it follows from the Euclidean algorithm that there exist polynomials $r_i(x)$ such that $\sum_{i=1}^{k} r_i(x)f_i(x) = 1$. Clearly we may replace x by T in this equation, obtaining $\sum_{j=1}^{k} r_j(T)f_j(T) = \mathtt{i}$.

Let $v \in \ker(T-\lambda_i\mathtt{i})^{m_i}$. If $j \neq i$ then $f_j(T)(v) = 0$, since $f_j(x)$ is divisible by $(x-\lambda_i)^{m_i}$. Now we have

$$v = \mathtt{i}(v) = \sum_{j=1}^{k} r_j(T)(f_j(T)(v)) = f_i(T)(r_i(T)(v)) \in \operatorname{im} f_i(T).$$

Hence we have shown that the generalized eigenspace is contained in the image of $f_i(T)$. To prove the reverse inclusion we must show that if $u \in \operatorname{im} f_i(T)$ then u is in the kernel of $(T-\lambda_i\mathtt{i})^{m_i}$. Thus we must show that

$$\big((T-\lambda_i\mathtt{i})^{m_i} f_i(T)\big)(w) = 0$$

for all $w \in V$. But since $(x-\lambda_i)^{m_i} f_i(x) = c_T(x)$, this amounts to showing that the operator $c_T(T)$ is zero. This fact, that a linear operator satisfies its own characteristic equation, is the Cayley-Hamilton Theorem, which is proved below. See also Exercise 10 at the end of this chapter. □

9.34 THE CAYLEY-HAMILTON THEOREM *If A is an $n \times n$ matrix over the field F and $c(x) = \det(A - xI)$ the characteristic polynomial of A, then the matrix $c(A)$ is zero.*

Proof. Let $E = A - xI$. The diagonal entries of E are polynomials of degree 1, and the other entries are scalars. We investigate the cofactors of E.

Calculating $\operatorname{cof}_{ij}(E)$ involves addition and subtraction of various products of $n-1$ elements of E. Since elements of E have degree at most 1, a product of $n-1$ elements of E is a polynomial of degree at most $n-1$. Hence $\operatorname{cof}_{ij}(E)$ is also a ploynomial of degree at most $n-1$. Let $B_{ij}^{(r)}$ be the coefficient of x^r in $\operatorname{cof}_{ij}(E)$, so that

$$\operatorname{cof}_{ij}(E) = B_{ij}^{(0)} + xB_{ij}^{(1)} + \cdots + x^{n-1}B_{ij}^{(n-1)}.$$

For each r from 0 to $n-1$ let $B^{(r)}$ be the matrix with (i,j)-entry $B_{ij}^{(r)}$, and consider the matrix

$$B = B^{(0)} + xB^{(1)} + \cdots + x^{n-1}B^{(n-1)}.$$

The (i,j)-entry of B is just $\sum_{r=1}^{n-1} x^r B_{ij}^{(r)}$, which is $\mathrm{cof}_{ij}(E)$, and so we see that $B = \operatorname{adj} E$, the adjoint of E. Hence Theorem 8.25 gives

9.34.1 $$(A - xI)(B^{(0)} + xB^{(1)} + \cdots + x^{n-1}B^{(n-1)}) = c(x)I$$

since $c(x)$ is the determinant of $A - xI$.

Let the coefficient of x^r in $c(x)$ be c_r, so that the right hand side of 9.34.1 may be written as $c_0 I + xc_1 I + \cdots + x^n c_n I$. Since two polynomials are equal if and only if they have the same coefficient of x^r for each r, it follows that we may equate the coefficients of x^r in 9.34.1. This gives

$$\begin{aligned}
(0) \qquad & AB^{(0)} = c_0 I \\
(1) \qquad & -B^{(0)} + AB^{(1)} = c_1 I \\
(2) \qquad & -B^{(1)} + AB^{(2)} = c_2 I \\
& \qquad\qquad \vdots \\
(n-1) \qquad & -B^{(n-2)} + AB^{(n-1)} = c_{n-1} I \\
(n) \qquad & -B^{(n-1)} = c_n I.
\end{aligned}$$

Multiply equation (i) by A^i and add the equations. On the left hand side everything cancels, and we deduce that

$$0 = c_0 I + c_1 A + c_2 A^2 + \cdots + c_{n-1}A^{n-1} + c_n A^n,$$

which is what we were to prove. □

Exercises

1. Find a matrix T such that $T^{-1}AT$ is in Jordan canonical form, where A is the matrix in #1 above.

2. Let $A = \begin{pmatrix} 1 & -1 & 2 \\ -2 & 1 & 3 \\ -1 & -1 & 4 \end{pmatrix}$. Find T such that $T^{-1}AT$ is in Jordan form.

3. Let $\boldsymbol{b} = (v, w, x, y, z)$ be a basis for a vector space V and let T be a linear operator on V such that $Tv = x + 5z$, $Tw = 2y$, $Tx = 4v$, $Ty = 2w$ and $Tz = v$.

(*i*) Let A be the matrix of T relative to $\boldsymbol{b}$. Find A.

(*ii*) Find B, the matrix of T relative to the basis (w, y, v, x, z).

(*iii*) Find P such that $P^{-1}AP = B$.

(*iv*) Show that T is diagonalizable, and find the dimensions of the eigenspaces.

4. Let $T\colon V \to V$ be a linear operator. Prove that a subspace of V of dimension 1 is T-invariant if and only if it is contained in an eigenspace of T.

5. Prove Proposition 9.22.

6. Prove Lemma 9.25.

7. How many similarity classes are there of 10×10 nilpotent matrices?

8. Describe all diagonalizable nilpotent matrices.

9. Find polynomials $r(x)$, $s(x)$ and $t(x)$ such that

$$x(x-1)r(x) + (x-1)(x+1)s(x) + x(x+1)t(x) = 1.$$

10. Use Theorem 9.20 to prove the Cayley-Hamilton Theorem for algebraically closed fields.

(Hint: Let $v \in V$ and use the decomposition of V as the direct sum of generalized eigenspaces to write $v = \sum_i v_i$ with v_i in the generalized λ_i eigenspace. Observe that it is sufficient to prove that $c_T(T)(v_i) = 0$ for all i. But since we may write $c_T(T) = f_i(T)(T - \lambda_i \mathtt{i})^{m_i}$ this is immediate from the fact that $v_i \in \ker(T - \lambda_i \mathtt{i})^{m_i}$.)

11. Prove that every complex matrix is similar to its transpose, by proving it first for Jordan blocks.

12. The *minimal polynomial* of a matrix A is the monic polynomial $m(x)$ of least degree such that $m(A) = 0$. Use the division algorithm for polynomials and the Cayley-Hamilton Theorem to prove that the minimal polynomial is a divisor of the characteristic polynomial.

13. Prove that a complex matrix is diagonalizable if and only if its minimal polynomial has no repeated factors.

14. Let J be a Jordan matrix, with eigenvalues λ_i for i from 1 to k. For each i let q_i be the size of the largest Jordan block in the λ_i-primary component. Prove that the minimal polynomial of J is $\prod_i (x - \lambda_i)^{q_i}$.

15. How many similarity classes of complex matrices are there for which the characteristic polynomial is $x^4(x-2)^2(x+1)^2$ and the minimal polynomial is $x^2(x-2)(x+1)^2$? (Hint: Use Exercise 14.)

Index of notation

Index of examples

Chapter 1

Chapter 2

Index of examples

Chapter 3

Index of examples

Index of examples

Chapter 7

Chapter 8

Chapter 9