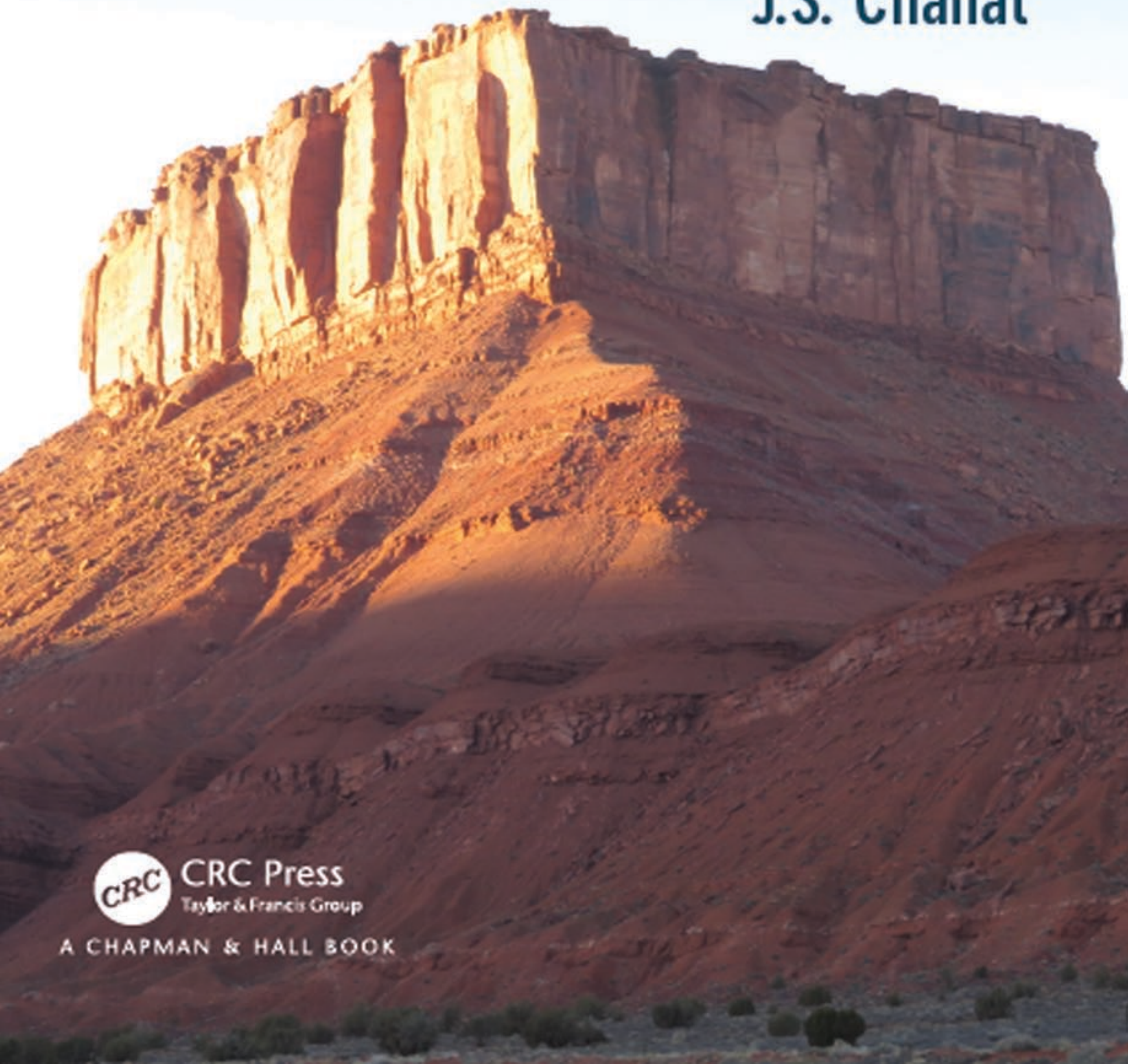
TEXTBOOKS IN MATHEMATICS

FUNDAMENTALS OF LINEAR ALGEBRA

J.S. Chahal



CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Fundamentals of Linear Algebra

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Fundamentals of Linear Algebra

J. S. Chahal

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Cover photo courtesy of J. S. Chahal, Castle Valley, Utah.

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20181026

International Standard Book Number-13: 978-1-138-59050-2 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Preface

This book is based on a one-semester course on linear algebra I have taught numerous times at Brigham Young University. With so many books on the subject already out there, it is legitimate to ask why one more is necessary.

No textbook on the subject served all my needs while teaching the course. For example, most texts do not provide satisfactory introductions to some important definitions. Their definitions seem to appear suddenly out of nowhere. So, for my lectures I prepared my own notes, and hence this book. Whenever possible, I have tried to motivate by taking the reader along paths which lead naturally to our definitions. The other salient features of the book are:

1. It gives a brief but adequate presentation of the fundamentals of the subject in as few pages as possible so that it can be covered in a semester without missing anything significant in textbooks with 500 to 700 pages.
2. Although most students taking the course were non math majors, the rigor has not been compromised. To help them cope with it, the prerequisite material has been assembled in Chapter 1.
3. Rather than present linear algebra as a hodgepodge collection of seemingly unrelated topics, I have tried to present it as a single theme – the study of linear maps – with matrices as a convenient tool to capture and keep track of them but only when their domains and co-domains are finite dimensional. Conversely, by treating matrices as linear maps, some of the properties of matrices themselves, such as the associativity of matrix multiplication, become obvious. This reduces the number of pages required for the subject.
4. Contrary to the usual practice of doing linear algebra over the reals, or at most over the complex numbers, I have put no restriction on the field of scalars. This widens the scope for applications of linear algebra without increasing the level of difficulty or abstraction. Ironically, when the applications were not the order of the day, the books on linear algebra of the last generation (e.g., [4], [9], [10] and [16]) used to begin with an introduction to fields, not only as a first step towards the abstraction needed for the course but also for its applications.

5. For the sake of those who have no interest in fields of scalars other than the reals or complex numbers, I have marked the few items in the main body of the book that pertain to other fields with asterisks so that they may be omitted. On the other hand, those not interested in non theoretical applications may skip the items marked with daggers.

6. The conceptual part of linear algebra is as important, if not more, as acquiring computation skills the students often think math is all about. To convince them of this, I have included a special chapter with selected applications in their own respective majors (computer science, engineering, math and physics) which require more than the ability to handle problems involving only concrete numbers.

The only prerequisite for this book is mathematical maturity. It may be used for an advanced undergraduate or a beginning graduate course on linear algebra.

I would like to thank Lonette Stoddard for preparing the LaTeX file of the manuscript. I also thank my colleagues, Sum Chow for his help with compiling the answers to numerical problems and Jeff Humpherys for preparing Figure 9.1. I would also like to thank Wolfgang Herfort, Vienna Technical University, Vienna (Austria), Jörg Thuswaldner, University of Leoben (Austria), Dipendra Prasad, Tata Institute of Fundamental Research, Mumbai (India) and Michael Schein, Bar-Ilan University, Ramat-Gan (Israel) for sending detailed lists of typos and suggestions. However, I take full responsibility for the errors that still escaped scrutiny. I would appreciate having any errors or suggestions sent to me at chahal@mathematics.byu.edu.

J. S. Chahal
30 May 2018
Provo, Utah, USA

Advice to the Reader

Even if you are a non-math major, learning a hodgepodge of recipes is not the way to learn mathematics. If you have learned a subject properly, you can come up with your own recipes. To learn linear algebra properly, you should not only memorize the recipes but also try to grasp the concepts, for which you need to learn how to read and write proofs and occasionally come up with your own. Students who have never seen a proof in a math course and even those who have, are strongly advised to read the section on proofs in Chapter 1.

Some students also found it very useful to go through Book 1 of Euclid's *Elements* to learn how to compose proofs. In this book the structure of mathematical proofs was laid out almost two and a half millennia ago, and has served, to a great extent, as a model for every math book written since then.

Every discipline has its own vocabulary and so does mathematics. The language of higher mathematics is set theory. For example, a vector space will be a nonempty set, which may have apples and oranges in it, to be called vectors. Yes, an apple can be a vector! (See Example 2*, Section 3.1.) Similarly, a linear map will be an abstract function, with prescribed properties. We review this language briefly in Chapter 1. You may also learn set theory from the lively, little and easy to read book [8] by P. R. Halmos, *Naive Set Theory*, UTM, Springer (1974).

Some preconceived notions about vectors and functions from previous courses may actually hinder, more than help you in this course. They may make it difficult for you to accept the extended meanings of some technical terms. For example, you may get lost if we refer to a differentiable function as a vector, because it does not have length and direction, like an arrow. So it is advisable that you forget about the previous notions and start with a clean slate. It is not hard to learn a concept without actively grappling with it many times in different settings and connecting it with previously understood concepts. A systematic development of the subject, with sufficiently many examples and exercises, can provide another and perhaps better approach for learning it.

The technology is indispensable when the amount of data is huge. But for learning this course, it is better if you depend more on paper and pencil than on technology. Overdependence on technology can be like using a GPS to reach a destination. Not only are you likely to pay no attention to the landmarks on the way, but if the GPS stops working, without a map and knowing how to read it, you will not know where you are.

The purpose of the theory is not to prepare the students for homework assignments and tests. On the contrary, the purpose of examples and exercises is to explain, enlarge and ingrain in the learner's mind the ideas involved therein. You are encouraged to attempt all the problems, not just odd or even, as is customary with most textbooks. Each exercise has been chosen to help you understand a concept. We have refrained from providing redundant numerical exercises for repeated drills, a practice which often obscures their real purpose.

1

Preliminaries

1.1 What Is Linear Algebra?

Manipulating matrices is not what linear algebra is all about. The matrices are only a convenient tool to represent and keep track of linear maps. And that too when the domain (and hence the range also) of such a function is finite dimensional. In its full generality, linear algebra is the study of functions in the most general context, which behave like the real valued function

$$f(x) = mx \tag{1.1}$$

of real variable x. The graph of (1.1) is a straight line through the origin with fixed slope m. Hence the name *linear algebra*.

The function $y = f(x) = mx$ has a defining property: For constants c_1, c_2,

$$f(c_1x_1 + c_2x_2) = c_1f(x_1) + c_2f(x_2), \tag{1.2}$$

which is equivalent to the following two conditions:

1) $f(x_1 + x_2) = f(x_1) + f(x_2)$
2) $f(cx) = cf(x)$.

This is to say that any real valued function $f(x)$ of a real variable with the property (1.2) has to be as in (1.1). In fact if $f(1) = m$, then by condition 2), $f(x) = f(x1) = xf(1) = mx$.

The notation $y = f(x)$ for a function is not adequate, unless one says $y = f(x)$ is a real valued function of a real variable x. A better and informative way to write it is $f : \mathbb{R} \to \mathbb{R}$. In (1.1), the domain, which is the real line $\mathbb{R}$, is a 1-dimensional space. The values are also in the 1-dimensional space $\mathbb{R}$. If $\mathbb{R}^2$ is the plane consisting of points (x, y) and $\mathbb{R}^3$ is the 3-dimensional space consisting of points $P = (x, y, z)$, we can add and scale points in $\mathbb{R}^n$ ($n = 2$ or 3), considered as vectors. Thus we can also consider functions $F : \mathbb{R}^3 \to \mathbb{R}^2$ and call them *linear* if they have the property

$$F(c_1P_1 + c_2P_2) = c_1F(P_1) + c_2F(P_2) \tag{1.3}$$

similar to property (1.2) of the function $f(x) = mx$. In general, one needs to study functions $F : V \to W$, where V, W are spaces in the most general sense and the property (1.3) still makes sense. The spaces V, W that arise in various contexts will be defined in a unified way and will be called vector spaces or more appropriately, linear spaces. The functions $F : V \to W$ having the property (1.3) are *linear maps*, *linear transformations*, or simply *linear.* In this book, we study such spaces V, W and the linear maps $F : V \to W$.

After making it precise what is meant by the dimension of a vector space, we shall show that if a vector space is finite dimensional, its elements are column vectors in a frame of reference to be called a basis. Moreover, if V and W are both finite dimensional and $F : V \to W$ is linear, then

$$F(\boldsymbol{x}) = M\boldsymbol{x} \tag{1.4}$$

where M is a matrix. The matrix M is obtained in a way similar to the 1×1 matrix $M = (m)$ in the 1-dimensional case above that was determined by the value $m = f(1)$ of the basis vector $\boldsymbol{v} = (1)$ of $V = \mathbb{R}^1$. This is a generalization of (1.1). In this (finite dimensional) case F can be identified with its matrix M.

Linear maps can be added, scaled and composed. The matrices can also be added, scaled and multiplied. We shall show that the algebra of linear maps $F : V \to W$ is the same as matrix algebra, provided V and W are finite dimensional.

The solution space of a homogeneous matrix equation corresponds to the kernel of the corresponding linear map. However, the concept of kernel is more general. For example, the domain of a linear differential operator D is an infinite dimensional vector space and the kernel of D is the solution space of the differential equation $Dy = 0$. There is no matrix theoretic analog in this situation. Thus for wider applications, some concepts like eigenvalues and eigenspaces should not be restricted to matrices.

As a final remark, it cannot be overemphasized that the language of linear algebra is set theory, which we now recall briefly.

1.2 Rudimentary Set Theory

A *set* is a collection of objects. The symbol $x \in X$ or $X \ni x$ means that x is an element of the set X. If x is not in X we write it as $x \notin X$. The notation $\{x \mid P(X)\}$ stands for the set of all x which have the prescribed property $P(x)$. For example, $\{x \mid x \in \mathbb{R}, a \leq x \leq b\}$ is the closed interval $[a, b]$ from a to b

on the real line $\mathbb{R}$. The set $[a, b]$ may also be written as $\{x \in \mathbb{R} \mid a \leq x \leq b\}$ which one reads as "the set of all real numbers x such that $a \leq x \leq b$."

If A is a *subset* of a set B, that is, if every element of A is also an element of B, we write it as $A \subseteq B$. Many books write $A \subset B$ but do not exclude the possibility $A = B$, which is confusing. If $A \subseteq B$, but $A \neq B$ we write it as $A \subsetneq B$ and call A a *proper subset* of B. The empty set is denoted by ϕ. The set ϕ is a proper subset of every non-empty set A. To show that A is a proper subset of B, one often proves i) $a \in A$ implies $a \in B$, and ii) there is a b in B such that $b \notin A$. For two sets A and B, $A - B = \{x \in A \mid x \notin B\}$. The *union* $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$, whereas the *intersection* $A \cap B = \{x \mid x \in A$ and $x \in B\}$. The union and the intersection of more than two sets are defined in a similar manner. A set X is the *disjoint union* of its subsets A and B if i) $X = A \cup B$, and ii) $A \cap B = \emptyset$.

1.3 Cartesian Products

If A, B are two non-empty sets, their *Cartesian product* is the set $A \times B = \{(a, b) \mid a \in A, b \in B\}$ of all ordered pairs (a, b) with a in A and b in B. More generally, for non-empty sets $A_1, \ldots, A_n$, their *Cartesian product*, $A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) \mid a_j \in A_j\}$ is the set of all n-tuples $(a_1, \ldots, a_n)$ such that the jth *coordinate* a_j is taken from the set A_j. If $A_1 = \cdots = A_n = A$, say, then we write A^n for $A_1 \times \cdots \times A_n$. Thus $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the *Euclidean-plane* and $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ is the *Euclidean* 3-space. In general, for an integer $n \geq 1, \mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_j \in \mathbb{R}\}$ is the *Euclidean* n-space. Its elements, $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_n)$, $\boldsymbol{z} = (z_1, \ldots, z_n)$, etc. are called *points* or *vectors* in $\mathbb{R}^n$. Clearly, $\boldsymbol{x} = \boldsymbol{y}$ if and only if $x_1 = y_1, \ldots, x_n = y_n$.

The set $V = \mathbb{R}^n$ is more than just a set. Its elements can be added and scaled by elements of $\mathbb{R}$, coordinate-wise, that is,

$$\begin{aligned} \boldsymbol{x} + \boldsymbol{y} &= (x_1 + y_1, \ldots, x_n + y_n) \text{ and} \\ c\boldsymbol{x} &= (cx_1, \ldots, cx_n). \end{aligned} \tag{1.5}$$

When $n = 2$ or 3, it can be seen that the first equation in (1.5) amounts to the parallelogram law of addition. Of course, for $n = 1$, it is just the addition of real numbers.

1.4 Relations

A *relation* between two nonempty sets A and B is a subset R of the Cartesian product $A \times B$. An element a of A is *related to* an element b of B if $(a, b) \in R$. In this section, it suffices to suppose that $A = B$. A *partial order* on A is a relation R on $A \times A$ which is

1. *Reflexive*: $R \supseteq \Delta = \{(a, a) \mid a \in A\}$, the *diagonal* of $A \times A$, i.e. every a in A is related to itself,
2. *Asymmetric*: If $(a, b) \in R$ and $(b, a) \in R$, then $a = b$,
3. *Transitive*: If $(a, b) \in R$, $(b, c) \in R$, then $(a, c) \in R$.

From now on we will write (a, b) as $a \leq b$ and a partially ordered set, i.e. a set A with partial order $\leq$ as $(A, \leq)$. "Partial" means given a and b in A, it is not required that either $a \leq b$ or $b \leq a$. If for any two a, b in A, either $a \leq b$ or $b \leq a$, then $\leq$ is a *total order.*

Examples.

1. Ancestry is a relation on the set of people, which is only transitive.
2. Let $\mathcal{P}(X)$ be the set of all subsets of a set X, called the *power set* of X. The inclusion $\subseteq$ is a partial order on the set $A = \mathcal{P}(X)$.
3. The relation $\leq$ on $\mathbb{R}$ is a total order.

Definition. A *chain* in a partially ordered set $(A, \leq)$ is a totally ordered subset $\mathcal{C}$ of A under $\leq$. An element a of a partially ordered set $(A, \leq)$ is a *maximal element* of A if there is no $b \neq a$ in A with $a \leq b$. The following is a postulate in set theory that we will need later on.

Zorn's Lemma. *If, in a partially ordered set $(A, \leq)$, every chain $\mathcal{C}$ has an* upper bound *(an element b of A with $a \leq b$ for all a in $\mathcal{C}$), then A has a maximal element.*

1.5 Concept of a Function

Suppose A and B are non-empty sets. A *function* from A to B is a subset S of the Cartesian product $A \times B$ such that for each a in A, there is a unique (one and only one) b in B with (a, b) in S. We may rephrase it as follows: A *function* or a *map* consists of

1) a non-empty set A, called the *domain*,
2) a set B called the *codomain*, and
3) a rule f which assigns to each element a of A, a unique (one and only one) element $b = f(a)$ of B. We write it as $f : A \to B$ which is read as "f is a function from A to B."

It is a misconception that the rule $f(a)$ is a "formula."

Example. Let A be the set of humans and B the set of women. Then $m : A \to B$ given by the rule $m(a)=$ "the mother of a" is a function. [We are thinking of real people, not legendary figures born out of sun, rain, or wind, etc.] This rule for $m(a)$ would defy all attempts to describe it by a mathematical formula. In the same context, $s(a)=$ sister of a is not a function. This is obvious, not every a in A has a sister, and whenever it does, it may not be unique.

Two major issues when we study functions $f : A \to B$ are injectivity and surjectivity. Before defining these terms, let us emphasize that a given function is not just the rule $f(a)$, but has three components as indicated in the notation $f : A \to B$. Two functions $f : A \to B$ and $g : X \to Y$ are equal if and only if $X = A$, $Y = B$ and $f(a) = g(a)$ for all a in $A = X$. The function $1_A : A \to A$ given by $1_A(a) = a$ for all a in A is called the *identity function on A*. If $f : X \to Y$ and $A \subset X$, the *restriction* of f to A is the function $f_{|A} : A \to Y$ given by $f_{|A}(a) = f(a)$ for a in A.

Definition. A function $f : A \to B$ is *injective* or *one-to-one* if $f(a_1) = f(a_2)$ implies $a_1 = a_2$, that is, no two a in A have the same values $f(a)$ in B. It is *surjective* or *onto* if for each b in B, there is an a in A with $f(a) = b$. It is *bijective* if it is both injective and surjective.

Examples.

1. Consider the following four functions, all given by the same rule $f(x) = x^2$.

#1 $f : \mathbb{R} \to \mathbb{R}$

#2 $f : \mathbb{R}^+ \to \mathbb{R}$

#3 $f : \mathbb{R} \to \mathbb{R}^+$

#4 $f : \mathbb{R}^+ \to \mathbb{R}^+$

Here $\mathbb{R}^+$ is the set of strictly positive real numbers. The function #1 is neither injective nor surjective, because whereas $f(-1) = f(1)$ and -1 is not the square of any real number x. The function #2 is injective but not surjective, whereas #3 is surjective but not injective. Finally, the function #4 is bijective.

2. Our earlier example, $m : A \to B$ given by $m(a) =$ "the mother of a" is neither injective nor surjective. (Why?)

3. A bijective map $\sigma : X \to X = \{1, \dots, n\}$ is called a *permutation* on n symbols $1, \dots, n$. For example, If $X = \{1, 2, 3\}$, then $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ is a *cycle on three symbols* $1, 2, 3$ whereas $\mu(1) = 2$, $\mu(2) = 1$, and $\mu(3) = 3$ is a permutation that switches 1 and 2, but leaves 3 fixed.

Definition. If A and B are two sets, we say that A and B have the same *number of elements*, or have the same *cardinality*, if there is a bijection $f : A \to B$.

It is easy to see that $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality but $\mathbb{Q}$ and $\mathbb{R}$ don't.

Definition. Suppose $f : A \to B$ is a function. Its *image* or *range* is the subset $f(A) = \{f(a) \mid a \in A\}$ of B. Thus f is surjective if $f(A) = B$.

Now suppose a given function $f : A \to B$ is bijective, so that for each b in B there is one and only one a in A with $f(a) = b$. We define a function $g : B \to A$ by $g(b) = a$ if and only if $b = f(a)$, called the *inverse* of $f : A \to B$. We write $g = f^{-1}$.

Examples.

1. For the function #4 only (in the example above), which is bijective, $f^{-1}(y) = \sqrt{y}$.

2. The *exponential function* $\exp : \mathbb{R} \to \mathbb{R}^+$ given by $\exp(x) = e^x$ is bijective. Its inverse $\exp^{-1} = \ln : \mathbb{R}^+ \to \mathbb{R}$ is called the (natural) logarithm.

3. For $\sin : [\frac{-\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$, $\sin^{-1}$ is often denoted by arcsin.

4. It is easy to check that $f : \mathbb{R} \to \mathbb{R}$ given by $y = f(x) = 2x + 3$ is bijective. Its inverse is obtained by solving for x in terms of y, so $x = f^{-1}(y) = \frac{1}{2}(y - 3)$.

5. The linear map $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by $(u, v) = T(x, y) = (x + y, x - y)$ is bijective and $(x, y) = T^{-1}(u, v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right)$.

1.6 Composite Functions

If $f : A \to B$ and $g : C \to D$ with $f(A) \subseteq C$, their *composition* is the *composite map* $g \circ f : A \to D$ given by $(g \circ f)(a) = g(f(a))$. It is the so-called "*function of a function.*" It is easy to check that the composition of maps is *associative*: $h \circ (g \circ f) = (h \circ g) \circ f$.

Examples.

1. If $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ is given by $g(y) = 2y + 5$, then $(g \circ f)(x) = 2x^2 + 5$.

2. If $f : A \to B$ is bijective and $g = f^{-1}$, then $g \circ f = 1_A$ and $f \circ g = 1_B$.

3. It is easy to check that the functions like $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$T(x, y) = (3x + 5y, 2x + 3y) \tag{1.6}$$

satisfy the condition (1.3) for linearity. If $T(x, y) = (u, v)$, we can write (1.6) as

$$\left.\begin{aligned} u &= 3x + 5y \\ v &= 2x + 3y \end{aligned}\right\}. \tag{1.7}$$

Let us take another linear map $S : \mathbb{R}^2 \to \mathbb{R}^2$ given by $S(u, v) = (u + v, u - v)$. Now if $S(u, v) = (w, z)$, then

$$\left.\begin{aligned} w &= u + v \\ z &= u - v \end{aligned}\right\}. \tag{1.8}$$

The composite map $S \circ T : \mathbb{R}^2 \to \mathbb{R}^2$ is obtained by substituting (1.7) in (1.8), i.e.

$$\left.\begin{aligned} w &= 5x + 8y \\ z &= x + 2y \end{aligned}\right\}.$$

Therefore,

$$S \circ T(x, y) = (5x + 8y, x + 2y). \tag{1.9}$$

Note that $S \circ T$ also satisfies the condition (1.3) for linearity. It is true that in general, the composite of linear maps is again linear.

1.7 Fields of Scalars

In contemporary textbooks on linear algebra, the term “scalar” means a real number. However, this is not only unnecessarily restrictive, but is also inadequate for some interesting applications of linear algebra such as to the currently popular subject of cryptography. We shall also vary the fields of scalars to prove the impossibility of the ancient Greek problems of trisecting an angle and duplicating cubes (using straightedge and compass only). It is often convenient to write a function $f : A \to B$ which takes an element a of A to $b = f(a)$ of B by $A \ni a \mapsto b = f(a) \in B$.

Definition. A *field* is a set K with at least two elements, denoted by 0 and 1, together with two functions namely an *addition* $K \times K \ni (x, y) \mapsto x + y \in K$, and a *multiplication* $K \times K \ni (x, y) \mapsto x \cdot y \in K$ satisfying the following rules for arithmetic. [We shall write $x \cdot y$ simply as xy.]

1) $0 + x = x$ for all x in K.

2) $1x = x$ for all x in K.

3) Existence of an *additive inverse*: given x in K, there is y in K with $x + y = 0$. [We write y as $-x$.]

4) Existence of a *multiplicative inverse*: given $x \neq 0$ in K, there is y in K with $xy = 1$. [We write y as x^{-1} or $\frac{1}{x}$.]

5) *Commutativity* for addition: $x + y = y + x$ for all x, y in K.

6) *Associativity* for addition: $x + (y + z) = (x + y) + z$ for all x, y, z in K.

7) *Commutativity* for multiplication: $xy = yx$ for all x, y in K.

8) *Associativity* for multiplication: $x(yz) = (xy)z$ for all x, y, z in K.

9) *Distributive Law*: $x(y + z) = xy + xz$ for all x, y, z in K.

Examples. It is expected that the reader is already familiar with the following three fields:

1. The field $\mathbb{Q}$ of *rationals*, that is, fractions of the form $\frac{m}{n}$ where m, n are integers and $n > 0$.
2. The field $\mathbb{R}$ of real numbers.
3. The field $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$ of *complex numbers.*

The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of *natural numbers* is not a field for a variety of reasons. The set $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ of *integers* (or whole numbers) is not a field because of the lack of multiplicative inverses.

Note. Before giving further examples, a historical remark is in order. It was the German school of number theorists who pioneered the study of fields. Hence, it is traditional to use the letter K or k (after the German word *Körper* for field).

Example. If k is a field, we denote by $k[x]$ the set of *polynomials*

$$f(x) = c_0 + c_1 x + \ldots + c_n x^n, \tag{1.10}$$

over k, that is, the expressions (1.10) with *coefficients* c_j in k. The polynomials are added and multiplied in the usual way. If $c_n \neq 0$, we call it the *leading coefficient* of $f(x)$ and n the *degree* of $f(x)$. We denote the degree of $f(x)$ by $\deg(f)$. We call $f(x)$ *monic* if $a_n = 1$.

Certainly, $k[x]$ is not a field, because if $\deg(f) \geq 1$, $f(x)g(x) = 1$ cannot hold for any $g(x)$ in $k[x]$. However, the set $K = k(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], g(x) \neq 0 \right\}$ of *rational functions over* k is a field.

Definition. Suppose k is a subset of a field K, such that $0, 1 \in k$. We call k a *subfield* of K if for all x, y in K, $x - y$ and xy^{-1} are also in k. [Whenever we write y^{-1} or $\frac{1}{y}$, it is understood that $y \neq 0$.]

Examples.

1. $\mathbb{R}$ is a subfield of $\mathbb{C}$, $\mathbb{Q}$ is a subfield of both $\mathbb{R}$ and $\mathbb{C}$. Both $\mathbb{Q}$ and $\mathbb{R}$ are subfields of $\mathbb{C}$.

2. Suppose $d = 2, 3, 5, 6, 7, 10, \ldots$ is a positive integer with no square factor larger than 1. Then $k = \mathbb{Q}(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

Finite Fields

A *finite field* is a field with only finitely many elements. These fields are becoming increasingly popular for their use in cryptography. Finite fields are based on *modular arithmetic*. Suppose $p = 2, 3, 5, 7, \ldots$ is a given prime number. Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ denote the set of all possible remainders r $(0 \leq r < p)$ under division by p. The following rules for addition and multiplication turn the set $\mathbb{F}_p$ into a field. For r, s in $\mathbb{F}_p$,

- $r \oplus s =$ the remainder of $r + s$ under division by p and

- $r \odot s =$ the remainder of rs under division by p.

Examples.

1. Suppose $p = 5$. Then $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. In $\mathbb{F}_5$,
   - $3 \oplus 4 = 2$ (the remainder of $3 + 4 = 7$ under division by 5) and
   - $3 \odot 4 = 2$ (being the remainder of $3 \cdot 4 = 12$ under division by 5).

2. Integers and polynomials have striking similarities. Both have the *division algorithm*: Given a, d in $A = \mathbb{Z}$ or $k[x]$ with $d \neq 0$, there are unique q and r in A such that

$$a = qd + r \ (r \prec d). \tag{1.11}$$

[The symbol $r \prec d$ means $0 \leq r < \ \mid d \mid$ if $A = \mathbb{Z}$ and $\deg(r) < \deg(d)$ if $A = k[x]$.]

One says that a is *divisible* by $d \neq 0$ if it leaves no remainder under division by d, that is, if in (1.11) the remainder $r = 0$. If a is divisible by d, we say that d is a *factor* of a and a is a *multiple* of d. An element p of $A = \mathbb{Z}$ or $k[x]$ is *prime* (in the case of $A = k[x]$ also called *irreducible over* k) if it has no nontrivial factors. This is to say that the only factors of p are c and cp, where $c = \pm 1$ for $A = \mathbb{Z}$ and $c \in k^{\times} = \{\alpha \in k \mid \alpha \neq 0\}$ if $A = k[x]$.

Now suppose that $P(x)$ is an irreducible polynomial of degree > 1 over k, and let $K = \{r(x) \in k[x] \mid \deg(r) < \deg(P)\}$. In other words, K consists of all possible remainders under (long) division by $P(x)$. Just like $\mathbb{F}_p$, the set K also becomes a field if we define $\oplus$ and $\odot$ in the same manner, namely: for $r(x)$, $s(x)$ in K,

- $r(x) \oplus s(x) =$ the remainder of $r(x) + s(x)$ under division by $P(x)$, and
- $r(x) \odot s(x) =$ the remainder of $r(x)s(x)$ under division by $P(x)$.

We denote this field by $k[x]/(P(x))$.

In particular, if $k = \mathbb{F}_p$, K has $q = p^n$ elements, where $n = \deg(P)$. This is so because, each of the n coefficients of a remainder $r(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ has p choices. We denote this finite field by $\mathbb{F}_q$ or $\mathbb{F}_{p^n}$. Any finite field (i.e., a field with finite number of elements) is $\mathbb{F}_q$ for a prime power $q = p^n$. Sometimes we shall write a finite field simply as $\mathbb{F}$.

1.8 Techniques for Proving Theorems

A *theorem* is a mathematical statement which is true. But no mathematical statement is a theorem unless proved to be true. A theorem cannot be proved by examples. There are different ways to prove theorems. We illustrate them below with some theorems that are easy to prove.

1. *Direct Proof.*

   Most of the proofs in this book are direct. They are mostly trivial consequences of definitions. Here is an example of such a proof.

   Definition. An integer n is *even* if it is twice another integer r, i.e. $n = 2r$. Similarly, an integer m is *odd* if it is not even, i.e. if $m = 2s + 1$ for an integer s.

   Theorem. *The sum of two odd integers is even.*

   Proof. Let the two odd integers be $m = 2r + 1$, $n = 2s + 1$. Their sum is $(2r + 1) + (2s + 1) = 2(r + s + 1)$, which is twice another integer $r + s + 1$. Hence, by our definition $m + n$ is even. □

2. *Proof by Contradiction.*

   To prove a theorem by contradiction, one assumes it is false. Following a sequence of logical arguments, one arrives at a conclusion, which is a contradiction. Most mathematical facts are stated as theorems, propositions, corollaries, etc., like

   Theorem. *"Given this", "then that" or "If this", "then that".*

   "Given this" is called the *hypothesis*, "then that" is the *conclusion* of the theorem.

   Theorem. *If m and n are both even, then $m + n$ is also even.*

   Proof. By contradiction. Suppose $m = 2r$, $n = 2s$ are even, but $m + n$ is not even. Then $m + n$ is odd. Let $m + n = 2t + 1$. Also, $m+n = 2r+2s = 2(r+s)$. Hence $2(r+s) = 2t+1$, or $1 = 2(r+s-t)$, i.e. 1 is even, which is a contradiction. □

3. *Proof by Induction.*

If $S(n)$ is a statement about natural numbers $n = 1, 2, 3, \dots$, it may or may not be true. For example

$$S(n) : 1 + 2 + 3 + \cdots + n = n^2 + 1$$

is not true for most n. In fact, it is false for all $n \geq 1$. However,

$$S(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \qquad (*)$$

is a true statement for all n.

To prove $(*)$ by induction one first proves it for a *base case* $n = 1$, 2 or the smallest n_0 for which it makes sense and is true. Then one assumes $S(n)$ is true for any given $n \geq n_0$ and shows that it leads to $S(n+1)$ is also true.

Theorem. *For all integers $n \geq 2$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.*

Proof. Let $S(n) : 1+2+\cdots+n = \frac{n(n+1)}{2}$. Then $S(2) : 1+2 = \frac{2(2+1)}{2}$ is true. Now suppose $S(n)$ is true for any given $n \geq n_0 = 2$. Then $1+2+\cdots+n+(n+1) = (1+2+\cdots+n)+(n+1) = \frac{n(n+1)}{2}+n+1 = (n+1)\left(\frac{n}{2}+1\right) = \frac{(n+1)[(n+1)+1]}{2}$, which shows that $S(n+1)$ is also true. Hence it is true for all $n \geq n_0 = 2$. □

4. *Original Proof.*

Sometimes the original proof, which led to the discovery, is the most illuminating proof. Folklore attributes the following proof of the above theorem to C. F. Gauss. He discovered it when he was still a little boy. He was challenged to add all the numbers up to n, with higher and higher n. This is how he discovered it.

If we add n terms of the sum

$$N = 1 + 2 + \cdots + n$$

to itself in reverse order, we get $2N$ equal to

$$\begin{array}{c} 1 + \quad 2 \quad + \cdots + (n-1) + n \\ n + n - 1 \; + \cdots + \quad\; 2 \quad\; + 1 \\ \hline (n+1) + (n+1) + \cdots + (n+1) \end{array}$$

which is $(n+1)$ taken n times. Hence

$$2N = n(n+1),$$

i.e.

$$N = \frac{n(n+1)}{2}.$$

5. *Constructive Proof*

In mathematics it is often claimed that such and such objects exist. Examples are the *determinant* $\det(A)$ of a square matrix A, an *antiderivative* of a continuous function. One shows the existence by exhibiting or constructing it. The antiderivative of a function $f(x)$ is a function $F(x)$, such that its derivative $F'(x) = f(x)$.

Fundamental Theorem of Calculus. *If $f(x)$ is a real valued continuous function defined on a closed interval $[a, b]$, then its antiderivative $F(x)$ exists, and the area under the graph of $y = f(x)$ from $x = a$ to $x = b$, i.e.*

$$\int_a^b f(x)dx = F(b) - F(a).$$

Proof. For x in $[a, b]$, to construct $F(x)$, put

$$F(x) = \int_a^x f(t)dt.$$

Clearly,

$$\int_a^b f(x)dx = F(b) - F(a),$$

since $F(a) = 0$.

We now show that $F'(x) = f(x)$. For x in the open interval (a, b), the ratio rise/run for $F(x)$, i.e.,

$$\begin{aligned}\frac{F(x+h) - F(x)}{h} &= \frac{\text{area of the shaded strip}}{h} \\ &= \frac{h\,f(x)}{h} + \epsilon(h) = f(x) + \epsilon(h),\end{aligned}$$

where the error $\epsilon(h) \to 0$ as $h \to 0$ (see Figure 1.1). Taking the limit,

$$F'(x) = \lim_{h\to 0} \frac{F(x+h) - F(x)}{h} = \lim_{h\to 0} (f(x) + \epsilon(h)) = f(x). \quad \square$$

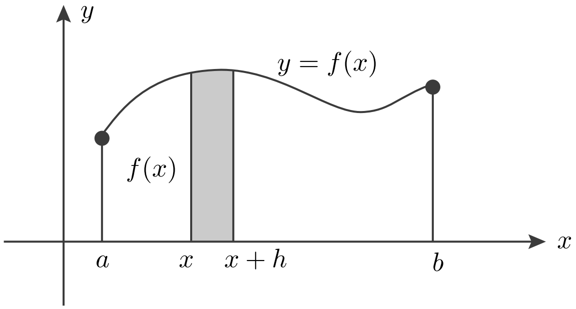


FIGURE 1.1: Fundamental Theorem of Calculus

EXERCISES

1. Find the flaw in the proof by induction that everybody is poor, by proving the following statement: $S(n)$: A person with n pennies is poor.

   Proof. We prove that $S(n)$ is true for all $n \geq 0$.

   $S(0)$ is clearly true, since a penniless person is poor. So suppose $S(n)$ is true, i.e. a person with n pennies ($n \geq 0$) is poor. One more penny is not going to turn a poor person into a rich person. So $S(n+1)$ is also true. Thus by induction, $S(n)$ is true for all n.

2. Show that the composition of injective (resp. surjective, bijective) maps is again injective (resp. surjective, bijective).

3. (a) Suppose X is a finite set. Show that a function $f : X \to X$ is injective if and only if f is surjective.

   (b) Show that (a) is always false if X is not finite.

   [Thus, one way to define a finite set is if (a) holds.]

4. Suppose A and S are finite sets with cardinalities a and s, respectively. Let A^S denote the set of all functions $f : S \to A$. Show that the cardinality of A^S is a^s.

   [This explains the notation A^S.]

5. Show that $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality but $\mathbb{Q}$ and $\mathbb{R}$ don't.

6. Show that $\mathbb{Q}$ is a subfield of every subfield k of $\mathbb{R}$.

7. Prove the uniqueness of the additive and the multiplicative inverses of field elements.

8. Prove that in a field K, the cancellation is valid, that is, if a is a nonzero element of K, then $ax = ay$ implies $x = y$. [This is not true if $a = 0$.]

9. Show that $\mathbb{Q}(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s, \in \mathbb{Q}\}$ is a subfield of $\mathbb{R}$.

10. Show that $\mathbb{F}_p$ is a field. [For multiplicative inverse, if $0 < a < p$, then the only common factor of a and p is 1. So computing the remainder by the Euclidean algorithm, and solving backward for it, one gets $1 = ax + by$ for some integers x and y . Then $a^{-1} = \overline{x}$, the remainder of x under division by p (see [4, p. 7]. If p were not prime, $1 = ax + py$ is possible if and only if a and p have no common factor > 1.]

11. **Modular Arithmetic.**

    This exercise will be used in the application of linear algebra to cryptography.

    Finite fields are examples of a more general and the so-called *modular arithmetic.* Given any integer $m > 1$ (or a polynomial of degree > 1) we perform addition and multiplication on the set $\{0, 1, \ldots, m-1\}$ of remainders under division by m as follows. Add or multiply, as the case may be, but keep only the remainders of sums and products. For example, if $m = 10$, $7 + 5 = 12 \equiv 2 \bmod 10$ (this symbol means when 12 is divided by 10, it leaves the remainder 2). Similarly, $7 \cdot 4 = 28 \equiv 8 \bmod 10$, whereas $4 \cdot 5 = 20 \equiv 0$ mod 10. Thus if m is not prime, the product of remainder r, s with neither r nor s zero can be zero. Therefore a nonzero remainder a may not have a multiplicative inverse b in the sense $ab \equiv 1 \mod m$. However, prove that the following is true.

    (a) Suppose a with $0 < a < m$ has no common factor > 1 with m. Then it has a multiplicative inverse b in the set $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$.

    Hint: Again use the Euclidean algorithm.

    (b) Let $m = 26$ and identify the letters A–Z of the alphabet with the remainders 0–25 with A = 0, B = 1, …, Z = 25. Find the letter A–Z which is the multiplicative inverse of the letter H mod 26.

12. Show that for a polynomial $p(x)$ of degree n, and irreducible over k with modular arithmetic modulo $p(x)$, $K = k[x]/(p(x)) = \{f(x) \mid \deg f(x) < n\}$ is a field. [Hint: Ditto Exercise 10].

    Note. "*$p(x)$ irreducible over k*" means it does not factor nontrivially in $k[x]$. For example, $x^2 + 1$ is irreducible over $\mathbb{R}$, but not over $\mathbb{C}$ as $x^2 + 1 = (x + i)(x - i)$.

13. Let $K = \mathbb{F}_7 = \{0, 1, \ldots, 6\}$. What is $\frac{1-4^2}{5^3+3}$ in K?

14. Suppose a is an element of a field K. We say that a is a *square* in K if $a = b^2$ for some b in K. It is obvious that 0 and 1 are both squares in any given field. If we do not count 0, precisely "half" of the real numbers (the positive reals) are squares. The other half (the negative reals) are non-squares.

    Experiment with all primes p in the range $2 < p < 20$ if the same is true for squares in $K = \mathbb{F}_p$. [Note that for $K = \mathbb{F}_2$ and $\mathbb{C}$, every a in K is a square in K.]

15. Prove or disprove your observation in Exercise 14 above.

16. Let k be a subfield of K, $f(x) = c_0 + c_1x + \cdots + c_nx^n \in k[x]$. We say that an element α of K is a *root* of $f(x)$ if $f(\alpha) = c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$.

    Suppose $f(x) \in k[x]$ and $\deg(f) \leq 3$. Show that $f(x)$ is prime (that is, irreducible over k) if and only if $f(x)$ has no root in k.

17. By Exercise 16 above, $p(x) = x^2 + 1$ is prime in $\mathbb{R}[x]$, therefore by Exercise 12 above, $K = \mathbb{R}[x]/(x^2 + 1)$ is a field.

    (a) Can you identify K with a field which is already familiar to you? In that field, what does the remainder x in K correspond to?

    (b) In K, find the multiplicative inverse of $1 - x$.

    [Hint: Note that $1 + x^2$ is zero in K and $\frac{1}{1-x} = \frac{1}{1-x} \times \frac{1+x}{1+x} = \frac{1+x}{2-(1+x^2)}$.]

18. Use Exercise 16 to show that $p(x) = x^2 + x + 2$ is a prime element of $\mathbb{F}_5[x]$, hence $K = \mathbb{F}_5/(x^2 + x + 2)$ is a field. Compute $\frac{1}{2+3x}$ in K.

    Remark. Let $A = \mathbb{Z}$ or $k[x]$. Suppose p is a prime element of A and $a \neq 0$ with $a \prec p$. By the Euclidean algorithm, one can write the g.c.d. (the greatest common divisor) of a and p, which is 1 as $1 = \lambda a + \mu p$, with λ, μ in A. Since μp is zero in $K = \mathbb{F}_p$ (resp. $k[x]/(p)$), we have $a^{-1} = \lambda$ in K. Thus Euclidean algorithm also provides an algorithm to compute the multiplicative inverses of a in such a field K.

19. Suppose k is a subfield of a field K (e.g. $k = \mathbb{Q}$, $K = \mathbb{R}$) and $f(x) \in k[x]$. Show that

    (a) α in K is a root of $f(x)$ if and only if $x - \alpha$ divides $f(x)$ in $K[x]$.

    (b) $f(x)$ has at most $n = \deg(f)$ roots in K.

2

Matrix Algebra

Linear algebra is the study of linear maps, the vector-valued functions $\boldsymbol{u} = L(\boldsymbol{x})$ of a vector variable $\boldsymbol{x}$, having the linearity property: $L(a\boldsymbol{x} + b\boldsymbol{y}) = aL(\boldsymbol{x}) + bL(\boldsymbol{y})$, where a, b are scalars. Such functions can be scaled and added, provided their domains and codomains are the same. We can even multiply or compose two such functions, provided the range of the first is a subset of the domain of the second. We shall see in Chapter 4 that when the domains and codomains are "finite dimensional vector spaces," the algebra of such functions is basically the matrix algebra which we study in this chapter.

2.1 Matrix Operations

Let K be a given field, for example, the field $\mathbb{R}$ of real numbers. If $m, n \geq 1$ are integers, an *$m \times n$ matrix over the field K* of scalars is an $m \times n$ array

$$A = (a_{ij}) = \begin{pmatrix} a_{11} \dots & a_{1n} \\ \vdots & \\ a_{m1} \dots & a_{mn} \end{pmatrix}$$

with a_{ij} in K. The scalar a_{ij} is called the ij-th or *(i, j)-th entry* of A. We call $m \times n$ the *size of the matrix A*. Note that $m \times n$ is not the same size as $n \times m$, unless $m = n$. A *square matrix* of size n is an $n \times n$ matrix. Two matrices $A = (a_{ij}), B = (b_{ij})$ over K are *equal* if and only if i) they are of the same size, and ii) $a_{ij} = b_{ij}$ for all i, j.

The square matrix $A = (a_{ij})$ of size n with

$$a_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

is called the *identity matrix* of size n and is denoted by I_n or simply I if its size is clear from the context. The $m \times n$ matrix, not necessarily a square one, with every entry equal to zero is denoted by 0, and is called the *zero matrix*. A square matrix $D = (d_{ij})$ with $d_{ij} = 0$ if $i \neq j$ is called the *diagonal matrix.* A square matrix $A = (a_{ij})$ is *upper triangular* if every entry below the diagonal is zero, i.e. $a_{ij} = 0$ if $i > j$. It is *lower triangular* $a_{ij} = 0$ for $i < j$.

Suppose $A = a_{ij}$ is an $m \times n$ matrix. Its j-th *column* is the $m \times 1$ matrix $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ and its i-th *row* is the $1 \times n$ matrix $(a_{i1} \dots a_{in})$. Thus A has m rows and n columns.

For given $m, n \geq 1$, we will let $M(m \times n, K)$ denote the set of all $m \times n$ matrices over K. We shall write $M(n, K)$ for $M(n \times n, K)$.

2.1.1 Addition and Scaling of Matrices:

The matrices in the set $V = M(m \times n, K)$ can be added and scaled by elements c of K entry-wise: if $A = (a_{ij})$, $B = (b_{ij})$ are in V, then

$$\begin{aligned} A + B &= (a_{ij} + b_{ij}) \text{ and} \\ cA &= (ca_{ij}). \end{aligned} \tag{2.2}$$

Examples.

1. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ if and only if $a = 1$, $b = 2$, $c = 3$, and $d = 4$.

2. If $A = \begin{pmatrix} 1 & 2 \\ -2 & 3 \end{pmatrix}, B = \begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix}$ then $A + B = 4I$.

Many properties of matrix addition and scalar multiplication are almost immediate. We shall prove a couple of them and leave others as exercises.

1) $A + 0 = A$, because if $A = (a_{ij})$, then $A + 0 = (a_{ij} + 0) = (a_{ij}) = A$.

2) $A + B = B + A$. Let $A = (a_{ij})$ and $B = (b_{ij})$. Then $A + B = (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = (b_{ij}) + (a_{ij}) = B + A$.

EXERCISES

1. Compute $aA + bB$ for $a = -2$, $b = 3$ and

$$A = \begin{pmatrix} 10 & 0 & -6 \\ -4 & 2 & 1 \\ 5 & -7 & 11 \end{pmatrix}, \quad B = \begin{pmatrix} -4 & 1 & 6 \\ 5 & 7 & 3 \\ 1 & 11 & 9 \end{pmatrix}.$$

2. Prove the following properties of the matrix addition and the scalar multiplication.
   (a) $(A+B)+C = A+(B+C)$, $A+(-1)A = 0$,
   (b) For scalars c, d; $(c+d)A = cA + dA$, $c(A+B) = cA + cB$,
   (c) $(cd)A = c(dA)$, $1A = A$.

Note. The Euclidean n-space $\mathbb{R}^n$ may be regarded either as $M(n \times 1, \mathbb{R})$ or $M(1 \times n, \mathbb{R})$. In either case, the vector addition and the multiplication of a vector by a scalar are the same as the matrix addition and the scalar multiplication of matrices. More generally, the Cartesian product $\underbrace{V \times \cdots \times V}_{m \text{ times}}$, where $V = K^n$ may be viewed as $M(m \times n, K)$, where the i-th component of an element of $V \times \ldots \times V$ is the i-th row of the corresponding matrix in $M(m \times n, K)$.

Prelude. The above properties of the addition and scalar multiplication make $V = M(m \times n, K)$ into a mathematical object we shall call a vector (or a linear) space. Thus a vector may be a matrix, not just an arrow as some students habitually tend to think.

2.1.2 Matrix Multiplication

Motivation

As remarked at the beginning of Chapter 1, linear algebra is the study of linear maps. The matrices provide a convenient way to keep track of some (but not all of them). Some examples of linear maps are linear substitutions like

$$S : w = u + v, \;\; z = u - v$$

and

$$T : u = 2x + 3y, \;\; v = 3x + 5y.$$

To recall a classical application of linear substitutions, suppose we want to know which conic section is represented by the equation

$$6x^2 + 15y^2 + 19xy = 1.$$

The substitution T above clears the mixed term $19xy$ from the quadratic form $6x^2 + 15y^2 + 19xy$ and we get

$$uv = 1.$$

Clearing mixed terms from quadratic forms is one of the goals of the chapter on diagonalization. Making further the linear substitution S, we transform the last equation to

$$w^2 - z^2 = 4$$

which as we know represents a hyperbola.

In the language recalled briefly in Chapter 1, the linear substitutions above are nothing but the linear maps S, $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by

$$S(u, v) = (u + v, u - v)$$

and

$$T(x, y) = (2x + 3y, 3x + 5y).$$

The reduction of the quadratic form $6x^2 + 15y^2 + 19xy$ to $w^2 - z^2$ involves computing the composite map $S \circ T : \mathbb{R}^2 \to \mathbb{R}^2$, which again is linear, as can be checked by verifying the requirement (1.3) for it to be so.

In Chapter 4, we will associate to each linear substitution its matrix. Now recall we also asserted at the beginning of Chapter 1 that the algebra of linear maps, say $T : \mathbb{R}^n \to \mathbb{R}^n$ can be identified with (cf. Theorem 4.14) the algebra of $n \times n$ matrices over $\mathbb{R}$, where the composition of linear maps S, $T : \mathbb{R}^n \to \mathbb{R}^n$ corresponds to the multiplication of their respective matrices, if defined properly.

To guess the right multiplication, we compute the composite map $S \circ T$.

$$\begin{aligned}(w, z) &= S \circ T(x, y) = S(T(x, y))\\ &= S(2x + 3y, 3x + 5y)\\ &= ((2x + 3y) + (3x + 5y), (2x + 3y) - (3x + 5y))\\ &= ((1 \cdot 2 + 1 \cdot 3)x + (1 \cdot 3 + 1 \cdot 5)y, (1 \cdot 2 - 1 \cdot 3)x + (1 \cdot 3 - 1 \cdot 5)y).\end{aligned}$$

The (standard) matrix of T (see Example 1, Section 4.3) is

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$$

and, similarly, that of S is

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

If the matrix product BA is to correspond to the linear map $S \circ T$ we computed above, then

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

must be equal to

$$\begin{pmatrix} 1 \cdot 2 + 1 \cdot 3 & 1 \cdot 3 + 1 \cdot 5 \\ 1 \cdot 2 - 1 \cdot 3 & 1 \cdot 3 - 1 \cdot 5 \end{pmatrix}$$

i.e.

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} =$$

$$\begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}.$$

In other words, the (i,j)-th entry of BA is $\sum\limits_{s=1}^{2} b_{is}a_{sj}$. Changing the role of A and B, we could also put it as: if $C = (c_{ij}) = AB$, then $c_{ij} = \sum\limits_{s=1}^{2} a_{is}b_{sj}$.

Thus, if we want the multiplication of matrices to correspond to the composition of linear maps they have been associated to, there is no other way but to have the following

Definition. Suppose $A = (a_{ij})$ is an $m \times r$ matrix and $B = (b_{ij})$ is an $r \times n$ matrix. The *product* AB is the $m \times n$ matrix $C = (c_{ij})$ whose ij-th entry

$$c_{ij} = \sum_{s=1}^{r} a_{is}b_{sj}. \tag{2.3}$$

Before working out some numerical examples, we emphasize that in order for AB to be defined, the number of columns of A must be equal to the number of rows of B for (2.3) to make sense. The product AB has as many rows (resp. columns) as the matrix A (resp. B) does. [In the numerical examples, unless stated otherwise, the field of scalars $K = \mathbb{R}$.] It is convenient to look at the equation (2.3) as follows. Suppose $\boldsymbol{x} = (x_1 \dots x_n) \in M(1 \times n, K)$ and $\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in M(n \times 1, K)$. Define the *twisted dot product* $\boldsymbol{x} \cdot \boldsymbol{y} = x_1y_1 + \cdots + x_ny_n$. Note that $\boldsymbol{x} \cdot \boldsymbol{y}$ is a scalar. Now let $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ be the rows of A and $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n$ be the columns of B. For every i, j the quantity $\boldsymbol{a}_i \cdot \boldsymbol{b}_j$ is a well defined scalar. The rule (2.3) says that the product $AB = (\boldsymbol{a}_i \cdot \boldsymbol{b}_j)$. In other words, the ij-th entry of the $m \times n$ matrix AB is $\boldsymbol{a}_i \cdot \boldsymbol{b}_j$.

Examples.

1. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 3 & -1 \\ -2 & 5 \end{pmatrix}$

(a) $AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} 1 \cdot 3 + 2 \cdot (-2) & 1 \cdot (-1) + 2 \cdot 5 \\ 3 \cdot 3 + 4 \cdot (-2) & 3 \cdot (-1) + 4 \cdot 5 \end{pmatrix} = \begin{pmatrix} -1 & 9 \\ 1 & 17 \end{pmatrix}.$

(b) $BA = \begin{pmatrix} 3 & -1 \\ -2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3\cdot 1 + (-1)\cdot 3 & 3\cdot 2 + (-1)\cdot 4 \\ (-2)\cdot 1 + 5\cdot 3 & (-2)\cdot 2 + 5\cdot 4 \end{pmatrix}$

$$= \begin{pmatrix} 0 & 2 \\ 13 & 16 \end{pmatrix}.$$

We see that $AB \neq BA$. In other words, the commutative law does not hold for matrix multiplication.

2. $A = \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 3 & 4 \end{pmatrix}$

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

This example shows that, unlike scalars, $AB = 0$ does not imply that either $A = 0$ or $B = 0$.

3. Let A be any of the six 2×2 matrices, one for each possible choice of sign. $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $A^2 = I$. One may want to call any six of these A, a *square root* of I. [Are there other square roots of I?] Note that a real number a has at most two square roots.

4. $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$

$$AB = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}.$$

5. If $S = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

then $SA = \begin{pmatrix} a+\alpha c & b+\alpha d \\ c & d \end{pmatrix}$, $TA = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$, $AS = \begin{pmatrix} a & b+\alpha a \\ c & d+\alpha c \end{pmatrix}$, $AT = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$

Note that the effect of multiplying A on the left by S is to add α-times its second row to the first, and multiplying A on the left by T interchanges its rows. Multiplying by S and T on the right has a similar effect on the columns of A.

6. Let $D = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Then $DA = \begin{pmatrix} pa & pb \\ qc & qd \end{pmatrix}$, and $AD = \begin{pmatrix} pa & qb \\ pc & qd \end{pmatrix}$.

Note that the multiplication on the left by a diagonal matrix scales its rows. The columns are scaled by multiplying A on the right by D.

We now prove one of the expected properties of matrix multiplication and leave the rest as exercises.

Theorem 2.1. *The distributive law $A(B+C) = AB + AC$ holds for matrix multiplication.*

Proof. Let $A = (a_{ij}), B = (b_{ij})$, and $C = (c_{ij})$. Then

$$\begin{aligned} A(B+C) &= (a_{ij})(b_{ij} + c_{ij}) \\ &= \left(\sum_{s=1}^{r} a_{is}(b_{sj} + c_{sj})\right) \\ &= \left(\sum_{s=1}^{r} a_{is}b_{sj}\right) + \left(\sum_{s=1}^{r} a_{is}c_{sj}\right) \\ &= AB + AC. \end{aligned}$$ □

EXERCISES

1. Compute AB if

(a) $A = \begin{pmatrix} 7 & 2 \\ 1 & 3 \end{pmatrix}, B = \begin{pmatrix} -2 & 4 \\ 5 & -1 \end{pmatrix}$,

(b) $A = \begin{pmatrix} 5 & -2 \\ -1 & 4 \\ 4 & 3 \end{pmatrix}, B = \begin{pmatrix} 8 & 11 & -5 \\ 9 & -1 & 2 \end{pmatrix}$,

(c) $A = \begin{pmatrix} 2 & -5 & 4 \\ 3 & 1 & 10 \end{pmatrix}, B = X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

2.* Let the scalars be $\{0, 1, \ldots, 9\} = \mathbb{Z}/10\mathbb{Z}$ in the modular arithmetic mod 10. Multiply

$$A = \begin{pmatrix} 6 & 7 \\ 5 & 9 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 & 5 \\ 4 & 1 \end{pmatrix}$$

and write your answer as $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $0 \le a, b, c, d \le 9$.

3. If $A = \begin{pmatrix} 2 & -5 & 4 \\ 3 & 1 & 0 \end{pmatrix}$ and $C = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$, for which of the following X is $AX = C$?

(a) $X = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}$,

(b) $X = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

4.* Let $K = \mathbb{F}_{11}$, $A = \begin{pmatrix} 3 & 2 \\ 4 & 7 \end{pmatrix}$, $X = \begin{pmatrix} 5 \\ 8 \end{pmatrix}$, $B = \begin{pmatrix} 6 \\ 9 \end{pmatrix}$. Compute $AX+B$.

5. Let E_{ij} be the $n \times n$ matrix with 1 at the (i, j)-th place and zero elsewhere. For a scalar c in K, put $S = I + cE_{ij}$, $i \neq j$. And let T be the $n \times n$ matrix obtained from the identity matrix as follows. In I replace 1 at the (i, i)-th and (j, j)-th entries by zero. Replace zeros at the (i, j)-th and (j, i)-th entry by 1. Suppose A is an $n \times n$ matrix. Compute SA, AS, TA, and AT to conclude what does the multiplication on the left or right by S or T do to the rows or columns of A.

   Definition. The matrices S, T and their products are called *elementary matrices.*

6. Prove the following. Here I is the identity matrix

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

   (a) $IA = AI = A$,

   (b) $(A + B)C = AC + BC$,

   (c) For a scalar c, $c(AB) = (cA)B = A(cB)$,

   (d) $(AB)C = A(BC)$.

7. By 6 (d), the symbol $A^n = \underbrace{A \cdot \ldots \cdot A}_{n \text{ times}}$ makes sense. Suppose $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Prove by induction on n that $A^n = \begin{pmatrix} 1 & na \\ 0 & 1 \end{pmatrix}$.

8. Define the *transpose* A^* of a matrix $A = (a_{ij})$ by $A^* = (a_{ji})$, i.e. the i-th column of A^* is the i-th row of A. (See the example below.) If A, B are matrices of compatible sizes for the matrix operations and c is a scalar, show that

   (a) $(A + B)^* = A^* + B^*$

   (b) $(cA)^* = cA^*$

   (c) $(AB)^* = B^*A^*$

9. The *trace* $\mathrm{tr}(A)$ of a square matrix $A = (a_{ij})$ is the sum $a_{11} + \cdots + a_{nn}$ of its diagonal entries. Show that

(a) $\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B)$.

(b) $\operatorname{tr}(cA) = c\operatorname{tr}(A)$ for any scalar c.

(c) $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Notes.

1. Another notation for transpose is A^T, but for an elementary matrix T, T^T looks nonsensical.
2. Parts (a) and (b) of Exercises 8 and 9 say that these operations are "linear transformations" to be defined later.

Example. The transpose of $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ is $\begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.

2.2 Geometric Meaning of a Matrix Equation

One learns in analytic geometry that two simultaneous equations

$$\begin{aligned} ax + by &= d_1 \\ cx + dy &= d_2 \end{aligned} \tag{2.4}$$

represent points common to the two straight lines in the plane defined by these two equations. There are three possibilities:

1) The two lines overlap. This happens if there is a nonzero scalar λ, such that $a = c\lambda$, $b = d\lambda$, and $d_1 = d_2\lambda$.

2) However, if $a = c\lambda$, $b = d\lambda$, and $d_1 \neq d_2\lambda$, the lines are parallel at a positive distance and have no point in common. We also say that the system (2.4) of two linear equations in two variables x, y is *inconsistent*, if there is no solution.

3) The lines intersect at exactly one point. This happens if $ad - bc \neq 0$.

In matrix notation, (2.4) is the same as a single matrix equation $AX = C$, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$, and $C = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$.

The three cases now can be restated as follows:

1) The first row of the *augmented matrix* $\begin{pmatrix} a & b & d_1 \\ c & d & d_2 \end{pmatrix}$ is a scalar multiple of the second.

2) Only the first row of A is a scalar multiple of the second row of A.

3) The rows of A are not scalar multiples of each other.

Next, if $A = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$, and $C = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$, the matrix equation $AX = C$ represents the intersection of two planes

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1 \\ a_2x + b_2y + c_2z &= d_2. \end{aligned} \tag{2.5}$$

In analytic geometry, one learns that these planes overlap, have no points in common (inconsistent) or intersect in a line depending on the relationship between the rows of the augmented matrix $\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \end{pmatrix}$.

Finally, the system of three equations

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1 \\ a_2x + b_2y + c_2z &= d_2 \\ a_3x + b_3y + c_3z &= d_3 \end{aligned} \tag{2.6}$$

represents the intersection of three planes in $\mathbb{R}^3$.

EXERCISES

1. Describe geometrically the various possibilities in terms of the rows of A and of the augmented matrix $(A : C)$ by writing (2.6) as a single matrix equation $AX = C$.

2. Write each of the following systems of linear equations as a single matrix equation $AX = C$.

   (a) $4x - y = 6$
   $3x + y = 1$

   (b) $3x + 2y - z = -1$
   $-\,3x - y + z = 1$

   (c) $x + y = -1$
   $x - y = -2$
   $2y = 3$

(d) $x + y - z = 1$
$- x - y + z = 2$
$x + y + z = 3$

3. Which of the systems of linear equations in Exercise 2 above have a common solution and which don't?

2.3 Systems of Linear Equations

The above discussion may be extended as follows. Without loss of generality, we may assume that $m \leq n$. By solving the system

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= c_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= c_m \end{aligned} \tag{2.7}$$

of m equations in n variables $x_1, \ldots, x_n$ we mean finding all points $(x_1, \ldots, x_n)$ with coordinates x_j in the given field K of scalars satisfying (2.7). Each equation in (2.6) represents a plane in K^3, if $n = 3$. If n is generic, we call it a *hyperplane* (for the lack of a better name). For $n = 2$, the hyperplanes are straight lines. The system (2.7) represents the intersection of m hyperplanes in $K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$.

For another perspective, recall the definition of a function $f : X \to Y$. It is convenient to define another term.

Definition. For x in X, $y = f(x)$ is called the *image* of x. For a given y in Y, the set $\{x \in X \mid y = f(x)\}$ is called the *preimage* of y and is denoted by $f^{-1}(y)$. If the function $f : X \to Y$ is not surjective, the preimage $f^{-1}(y)$ is empty for at least one y.

Now let us denote the elements of K^n as column vectors $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.
Suppose $A = (a_{ij})$ is an $m \times n$ matrix over K. Consider the function
$L : K^n \to K^m$ given by $L(X) = AX$. Solving the system (2.7) is to determine the preimage $L^{-1}(C)$ of $C = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$ in K^n. If $L^{-1}(C)$ is empty, the system is, by definition, *inconsistent*. We shall assume that, unless stated otherwise, the system is consistent. If $c_1 = \ldots = c_n = 0$, the system is said to be *homogeneous*. A homogeneous system is always consistent.

Gaussian Elimination

In a course on analytic geometry, one learns the *Gaussian Elimination* to find the intersection of two lines. We illustrate it by solving

$$\begin{aligned} 3x + 4y &= 2 \\ 2x + 3y &= 1. \end{aligned} \tag{2.8}$$

Example. To solve (2.8), we multiply the first equation by 2, second by 3, and subtract to get $y = -1$. Now plugging this value of y in either of the equations in (2.8), we find that $x = 2$. Thus $x = 2$, $y = -1$ is a solution to (2.8) as can be checked.

Example.* Now let us consider the equations (2.8) as equations over the field $\mathbb{F}_7 = \{0, 1, \ldots, 6\}$ of seven elements. To solve, we multiply the first equation in (2.8) by $2 \cdot 3^{-1} = 2 \cdot 5 = 3$ and get

$$\left.\begin{aligned} 2x + 5y &= 6 \\ 2x + 3y &= 5 \end{aligned}\right\} .$$

Subtracting, we get $2y = 1$ or $y = 2^{-1} \cdot 1 = 4 \cdot 1 = 4$. Plugging $y = 4$ in one of the two equations of (2.8) we get $x = 0$. Thus $x = 0$, $y = 4$ is a solution to (2.7) in $\mathbb{F}_7$. It is easy to check that again, it is the only solution to (2.8).

When there are a large number of variables, it is convenient to write (2.7) in the matrix notation $AX = C$ and use the following *row reduction* method. We work with the so-called *augmented matrix*

$$(A : C) = \left(\begin{array}{ccc|c} a_{11} & \ldots & a_{1n} & c_1 \\ \vdots & & & \vdots \\ a_{m1} & \ldots & a_{mn} & c_m \end{array}\right)$$

of this system. Multiplying an equation in (2.7) by c is equivalent to scaling the corresponding row of $(A : C)$ by c. A similar statement holds for adding a scalar multiple of an equation in (2.7) to another one as well as for interchanging two equations in (2.7). The advantage of working with the augmented matrix is that we do not have to keep writing the variables. The j-th column of $(A : C)$ keeps track of the j-th variable x_j. If a column of A consists of zeros only, the corresponding variable is missing from the system. Hence we may assume that no column of A is zero.

By interchanging rows of $(A : C)$, if necessary, we assume that $a_{11} \neq 0$. Further, on dividing the first row by a_{11}, we can actually take $a_{11} = 1$. Then on subtracting suitable multiples of the first row from the subsequent ones, we reduce $(A : C)$ to

$$\left(\begin{array}{c|cccc} 1 & b_{12} & \ldots & b_{1n} & b_1 \\ 0 & b_{22} & \ldots & b_{2n} & b_2 \\ \vdots & & & & \vdots \\ 0 & b_{m2} & \ldots & b_{mn} & b_n \end{array}\right).$$

Now in the first column of $B = \begin{pmatrix} b_{22} & \dots & b_{2n} \\ \vdots & & \\ b_{m2} & \dots & b_{mn} \end{pmatrix}$ all entries can be zero (in which case $b_{12} \neq 0$). We go to the first nonzero column $\begin{pmatrix} b_{2r} \\ \vdots \\ b_{mr} \end{pmatrix}$ of B and apply the previous process to the augmented submatrix $\begin{pmatrix} b_{2r} & \dots & b_{2n} & b_2 \\ \vdots & & & \\ b_{mr} & \dots & b_{mn} & b_n \end{pmatrix}$.

If we continue this *row reduction*, we arrive at the so-called *row echelon form* of the matrix $(A : C)$, in which

1) (1,1) entry is 1,
2) Every entry below (1,1) is zero,
3) The first nonzero entry (if there is any) in each subsequent row is 1, and
4) The number of zeros before 1 appearing in a row is more than that in a previous row. [The position where the first nonzero entry 1 appears in a row is called a *pivot*.]
5) If $m > n$, all except possibly top n rows of the echelon form of A consist of zeros only.

Remark. The system (2.7) is inconsistent if and only if the row echelon form of the augmented matrix $(A : C)$ has a row with nonzero entry only in the last column.

Example. By the above procedure, the matrix

$$\begin{pmatrix} 0 & -3 & -6 & 4 & 9 \\ -2 & -3 & 0 & 3 & -1 \\ -1 & -2 & -1 & 3 & 1 \\ 1 & 4 & 5 & -9 & -7 \end{pmatrix}$$

row reduces to an echelon form

$$\begin{pmatrix} \textcircled{1} & 4 & 5 & -9 & -7 \\ 0 & \textcircled{1} & 2 & -3 & -3 \\ 0 & 0 & 0 & \textcircled{1} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We have circled the pivots.

The row reduction reduces a consistent system (2.7) to one of the form

$$\left.\begin{array}{l}
x_1 + c_{12}x_2 \qquad\quad + \cdots + c_{1n}x_n = d_1 \\
\;x_r + c_{2(r+1)}x_{r+1} + \cdots + c_{2n}x_n = d_2 \\
\;x_s + c_{3(s+1)}x_{s+1} + \cdots + c_{3n}x_n = d_3 \\
\;\vdots \\
\quad x_t + c_{k(t+1)}x_{t+1} + \cdots + c_k x_n \;\; = d_t
\end{array}\right\} \tag{2.9}$$

and 5) above says that (2.9) has no more than n independent equations. Substituting the value of the first variable x_t appearing in the last equation of (2.9) and continuing in this way, we can solve system (2.7). All variables not in a pivot column are *parameters.*

Examples.

1.* Let us solve again

$$\begin{aligned} 3x + 4y &= 2 \\ 2x + 3y &= 5 \end{aligned}$$

over the field $\mathbb{F} = \{0, 1, \ldots, 6\}$ of seven elements. The augmented matrix $(A : C) = \left(\begin{array}{cc|c} 3 & 4 & 2 \\ 2 & 3 & 5 \end{array}\right)$. Our steps in the Gaussian elimination correspond to the following steps in the row reduction of the augmented matrix. $\left(\begin{array}{cc|c} 3 & 4 & 2 \\ 2 & 3 & 5 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & 6 & 3 \\ 2 & 3 & 5 \end{array}\right) \rightarrow$ $\left(\begin{array}{cc|c} 1 & 6 & 3 \\ 0 & 5 & 6 \end{array}\right) \rightarrow \left(\begin{array}{cc|c} 1 & 6 & 3 \\ 0 & 1 & 4 \end{array}\right).$

The last matrix is the echelon form of $(A : C)$, which corresponds to

$$\begin{aligned} x + 6y &= 3 \\ y &= 4. \end{aligned}$$

Hence $x = 3 - 6y = 3 - 6 \cdot 4 = 0$.

2. We take $K = \mathbb{Q}$, $m = 2, n = 3$.

$$\begin{aligned} x + y - 2z &= 1 \\ 2x + y + 2z &= 3 \end{aligned} \tag{2.10}$$

The augmented matrix $(A : C) = \left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 2 & 1 & 2 & 3 \end{array}\right).$

Subtracting two times the first row from the second, which we abbreviate as $R_2 - 2R_1$, and continuing

$$\left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 2 & 1 & 2 & 1 \end{array}\right) \xrightarrow{R_2 - 2R_1} \left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 0 & -1 & 6 & -1 \end{array}\right)$$

$$\xrightarrow{(-1)R_2} \left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 0 & 1 & -6 & 1 \end{array}\right),$$

which is in the echelon form and our system is equivalent to

$$\begin{aligned} x + y - 2z &= 1 \\ y - 6z &= 1. \end{aligned}$$

Let $z = t$. Then $y = 6t + 1$ and

$$\begin{aligned} x &= 2z - y + 1 \\ &= 2t - (6t + 1) + 1 \\ &= -4t. \end{aligned}$$

Hence, $x = -4t$ and $y = 6t + 1$, $z = t$ is a one parameter solution of (2.10). It represents, as expected, a straight line in the so called parametric form.

3. Again $K = \mathbb{Q}$, but $m = 3$, $n = 3$.

$$\begin{aligned} x + y - 2z &= 1 \\ 2x + y + 2z &= 3 \\ 3x + 2y \phantom{{}+2z} &= 4 \end{aligned} \tag{2.11}$$

First, we row reduce the augmented matrix of the system to the echelon form.

$$\left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 2 & 1 & 2 & 3 \\ 3 & 2 & 0 & 4 \end{array}\right) \xrightarrow{R_3 - (R_1 + R_2)} \left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 2 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{R_2 - 2R_1}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 0 & -1 & 6 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{(-1)R_2} \left(\begin{array}{ccc|c} 1 & 1 & -2 & 1 \\ 0 & 1 & -6 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

It is now obvious that (2.11) is similar to (2.10), which we have already solved.

4*. We solve the system of equations

$$2x + y = 3 \tag{1}$$

$$x + 3y = 4 \tag{2}$$

over $\mathbb{Z}/6\mathbb{Z} = \{0, 1, \ldots, 5\}$.

Multiply equation (2) by 2 and subtract from (1) to get

$$-5y = -5$$

so $y = 1$. (Why? Cancellation holds only in fields.) Now putting $y = 1$ in equation (2), $x = 1$.

Note. Because $1 + 5 = 6 \equiv 0 \mod 6$, 5 is the "negative" of 1.

EXERCISES

1. Solve the following systems over the field $\mathbb{Q}$ of rational numbers.

(a)
$$\begin{aligned} 4x_1 + 3x_2 &= 1 \\ \tfrac{2}{3}\, x_1 + 2x_2 &= -1 \end{aligned}$$

(b)
$$\begin{aligned} x + 2y - z &= 3 \\ 2x - y + z &= 1 \\ -x + 2y + 3z &= 5 \end{aligned}$$

2. Solve

$$(1+i)x + \frac{3}{2}\, iy = \frac{1+\sqrt{3}i}{2}$$

$$(1-i)x + iy = \frac{1-\sqrt{3}i}{2}$$

over $\mathbb{C}$.

3.* Use the Gaussian elimination to solve the following systems over the given field of scalars.

(a) $3x + 4y = 2$

$2x + 3y = 1$

over the field $\{0, 1, \ldots, 4\}$ of five elements.

(b) $x + y + 5z = 1$

$2x + y + 2z = 3$

over the field $\{0, 1, \ldots, 6\}$ of seven elements.

(c) What is the total number of solutions in parts (a) and (b)? Explain your answer.

4. True or False? The system

$$a_1x + b_1y = c_1$$
$$a_2x + b_2y = c_2$$

is consistent if and only if $a_1 : a_2 = b_1 : b_2 = c_1 : c_2$, i.e. if and only if the respective a_j, b_j, c_j are proportional.

5.* Solve the system

$$5x + 4y = 2$$
$$3x + 7y = 7$$

over $\mathbb{Z}/10\mathbb{Z}$.

6. For what a, b, c, d is the system

$$ax + by = m$$
$$cx + dy = n$$

consistent for all m and n?

7. Find a row echelon form of the following matrices:

(a) $\begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 6 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 2 & 1 \\ 2 & 4 & 5 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 0 & -3 & -6 & 4 & 9 \\ -1 & -2 & -1 & 3 & 1 \\ -2 & -3 & 0 & 3 & -1 \\ 0 & -3 & -6 & 4 & 9 \end{pmatrix}$

2.4 Inverse of a Matrix

Recall that a scalar equation

$$ax = c \tag{2.12}$$

has the solution $x = a^{-1}c$, provided $a \neq 0$. The system (2.7) of linear equations is the same as the single matrix equation

$$AX = C \tag{2.13}$$

with

$$A = (a_{ij}),\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ and } C = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}.$$

It would be nice if we could imitate solving (2.12) to solve (2.13), as $X = A^{-1}C$. However, the condition $A \neq 0$ is not sufficient to do so.

If $m = n$, the system $AX = C$ can also be solved, by inverting the matrix A, provided it is invertible.

Definition. Suppose A is a square matrix over a field K. We say that A is *invertible*, if $AB = BA = I$ for a matrix B over K. The matrix B is uniquely determined by A, we call it the *inverse* of A and write it as A^{-1}.

Suppose A is invertible and $AX = C$ is the given system of n equations in n variables $x_1, \ldots, x_n$. Multiplying on the left by A^{-1}, we get $A^{-1}(AX) = A^{-1}C$. But $A^{-1}(AX) = (A^{-1}A)X = IX = X$. Hence $X = A^{-1}C$ is the solution, which is unique for if X_1 and X_2 are two solutions then $AX_1 = AX_2$ implies that $A^{-1}(AX_1) = A^{-1}(AX_2)$ which shows that $X_1 = X_2$.

Inverse of a 2 × 2 Matrix

A 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, if and only if, $ad - bc \neq 0$, in which case, $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

[The quantity $ad - bc$ is called the *determinant* of A, and is denoted by $\det(A)$.]

To verify this, we only need to multiply the two matrices.

$$\begin{aligned} &\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ =&\frac{1}{ad-bc}\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ =&\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I. \end{aligned}$$

Example. To solve

$$\begin{aligned} 3x + 2y &= -1 \\ 10x + 7y &= 5, \end{aligned}$$

first we invert $A = \begin{pmatrix} 3 & 2 \\ 10 & 7 \end{pmatrix}$. Here $ad - bc = 3 \cdot 7 - 2 \cdot 10 = 1$. Hence $A^{-1} = \begin{pmatrix} 7 & -2 \\ -10 & 3 \end{pmatrix}$.

So, $\begin{pmatrix} x \\ y \end{pmatrix} = X = A^{-1}C = \begin{pmatrix} 7 & -2 \\ -10 & 3 \end{pmatrix} \begin{pmatrix} -1 \\ 5 \end{pmatrix} = \begin{pmatrix} -17 \\ 25 \end{pmatrix}$.

Hence $x = -17$ and $y = 25$ is the solution.

Example.* Consider

$$\begin{aligned} 3x + 4y &= 2 \\ 2x + 3y &= 1 \end{aligned}$$

as an equation over the field $\mathbb{F}_5$ of five elements. It can be checked that

$$ad - bc = 1$$

so that

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix}.$$

Therefore,

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

It can be checked (using the field operations in $\mathbb{F}_5$) that $x = 2$ and $y = 4$ is indeed a solution.

Computing Inverse by Row Reduction

In general, the inverse of an $n \times n$ invertible matrix may be computed by the following algorithm, called the *inverse by row reduction*.

By row operations, bring the augmented matrix $(A : I)$ to the form $(I : B)$. [This is possible, because A is invertible.] Then $B = A^{-1}$. To see this, recall that to carry out row operations, one multiplies on the left by elementary matrices S, T and diagonal matrices D. Let B be their product so that $BA = I$. But then I is transformed to $BI = B$.

Example. To compute A^{-1} for

$$A = \begin{pmatrix} 1 & 4 & 3 \\ -1 & -2 & 0 \\ 2 & 2 & 3 \end{pmatrix},$$

$$\left(\begin{array}{ccc|ccc} 1 & 4 & 3 & 1 & 0 & 0 \\ -1 & -2 & 0 & 0 & 1 & 0 \\ 2 & 2 & 3 & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_2+R_1,R_3-2R_1}\left(\begin{array}{ccc|ccc} 1 & 4 & 3 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 0 & -6 & -3 & -2 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_3+3R_2}\left(\begin{array}{ccc|ccc} 1 & 4 & 3 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{array}\right)$$

$$\xrightarrow{(1/2)R_3}\left(\begin{array}{ccc|ccc} 1 & 4 & 3 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 0 & 0 & 3 & \frac{1}{2} & \frac{3}{2} & \frac{1}{2} \end{array}\right)$$

$$\xrightarrow{R_1-R_3,R_2-R_3}\left(\begin{array}{ccc|ccc} 1 & 4 & 0 & \frac{1}{2} & \frac{-3}{2} & \frac{-1}{2} \\ 0 & 2 & 0 & \frac{1}{2} & \frac{-1}{2} & \frac{-1}{2} \\ 0 & 0 & 3 & \frac{1}{2} & \frac{3}{2} & \frac{1}{2} \end{array}\right)$$

$$\xrightarrow{R_1-2R_2}\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} \\ 0 & 2 & 0 & \frac{1}{2} & \frac{-1}{2} & \frac{-1}{2} \\ 0 & 0 & 3 & \frac{1}{2} & \frac{3}{2} & \frac{1}{2} \end{array}\right)$$

$$\xrightarrow{(1/2)R_2,(1/3)R_3}\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & \frac{1}{4} & \frac{-1}{4} & \frac{-1}{4} \\ 0 & 0 & 1 & \frac{1}{6} & \frac{1}{2} & \frac{1}{6} \end{array}\right)$$

Hence $A^{-1}=\begin{pmatrix} \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} \\ \frac{1}{4} & \frac{-1}{4} & \frac{-1}{4} \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{6} \end{pmatrix}$.

Permutation Matrices

A class of invertible matrices are the permutation matrices. A permutation on the set X of n symbols $1, 2, \ldots, n$ is a bijection $f : X \to X$. Such an f can be represented by its *permutation matrix*, an $n \times n$ matrix $P(f)$ with only one nonzero entry 1 in any given row or column. We define it by $P(f) = (\delta_{f(i)j})$, where

$$\delta_{ik} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{otherwise} \end{cases}$$

are the *Kronecker's deltas.*

Example. Let f be the cycle: $f(1) = 2$, $f(2) = 3$, $f(3) = 1$ on three symbols. Then $P(f) =$

$$\begin{pmatrix} \delta_{f(1)1} & \delta_{f(1)2} & \delta_{f(1)3} \\ \delta_{f(2)1} & \delta_{f(2)2} & \delta_{f(2)3} \\ \delta_{f(3)1} & \delta_{f(3)2} & \delta_{f(3)3} \end{pmatrix} = \begin{pmatrix} \delta_{21} & \delta_{22} & \delta_{23} \\ \delta_{31} & \delta_{32} & \delta_{33} \\ \delta_{11} & \delta_{12} & \delta_{13} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

If symbols are represented by the column vector $X = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, then $P(f)X =$

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

Thus $P(f)$ sends the vector X to $\begin{pmatrix} f(1) \\ f(2) \\ f(3) \end{pmatrix}$. It is easy to verify that $P(f)^{-1} = P(f)^*$, the transpose of $P(f)$.

EXERCISES

1. If for an integer $m \geq 1$, $(I - A)^m = 0$, show that A is invertible.
2. Suppose A, B are $n \times n$ matrices. Show that if any two of A, B, AB and BA are invertible, then they are all invertible.
3. Suppose A, B, and X are $n \times n$ matrices with X and $A - AX$ invertible. If $(A - AX)^{-1} = X^{-1}B$, show that B is invertible.
4. If A is an $n \times n$ matrix and $A\boldsymbol{x} = \boldsymbol{b}$ has a solution for each $\boldsymbol{b}$ in $\mathbb{R}^n$, show that A is invertible.
5. Suppose $P(f)$ is an $n \times n$ permutation matrix. Show that i) $P(f)^{-1} = P(f^{-1})$ and ii) $P(f)^{-1} = P(f)^*$.
6. Compute the permutation matrix $P(f)$ and its inverse $P(f)^{-1}$ for the cycle $f : X \to X = \{1, 2, 3, 4\}$ given by $f(i) = i+1$, for $i = 1, 2, 3$ and $f(4) = 1$.

Compute the inverse of A, and use A^{-1} to solve $AX = C$.

7. $A = \begin{pmatrix} 2 & -1 \\ 5 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

8. $A = \begin{pmatrix} 3 & 2 \\ 2 & -3 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

9. $A = \begin{pmatrix} 1 & 4 & 5 \\ 0 & 2 & 6 \\ 0 & 0 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$

10. $A = \begin{pmatrix} -1 & -3 & 3 \\ 2 & 6 & 1 \\ 3 & 8 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

11. $A = \begin{pmatrix} 2 & 2 & 2 & 1 \\ 3 & 4 & 4 & 2 \\ 2 & 3 & 3 & 1 \\ 2 & 2 & 3 & 2 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ -4 \\ 3 \\ -5 \end{pmatrix}$

12. $A = \begin{pmatrix} 3 & 5 & 3 & 4 \\ 2 & 2 & 1 & 1 \\ 4 & 9 & 6 & 10 \\ 4 & 14 & 10 & 20 \end{pmatrix}$, $C = \begin{pmatrix} 2 \\ 3 \\ 5 \\ 7 \end{pmatrix}$

2.5 The Equation $A\boldsymbol{x} = \boldsymbol{b}$

As a prelude to the theory of vector spaces, we call the $n \times 1$ matrix X a *column vector* and denote it by the lower case bold face letter $\boldsymbol{x}$. Thus we write the matrix equivalent $AX = B$ of a system of linear equations as $A\boldsymbol{x} = \boldsymbol{b}$, where

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \; \boldsymbol{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

It can be checked that $A\boldsymbol{x} = \boldsymbol{b}$ is the same as

$$\boldsymbol{b} = x_1\boldsymbol{a}_1 + \cdots + x_n\boldsymbol{a}_n, \tag{2.14}$$

where the vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ are the columns of the matrix A.

The sum on the right of (2.14) of scalar multiples of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ is called a *linear combination* of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. Therefore, the system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ is consistent if and only if $\boldsymbol{b}$ is a linear combination of the columns of A. If this is the case, we also say that $\boldsymbol{b}$ is in the span of the columns of A. By definition the *span* of $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ is the set of linear combinations

$x_1\boldsymbol{a}_1 + \cdots x_n\boldsymbol{a}_n$ with all possible choices of the scalars $x_1, \dots, x_n$. We write it as $\operatorname{span}\{\boldsymbol{a}_1, \dots, \boldsymbol{a}_n\}$.

Example. The system of linear equations

$$\begin{aligned} x_1 + 3x_2 &= 2 \\ 2x_1 + 5x_2 &= 3 \end{aligned}$$

can be written as

$$\begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

or

$$x_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + x_2 \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

This holds for $x_1 = -1$, $x_2 = 1$, which thus is a solution of the above system of linear equations.

EXERCISES

Solve the system of equations $A\boldsymbol{x} = \boldsymbol{b}$ and express $\boldsymbol{b}$ as a linear combination of the columns $\boldsymbol{c}_1, \boldsymbol{c}_2, \dots$ of A if

1. $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$,
2. $A = \begin{pmatrix} 2 & 4 & 3 \\ 3 & -1 & 2 \\ 1 & 4 & 1 \end{pmatrix}, \boldsymbol{b} = \begin{pmatrix} 1 \\ 7 \\ -2 \end{pmatrix}$.

2.6† Basic Applications

In this section we discuss some of the most down-to-earth applications of linear algebra.

2.6.1 Traffic Flow

In a downtown, a certain block is bordered by one-way streets going around it in clockwise direction. During rush hours, the number of vehicles entering and leaving the intersections at the four corners of the block is shown in Figure 2.1.

We want to determine the traffic flow on each street around the block. Let the number of vehicles entering the four streets be x_1, x_2, x_3, x_4 (cf. Figure 2.1).

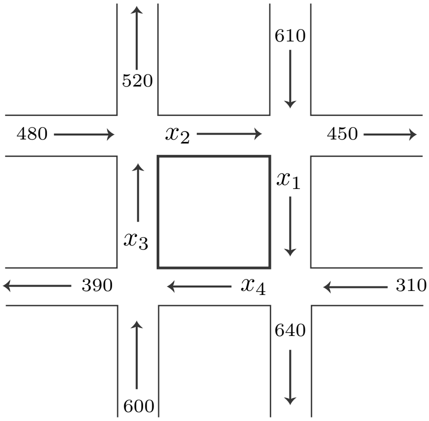


FIGURE 2.1: Traffic flow

At each intersection, the number of vehicles entering and leaving is the same. Hence we have four linear equations in four unknowns x_1, x_2, x_3, x_4.

$$x_1 + 450 = x_2 + 610$$

or

$$\text{similarly}\qquad \left.\begin{array}{rrrrl} x_1 & - x_2 & & & = 160\\ & x_2 & - x_3 & & = -40\\ & & x_3 & - x_4 & = 210\\ x_1 & & & - x_4 & = 330 \end{array}\right\}$$

This is a consistent system of four linear equations in four variables. It has one free variable. For example, if it has been observed that $x_4 = 150$, then $x_1 = 480$, $x_2 = 320$, and $x_3 = 360$.

2.6.2 Barter Systems

There are villages in many Third World countries which are independent economic units and use no cash. The people belonging to different professions use barter systems to exchange among themselves the goods they produce. The system is governed by an economic model formalized by Wassily Wassilyovich Leontief.

Example. In a certain village there are three communities: 1) farmers, 2) blacksmiths and carpenters who make furniture, tools, and utensils, and 3) artisans consisting of weavers, tailors, and shoemakers. Each community keeps a portion of its produce (and/or labor) to itself and gives the rest to the other two in a traditionally set ratio. The blacksmiths and carpenters divide their produce evenly among the three groups, the farmers keep half of their produce and then give a fourth to the blacksmiths and carpenters, and the remaining fourth to the artisans. The artisans give half of their produce to the farmers, and divide the remaining half equally between themselves and the group consisting of blacksmiths and carpenters. We show it pictorially in Figure 2.2.

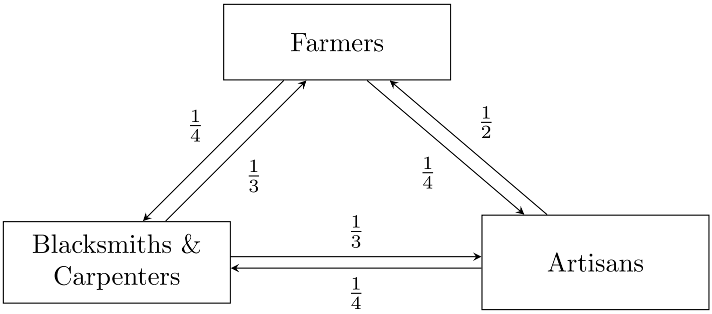


FIGURE 2.2: A barter system

Any barter system is based on the quality of the goods produced by each community. Suppose the value assigned to the goods produced by the farmers, the blacksmiths-carpenters, and the artisans is x_1, x_2, x_3 respectively. According to the barter system used in this village, the value of the farm produce given by the farmers to the other two groups is the same as the value of the goods received by the farmers from those two communities. Thus

$$\frac{1}{3}x_2 + \frac{1}{2}x_3 = \frac{1}{2}x_1.$$

Similarly,

$$\frac{1}{4}x_1 + \frac{1}{4}x_3 = \frac{2}{3}x_2$$

and

$$\frac{1}{4}x_1 + \frac{1}{3}x_2 = \frac{3}{4}x_3.$$

This is a homogeneous system of three linear equations in three variables:

$$\left.\begin{aligned} \frac{1}{2}\,x_1 - \frac{1}{3}\,x_2 - \frac{1}{2}\,x_3 = 0 \\ \frac{1}{4}\,x_1 - \frac{2}{3}\,x_2 + \frac{1}{4}\,x_3 = 0 \\ \frac{1}{4}\,x_1 + \frac{1}{3}\,x_2 - \frac{3}{4}\,x_3 = 0 \end{aligned}\right\} .$$

Its solution set is a 1-dimensional subspace of $\mathbb{R}^3$ spanned by, say $(x_1, x_2, x_3) = (5, 3, 3)$. This means the goods produced by the three groups have the proportional values

$$x_1 : x_2 : x_3 = 5 : 3 : 3.$$

2.6.3 Electric Circuits

The amount of electric current i (measured in amperes or amps) between two points of an electric circuit is determined by the resistance R (in ohms) and the voltage difference E (in volts) between these points by the following laws.

Ohm's Law: *The voltage drop $E = iR$.*

At any node (a point into and out of which currents are flowing) the electric flow is governed by

Kirchhoff's Laws:

1. *At any node, the amount of electric current flowing into it is the same as flowing out of it.*
2. *At any part of a closed electric circuit, the voltage drop between two points is the algebraic sum of the voltage drops between them.*

Example. Let us find the amount of electric currents i_1, i_2, i_3 in each circuit between nodes A and B of the following electric network (Figure 2.3).

In electric circuitry, $||$ or $+/-$ is usually a battery of given voltage. The current flows away from $+$ and toward $-$ sign. By Kirchhoff's first law, we have at A, as well as at B,

$$i_1 - i_2 + i_3 = 0. \tag{2.15}$$

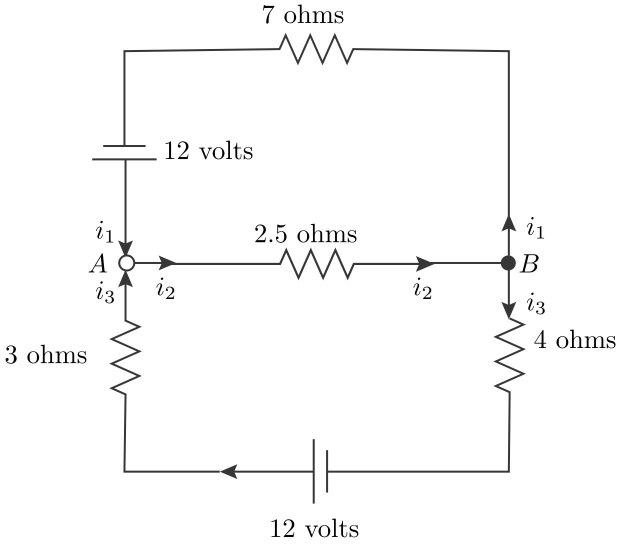


FIGURE 2.3: An Electric circuit

By Kirchhoff's second law and the Ohm's Law,

$$\left.\begin{aligned} 7i_1 + \frac{5}{2}\,i_2 &= 12 \\ \frac{5}{2}\,i_2 + 7i_3 &= 12 \end{aligned}\right\} \tag{2.16}$$

It is easily seen that $i_1 = 1$, $i_2 = 2$ and $i_3 = 1$ satisfy both (2.15) and (2.16).

2.6.4 Chemical Reactions

Trees and plants use sunlight to convert carbon dioxide CO_2 and water H_2O into glucose $C_6H_{12}O_6$ and oxygen O_2. This chemical reaction is denoted by an equation of the form

$$x_1\mathrm{CO}_2 + x_2\mathrm{H}_2\mathrm{O} \overset{\rightarrow}{=} x_3\mathrm{O}_2 + x_4\mathrm{C}_6\mathrm{H}_{12}\mathrm{O}_6. \tag{2.17}$$

To balance the equation one must choose x_1, x_2, x_3 and x_4 so that the numbers of carbon, hydrogen, and oxygen atoms on each side of the equation are the same. The carbon dioxide contains one carbon atom, whereas glucose contains six, so we must have

$$x_1 = 6x_4.$$

Similarly, looking at the hydrogen and oxygen atoms, we get

$$\begin{aligned} 2x_2 &= 12x_4 \\ 2x_1 + x_2 &= 2x_3 + 6x_4, \end{aligned}$$

respectively. Thus we have a homogeneous system of three linear equations in four variables:

$$\left.\begin{array}{rrrrl} x_1 & & & -\ \ 6x_4 & = 0 \\ & 2x_2 & & -12x_4 & = 0 \\ 2x_1 + & x_2 & -\ 2x_3 & -\ \ 6x_4 & = 0 \end{array}\right\}$$

The set of its solution is a 1-dimensional subspace of $\mathbb{R}^4$ spanned by $(6, 6, 6, 1)$. Hence (2.17) becomes

$$6\,\mathrm{CO_2} + 6\,\mathrm{H_2O} \overset{\rightarrow}{=} 6\,\mathrm{O_2} + \mathrm{C_6H_{12}O_6}.$$

2.6.5 Economics

A barter system discussed in Section 2.6 is an example of a closed (or self-sustaining) economy, where each group or sector produces something and barters a part of its produce for goods produced by other groups. In a larger economy such that as of a country, apart from the production sectors like agriculture, manufacturing and utilities, there is another sector, namely the consumers, which does not produce anything, but consumes what other sectors produce. This is an example of an open economy, a mathematical model of which was developed by Wassily Leontief (see [14]). For his contribution, which we explain below, Leontief was awarded the Nobel Prize for economics in 1973.

In order to produce its goods, each sector consumes some of its own produce as well as produce of other sectors. For example, to produce 1 unit (in dollar amount) of farm goods, the agriculture sector may use 50¢ of its own produce to feed its workforce and cattle. In addition to this, it may need 10¢ of farm equipment produced by the manufacturing sector and 30¢ of utilities such as diesel and electricity. If we order these three sectors alphabetically, the *consumption vector* for the agricultural sector is defined to be

$$\boldsymbol{c}_1 = \begin{pmatrix} .50 \\ .10 \\ .30 \end{pmatrix}.$$

Similarly, let the consumption vectors for manufacturing and utilities sectors be

$$\boldsymbol{c}_2 = \begin{pmatrix} .20 \\ .50 \\ .10 \end{pmatrix}, \quad \boldsymbol{c}_3 = \begin{pmatrix} .30 \\ .10 \\ .40 \end{pmatrix},$$

respectively. This means, for example, to produce 1 unit of manufactured goods, the manufacturing sector uses 20¢ of agricultural goods, 50¢ of its own produce and spends 10¢ on utilities. The matrix

$$C = \begin{pmatrix} .5 & .3 & .3 \\ .1 & .5 & .1 \\ .3 & .1 & .4 \end{pmatrix}$$

whose columns are $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$ is called the *consumption matrix*.

Now suppose that the outside demands (by consumers) is d_1 units of agricultural goods, d_2 units of manufactured goods and d_3 units of utilities. To satisfy everybody's demand, if the number of units produced by the three sectors (listed alphabetically) is x_1, x_2, x_3 respectively, then we must have

$$\begin{aligned} x_1 &= .5x_1 + .3x_2 + .3x_3 + d_1 \\ x_2 &= .1x_1 + .5x_2 + .1x_3 + d_2 \\ x_3 &= .3x_1 + .1x_2 + .4x_3 + d_3 \end{aligned}$$

If we let

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad \boldsymbol{d} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix},$$

we can write this system of linear equations as a single matrix equation $\boldsymbol{x} = C\boldsymbol{x} + \boldsymbol{d}$. Thus the number of units x_1, x_2, x_3 of goods that the three sectors have to produce to meet everybody's demand is a solution of the system of linear equations

$$(I - C)\boldsymbol{x} = \boldsymbol{d}.$$

In general, in an open economy, there are several, say n production sectors. The production sectors are arranged in an arbitrary but fixed order. To produce 1 unit of its goods, the i-th production sector uses c_{ij} units of goods produced by the j-th production sector and d_i is the external demand (by consumers) for the goods produced by the i-th sector. In order to meet the demand of every sector (including the consumers) if the i-th production sector has to produce x_i units of its goods, then by the same argument as above

$$\boldsymbol{x} = C\boldsymbol{x} + \boldsymbol{d}$$

with

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad \boldsymbol{d} = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \text{ and } C = (c_{ij}).$$

The obvious assumption on the *consumption matrix* C for the economy to be viable is for the column sums of C to be less than 1. The matrix $I - C$, called the *Leontief matrix*, is invertible. (See the theorem below.) Therefore, the production *vector* $\boldsymbol{x}$ is given by

$$\boldsymbol{x} = (I - C)^{-1}\boldsymbol{d} \tag{2.18}$$

if the *demand vector* $\boldsymbol{d}$ is known.

Theorem 2.2. *Suppose C is a square matrix over $\mathbb{R}$ with all entries nonnegative. If all the column sums (a column sum is the sum of column entries) are less than one, then $I - C$ is invertible.*

Proof. (cf. Chapter 6 for the definition of eigenvalues.) The *spectral radius* $\rho(A)$ of a matrix A is defined by $\rho(A) = \max\{|\lambda| \mid \lambda \in \mathbb{C}$ is an eigenvalue of $A\}$. By Theorem 8.1.22 of [7], all the eigenvalues of C are in the open unit disk

$$\{z \in \mathbb{C} \mid |z| < 1\}.$$

Consequently, no eigenvalue of $I - C$ is zero, hence it is invertible. □

EXERCISES

In the following, the consumption matrix C and the demand vector $\boldsymbol{d}$ are given. Compute the production vector $\boldsymbol{x}$.

1. $C = \begin{pmatrix} .5 & .2 \\ .4 & .1 \end{pmatrix}, \quad \boldsymbol{d} = \begin{pmatrix} 700 \\ 400 \end{pmatrix}.$

2. $C = \begin{pmatrix} .5 & .3 & .3 \\ .1 & .5 & .1 \\ .3 & .1 & .4 \end{pmatrix}, \quad \boldsymbol{d} = \begin{pmatrix} 3950 \\ 7900 \\ 1975 \end{pmatrix}.$

3

Vector Spaces

The vector spaces are the domains and codomains of linear maps that unify different and seemingly unrelated branches of mathematics. We strongly recommend that the reader be familiar with the contents of Chapter 1 before reading this chapter.

3.1 The Concept of a Vector Space

Consider the following sets V:

1. $V = \mathbb{R}^n$ $(n \geq 1)$, the Euclidean n-space whose elements are called vectors.
2. $V = M(m \times n, K)$, the set of $m \times n$ matrices with entries from a given field K.
3. $V = K[x]$, the set of polynomials with coefficients in a field K.
4. $V =$ the set of all solutions of the differential equation $\frac{d^2y}{dt^2} + \mu y = 0$ for a fixed $\mu > 0$, and
5. $V =$ the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$.

All these sets share some common properties, the properties that make them what we shall call vector spaces. In all these sets, there is a way to "add" two elements of V and to "scale" an element of V by a scalar (an element of the given field $K = \mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, etc.). Although adding two matrices is not the same as adding two differentiable functions, adding and scaling the elements of V, irrespective of what V we take, have similar properties. A minimal set of basic properties of these two operations, from which other properties common to all these V follow, will be our defining axioms of a vector space.

Definition. A *vector space* (or more appropriately a *linear space*) *over* a field K is a non-empty set V, of objects called *vectors*, together with two maps

1) $V \times V \ni (\boldsymbol{u}, \boldsymbol{v}) \to \boldsymbol{u} + \boldsymbol{v} \in V$, called an *addition*, and

2) $K \times V \ni (c, v) \to c\boldsymbol{v} \in V$, called a *scalar multiplication*, or *scaling*. Moreover, for all $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ in V and all *scalars* a, b in K, we must have

3) $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$ (*commutative law*),

4) $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$ (*associative law*),

5) there is a vector $\boldsymbol{\Theta}$, called a *zero vector* in V such that $\boldsymbol{v}+\boldsymbol{\Theta} = \boldsymbol{v}$,

6) given $\boldsymbol{v}$ in V, there is $\boldsymbol{u}$ in V called a *negative* of v such that $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{\Theta}$,

7) $(a + b)\boldsymbol{v} = a\boldsymbol{v} + b\boldsymbol{v}$,

8) $a(\boldsymbol{u} + \boldsymbol{v}) = a\boldsymbol{u} + a\boldsymbol{v}$,

9) $(ab)\boldsymbol{v} = a(b\boldsymbol{v})$, and finally,

10) $1\boldsymbol{v} = \boldsymbol{v}$.

If the vector $\boldsymbol{\Theta}$ in 5 and $\boldsymbol{u}$ in 6 exist, we shall show that they are unique and denote them by $\mathbf{0}$ and $-\boldsymbol{v}$, respectively.

Examples. The five sets $V = \mathbb{R}^n$, $M(m \times n, K), \ldots$ above, under the usual operations of addition and scalar multiplication are vector spaces. In some of the next examples, we shall equip familiar sets with unusual "additions" and "scalar multiplications" which may or may not make them into vector spaces. To avoid the confusion with the usual operations, we shall denote the unusual addition and scalar multiplication by $\oplus$ and $*$, respectively, so that $\boldsymbol{u} \oplus \boldsymbol{v}$ is the sum of $\boldsymbol{u}$ and $\boldsymbol{v}$, and $c * \boldsymbol{v}$ is the scaling of $\boldsymbol{v}$ by a scalar c.

1. Identify a field K with the vector space $V = M(1, K)$ over K. Thus K may be considered as a vector space over itself.

2* Identify the set $V = \{a, b, c\}$ of the three fruits, a for apple, b for banana, and c for cranberry, with the three elements $a = 0$, $b = 1$, and $c = 2$ of the field $\mathbb{F}_3$ of three elements. By Example 1, V is a vector space over the field $K = \mathbb{F}_3$.

3. On $V = M(n, K)$, the set of $n \times n$ matrices over a field K, define $A \oplus B = AB - BA$, whereas $c * A = cA$, the usual scaling of A by c. This is not a vector space because the commutative law fails.

4. On $V = K = \mathbb{R}$, define $x \oplus y = \min\{x, y\}$ whereas the scaling of x by c is the usual multiplication in $\mathbb{R}$. Now there is no zero vector Θ. In fact, for Θ to be a zero vector, $x \oplus \Theta = \min\{x, \Theta\} = x$ for all x, meaning $\Theta \geq x$ for all x. But there is no real number Θ for which this is true, so this is not a vector space.

5. For this example, take $K = \mathbb{R}$ and denote by $[a]$ the largest integer $\leq a$ for a in $\mathbb{R}$. For example $[\pi] = 3$ whereas $[-\pi] = -4$. Take now $V = \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$, the set of all integers. Define $m \oplus n$ to be the usual sum of m and n, but $a * m = [a]m$. Clearly $a * m$ is in V. However, if we take $a = b = 1/2$ and $m = 1$, $(a+b)*m = a*m + b*m$ doesn't hold. Hence it is not a vector space.

6. On $V = \mathbb{R}^2$, we keep the usual addition rule for vectors in V, but define $a * (x, y) = \mathbf{0}$. It can be checked that all (except the last) axioms hold. So this is not a vector space either.

7. Now on $V = \mathbb{R}^2$, keep the usual scalar multiplication but define a new addition by

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, 0).$$

It is easy to see that there are infinitely many zero vectors $\boldsymbol{\Theta} = (0, y)$, contradicting the uniqueness of the zero vector (to be proved shortly).

8. On $V = \mathbb{R}^+$, the set of positive reals, define $x \oplus y = x/y$ and $c * x = x^c$. This is not a vector space. (Which axioms break down?)

9. Let $V = \mathbb{R}^2$, $\boldsymbol{u} \oplus \boldsymbol{v} = \boldsymbol{u} + \boldsymbol{v}$ (the usual vector sum) but $a*(x, y) = (2ax, 2ay)$. (Which axioms fail?)

10. On $V = K = \mathbb{R}$, take $x \oplus y = [x + y]$ and $a * x = ax$. Now which axioms do not hold?

11. This is perhaps the most illuminating example. Let $V = \mathbb{R}^+$, $K = \mathbb{R}$ and define $x \oplus y = xy$ and $a * x = x^a$. It can, and should, be checked that all the axioms hold. Note that the zero vector $\Theta = 1$ and the negative of x is $\frac{1}{x}$. Therefore it is a vector space. We shall show that as a vector space, it is the same as the 1-dimensional Euclidean space $V = \mathbb{R}^1$.

12. In 11 above, define the scaling by a as $a * x = x^{|a|}$. Is $\mathbb{R}^+$ again a vector space over $\mathbb{R}$?

13. Both $\mathbb{R}$ and $\mathbb{C}$ are vector spaces over $\mathbb{Q}$. In general, if k is a subfield of a field K, then K is a vector space over k.

If you have studied *Book 1* of Euclid's *Elements*, you know that in the Euclidean geometry, facts about geometric figures (such as the sum of three angles of a triangle is 180°) can be derived, step by step, from the five postulates laid down by Euclid more than two millennia ago. The same is true for vector spaces, which we do now.

Proposition 3.1. *The zero vector* $\mathbf{0}$ *is unique.*

Proof. Let $\mathbf{0}_1$ and $\mathbf{0}_2$ be two zero vectors.

$$\text{Then } \mathbf{0}_1 + \mathbf{0}_2 = \mathbf{0}_1 \text{ (using } \mathbf{0}_2 \text{ as zero)}$$

$$\text{and } \mathbf{0}_1 + \mathbf{0}_2 = \mathbf{0}_2 \text{ (using } \mathbf{0}_1 \text{ as zero).}$$

$$\text{Hence } \mathbf{0}_1 = \mathbf{0}_2.$$ □

Proposition 3.2. *Suppose c is any scalar and $\boldsymbol{v}$ is any vector. Then*

1) $c\mathbf{0} = \mathbf{0}$, and

2) $0\boldsymbol{v} = \mathbf{0}$.

Proof.

1) The vector $c\mathbf{0} = c(\mathbf{0}+\mathbf{0}) = c\mathbf{0} + c\mathbf{0}$ by the distributive law. Adding the negative $-c\mathbf{0}$ of $c\mathbf{0}$ to both sides, we have

$$\begin{aligned} c\mathbf{0} + (-c\mathbf{0}) &= (c\mathbf{0} + c\mathbf{0}) + (-c\mathbf{0}) \\ &= c\mathbf{0} + (c\mathbf{0} + (-c\mathbf{0})) \text{ (assoc. law)} \\ &= c\mathbf{0} + \mathbf{0} \text{ (axiom 8)} \\ &= c\mathbf{0}. \end{aligned}$$

This shows that $c\mathbf{0} = c\mathbf{0} + (-c\mathbf{0}) = \mathbf{0}$.

2) Now, $0\boldsymbol{v} = (0+0)\boldsymbol{v} = 0\boldsymbol{v} + 0\boldsymbol{v}$. On adding the negative of $0\boldsymbol{v}$ to both sides, by similar arguments, we obtain $0\boldsymbol{v} = 0$. □

Proposition 3.3. *For any vector $\boldsymbol{v}$, $(-1)\boldsymbol{v} = -\boldsymbol{v}$*

Proof. Once we understand what the proposition says, the proof is trivial:

$$\begin{aligned} (-1)\boldsymbol{v} + \boldsymbol{v} &= (-1)\boldsymbol{v} + 1\boldsymbol{v} \\ &= (-1+1)\boldsymbol{v} \\ &= 0\boldsymbol{v} \\ &= \mathbf{0}, \end{aligned}$$

by Proposition 3.2. Thus $(-1)\boldsymbol{v}$ is the negative of $\boldsymbol{v}$. □

Definition. By a *linear combination* of the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ $(n \geq 1)$ we mean the vector

$$\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n \tag{3.1}$$

with scalars c_j in K. The *span* of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is the set

$$\operatorname{span}\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} = \{c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n \mid c_j \in K\}$$

of all linear combinations of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$. If S is an infinite set of vectors in V, by the *linear span* of S we mean the set

$$\operatorname{span}(S) = \{c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n \mid \boldsymbol{v}_j \in S,\ c_j \in K, n \in \mathbb{N}\}$$

of all linear combinations of finite sets $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of vectors in S.

Examples.

1. Let $V = \mathbb{R}^n$,

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \boldsymbol{e}_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

It is easy to see that $\operatorname{span}\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\} = \mathbb{R}^n$. In particular, $\boldsymbol{R}^3$ is the span of $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$, the span of $\boldsymbol{i}$ is the x-axis, the span of $\boldsymbol{i}$, $\boldsymbol{j}$ is the xy-plane, and so on.

2. Let $V = M(2, \mathbb{R})$ and

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \ E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \ E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

The $\operatorname{span}\{E_{11}, E_{12}, E_{22}\}$ is the set of upper triangular matrices, whereas $\operatorname{span}\{E_{11}, E_{22}\}$ is the set of diagonal matrices. Finally, $M(2, \mathbb{R}) = \operatorname{span}\{E_{ij} \mid 1 \leq i, j \leq 2\}$.

3. Let $V = \mathbb{R}[x]$, the vector space of polynomials over $\mathbb{R}$ and $S = \{x^n \mid n = 0, 1, 2, 3, \ldots\}$. Then $\operatorname{span}(S) = \mathbb{R}[x]$.

4. Considered as a vector space over $\mathbb{R}$, $\mathbb{C}$ is spanned by 1 and i, i.e. $\mathbb{C} = \operatorname{span}\{1, i\}$.

5. One learns in a course on differential equations that every solution $x = x(t)$ of the homogeneous linear differential equation

$$\frac{d^2x}{dt^2} + \mu^2 x = 0 \quad (\mu > 0)$$

is in $\operatorname{span}\{\cos \mu t, \sin \mu t\}$.

EXERCISES

1. On the set $V = \{O\}$, where O stands for an orange, define $O + O = O$ and for any scalar c in $\mathbb{R}$, define $cO = O$. Show that V is a vector space over $\mathbb{R}$. This represents the smallest vector space, the zero vector space $V = \{\mathbf{0}\}$.

2. Suppose K is any field. Show that for an integer $n \geq 1$, the set $K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$ is a vector space, if the addition and the scalar multiplication are defined componentwise.

3.* Let $K = \mathbb{F}_p$, the finite field of p elements. How many vectors does the vector space $V = K^n$ have?

4. Show that if $c\boldsymbol{v} = \mathbf{0}$, then either the scalar $c = 0$ or $\boldsymbol{v}$ is the zero vector.

5. Show that the negative $-\boldsymbol{v}$ of every vector $\boldsymbol{v}$ is unique and $-\mathbf{0} = \mathbf{0}$.

6. What is the span of the vectors $1 + x$ and $1 - x$ in $\mathbb{R}[x]$?

7. Prove or disprove that $\text{span}\{\boldsymbol{u} + \boldsymbol{v}, \boldsymbol{u} - \boldsymbol{v}\} = \text{span}\{\boldsymbol{u}, \boldsymbol{v}\}$ for $\boldsymbol{u}$, $\boldsymbol{v}$ in a vector space V. [It is given that the field of scalars does not contain $\mathbb{F}_2$ as a subfield.]

3.2 Subspaces

A vector space V contains certain subsets, which are vector spaces in their own right with the operations inherited from V. Not every subset of V has this property. In fact, if a subset of V is taken at random, most likely, it will not be a vector space. Since all the vector space axioms except 1, 2, 5, and 6 do not depend whether or not the vectors $\boldsymbol{u}$, $\boldsymbol{v}$, and $\boldsymbol{w}$ are in a subset W of V, in order for W to be a vector space, all it needs is to be closed under addition and scalar multiplication.

Definition. A non-empty subset W of a vector space V over a field K is a (vector) *subspace* of V if for all $\boldsymbol{u}$,$\boldsymbol{v} \in W$ and all scalars a, b in K, $a\boldsymbol{u}+b\boldsymbol{v} \in W$. We say W is a *proper subspace* of V if $\{\mathbf{0}\} \subsetneqq W \subsetneqq V$.

It is easily seen that this single condition is equivalent to the following two:

1) $\boldsymbol{u} + \boldsymbol{v} \in W$ whenever $\boldsymbol{u}$, $\boldsymbol{v} \in W$

2) $c\boldsymbol{u} \in W$ for all c in K and $\boldsymbol{u}$ in W.

Examples.

1. If S is a non-empty subset of a vector space V, then $\operatorname{span}(S)$, the linear span of S is a subspace of V.

2. Let $V = M(n, K)$. If W is the subset of V consisting of the upper triangular matrices

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

with $a_{ij} = 0$ if $i > j$, then W is a subspace of V.

Definition. A square matrix $A = (a_{ij})$ is *symmetric* if $A = A^*$, i.e. $a_{ij} = a_{ji}$ for every pair i, j of indices.

3. Let $V = M(n, K)$, but now W is the set of all symmetric matrices in V. Then W is a subspace of V.

4. Suppose $V = \mathbb{R}^3$ and W is any plane through the origin or any straight line, also through the origin. Then W is a subspace of V.

5. Let $V = K[x]$, the vector space of polynomials over a field K. For a given integer $n \geq 1$, let $P_n(K)$ or simply P_n denote the subset of V of all polynomials

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Then P_n is a subspace of V.

By varying K, this example will be used to prove the impossibility of the ancient Greek problems of trisecting angles and duplicating cubes.

6. The set W of differentiable functions $f : \mathbb{R} \to \mathbb{R}$ is a subspace of the vector space V of continuous functions $g : \mathbb{R} \to \mathbb{R}$.

7. $\mathbb{R}$ is a subspace of the vector space $\mathbb{C}$ over $\mathbb{Q}$.

8. A plane or a straight line which does not pass through the origin is not a subspace of $\mathbb{R}^3$.

Definition. A function $f : K \to K$ is called an *even function* if $f(-x) = f(x)$ for all x in the field K, and it is an *odd function* if $f(-x) = -f(x)$, for all x in K.

9. Let V be the vector space of functions $f : K \to K$. [The functions are added and scaled in the usual manner.] The set of all even functions in V is a subspace of V. What about the set of odd functions?

10. Every intersection $\bigcap_{i \in I} W_i$ of subspaces W_i of V is a subspace of V.

Proposition 3.4. *Suppose W is a subspace of a vector space V. Then*

i) For every $\boldsymbol{u}$ in W, $-\boldsymbol{u} \in W$.

ii) The zero vector $\mathbf{0} \in W$.

Proof.

i) This is a part of the definition, with $c = -1$.

ii) Since W is a non-empty, choose $\boldsymbol{u}$ in W. First, by i),

$$-\boldsymbol{u} \in W.$$

Then, by 1) of the definition,

$$\mathbf{0} = \boldsymbol{u} - \boldsymbol{u} \in W. \qquad \square$$

EXERCISES

In 1–3, is the subset W of a given vector space V a subspace of V? Explain!

1. V is any vector space, W is the union $W_1 \cup W_2$ of two subspaces W_1 and W_2 of V.

2. V is the vector space of continuous functions $f : [a, b] \to \mathbb{R}$ and $W = \{f \in V \mid f(a) = f(b)\}$. What about $W = \{f \in V \mid f(a) \neq f(b)\}$?

3. Suppose M is an $m \times n$ matrix over K. Show that $W = \{\boldsymbol{x} \in K^n \mid M\boldsymbol{x} = \mathbf{0}\}$ is a subspace of K^n. Here

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

is a column vector.

4. Suppose $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ $(n \geq 1)$ are in a vector space V over K. Show that $\operatorname{span}\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} = \{c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n \mid c_j \in K\}$ is a subspace of V.

5. Let S be a subset of a vector space V over K, S not necessarily nonempty. Show that the intersection W of all subspaces of V that contain S is the smallest subspace of V containing S. We may define W to be the *span* of S. Thus the span of the empty set is $\{\mathbf{0}\}$.

6. If W_1, W_2 are subspaces of a vector space V over K, put $W = W_1 + W_2 = \{\boldsymbol{w}_1 + \boldsymbol{w}_2 \mid \boldsymbol{w}_j \in W_j\}$. Show that W is a subspace of V.

7. Suppose W_1, W_2 are two subspaces of a vector space V. Show that $W_1 \cup W_2$ is a subspace of V if and only if $W_1 \subseteq W_2$ or $W_2 \subseteq W_1$.

8. **Definition** A complex number α is *algebraic*, if α is a root of a polynomial in $\mathbb{Q}[x]$. A number is *transcendental*, if it is not algebraic.

   Consider $V = \mathbb{C}$ as a vector space over $\mathbb{Q}$. Is the subset W of transcendental numbers a subspace of V?

9. Let W be the set of algebraic numbers. [W is usually denoted by $\overline{\mathbb{Q}}$ and called the algebraic closure of $\mathbb{Q}$.] Prove that W is a subspace of $V = \mathbb{C}$ over $\mathbb{Q}$.

10. **Quotient Spaces**

    Let W be the subspace of a vector space V. For $\boldsymbol{v}$ in V, let $\boldsymbol{v}+W = \{\boldsymbol{v}+\boldsymbol{w} \mid \boldsymbol{w} \in W\}$. The set V/W of *cosets* $\{\boldsymbol{v}+W \mid \boldsymbol{v} \in V\}$ is called the *quotient* of V by W. The vector $\boldsymbol{v}$ is called a *coset representative* of the coset $\boldsymbol{v}+W$. We take $\mathbf{0}$ to be the natural representative of the coset W.

    i) Prove that $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ represent the same coset if and only if $\boldsymbol{v}_1 - \boldsymbol{v}_2 \in W$.

    ii) Show that the addition

    $$(\boldsymbol{v}_1 + W) \oplus (\boldsymbol{v}_2 + W) = (\boldsymbol{v}_1 + \boldsymbol{v}_2) + W$$

    and the scaling

    $$c \odot (\boldsymbol{v} + W) = c\boldsymbol{v} + W$$

    are well defined, i.e. do not depend on the choice of coset representatives.

    iii) Show that the set V/W of cosets is a vector space under the operations defined in ii).

Definition. The vector space V/W in iii) is called the *quotient (space)* of V by W.

3.3 The Dimension of a Vector Space

To motivate the definition of the dimension of a vector space V, consider $V = \mathbb{R}^3$. If $\boldsymbol{v}_1 \neq \mathbf{0}$ is in $\mathbb{R}^3$, the set V_1 of all scalar multiples of $\boldsymbol{v}_1$ is a subspace of $\mathbb{R}^3$. In fact, it is a line – a 1-dimensional object sitting inside $\mathbb{R}^3$. If a vector $\boldsymbol{v}_2$ is in $\mathbb{R}^3$ but not in V_1, the set $V_2 = \operatorname{span}\{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ consisting of all linear combinations $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2$ (c_j in $\mathbb{R}$) is a subspace of $\mathbb{R}^3$. This one is a plane, a 2-dimensional object sitting inside $\mathbb{R}^3$. Finally, if we pick any $\boldsymbol{v}_3$ in $\mathbb{R}^3$, which is not in V_2, then $V_3 = \operatorname{span}\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3\}$ is $\mathbb{R}^3$ itself. We cannot find an *ascending chain*

$$\{\mathbf{0}\} \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_n$$

of subspaces of $\mathbb{R}^3$ with $n > 3$. Since the dimension of $\mathbb{R}^3$ is to be 3, intuitively, the dimension of a vector space V is the maximum number of distinct subspaces one can squeeze between $\{\mathbf{0}\}$ and V in the following sense.

Definition. The *dimension* $\dim_K V$ of a vector space V over K is the largest $n \geq 0$, which could be infinite, such that there is an ascending chain

$$\{\mathbf{0}\} = V_0 \subsetneqq V_1 \subsetneqq \cdots \subsetneqq V_n$$

of subspaces of V.

A vector space is *finite-dimensional* or *infinite-dimensional* according as n is finite or infinite. If n is finite, then $V = V_n$.

The dimension $\dim_K V$ is well-defined. We often write it simply as $\dim V$ when the field of scalars K is clear from the context. Clearly, $\dim\{\mathbf{0}\} = 0$. If $\dim V$ is positive but finite, every minimal spanning set contains exactly $n = \dim V$ vectors. Such a minimal set $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ may be obtained by choosing $\boldsymbol{v}_i$ in $V_i - V_{i-1}$, $i = 1, \ldots, n$.

Definition. A minimal spanning set $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of a finite dimensional vector space $V \neq \{\mathbf{0}\}$ is called a *basis* of V *over* K, or simply a basis of V if K is clear from the context.

In the next section we will define the concept of a basis in general and show that every vector space has a basis.

Remarks. According to our definition,

1. A basis $\mathcal{B}$ does not contain the zero vector.

2. A basis is not unique, but any two bases of a finite dimensional vector space have the same number of vectors, namely $n = \dim V$.

3. Every vector $\boldsymbol{v}$ in V is a linear combination

$$\boldsymbol{v} = \sum_{\alpha \in I} c_\alpha \boldsymbol{v}_\alpha$$

with I a finite indexing set, c_α in K and $\boldsymbol{v}_\alpha$ in $\mathcal{B}$.

4. If W is a subspace of V, then $\dim W \leq \dim V$. The equality holds if and only if $W = V$.

5. In many settings, one can define the *dimension of a geometric object* X as the maximum number n of (irreducible) subobjects X_j with

$$X_0 \underset{\neq}{\subsetneq} X_1 \underset{\neq}{\subsetneq} \cdots \underset{\neq}{\subsetneq} X_n.$$

[Note that every subspace of a vector space is automatically *irreducible* – not a union of two proper subspaces (cf. Exercise 7, Section 3.2).]

For example, if the geometric object is a surface X, intuitively its dimension is two. To apply our definition, choose $X_0 = \{x_0\}$ with x_0 any point on X, an irreducible curve X_1 on X passing through x_0 and $X_2 = X$ itself.

Examples.

1. The dimension $\dim \mathbb{R}^3 = 3$ and $\{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ is a basis of $\mathbb{R}^3$.

2. $\{1, x, x^2\}$ is a basis of P_3, the vector space of polynomials of degree < 3, whose dimension is 3.

$\{1 + x, 1 - x, 1 + x + x^2\}$ is another basis of P_3.

3. Let $K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$. Then $\dim K^n = n$. The so-called *standard basis* of K^n consists of

$$\begin{aligned} \boldsymbol{e}_1 &= (1, 0, \ldots, 0) \\ \boldsymbol{e}_2 &= (0, 1, 0, \ldots, 0) \\ &\vdots \\ \boldsymbol{e}_n &= (0, \ldots, 0, 1). \end{aligned}$$

4. $\dim M(m \times n, \mathbb{R}) = mn$. The *standard basis* for $M(m \times n, K)$ consists of mn matrices E_{ij} having 1 at the (ij)-th place and zero elsewhere.

5. Recall from Chapter 1 the field

$$K = \mathbb{Q}(\sqrt{d}) = \{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\}.$$

When considered as a vector space over $\mathbb{Q}$, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$, and $\{1, \sqrt{d}\}$ is a basis of K over $\mathbb{Q}$.

6. $\dim_{\mathbb{R}} \mathbb{C} = 2$ and $\{1, \sqrt{-1}\}$*is a basis of* $\mathbb{C}$ *over* $\mathbb{R}$.

7. It is a non-trivial fact that the set $\{\cos \mu x, \sin \mu x\}$ is a basis of the solution space of the linear differential equation

$$\frac{d^2y}{dx^2} + \mu^2 y = 0 \quad \text{(for a fixed } \mu > 0\text{)},$$

which is 2-dimensional.

3.4 Linear Independence

Often it is convenient to have an equivalent description of bases using the concept of linear independence. Roughly speaking, a non-empty subset S of a vector space V, over the field of scalars K, is *linearly dependent*, if there is a vector $\boldsymbol{v}$ in S such that $\boldsymbol{v}$ is a linear combination

$$\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$$

of some other vectors $\boldsymbol{v}_j (\neq \boldsymbol{v})$ in S, equivalently

$$1\boldsymbol{v} - c_1\boldsymbol{v}_1 - \cdots - c_n\boldsymbol{v}_n = \mathbf{0}$$

which suggests the most general description of linear dependence.

Definition. A non-empty set S of a vector space V is *linearly independent* if the equation

$$c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0} \quad (\boldsymbol{v}_j \in S)$$

is possible only with $c_1 = \cdots = c_n = 0$.

The set S is *linearly dependent* if it is not linearly independent.

Clearly, any set containing the zero vector is linearly dependent because $1\mathbf{0} = \mathbf{0}$.

Theorem. (Criterion for Linear Independence) *A non-empty set S, not containing $\mathbf{0}$, is linearly independent if and only if no vector $\boldsymbol{v}$ in S is a linear combination*

$$\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n \tag{3.2}$$

with all $\boldsymbol{v}_j$ in $S - \{\boldsymbol{v}\}$.

Proof. We show that S is linearly dependent if and only if a vector $\boldsymbol{v}$ in S is a linear combination as in (3.2).

But this is obvious, because there is a non-trivial relation

$$c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n = \mathbf{0}$$

with $\boldsymbol{v}_j$ in S and say $c_1 \neq 0$ (which may be assumed to be -1) if and only if

$$\boldsymbol{v}_1 = c_2\boldsymbol{v}_2 + \cdots + c_n\boldsymbol{v}_n. \qquad \square$$

Examples.

1. We show that the three polynomials $1+x$, $1-x$ and $1+x+x^2$ are linearly independent. Start with

$$c_1(1+x) + c_2(1-x) + c_3(1+x+x^2) = 0$$

which is

$$(c_1+c_2+c_3) + (c_1-c_2+c_3)x + c_3x^2 = 0.$$

But a polynomial is zero, only if all its coefficients are zero. So

$$\begin{aligned} c_1 + c_2 + c_3 &= 0 \\ c_1 - c_2 + c_3 &= 0 \\ c_3 &= 0 \end{aligned}$$

We solve these three equations in three unknowns c_1, c_2, and c_3. If we do that, we find that $c_1 = c_2 = c_3 = 0$. Hence $1+x$, $1-x$ and $1+x+x^2$ are linearly independent.

On the other hand, it is trivial that the infinite set $\{x^n \mid n = 0, 1, 2, \ldots\}$ is linearly independent, because again, a polynomial is zero only if all its coefficients are zero.

2. In $\mathbb{R}^3$, the three vectors $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$ are linearly independent, because $x\boldsymbol{i}+y\boldsymbol{j}+z\boldsymbol{k} = \mathbf{0}$ implies that the vector $(x,y,z) = \mathbf{0}$ which means that $x = y = z = 0$.

The following theorem allows us to give an alternative definition of a basis.

Theorem 3.5. *Suppose $V \neq \{\mathbf{0}\}$ is a vector space over K and $\mathcal{B}$ is a non-empty subset of V. The following two statements are equivalent:*

1) $\mathcal{B}$ is a minimal spanning set.

2) $\mathcal{B}$ is a maximal linearly independent set.

Proof. If $\mathcal{B}$ is a minimal spanning set, but not a maximal linearly independent set, there is a vector $\boldsymbol{v}$ in V such that $\mathcal{B} \cup \{\boldsymbol{v}\}$ is also linearly independent. But then $\boldsymbol{v}$ is not in the span of $\mathcal{B}$. Conversely, if $\mathcal{B}$ is a maximal linearly independent set, but does not span V, take a vector $\boldsymbol{v}$ not in the span of $\mathcal{B}$. Then $\mathcal{B} \cup \{\boldsymbol{v}\}$ is linearly independent, contradicting the maximality of $\mathcal{B}$. □

Definition. A *basis* of a vector space $V \neq \{\mathbf{0}\}$ is a minimal spanning set, or equivalently, a maximal linearly independent set of vectors in V.

Corollary. *A subset of V is a basis of V if it i) spans V and ii) is linearly independent.*

Example. $\dim K[x] = \infty$ and $\{x^n \mid n = 0, 1, 2, \ldots\}$ is a basis of $K[x]$. We call it the *standard basis of* $K[x]$. Another basis of $K[x]$ is $\{1, 1 + x, 1 + x + x^2, \ldots, 1 + x + \cdots + x^n, \ldots\}$.

Theorem. (Existence of a basis) *Every vector space $V \neq \{\mathbf{0}\}$ has a basis over K.*

The proof is an easy consequence of the so-called Zorn's Lemma (cf. Chapter 1).

Proof. We show that V has a maximal linearly independent set. Let $\mathcal{S}$ be the set of all linearly independent sets in V. It is partially ordered by the inclusion $\subseteq$. We claim that $\mathcal{S}$ has a maximal linearly independent set. We invoke Zorn's Lemma. Let $\mathcal{C}$ be any chain in $\mathcal{S}$. We claim that $T = \bigcup_{S \in \mathcal{C}} S$ is in $\mathcal{S}$ and is an upper bound for $\mathcal{C}$. Since for every S in $\mathcal{C}$, $S \subseteq T$, all we need to show is that $T \in \mathcal{S}$. For that, let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in T$. Then each $\boldsymbol{v}_j$ is in some $S_j \in \mathcal{C}$. Since $\mathcal{C}$ is totally ordered, we can relabel $\boldsymbol{v}_j$, if necessary, so that $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n$. Thus all $\boldsymbol{v}_j$ are in S_n, hence linearly independent. By Zorn's Lemma, $\mathcal{S}$ has a maximal element. □

Remarks.

1. Suppose $\dim V = n < \infty$ and S is a non-empty subset of V.

(a) If S has more than n vectors, it is linearly dependent.

(b) If S has less than n vectors, then S cannot span V.

(c) Any set of n linearly independent vectors is a basis of V.

2. Suppose $S \subseteq V$ is linearly independent. If $\operatorname{span}(S) \neq V$, there is a basis $\mathcal{B}$ of V such that $S \subsetneqq \mathcal{B}$. We say that S can be extended to a basis $\mathcal{B}$ of V.

For the next theorem, recall that if W_1, W_2 are subspaces of V, then so are $W_1 + W_2$ and $W_1 \cap W_2$.

Theorem 3.6. *Suppose W_1, W_2 are subspaces of a vector space V. Then*

$$\dim W_1 + \dim W_2 = \dim(W_1 + W_2) + \dim(W_1 \cap W_2).$$

Proof. Assume that $\dim W_j < \infty$ $(j = 1, 2)$, otherwise there is nothing to prove. Let $\dim W_1 = m$, $\dim W_2 = n$, and $\dim(W_1 \cap W_2) = r$. There is nothing to prove if $m = n = r$. So assume that at least one of m, n, say $n > r$. Choose a basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ of W_1 and $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ that of W_2 with first r vectors of each in $W_1 \cap W_2$.

Clearly, the set $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{v}_{r+1}, \dots, \boldsymbol{v}_n\}$ spans $W_1 + W_2$. It is also linearly independent because for it to be linearly dependent, some $\boldsymbol{v}_j (j > r)$ has to be a linear combination of $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$, which would imply that $\boldsymbol{v}_j$ is in $W_1 \cap W_2$, contradicting the choice of $\boldsymbol{v}_j$. Hence

$$\begin{aligned}\dim(W_1 + W_2) &= m + n - r \\ &= \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2). \qquad \square\end{aligned}$$

EXERCISES

In Problems 1–6, determine whether the set S of the given vector space is linearly dependent or linearly independent.

1. The subset $S = \left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 7 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right\}$ of $\mathbb{R}^3$.
2. The subset $S = \left\{ \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix}, \begin{pmatrix} -3 \\ -5 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ -6 \end{pmatrix} \right\}$ of $\mathbb{R}^3$.
3. The subset $S = \{1 + 2x + 3x^2, 4 + 5x + 7x^2, 2 + x + x^2\}$ of $K[x]$.
4. The subset $S = \{1 + 3x - 2x^2, -3 - 5x + 6x^2, 5x - 6x^2\}$ of $K[x]$.
5. The set $S = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 5 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \right\}$ of $M(2, K)$.
6. The set $S = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} -3 & -5 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 5 \\ 0 & -6 \end{pmatrix} \right\}$ of $M(2, K)$.
7. While doing problems 1-6, did you realize you were doing the same two problems all over again? You were working in the so-called *isomorphic vector spaces*.
8. Find three vectors in $\mathbb{R}^3$, which are linearly dependent, but any two of them are linearly independent.
9. If α is transcendental, show that

   $$S = \{\alpha^n \mid n = 0, 1, 2, \dots\}$$

   is a linearly independent subset of the vector space $\mathbb{C}$ over $\mathbb{Q}$.

10. Suppose A, B are subsets of a vector space V such that $A \subseteq B$. Prove that

    (a) If A is linearly dependent, then so is B.

    (b) If B is linearly independent, then so is A.

11. If $\boldsymbol{u}$, $\boldsymbol{v}$ are linearly dependent, show that one of them is a scalar multiple of the other.

12. Use Problem 11 to show that $\cos x$ and $\sin x$ are linearly independent.

13. Compute $\dim_K V$, if

    (a) $V = \{A \in M(n, K) \mid A \text{ is upper triangular}\}$. [Recall that a matrix $A = (a_{ij})$ is upper triangular if $a_{ij} = 0$ whenever $i > j$.]

    (b) $V = \{A \in M(n, K) \mid A \text{ is symmetric}\}$.

    (c) $V = \{A = (a_{ij}) \in M(n, K) \mid \operatorname{tr}(A) = a_{11} + \cdots + a_{nn} = 0\}$.

    Hint: Use one of the following: i) $\operatorname{tr}(A) = 0$ is one linear equation in n^2 variable, ii) exhibit explicitly a basis of V over K, and iii) use Theorem 4.5.

    (d) $V = M(m \times n, \mathbb{C})$ as a vector space over $K = \mathbb{R}$.

14. Let $V = \mathbb{C}$, as a vector space over $\mathbb{Q}$. Let $W = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic}\}$. What is $\dim_{\mathbb{Q}} W$?

15. Suppose k is a subfield of K and K is a subfield of L (so that k is a subfield of L). Show that, as a vector space,

$$\dim_k L = \dim_k K \cdot \dim_K L.$$

    Hint: If any of the three dimensions appearing in the equality is ∞, there is nothing to prove. So suppose $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of K over k and $\{\beta_1, \ldots, \beta_n\}$ is a basis of L over K. Put $S = \{\alpha_i\beta_j \mid i = 1, \ldots, m; j = 1, \ldots, n\}$. Show that

    (a) S spans L over k, and

    (b) S is linearly independent over k.

16. Let V be the vector space over $\mathbb{R}$ of continuous functions $f : [0, 1] \to \mathbb{R}$ and $\mathcal{B}$ is a basis of V over $\mathbb{R}$. Can we write $\mathcal{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_3, \ldots\}$? In other words, do $\mathcal{B}$ and $\mathbb{N}$ have the same cardinality? Explain.

3.5† Application of Knowing dim(V)

Mechanical movements obey the laws of physics and are described in general by differential equations. Linear algebra plays a crucial role in seeking their solutions. The motion (called a simple harmonic motion) of a piston in an engine or the vibration of a weight W hung from a spring, pulled down and let go (Figure 3.1) is governed by a differential equation

$$\frac{d^2y}{dt^2} + \mu^2 y = 0, \quad (\mu > 0) \tag{3.3}$$

Here $y = y(t)$ denotes the vertical displacement of W with respect to time t from the equilibrium position $y = 0$ at time $t = 0$. The constant $\mu > 0$ depends on the specification of the engine or the strength of the spring, as the case may be. By a solution of (3.3) we mean a rule that describes the displacement $y = y(t)$ as a function of t satisfying equation (3.3).

We remarked earlier that the solutions of the second order linear differential equation (3.3) form a two-dimensional vector space over $\mathbb{R}$. The two obvious solutions of (3.3) are $y_1 = \cos \mu x$ and $y_2 = \sin \mu x$. Clearly y_1 and y_2 are linearly independent, because otherwise $\sin x = c \cdot \cos x$ would imply that $\tan x = c$ is a constant function. Thus y_1, y_2 span this two-dimensional vector space over $\mathbb{R}$.

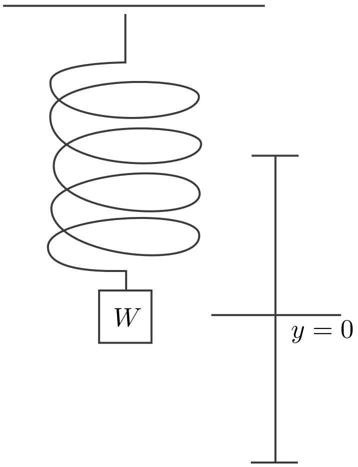


FIGURE 3.1: A suspended weight in equilibrium

In general, we consider an *ordinary homogeneous linear differential equation*

$$\frac{d^n y}{dx^n} + a_{n-1}\frac{d^{n-1}y}{dx^{n-1}} + \cdots + a_1\,\frac{dy}{dx} + a_0 y = 0 \tag{3.4}$$

with real coefficients c_j. The integer $n \geq 1$ is called the *order* of the differential equation (3.4). The solutions of (3.4) again form a vector space V over $\mathbb{R}$. In a course on differential equations, one learns which we take for granted that the dimension of V is equal to the order n.

Theorem 3.7. *The solution space of the differential equation* (3.4) *is n-dimensional.*

Since the order of the linear differential equation (3.3) is two, by this theorem, any solution of (3.3) is a linear combination

$$y = c_1 y_1 + c_2 y_2$$

of the basis vectors y_1, y_2.

When $n > 2$ there is an algorithm to find enough solutions of (3.4). The issue that concerns us here is the following.

Suppose we are given n solutions $y_1, \dots, y_n$ of (3.4). How can we determine if they form a basis of V? Since we know that $\dim V = n$, all we need to check is whether or not these n functions are linearly independent. A very simple procedure which does exactly that is as follows.

Given n functions $y_1, \dots, y_n$ of a real variable x, each having derivative of order up to $n-1$, we define their *Wronskian* to be the determinant (see Chapter 5)

$$W(y_1, \dots, y_n) = \begin{vmatrix} y_1 & \dots & y_n \\ y_1' & \dots & y_n' \\ \vdots & & \\ y_1^{(n-1)} & \dots & y_n^{(n-1)} \end{vmatrix}.$$

Theorem 3.8. *The functions $y_1, \dots, y_n$ are linearly independent if the Wronskian function $W(y_1, \dots, y_n)$ or simply $W(x)$ is not identically the zero function.*

Proof. If there are constants c_j, such that

$$c_1 y_1 + \cdots + c_n y_n = 0,$$

the identically zero function, then

$$\begin{array}{ccccccc} c_1 y_1' & + & \dots & + & c_n y_n' & = & 0 \\ \vdots & & & & & & \\ c_1 y_1^{(n-1)} & + & \dots & + & c_n y_n^{(n-1)} & = & 0. \end{array}$$

Since $W(x)$ is not identically a zero function, choose $x = a$ so that $W(a) \neq 0$. Then the matrix equation

$$\begin{pmatrix} y_1(a) & \dots & y_n(a) \\ y_1'(a) & \dots & y_n'(a) \\ \vdots & & \\ y_1^{(n-1)}(a) & \dots & y_n^{(n-1)}(a) \end{pmatrix} \begin{pmatrix} c_1 \\ \\ \vdots \\ c_n \end{pmatrix} = \mathbf{0}$$

in $c_1, \dots, c_n$ can have only the trivial solution $c_1 = \cdots = c_n = 0$. This proves that $y_1, \dots, y_n$ are linearly independent. □

Examples.

1. Let $\mu > 0$ and $y_1 = \cos \mu x$, $y_2 = \sin \mu x$. Their Wronskian

$$W = \begin{vmatrix} \cos \mu x & \sin \mu x \\ -\mu \sin \mu x & \mu \cos \mu x \end{vmatrix} = \mu > 0.$$

Hence y_1, y_2 are linearly independent. This shows that a general solution of (3.3) is $y = c_1 y_1 + c_2 y_2$ with c_1, c_2 constants.

2. Let $y_1 = x, y_2 = e^x, y_3 = \sin x$. If $W(x)$ is the Wronskian of these functions, an easy calculation shows that $W(\pi) = e^\pi \pi \neq 0$. Hence $x, e^x, \sin x$ are linearly independent.

EXERCISES

1. Show that $e^{ax} \cos bx$ and $e^{ax} \sin bx$ span the solution space of

$$\frac{d^2y}{dx^2} - 2a\frac{dy}{dx} + (a^2 + b^2)y = 0.$$

2. Show that e^{ax} and xe^{ax} span the solution space of

$$\frac{d^2y}{dx^2} - 2a\frac{dy}{dx} + a^2 y = 0.$$

3.6 Coordinates

Suppose V is a finite dimensional vector space of dimension n and $\mathcal{B} = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ is an ordered basis of V. It is easy to verify that each vector $\boldsymbol{v}$ in V has a unique representation

$$\boldsymbol{v} = x_1\boldsymbol{v}_1 + \cdots + x_n\boldsymbol{v}_n$$

as a linear combination of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$. The coefficients $x_1, \dots, x_n$ are called the *coordinates* (or *weights*) of $\boldsymbol{v}$ with respect to $\mathcal{B}$. We then denote $\boldsymbol{v}$ by

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}_{\mathcal{B}} \quad \text{or} \quad \boldsymbol{v}_{\mathcal{B}} = \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

We call $\boldsymbol{x}$ the *coordinate-vector* of $\boldsymbol{v}$ (with respect to $\mathcal{B}$).

Examples.

1. If $V = \mathbb{R}^n$, $\mathcal{B} = \{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ its *standard basis*, we write $\boldsymbol{v}$ simply as

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

2. Suppose $V = P_n$, the vector space of polynomials of degree less than n and call $\mathcal{B} = \{1, x, \dots, x^{n-1}\}$ the *standard basis of* P_n. If $f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, then $f(x)_{\mathcal{B}} = \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$.

3. If $V = P_3$ we take $\mathcal{B}' = \{1, 1+x, 1+x+2x^2\}$. Let $f(x) = 3 + x + 8x^2$. Since $3 + x + 8x^2 = 2 \cdot 1 - 3(1+x) + 4(1+x+2x^2)$, $f(x)_{\mathcal{B}'} = \begin{pmatrix} 2 \\ -3 \\ 4 \end{pmatrix}$.

Transition Matrix

Suppose $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ is the coordinate-vector of $\boldsymbol{v}$ in a given ordered basis $\mathcal{B} = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ of V. If we are given a new basis $\mathcal{B}' = \{\boldsymbol{v}'_1, \dots, \boldsymbol{v}'_n\}$ of V, how is the coordinate vector $\boldsymbol{x}' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = \boldsymbol{v}_{\mathcal{B}'}$ related to $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \boldsymbol{v}_{\mathcal{B}}$?

The answer is: there is an $n \times n$ invertible matrix P such that $\boldsymbol{x}' = P\boldsymbol{x}$ or $\boldsymbol{x} = Q\boldsymbol{x}'$ with $Q = P^{-1}$. We call P the *transition matrix* from $\mathcal{B}$ to $\mathcal{B}'$.

To compute Q, let $\boldsymbol{v}'_1 = q_{11}\boldsymbol{v}_1 + \cdots + q_{n1}\boldsymbol{v}_n, \ldots, \boldsymbol{v}'_n = q_{n1}\boldsymbol{v}_1 + \cdots + q_{nn}\boldsymbol{v}_n$. Then

$$\begin{aligned}
\boldsymbol{v} &= x'_1\boldsymbol{v}'_1 + \cdots + x'_n\boldsymbol{v}'_n \\
&= x'_1(q_{11}\boldsymbol{v}_1 + \cdots + q_{n1}\boldsymbol{v}_n) + \cdots + x'_n(q_{n1}\boldsymbol{v}_1 + \cdots + q_{nn}\boldsymbol{v}_n) \\
&= (q_{11}x'_1 + \cdots + q_{n1}x'_1)\boldsymbol{v}_1 + \cdots + (q_{n1}x'_1 + \cdots + q_{nn}x'_n)\boldsymbol{v}_n \\
&= x_1\boldsymbol{v}_1 + \cdots + x_n\boldsymbol{v}_n.
\end{aligned}$$

The last equality shows that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} q_{11} & \cdots & q_{1n} \\ & & \\ q_{n1} & & q_{nn} \end{pmatrix} \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$$

or $\boldsymbol{x} = Q\boldsymbol{x}'$. Clearly Q is invertible because its columns are the coordinate-vectors of $\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n$ (with respect to $\mathcal{B}$) which are linearly independent.

Remark. If P is the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$, then P^{-1} is the transition matrix from $\mathcal{B}'$ to $\mathcal{B}$.

Examples.

1. Let $V = \mathbb{R}^3$, $\mathcal{B} = \{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\}$ its standard basis. We take

$$\mathcal{B}' = \left\{ \begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ -1 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 0 \\ 3 \end{pmatrix} \right\}.$$

Since

$$\begin{pmatrix} 2 \\ -1 \\ 2 \end{pmatrix} = 2\boldsymbol{e}_1 - \boldsymbol{e}_2 + 2\boldsymbol{e}_3$$

$$\begin{pmatrix} 5 \\ -1 \\ 4 \end{pmatrix} = 5\boldsymbol{e}_1 - \boldsymbol{e}_2 + 4\boldsymbol{e}_3$$

$$\begin{pmatrix} 5 \\ 0 \\ 3 \end{pmatrix} = 5\boldsymbol{e}_1 + 0\boldsymbol{e}_2 + 3\boldsymbol{e}_3,$$

$$Q = \begin{pmatrix} 2 & 5 & 5 \\ -1 & -1 & 0 \\ 2 & 4 & 3 \end{pmatrix}.$$

Therefore, the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ is

$$P = Q^{-1} = \begin{pmatrix} 3 & -5 & -5 \\ -3 & 4 & 5 \\ 2 & -2 & -3 \end{pmatrix}.$$

2. Let $V = P_2$, $\mathcal{B} = \{1, x\}$ its standard basis. We take $\mathcal{B}' = \{\boldsymbol{v}_1', \boldsymbol{v}_2'\}$ with $\boldsymbol{v}_1' = 1 + x$, $\boldsymbol{v}_2' = 1 - x$. Then $\boldsymbol{v}_{1\mathcal{B}}' = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $\boldsymbol{v}_{2\mathcal{B}}' = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. So $Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ is

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

EXERCISES

1. Let $\mathcal{B}$ be the standard basis of $\mathbb{R}^3$. If $\mathcal{B}' = \left\{ \begin{pmatrix} 1 \\ -3 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -3 \end{pmatrix}, \begin{pmatrix} -2 \\ 4 \\ 4 \end{pmatrix} \right\}$ compute the transition matrix P from $\mathcal{B}$ to $\mathcal{B}'$.
2. Let $\mathcal{B} = \{1, x, x^2\}$ be the standard basis of P_3. If $\mathcal{B}' = \{1 + 2x + x^2, 2 + 5x, 3 + 3x + 8x^2\}$, compute the transition matrix P from $\mathcal{B}$ to $\mathcal{B}'$.

3.7 Rank of a Matrix

Suppose A is an $m \times n$ matrix over a field K. The rows of A may be regarded as vectors in $K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$.

Definition. The *row space* of A is the subspace of K^n spanned by the rows of A. The *row rank* of A is the dimension of the row space of A.

Clearly, the row rank r of A is no more than $n = \dim K^n$. Hence, there is no loss of generality in assuming that $m \leq n$. A matrix A is *row equivalent* to B if A can be row reduced to B. To row reduce A to its row echelon form is to find a basis for the row space of A. In particular, the number of nonzero rows (or equivalently pivots) in the row echelon form of A is the row rank of A. The *column space* and *column rank* of A is defined analogously. We show in a later chapter (Theorem 7.5) that row rank of A is the same as its column rank. We call the common value simply the *rank* of A. The dimension of the solution space Null(A) of $A\boldsymbol{x} = \mathbf{0}$ is called the *nullity* of A. We will also show that rank (A) + nullity $(A) = n$.

EXERCISES

1. Determine the ranks of the following matrices:

   (a) $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$

   (b) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$

   (c) $\begin{pmatrix} 2 & -8 & 6 \\ 3 & -9 & 5 \\ -3 & 0 & 1 \\ 1 & -4 & 0 \end{pmatrix}$

   (d) $\begin{pmatrix} 2 & -8 & 6 & 8 \\ 3 & -9 & 5 & 16 \\ -3 & 0 & 1 & -2 \end{pmatrix}$

   (e) $\begin{pmatrix} 2 & -8 & 6 & 8 \\ 3 & -9 & 5 & 10 \\ -3 & 0 & 1 & -2 \\ 1 & -4 & 0 & 6 \end{pmatrix}$

2. Construct 3×3 matrices, each with nonzero and distinct entries everywhere, and of rank 1, rank 2, and rank 3, respectively.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

4

Linear Maps

Now we come to the main topic of our study, namely, the functions in the most general context, which behave like the real valued function $y = mx$ of real variable x. Recall the defining property of this function $f(x) = mx$. For c_1, c_2 in $\mathbb{R}$, $f(c_1x_1 + c_2x_2) = c_1f(x_1) + c_2f(x_2)$. The probability of a randomly chosen function $T : V \to W$ to have this property is zero (see Exercise 1, Section 4.1).

4.1 Linear Maps

Suppose that V and W are vector spaces over the same field K. Recall the definition of a function from Chapter 1.

Definition. A *linear map* or a *linear transformation* is a function $T : V \to W$ such that for c_1, c_2 in K and $\boldsymbol{v}_1, \boldsymbol{v}_2$ in V, we have

$$T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2). \tag{4.1}$$

It is easy to see that, again, (4.1) is equivalent to the following two conditions: For $\boldsymbol{u}$ and $\boldsymbol{v}$ in V and c in K,

1) $T(\boldsymbol{u} + \boldsymbol{v}) = T(\boldsymbol{u}) + T(\boldsymbol{v})$
2) $T(c\boldsymbol{u}) = cT(\boldsymbol{u})$

To be precise, we should write conditions 1) and 2) above as

1) $T(\boldsymbol{u} \oplus_V \boldsymbol{v}) = T(\boldsymbol{u}) \oplus_W T(\boldsymbol{v})$
2) $T(c \odot_V \boldsymbol{u}) = c \odot_W T(\boldsymbol{u})$,

where $\oplus_V$ denotes the addition in the vector space V. The other symbols have similar meaning. Thus, the conditions 1) and 2) may be described by saying that T *preserves the vector space structure*, or that T is *compatible with the vector space operations.*

Examples.

1. Our first example is our starting point. We take $V = W = \mathbb{R}$, the 1-dimensional space over $\mathbb{R}$. The map $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = mx$ is linear.

2. Fix $0 \leq \theta < 2\pi$. The rotation $T : \mathbb{R}^2 \to \mathbb{R}^2$ through angle θ, given by $T(x, y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$, is a linear transformation. In matrix notation,

$$T(x, y) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

The matrix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is called the matrix of rotation.

3. In general, let M be an $m \times n$ matrix over $\mathbb{R}$. Suppose $V = \mathbb{R}^n$ and $W = \mathbb{R}^m$. The map $T_M : V \to W$ given by $T_M(\boldsymbol{x}) = M\boldsymbol{x}$ is a linear map. Here $\boldsymbol{x}$ is the column vector

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

(the same for vectors in $\mathbb{R}^m$) and $M\boldsymbol{x}$ is the product of the matrices M and $\boldsymbol{x}$.

In particular, if $r > 0$ and $M = rI$, I being the $n \times n$ identity matrix, then $T_M : \mathbb{R}^n \to \mathbb{R}^n$ is a *contraction* or *dilation* according as $r < 1$ or $r > 1$.

Another interesting example is a *horizontal shear* $T_M : \mathbb{R}^2 \to \mathbb{R}^2$ of the plane given by the matrix

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

the scalar s is called the *shear factor* (see Figure 4.1). A vertical shear is defined similarly.

The *reflection* of the points of $\mathbb{R}^2$ in the x-axis and y-axis are given by

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

respectively.

We shall see in due course that if V and W are finite dimensional, every linear map is T_M for some M.

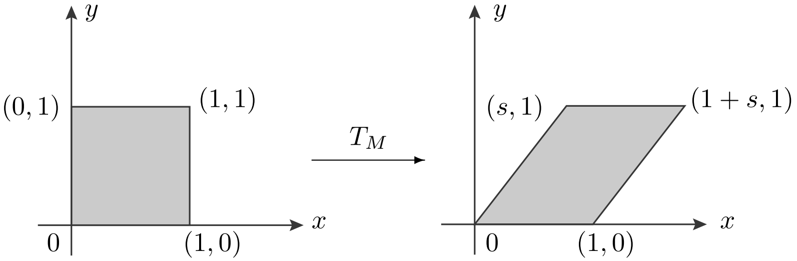


FIGURE 4.1: A horizontal shear

4. For any pair of vector spaces V and W, the map $T : V \to W$ given by $T(\boldsymbol{v}) = \mathbf{0}$ for all $\boldsymbol{v}$ in V, is a linear transformation. It is called the *zero transformation* and is often denoted by 0.

5. Let $V = P_n$, the vector space of polynomials of degree $< n$ over K. If $W = K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$, then the function $T : V \to W$ given by $T(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) = (c_0, c_1, \ldots, c_{n-1})$ is a *linear map.*

6. Consider $\mathbb{C}$ as a vector space over $\mathbb{R}$. The *conjugation* $\kappa : \mathbb{C} \to \mathbb{C}$, that is, $\kappa(a + ib) = a - ib$ is a linear map.

7. We shall denote throughout by $C^\infty(I)$ the vector space, over $\mathbb{R}$, of real valued functions on an open interval I (of finite or infinite length) which have derivatives of all orders.

Let $V = W = C^\infty(I)$. One learns in the first course on calculus that the map $D = \frac{d}{dx} : V \to W$ given by $D(f) = \frac{df}{dx}$ is a linear transformation: For f, g in $C^\infty(I)$ and c in $\mathbb{R}$,

(a) $\frac{d}{dx}(f + g) = \frac{d}{dx}(f) + \frac{d}{dx}(g),$ *and*

(b) $\frac{d}{dx}(cf) = c\,\frac{d}{dx}(f).$

More generally, let

$$D = \frac{d^n}{dx^n} + a_{n-1}\,\frac{d^{n-1}}{dx^{n-1}} + \cdots + a_1\,\frac{d}{dx} + a_0$$

be a *linear operator*, so that

$$D(y) = \frac{d^n y}{dx^n} + a_{n-1}\,\frac{d^{n-1}y}{dx^{n-1}} + \cdots + a_1\,\frac{dy}{dx} + a_0 y.$$

Then D is a linear map from the vector space $C^n(\mathbb{R})$ of functions $f : \mathbb{R} \to \mathbb{R}$ having the n-th order derivatives to the vector space $C^0(\mathbb{R})$ of continuous functions $g : \mathbb{R} \to \mathbb{R}$.

8. Let $V = C[a, b]$ be the vector space of continuous functions $f : [a, b] \to \mathbb{R}$ and $W = \mathbb{R}$. Both V and W are vector spaces over $\mathbb{R}$. The map $I : V \to W$ given by

$$I(f) = \int\limits_a^b f(x)dx$$

is linear.

9. Let K be any field and $V = M(m \times n, K)$. Suppose $W = K^{mn} = \{(x_{11}, \ldots, x_{mn}) \mid x_{ij} \in K\}$. For $A = (a_{ij})$ in V, we put

$$T(A) = (a_{11}, \ldots, a_{1n}, \ldots, a_{m1}, \ldots, a_{mn}).$$

Then $T : V \to W$ is a linear map.

10. Let $V = \mathbb{R}^n$. Recall the standard basis $\boldsymbol{e}_1 = (1, 0, \ldots, 0), \ldots, \boldsymbol{e}_n = (0, \ldots, 0, 1)$ of $\mathbb{R}^n$. We call the subspace $\mathbb{R}\boldsymbol{e}_j = \{c\boldsymbol{e}_j \mid c \in \mathbb{R}\}$ the j-th *axis* of $\mathbb{R}^n$. The j-th *projection* $p_j : \mathbb{R}^n \to \mathbb{R}^n$ on the j-th axis is the linear map $p_j(x_1, \ldots, x_n) = x_j\boldsymbol{e}_j$.

11. Again, let $V = K^n$, but with K being any field. The *standard* j*-th hyperplane* $H_j = \{(x_1, \ldots, x_n) \in V \mid x_j = 0\}$. The set H_j is a subspace of V. The j-th projection from V on $W = H_j$ is the linear map $P_j : V \to W$ given by $P_j(x_1, \ldots, x_n) = (x_1, \ldots, x_n) - x_j\boldsymbol{e}_j$.

EXERCISES

1. Which of the following functions are linear maps from $\mathbb{R}^2$ to $\mathbb{R}^2$? *Hint:* Consult the definition of a linear map.

   (a) $T(x, y) = (x^2, y^3)$

   (b) $T(x, y) = (x + y, x - y)$

   (c) $T(x, y) = (\cos x, \sin y)$

   (d) $T(x, y) = (e^x, y)$

2. Show that the translation $S : \mathbb{R}^2 \to \mathbb{R}^2$ by a fixed vector (a, b), that is, $S(x, y) = (x + a, y + b)$, is a linear transformation if and only if $(a, b) = (0, 0)$.

3. Show that $T(x, y, z) = (y + z, z + x, x + y)$ is a linear map from $\mathbb{R}^3$ to $\mathbb{R}^3$.

4. i) A (straight) *line* L through two distinct points $\boldsymbol{a}$ and $\boldsymbol{b}$ in the Euclidean space $\mathbb{R}^n$ is the set
$$L = \{\boldsymbol{a} + t(\boldsymbol{b} - \boldsymbol{a}) \mid t \in \mathbb{R}\}.$$
Show that any linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ takes lines to lines, i.e. $T(L)$ is a line for any line L in $\mathbb{R}^n$, unless $T(\boldsymbol{a}) = T(\boldsymbol{b})$ in which case it is a point.

   ii) The *line segment* joining two distinct points $\boldsymbol{a}$ and $\boldsymbol{b}$ in $\mathbb{R}^n$ is the set
$$[\boldsymbol{a}, \boldsymbol{b}] = \{\boldsymbol{a} + t(\boldsymbol{b} - \boldsymbol{a}) \mid 0 \le t \le 1\}.$$
Show that the image $T([\boldsymbol{a}, \boldsymbol{b}])$ of a line segment under a linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ is a line segment.

5. Suppose $V = M(n, K)$ and $A \in V$. Show that the function $T(X) = AX - XA$ is a linear map from V to itself.

6. Show that transposing i.e. $A \to A^*$ is a linear map from $M(m \times n, K)$ to $M(n \times m, K)$.

7. Suppose $V = W = \mathbb{Q}[x]$. Which of the following maps $F : V \to W$ are linear? $F(f(x)) =$

   (a) $xf(x)$

   (b) $x^2 + f(x)$

   (c) $f(0)f(x)$

   (d) $f(x) + 2f'(x) + 3f''(x)$.

8. Which of the following functions F are linear maps from V to W?

   (a) $V = C[a, b]$, $W = \mathbb{R}$, $F(f) = F(b) - F(a)$

   (b) $V = M(2, K)$, $W = K$, $F(A) = \det(A)$

   (c) $V = M(n, K)$, $W = K$, $F(A) = \operatorname{tr}(A)$

   (d) $V = C[a, b]$, $W = \mathbb{R}$, $F(f) = \left[\int_b^a (f(x))^2 dx\right]^{1/2}$.

9. When is the function $F(x, y, z) = (x + a, y + b, z + c)$ linear?

10. Consider $V = M(2, \mathbb{C})$ as a vector space over $K = \mathbb{R}$. Suppose $T(a_{ij}) = (\overline{a_{ij}})$, where $\overline{a}$ denotes the conjugate of a. Show that T is a linear transformation from V to itself.

11. **Extension by Linearity**.

    Suppose V, W are vector spaces over K and $B = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis of V. Let $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\} \subseteq W$. Show that there is a unique linear map $T : V \to W$, such that $T(\boldsymbol{v}_j) = \boldsymbol{w}_j$. We say that T is the *extension of* $T(\boldsymbol{v}_j) = \boldsymbol{w}_j$ *by linearity.*

(*Hint*: Write $\boldsymbol{v}$ in V as $\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$ and put $T(\boldsymbol{v}) = c_1\boldsymbol{w}_1 + \cdots + c_n\boldsymbol{w}_n$.)

4.2 Properties of Linear Maps

The axioms we chose to define a vector space is a minimal set of properties, such that the other properties we desire can be derived from them. In fact, so many interesting facts about the vectors follow almost immediately from the defining ten properties listed in the definition of a vector space. The same is true for linear transformations. Unless stated otherwise, $T : V \to W$ is a generic linear map.

Proposition 4.1.

1) $T(\mathbf{0}) = \mathbf{0}$, *and*

2) $T(-\boldsymbol{v}) = -T(\boldsymbol{v})$ *for all* $\boldsymbol{v}$ *in* V.

The proposition says that 1) a linear map takes the zero vector of V to the zero vector of W. [A clearer way to write 1) may be $T(\mathbf{0}_V) = \mathbf{0}_W$], whereas 2) says that it takes the negative of $\boldsymbol{v}$ to the negative of $T(\boldsymbol{v})$.

Proof.

1) Since $\mathbf{0} = \mathbf{0} + \mathbf{0}$ and T is linear, $T(\mathbf{0}) = T(\mathbf{0}) + T(\mathbf{0})$ which gives $T(\mathbf{0}) = \mathbf{0}$.

2) We know that $(-1)\,\boldsymbol{v} = -\boldsymbol{v}$. Hence,

$$\begin{aligned} T(-\boldsymbol{v}) &= T((-1)\boldsymbol{v}) \\ &= (-1)T(\boldsymbol{v}) \\ &= -T(\boldsymbol{v}). \end{aligned} \qquad \square$$

Theorem 4.2. *The image* $T(V) = \{T(\boldsymbol{v}) \mid \boldsymbol{v} \in V\}$ *is a subspace of* W.

Proof. Recall the definition of a subspace. Suppose $\boldsymbol{w}_1, \boldsymbol{w}_2 \in T(V)$ and $c_1, c_2 \in K$. Then $\boldsymbol{w}_j = T(\boldsymbol{v}_j)$ for some $\boldsymbol{v}_j \in V$. Since $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 \in V$,

$$\begin{aligned} c_1\boldsymbol{w}_1 + c_2\boldsymbol{w}_2 &= c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) \\ &= T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) \in T(V). \end{aligned} \qquad \square$$

Theorem 4.3. *The preimage* $T^{-1}(\mathbf{0}) = \{\boldsymbol{v} \in V \mid T(\boldsymbol{v}) = \mathbf{0}\}$ *is a subspace of* V.

Proof. If $\boldsymbol{v}_1, \boldsymbol{v}_2 \in T^{-1}(\mathbf{0})$ and $c_1, c_2 \in K$, then $T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) = c_1\mathbf{0} + c_2\mathbf{0} = \mathbf{0}$.

Hence $c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 \in T^{-1}(\mathbf{0})$. □

Definition. The subspace $T^{-1}(\mathbf{0}) = \{\boldsymbol{v} \in V \mid T(\boldsymbol{v}) = \mathbf{0}\}$ of V is called the *kernel* of T and is denoted by $\operatorname{Ker}(T)$.

Theorem 4.4. *A linear transformation* $T : V \to W$ *is injective, if and only if* $\operatorname{Ker}(T) = \{\mathbf{0}\}$.

Proof. We will use the abbreviation $(a) \Rightarrow (b)$ for (a) implies (b). If T is injective, only one vector can go to zero of W, which clearly is the zero vector of V. Conversely, suppose $\operatorname{Ker}(T) = \{\mathbf{0}\}$. If $T(\boldsymbol{v}_1) = T(\boldsymbol{v}_2)$, then $T(\boldsymbol{v}_1) - T(\boldsymbol{v}_2) = \mathbf{0} \Rightarrow T(\boldsymbol{v}_1 - \boldsymbol{v}_2) = \mathbf{0} \Rightarrow \boldsymbol{v}_1 - \boldsymbol{v}_2 \in \operatorname{Ker}(T) = \{\mathbf{0}\}$. Hence $\boldsymbol{v}_1 - \boldsymbol{v}_2 = \mathbf{0} \Rightarrow \boldsymbol{v}_1 = \boldsymbol{v}_2$. This shows that T is injective. □

Theorem 4.5. *Suppose* V, W *are vector spaces over a field* K *and* V *is finite dimensional. If* $T : V \to W$ *is a linear transformation, then* $\dim T(V) + \dim \operatorname{Ker}(T) = \dim V$.

Proof. Let $\dim V = n$, and dim $\operatorname{Ker}(T) = m \leq n$. Suppose $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ is a basis of $\operatorname{Ker}(T)$. If $m = n$, there is nothing to prove. Otherwise, extend it to a basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m, \boldsymbol{v}_{m+1}, \ldots, \boldsymbol{v}_n\}$ of V. Clearly, the set $S = \{T(\boldsymbol{v}_{m+1}), \ldots, T(\boldsymbol{v}_n\}$ spans $T(V)$. Therefore, to prove the theorem, it is enough to show that S is linearly independent.

Suppose $c_{m+1}T(\boldsymbol{v}_{m+1}) + \cdots + c_nT(\boldsymbol{v}_n) = \mathbf{0}$. Then $T(c_{m+1}\boldsymbol{v}_{m+1} + \cdots + c_n\boldsymbol{v}_n) = \mathbf{0}$, which shows that $c_{m+1}\boldsymbol{v}_{m+1} + \cdots + c_n\boldsymbol{v}_n \in \operatorname{Ker}(T) \Rightarrow c_{m+1}\boldsymbol{v}_{m+1} + \cdots + c_n\boldsymbol{v}_n = a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m$, or $a_1\boldsymbol{v}_1 + \cdots + a_m\boldsymbol{v}_m - c_{m+1}\boldsymbol{v}_{m+1} - \ldots - +c_n\boldsymbol{v}_n = \mathbf{0}$. The linear independence of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ now implies that $c_{m+1} = \ldots = c_n = 0$. This completes the proof. □

This theorem involves only the subspace $T(V)$ of W. Hence our statements will appear somewhat simpler, if we assume that $T : V \to W$ is surjective. In that case, we write W instead of $T(V)$.

Corollary 4.6. *Suppose* $T : V \to W$ *is a surjective linear map and* V *is finite dimensional. Then* $\dim W \leq \dim V$. *Moreover, the equality* $\dim W = \dim V$ *holds, if and only if,* T *is injective.*

Proof. The first statement is trivial, because

$$\dim V = \dim W + \dim \operatorname{Ker}(T)$$

The second statement is also trivial, because $\dim W = \dim V \Leftrightarrow \dim \operatorname{Ker} T = 0 \Leftrightarrow T$ is injective. □

Corollary 4.7. *If* $W = \{A \in M(n, \mathbb{R}) \mid \operatorname{tr}(A) = 0\}$, *then* $\dim W = n^2 - 1$.

Proof. Apply Theorem 4.5 to the linear map $T : M(n, \mathbb{R}) \to \mathbb{R}$ given by $T(A) = \operatorname{tr}(A)$. □

Theorem 4.8. *Suppose a linear map* $T : V \to W$ *is bijective. The inverse* $T^{-1} : W \to V$ *is also a linear map.*

Proof. Suppose $c_1, c_2 \in K$ and $\boldsymbol{u}_1 = T(\boldsymbol{v}_1), \boldsymbol{u}_2 = T(\boldsymbol{v}_2)$ are in $W = T(V)$ with $\boldsymbol{v}_j$ in V. Then

$$\begin{aligned} T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) &= c_1T(\boldsymbol{v}_1) + c_2T(\boldsymbol{v}_2) \\ &= c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2 \end{aligned}$$

Applying T^{-1} to both sides, in reverse order,

$$\begin{aligned} T^{-1}(c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2) &= T^{-1}(T(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2)) \\ &= c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2 \\ &= c_1T^{-1}(\boldsymbol{u}_1) + c_2T^{-1}(\boldsymbol{u}_2). \end{aligned}$$

This proves that T^{-1} is a linear transformation. □

Definition. Two vector spaces V and W over the same field K are *isomorphic*, written as $V \cong W$, if there is a bijective linear map $T : V \to W$. The bijective linear map T is called an *isomorphism*.

Theorem 4.9. *Suppose* V *and* W *are finite dimensional vector spaces over the same field* K *of scalars. Then* V *and* W *are isomorphic, if and only if* $\dim V = \dim W$, *equivalently if and only if there is a linear map* $T : V \to W$ *which takes the bases of* V *to that of* W.

Proof. One implication is obvious. For the other, let $\dim V = \dim W = n$. Suppose $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis of V and $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ is that of W. Define a map $T : V \to W$ as follows. If $\boldsymbol{v} = c_1\boldsymbol{v}_1 + \ldots + c_n\boldsymbol{v}_n$ is in V, put $T(\boldsymbol{v}) = c_1\boldsymbol{w}_1 + \ldots + c_n\boldsymbol{w}_n$. It is easy to show that T is a bijective linear map. We leave the proof of the equivalence as an easy exercise. □

Remarks

1. If $\dim V = \dim W = \infty$, it is not necessary that $V \cong W$. For example, if $V = \mathbb{Q}[x]$, $W = \mathbb{R}$, then $\dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}} W = \infty$, but $V \ncong W$. (Why?)
2. A finite dimensional vector space cannot be isomorphic to an infinite dimensional vector space.
3. The theorem says that given a field K and an integer $n \geq 0$, up to isomorphism, there is only one vector space over K of dimension n, and it is $K^n = \{(x_1, \ldots, x_n) \mid x_j \in K\}$.

Examples.

1. The vector space P_n of polynomials over K of degree $< n$ is isomorphic to K^n. An isomorphism $T : P_n \to K^n$ is given by $T(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) = (c_0, c_1, \ldots, c_{n-1})$. T*he basis* $\{1, x, \ldots, x^{n-1}\}$ of P_n is taken by T to the standard basis $\boldsymbol{e}_1 = (1, 0, \ldots, 0), \ldots, \boldsymbol{e}_n = (0, \ldots, 0, 1)$ of K^n.

2. $M(m \times n, K) \cong K^{mn}$. The isomorphism $T : M(m \times n, K) \to K^{mn}$, given by $T(a_{ij}) = (a_{11}, \ldots, a_{1n}, \ldots, a_{m1}, \ldots, a_{mn})$, takes the standard basis $\{E_{ij}\}$ of $M(m \times n, K)$ to the standard basis of K^{mn}.

3. As a vector space over $\mathbb{R}$, $\mathbb{C} \cong \mathbb{R}^2$. The map $\mathbb{C} \ni a + ib \mapsto (a, b) \in \mathbb{R}^2$ is an isomorphism. It takes the basis $\{1, i\}$ of $\mathbb{C}$ over $\mathbb{R}$, to the standard basis $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ of $\mathbb{R}^2$. We call $\mathbb{C}$ the *complex plane* when identified with $\mathbb{R}^2$.

4. Consider the vector space $V = \mathbb{R}^+$ over $\mathbb{R}$ in Example 11, Section 3.1. Let $W = \mathbb{R}$ and let $T : V \to W$ be the map. $T(x) = \ln x$. One learns in high school that T is a bijective linear map. Hence $V \cong W$.

EXERCISES

1. Construct linear transformations $T, T_1, T_2 : \mathbb{R}^2 \to \mathbb{R}^2$, such that
   (a) $T_1 \circ T_2 = 0$, and $T_2 \circ T_1 \neq 0$,
   (b) $T^2 = 0$. but $T \neq 0$
2. If $T_2 : \mathbb{R}^3 \to \mathbb{R}^2$ and $T_1 : \mathbb{R}^2 \to \mathbb{R}^3$, show that $T_1 \circ T_2$ cannot be invertible.

3. Construct a linear map T from an n-dimensional vector space to itself, such that $T^j \neq 0$ if $1 \leq j < n$, but $T^n = 0$. [Here $T^j = \underbrace{T \circ \cdots \circ T}_{j \text{ times}}$.]

4. If V is the vector space of $n \times n$ upper triangular matrices over K and W the vector space of $n \times n$ symmetric matrices over K, by Exercise 13, Section 3.4, $\dim V = \dim W$, and hence $V \cong W$. Construct an isomorphism $T : V \to W$.

5. Suppose V_1 is a subspace of a vector space V, W_1 that of W, and $T : V \to W$ is a linear map such that $T(V_1) \subseteq W_1$. Prove that $\overline{T} : V/V_1 \to W/W_1$ defined by $\overline{T}(v + V_1) = T(v) + W_1$ is a well-defined linear map.

6. If $T : V \to W$ is a linear map, prove that $T(V) \cong V/\operatorname{Ker}(T)$.

   Hint: In Exercise 5, take $V_1 = \operatorname{Ker}(T)$ and $W_1 = \{\mathbf{0}\}$.

4.3 Matrix of a Linear Map

In this section we show that any linear map $T : V \to W$, V and W finite dimensional, is given by a matrix. To begin with, let it be $T : \mathbb{R}^n \to \mathbb{R}^n$. We take $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ to be the standard bases of $\mathbb{R}^n$. Thus if $\boldsymbol{x} = x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n$, we write it as a column vector

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Then

$$\begin{aligned} T(\boldsymbol{x}) &= T(x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n) \\ &= x_1T\boldsymbol{e}_1 + \cdots + x_nT\boldsymbol{e}_n \\ &= x_1\boldsymbol{c}_1 + \cdots + x_n\boldsymbol{c}_n \\ &= A\boldsymbol{x}, \end{aligned}$$

$\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ being the columns of A. The matrix A is called the *standard matrix of the linear map* of T.

Examples.

1. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be given by

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x+3y \\ 3x+5y \end{pmatrix}.$$

The columns of A are $T\boldsymbol{e}_1 = T\binom{1}{0} = \binom{2}{3}$ and $T\boldsymbol{e}_2 = T\binom{0}{1} = \binom{3}{5}$. Hence the standard matrix of T is

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}.$$

2. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be the reflection in the line $y = x$. Since $\boldsymbol{c}_1 = T\boldsymbol{e}_1 = T\binom{1}{0} = \binom{0}{1}$ and $\boldsymbol{c}_2 = T\binom{0}{1} = \binom{1}{0}$, so $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This gives

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

General Case.

To prepare for the general case, let $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m\}$ be the standard basis of $\mathbb{R}^m$. The standard matrix A of $T : \mathbb{R}^n \to \mathbb{R}^m$ should multiply the coordinate vectors of points in $\mathbb{R}^n$ relative to the standard basis of $\mathbb{R}^n$. In particular,

$$T(\boldsymbol{e}_j) = \boldsymbol{c}_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = a_{1j}\boldsymbol{f}_1 + \cdots + \alpha_{mj}\boldsymbol{f}_m.$$

Suppose now that V and W are vector spaces of dimensions n and m, with ordered bases $\mathcal{B}_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$, $\mathcal{B}_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$, respectively. Thus we can write vectors $\boldsymbol{v}$ in V and $\boldsymbol{w}$ in W with respect to $\mathcal{B}_V$ and $\mathcal{B}_W$ as column vectors

$$\boldsymbol{v} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad \boldsymbol{w} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

For a linear map $T : V \to W$, let

$$T(\boldsymbol{v}_j) = a_{1j}\boldsymbol{w}_1 + \cdots + a_{mj}\boldsymbol{w}_m. \tag{4.2}$$

Then $\boldsymbol{w} = T(\boldsymbol{v}) = A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, with $A = (a_{ij})$ given by (4.2)

Examples. Below, the bases are ordered the way their elements are written.

1. Let $V = P_4, W = P_3$. [Recall that P_n is the vector space of polynomials of degree less than n.] Let $\mathcal{B}_V = \{1, x, x^2, x^3\}, \mathcal{B}_W = \{1, x, x^2\}$ be the respective standard bases. Now let $T = \frac{d}{dx} : V \to W$ be the differential operator which is linear. To compute its matrix, we write

$$\begin{aligned} T(1) &= 0 = 01 + 0x + 0x^2, \\ T(x) &= 1 = 11 + 0x + 0x^2, \\ T(x^2) &= 2x = 01 + 2x + 0x^2, \\ T(x^3) &= 3x^2 = 01 + 0x + 3x^2. \end{aligned}$$

Hence the matrix of T relative to $\mathcal{B}_V$ and $\mathcal{B}_W$ is

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

2. Now suppose $T : V \to W$ is as in Example 1, but $\mathcal{B}_V = \{1 + x, 1 - x, x^2 + x^3, x^2 - x^3\}$ and $\mathcal{B}_W = \{1, x, x^2\}$. Applying T to the basis vector in $\mathcal{B}$, we get

$$\begin{aligned} T(1 + x) &= 1 = 1 \cdot 1 + 0x + 0x^2 \\ T(1 - x) &= -1 = (-1)1 + 0x + 0x^2 \\ T(x^2 + x^3) &= 2x + 3x^2 = 0 \cdot 1 + 2x + 3x^2 \\ T(x^2 - x^3) &= 2x - 3x^2 = 0 \cdot 1 + 2x - 3x^2. \end{aligned}$$

Hence the matrix of T relative to the new bases $\mathcal{B}_V$ and $\mathcal{B}_W$ is

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

3. Let $V = W = \mathbb{R}^n$ and $p_j : V \to W$ be the projection onto the j-th coordinate axis, i.e. $p_j(x_1, \ldots, x_n) = (0, \ldots, x_j, \ldots 0)$. Again we take $\mathcal{B}_V = \mathcal{B}_W$ to be the standard basis. The standard matrix of the linear transformation p_j is the $n \times n$ matrix E_{jj} with 1 at the (j, j)-th place and zero elsewhere.

4. Regard $V = W = \mathbb{C}$ as a vector space over $\mathbb{R}$ with bases $\mathcal{B}_V = \mathcal{B}_W = \{1, i\}$. Let $\kappa : V \to W$ be the conjugation map $\kappa(a + ib) = a - ib$. The matrix of κ relative to $\mathcal{B}_V$ and $\mathcal{B}_W$ is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

EXERCISES

All the bases below are ordered in the way their elements are written.

In problems 1–4 find the standard matrix of a given linear transformation T.

1. $T : \mathbb{R}^2 \to \mathbb{R}^2$ is a vertical shear that maps $\boldsymbol{e}_1$ to $\boldsymbol{e}_1 - 2\boldsymbol{e}_2$ but leaves $\boldsymbol{e}_2$ unchanged.

2. $T : \mathbb{R}^2 \to \mathbb{R}^2$ is a horizontal shear that leaves $\boldsymbol{e}_1$ unchanged but maps $\boldsymbol{e}_2$ to $\boldsymbol{e}_2 + 2\boldsymbol{e}_1$.

3. $T : \mathbb{R}^2 \to \mathbb{R}^2$ rotates points about the origin through θ radians, counterclockwise.

4. $T : \mathbb{R}^2 \to \mathbb{R}^2$ reflects points first in x-axis and then in the line $y = x$.

5. What is the angle of rotation if $T : \mathbb{R}^2 \to \mathbb{R}^2$ that reflects points first through x-axis and then through y-axis? Write its matrix relative to the standard bases of $\mathbb{R}^2$.

6. Let $\mathcal{B}_1 = \left\{\binom{2}{1}, \binom{1}{2}\right\}$ and $\mathcal{B}_2 = \left\{\binom{1}{1}, \binom{1}{-1}\right\}$ be two bases of $V = W = \mathbb{R}^2$. Suppose $T : V \to W$ be the linear transformation given by $T(x, y) = (3x + 4y, 4x + 5y)$. Find the matrix of T relative to $\mathcal{B}_V = \mathcal{B}_i, \mathcal{B}_W = \mathcal{B}_j$ for all choices of $i, j = 1, 2$, i.e. relative to i) $\mathcal{B}_1, \mathcal{B}_1$, ii) $\mathcal{B}_1, \mathcal{B}_2$, iii) $\mathcal{B}_2, \mathcal{B}_1$, iv) $\mathcal{B}_2, \mathcal{B}_2$.

7. Let $V = W = M(2, \mathbb{R})$. Recall that
$$\mathcal{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$
is the standard basis of $M(2, \mathbb{R})$. Find the standard matrix of the linear map $T : V \to W$ given by $T(A) = A^*$ (the transpose of A).

8. Let $V = W$ be the subspace of $C^\infty(\mathbb{R})$ spanned by $\cos x$ and $\sin x$. Let $D : V \to W$ be the linear operator $D = \frac{d}{dx}$. Find the matrix of D relative to $\mathcal{B}_V = \mathcal{B}_W = \{\cos x, \sin x\}$.

9. Compute the matrix of the linear map $T : P_3 \to \mathbb{R}^3$, given by $T(f(x)) = \left(\int\limits_0^1 f(x)dx, f(0), f(1) \right)$, relative to their standard bases.

4.4 Matrix Algebra and Algebra of Linear Maps

Suppose K is a field and V, W are vector spaces over K of dimensions at least one. A linear transformation $T : V \to W$ is also called a *homomorphism* from V to W over K. The set of all homomorphisms $T : V \to W$ over K is denoted by $\mathrm{Hom}_K(V, W)$, or simply by $\mathrm{Hom}(V, W)$ if K is clear from the context. If $T, T_1, T_2 \in \mathrm{Hom}(V, W)$ and $c \in K$, we define the maps $T_1 + T_2, cT : V \to W$ by $(T_1 + T_2)(\boldsymbol{v}) = T_1(\boldsymbol{v}) + T_2(\boldsymbol{v})$ and $(cT)(\boldsymbol{v}) = cT(\boldsymbol{v})$.

Theorem 4.10. *With the addition and scalar multiplication, defined above, the set* $\mathrm{Hom}(V, W)$ *is a vector space over* K.

Proof. All one needs to do is to verify the axioms in the definition of the vector space. We will verify three of them (#1, #2, and #5) and leave the rest as an exercise.

1. Let T_1, $T_2 \in \mathrm{Hom}(V, W)$. For $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ in V,

$$\begin{aligned}(T_1 + T_2)(\boldsymbol{v}_1 + \boldsymbol{v}_2) &= T_1(\boldsymbol{v}_1 + \boldsymbol{v}_2) + T_2(\boldsymbol{v}_1 + \boldsymbol{v}_2)\\ &= T_1(\boldsymbol{v}_1) + T_1(\boldsymbol{v}_2) + T_2(\boldsymbol{v}_1) + T_2(\boldsymbol{v}_2)\\ &= (T_1(\boldsymbol{v}_1) + T_2(\boldsymbol{v}_1)) + (T_1(\boldsymbol{v}_2) + T_2(\boldsymbol{v}_2))\\ &= (T_1 + T_2)(\boldsymbol{v}_1) + (T_1 + T_2)(\boldsymbol{v}_2).\end{aligned}$$

   Hence $T_1 + T_2$ is also in $\mathrm{Hom}(V, W)$.

2. If $T \in \mathrm{Hom}(V, W)$ and a, $c \in K$, then for $\boldsymbol{u}$ in V,

$$(aT)(c\boldsymbol{v}) = aT(c\boldsymbol{v}) = acT(\boldsymbol{v}) = c(aT(\boldsymbol{v})).$$

   Hence aT is in $\mathrm{Hom}(V, W)$.

5. The linear map $0 : V \to W$ defined by $0(\boldsymbol{v}) = \mathbf{0}$ for all $\boldsymbol{v}$ in V is the Θ vector of $\mathrm{Hom}(V, W)$.

□

Theorem 4.11. *Suppose* V *and* W *are finite dimensional vector spaces over* K *of dimensions* n *and* m*, respectively. As a vector space over* K*,* $\mathrm{Hom}(V, W) \cong M(m \times n, K)$.

Proof. Choose ordered bases $\mathcal{B}_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of V and $\mathcal{B}_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ of W. Now Suppose that $T : V \to W$ is linear. Write the vector

$$T(\boldsymbol{v}_j) = \sum_{i=1}^{m} a_{ij}\boldsymbol{w}_i, \tag{4.3}$$

as a unique linear combination of the basis vectors in $\mathcal{B}_W$. Denote the $m \times n$ matrix (a_{ij}) by $\tau(T)$. This defines a map $\tau : \mathrm{Hom}(V, W) \to M(m \times n, K)$. We show that τ is a bijective linear map. It is trivial to check that τ is a linear transformation. It is also obvious that $\mathrm{Ker}(\tau) = \{0\}$, where 0 is the linear transformation from V to W which is identically zero. Hence τ is injective. In particular,

$$\dim \mathrm{Hom}(V, W) \leq mn = \dim M(m \times n, K). \tag{4.4}$$

Now define mn linear transformations $T_{ij} : V \to W$ ($i = 1, \ldots, m$; $j = 1, \ldots, n$) by $T_{ij}(\boldsymbol{v}_r) = \delta_{rj}\boldsymbol{w}_i$, where δ_{rj} are the Kronecker deltas

$$\delta_{rj} = \begin{cases} 1 & \text{if } r = j \\ 0 & \text{if } r \neq j \end{cases}$$

and extend them to V by linearity. We leave it as an exercise to check that T_{ij} are linearly independent. Hence,

$$\dim \mathrm{Hom}(V, W) \geq mn. \tag{4.5}$$

From (4.4) and (4.5), $\dim \mathrm{Hom}(V, W) = \dim M(m \times n, K)$. Hence, by Theorem 4.9, τ is also bijective. □

Theorem 4.12. *Suppose U, V, W are vector spaces over K and $T_1 : U \to V$, $T_2 : V \to W$ are linear maps. Then the composite map $T_2 \circ T_1 : U \to W$ is a linear transformation.*

Proof. If $c_1, c_2 \in K$ and $\boldsymbol{u}_1, \boldsymbol{u}_2 \in U$, then

$$\begin{aligned}(T_2 \circ T_1)(c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2) &= T_2(T_1(c_1\boldsymbol{u}_1 + c_2\boldsymbol{u}_2)) \\ &= T_2(c_1T_1(\boldsymbol{u}_1) + c_2T_1(\boldsymbol{u}_2)) \\ &= c_1T_2(T_1(\boldsymbol{u}_1)) + c_2T_2(T_1(\boldsymbol{u}_2)) \\ &= c_1(T_2 \circ T_1)(\boldsymbol{u}_1) + c_2(T_2 \circ T_1)(\boldsymbol{u}_2).\end{aligned}$$ □

The linear map $\tau : \mathrm{Hom}(V, W) \to M(m \times n, K)$, in the proof of Theorem 4.11, depends obviously on the ordered bases $\mathcal{B}_V$ and $\mathcal{B}_W$. Therefore, a better notation, especially for stating the theorem below, is $\tau = \tau_{\mathcal{B}_V, \mathcal{B}_W}$

Theorem 4.13. *Suppose V, W, and X are finite dimensional vector spaces over a field K, with given ordered bases $\mathcal{B}_V$, $\mathcal{B}_W$ and $\mathcal{B}_X$, respectively. Suppose $T_1 \in \mathrm{Hom}(V, W)$ and $T_2 \in \mathrm{Hom}(W, X)$. Then*

$$\tau_{\mathcal{B}_V, \mathcal{B}_X}(T_2 \circ T_1) = \tau_{\mathcal{B}_W, \mathcal{B}_X}(T_2)\tau_{\mathcal{B}_V, \mathcal{B}_W}(T_1).$$

Remark. The theorem says that under the identification of linear maps with matrices, the composition of linear transformations corresponds to matrix multiplication. Since the composition of maps is associative, so is the matrix multiplication.

Proof. Suppose $\dim V = n, \dim W = r, \dim X = m$ and $\mathcal{B}_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$, $\mathcal{B}_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$, $\mathcal{B}_X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$. Let $\tau(T_1) = A = (a_{ij})$ in $M(r \times n, K)$, $\tau(T_2) = B = (b_{ij})$ in $M(m \times r, K)$. To find the (ij)-th entry of the $m \times n$ matrix $\tau(T_2 \circ T_1)$, we express $(T_2 \circ T_1)(\boldsymbol{v}_j)$ as a linear combination of the vectors in the ordered basis $\mathcal{B}_X$.

$$\begin{aligned}(T_2 \circ T_1)(\boldsymbol{v}_j) = T_2(T_1(\boldsymbol{v}_j)) &= T_2\left(\sum_{k=1}^{r} a_{kj}\boldsymbol{w}_k\right)\\ &= \sum_{k=1}^{r} a_{kj} T_2(\boldsymbol{w}_k)\\ &= \sum_{k=1}^{r} a_{kj} \sum_{i=1}^{m} b_{ik}\boldsymbol{x}_i\\ &= \sum_{i=1}^{m} \sum_{k=1}^{r} b_{ik}a_{kj}\boldsymbol{x}_i.\end{aligned}$$

Hence $\tau(T_2 \circ T_1) = \left(\sum\limits_{k=1}^{r} b_{ik}a_{kj}\right) = BA.$ □

Remark. It is not possible, in general, to multiply vectors. However, sometimes, it is. Suppose $\mathcal{A}$ is a vector space over a field k, which also comes with multiplication, that is, a map $\mu : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$, called the *multiplication*. We denote the *product* $\mu(A, B)$ of A and B simply by AB. We say that $\mathcal{A}$ is an (associative) *algebra over k* if the multiplication is compatible with the vector space operations, that is, if for all A, B, C in $\mathcal{A}$ and a, b in k,

1. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$ (distributive law),
2. $(AB)C = A(BC)$ (associative law),
3. $a(AB) = (aA)B = A(aB)$.

We also require $\mathcal{A}$ to have an element I called the *identity*, such that for all A in $\mathcal{A}$, $AI = IA = A$ and identify the scalars with elements of $\mathcal{A}$ via $a \to aI$.

An algebra $\mathcal{A}$ over k is *commutative* if $AB = BA$ for all A, B in $\mathcal{A}$.

Some examples of algebras are:

1. $k[x]$ is a commutative algebra over k,

2. if k is a subfield of K, then K is also a commutative algebra over k,

3. $M(n, K)$ is a non-commutative algebra over K,

4. if V is a vector space over K, $\dim_K(V) \geq 2$ then $\mathrm{Hom}_K(V, V)$, with $\mu(T_1, T_2) = T_1 \circ T_2$, is an algebra over K, which is also non-commutative.

If $\mathcal{A}$ and $\mathcal{B}$ are algebras over K, we say that, as an algebra, $\mathcal{A}$ is *isomorphic* to $\mathcal{B}$ if there is a bijective linear map $\tau : \mathcal{A} \to \mathcal{B}$ such that for all A, B in $\mathcal{A}$, $\tau(AB) = \tau(A)\tau(B)$ and $\tau(I) = I$. In this section, we have proved the following fact.

Theorem 4.14. *If V is a finite dimensional vector space over K with $\dim_K(V) = n$, then as an algebra, $\mathrm{Hom}_K(V, V)$ is isomorphic to $M(n, K)$.*

EXERCISE

Show that the linear maps T_{ij}, defined in the proof of Theorem 4.11, are linearly independent.

4.5 Linear Functionals and Duality

If V and W are vector spaces of dimension n and m respectively, over a field K, then $\mathrm{Hom}_K(V, W) \cong M(m \times n, K)$. In particular, when K is considered as a vector space over itself, then $\mathrm{Hom}_K(V, K) \cong M(1 \times n, K) \cong K^n$. The elements of $\mathrm{Hom}_K(V, K)$ are called *linear functionals*. The vector space $\mathrm{Hom}_K(V, K)$ is usually denoted by V^*, and is called the *dual* of V. The dual $V^* \cong K^n \cong V$.

Suppose $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis of V. A linear transformation $T : V \to W$ is uniquely determined by its values $T(\boldsymbol{v}_j), j = 1, \ldots, n$ of the basis vectors. The n linear functionals $T_1, \ldots, T_n : V \to K$ defined by

$$T_i(\boldsymbol{v}_j) = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j. \end{cases}$$

form a basis of V^*, called the *dual of the basis $\mathcal{B}$*.

4.6 Equivalence and Similarity

The matrix of a linear transformation $T : V \to W$, where V and W are finite dimensional vector spaces, is always relative to a pair of ordered bases $\mathcal{B}_V$ and $\mathcal{B}_W$. In this section, we shall see what happens to this matrix when $\mathcal{B}_V$ and $\mathcal{B}_W$ are replaced by another pair of ordered bases of V and W, respectively.

Suppose $V \cong K^n$ and $W \cong K^m$ $(m, n \geq 1)$ are finite dimensional vector spaces over K with ordered bases $\mathcal{B}_V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ and $\mathcal{B}_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$, respectively. Thus vectors in V and W are to be considered as column vectors. Let $T : V \to W$ be a linear map and $A = \tau_{\mathcal{B}_V, \mathcal{B}_W}(T)$ be the matrix of T relative to $\mathcal{B}_V$ and $\mathcal{B}_W$ (see Section 4.4). Now suppose we are given another pair $\mathcal{B}'_V = \{\boldsymbol{v}'_1, \ldots, \boldsymbol{v}'_n\}$ and $\mathcal{B}'_W = \{\boldsymbol{w}'_1, \ldots, \boldsymbol{w}'_m\}$ of ordered bases of V and W. How are the matrices $A = \tau_{\mathcal{B}_V, \mathcal{B}_W}(T)$ and $B = \tau_{\mathcal{B}'_V, \mathcal{B}'_W}(T)$ related?

To answer this question, write

$$\boldsymbol{v}'_j = \sum_{i=1}^{n} p_{ij} \boldsymbol{v}_i, \ \ \boldsymbol{w}'_j = \sum_{i=1}^{m} q_{ij} \boldsymbol{w}_i.$$

Then $P = (p_{ij})$ and $Q = (q_{ij})$ are invertible matrices of order n and m, respectively. The matrices P and Q are called the *transition matrices*. Suppose $L_P : V \to V$ is the linear map corresponding to the multiplication by P on the left, when V is identified with vector space K^n of column vectors, whose coordinates are the components of vectors in V along $\boldsymbol{v}_j$. Similarly L_Q. Then by Theorem 4.13,

$$B = \tau_{\mathcal{B}'_V, \mathcal{B}'_W}(T) = \tau_{\mathcal{B}_W, \mathcal{B}'_W}(L_Q) \cdot \tau_{\mathcal{B}_V, \mathcal{B}_W}(T) \cdot \tau_{\mathcal{B}'_V, \mathcal{B}_V}(L_P) = QAP^{-1}.$$

To summarize, it is convenient to introduce the following terminology.

Definition. Suppose $A, B \in M(m \times n, K)$. We say that A is *equivalent* to B (over K), if there are invertible matrices P in $M(n, K)$ and Q in $M(m, K)$, such that $B = QAP^{-1}$. In particular, A and B are *similar* if $m = n$ and $P = Q$.

Now the effect of change of bases can be summarized as follows.

Theorem 4.15. *Suppose A is the matrix of a linear map T relative to a pair of ordered bases of V and W and B is the matrix of T relative to another pair of ordered bases of V and W. Then A and B are equivalent. In particular, if A and B are the matrices of $T : V \to V$ with respect to different bases of V, then A and B are similar.*

Remark. First note that P, Q are nothing but transition matrices from $\mathcal{B}_V$ to $\mathcal{B}'_V$ and $\mathcal{B}_W$ to $\mathcal{B}'_W$, respectively (Section 3.6).

Examples.

1. Suppose $V = W = \mathbb{R}^2, \mathcal{B}_V = \mathcal{B}_W = \{\boldsymbol{e}_1, \boldsymbol{e}_2\}, \mathcal{B}'_V = \left\{\binom{1}{2}, \binom{2}{1}\right\}$ and $\mathcal{B}'_W = \mathcal{B}_W$. To find the transition matrix P, we write

$$\boldsymbol{v}'_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 1\boldsymbol{e}_1 + 2\boldsymbol{e}_2$$

$$\boldsymbol{v}'_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2\boldsymbol{e}_1 + 1\boldsymbol{e}_2.$$

Hence, $P = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Thus $B = IAP^{-1} = AP^{-1}$.

2. Suppose $V = P_3$, $W = P_2$. Let the linear map be the derivation $D = \frac{d}{dx} : V \to W$. We take the first pair of ordered bases to be the standard ones, $\mathcal{B}_V = \{1, x, x^2\}$, $\mathcal{B}_W = \{1, x\}$. Let the new pair be $\mathcal{B}'_V = \{1, x + x^2, x - x^2\}$ and $\mathcal{B}'_W = \{1 + x, 1 - x\}$. Then it is easy to see that $P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$ and $Q = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. If we put $\tau_{\mathcal{B}_V, \mathcal{B}_W}(D) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} = A$, then $B = \tau_{\mathcal{B}'_V, \mathcal{B}'_W}(D) = QAP^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} 0 & \frac{3}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{2} & \frac{3}{2} \end{pmatrix}$.

EXERCISES

1. For $V = \mathbb{R}^2$, find the transition matrix P if

   (a) $\mathcal{B}_V = \left\{\binom{1}{2}\ \binom{2}{1}\right\}, \mathcal{B}_{V'} = \left\{\binom{1}{1}, \binom{1}{-1}\right\}$,

   (b) $\mathcal{B}_V = \left\{\binom{3}{-4}, \binom{1}{-1}\right\}, \mathcal{B}_{V'} = \left\{\binom{5}{7}, \binom{3}{2}\right\}$.

2. For $V = P_3$, find the transition matrix P, if $\mathcal{B}_V = \{1 + x, 1 - x, x^2\}, \mathcal{B}_{V'} = \{1, x + x^2, x - x^2\}$.

3. (a) Find the matrix A of the derivation $D = \frac{d}{dx} : P_4 \to P_3$ relative to the standard bases $\{1, x, x^2, x^3\}$ and $\{1, x, x^2\}$ of P_4 and P_3 respectively.

   (b) Find the matrix B of D in (a) relative to the pair $\mathcal{B}'_V = \{1 + x, 1 - x, x^2 + x^3, x^2 - x^3\}$ and $\mathcal{B}'_W = \{1, 1 + x, 1 + x^2\}$ of bases of $V = P_4$ and $W = P_3$, respectively.

(c) Find the matrices P and Q relative to the old and new bases of V and W, as in (a) and (b) respectively.

(d) Check that the matrices B, A, and P, Q obtained in (a), (b), and (c) satisfy $B = QAP^{-1}$.

4.7† Application to Higher Order Differential Equations

To solve the higher order differential equation (3.4), equivalently to find a basis of the kernel of the linear map L below, we first explain our notation. If we put $D = \frac{d}{dx}$, then $D^2 = \frac{d}{dx}\left(\frac{d}{dx}\right) = \frac{d^2}{dx^2}$, so $D^j = D(D^{j-1}) = \frac{d^j}{dx^j}$. Thus we can write the linear operator

$$\begin{aligned} L &= \frac{d^n}{dx^n} + a_{n-1}\frac{d^{n-1}}{dx^{n-1}} + \cdots + a_1\frac{d}{dx} + a_0 \\ &= D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0 \\ &= f(D) \end{aligned}$$

as a polynomial of degree n in D. The polynomial $f(D)$ is the *characteristic polynomial* of the differential equation (3.4), which now can be written as

$$L(y) = 0.$$

Clearly the solution set of (3.4) is $\operatorname{Ker}(L)$, which is a vector space. Its dimension is equal to the order of (3.4) (for proof see a book on differential equations) which is the same as $\deg f(D)$.

Theorem 4.16. *If L is the operator $f(D) = D^n + a_{n-1}D^{n-1} + \cdots + a_1 D + a_0$, $\dim \operatorname{Ker}(L) = n$.*

By this theorem, a general solution of (3.4) is $y = c_1y_1 + \cdots + c_ny_n$ if we can find a basis $\{y_1, \ldots, y_n\}$ for $\operatorname{Ker}(L)$.

We know that a polynomial of degree n has precisely n roots, counted with multiplicity. The following algorithm provides a basis $y_1, \ldots, y_n$ for $\operatorname{Ker}(L)$.

Theorem 4.17. *If α is a root of multiplicity r of the characteristic polynomial $f(D)$ of $L(y) = 0$, it contributes r linearly independent solutions $e^{\alpha x}, xe^{\alpha x}, \ldots, x^{r-1}e^{\alpha x}$. The solutions contributed by distinct roots of $f(D)$, taken together, form a basis of $\operatorname{Ker}(L)$.*

Proof. The proof can be found in most books on differential equations. Assuming $\dim \operatorname{Ker}(L) = n$, we sketch it when all the roots $\alpha = \alpha_1, \ldots, \alpha_n$ are real and distinct. If $y = e^{\alpha x}$, then

$$\frac{d^n y}{dx^n} + a_{n-1}\frac{d^{n-1}y}{dx^{n-1}} + \cdots + a_1\frac{dy}{dx} + a_0 y = f(D)y.$$

But $D^j y = \frac{d^j}{dx^j}e^{\alpha x} = \alpha^j e^{\alpha x}$, so $f(D)y = f(\alpha)e^{\alpha x} = 0$, since α is a root of $f(D)$. It can be checked by Theorem 3.8 that $e^{\alpha_1 x}, \ldots, e^{\alpha_n x}$ are linearly independent. □

Remarks.

1. A basis for Ker(L) is called a set of *fundamental solutions* of $Ly = 0$.

2. The imaginary roots of a polynomial with real coefficients occur in pairs of complex conjugates $\alpha = a + ib$, $\bar{\alpha} = a - ib$. By "Euler's identity," which in fact is the definition of *complex exponentiation*,

$$e^{\alpha x} = e^{ax+ibx} = e^{ax}(\cos bx + i\sin bx)$$

$$e^{\bar{\alpha}x} = e^{ax-ibx} = e^{ax}(\cos bx - i\sin bx).$$

This shows that span$\{e^{\alpha x}, e^{\bar{\alpha}x}\}$ = span$\{e^{ax}\cos bx, e^{ax}\sin bx\}$. Therefore in the set of fundamental solutions of $Ly = 0$ given by Theorem 4.17, the pair $\{e^{\alpha x}, x^{\bar{\alpha}x}\}$ may be replaced by $\{e^{ax}\cos bx, e^{ax}\sin bx\}$.

Examples.

1. For a general solution of

$$y'' - 5y' + 6y = 0,$$

its characteristic polynomial $f(D) = D^2 - 5D + 6 = (D-2)(D-3)$ with two real and distinct roots $\alpha = 2, 3$. Hence a general solution of this linear differential equation of order two is $y = c_1e^{2x} + c_2e^{3x}$.

2. $y'' - 4y' + 4y = 0$.

Now $f(D) = D^2 - 4D + 4 = (D-2)^2$, with one real root $D = 2$ of multiplicity two. Hence a general solution of this differential equation is $y = c_1e^{2x} + c_2xe^{2x}$.

3. $y''' - y = 0$.

Now $f(D) = D^3 - 1 = (D-1)(D^2 + D + 1)$ has one real root $D = 1$ and a pair of imaginary roots $\alpha, \bar{\alpha} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Hence a general solution $y = c_1e^x + c_2e^{-x/2}\cos\frac{\sqrt{3}}{2}x + c_3e^{-x/2}\sin\frac{\sqrt{3}}{2}x$.

EXERCISES

Find a general solution of the following linear differential equations:

1. $y'' - 3y' + 2y = 0$
2. $y'' - 6y' + 9y = 0$
3. $y'''' - y = 0$

5

Determinants

5.1 Motivation

Given a linear map $T : V \to V$, how can one check if it is invertible? When $\dim(V) < \infty$, we can, and from now on will, identify T with its matrix. To each square matrix A, we associate a scalar $\det(A)$ or $|A|$ and show that T is invertible if and only if $\det(A) \neq 0$, A being its matrix.

There are many ways to compute $\det(A)$. But before computing it we have to say what it is. The most familiar definition leaves one wondering from where it came. For example, when the determinant $\det(A)$ of a 2×2 matrix

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

is defined by $\det(A) = ad - bc$, one should ask: why not $= a + b + c + d$ or $= ab + cd$? The following discussion is supposed to answer this question. Those willing to accept the computational definition of $\det(A)$ may skip the first three sections and proceed directly to Section 5.4. But then proving some of the properties of $\det(A)$ are rather messy and will be left as exercises.

The area of the parallelogram formed by the vectors $\boldsymbol{u} = (a, b)$, $\boldsymbol{v} = (c, d)$ in the Euclidean plane $\mathbb{R}^2$ is the absolute value of $ad - bc$. [See Exercise 9, Section 7.1.] Thus $\boldsymbol{u}$, $\boldsymbol{v}$ form a basis of $\mathbb{R}^2$ (See Figure 5.1) if and only if this area is nonzero, i.e. $\det(A) \neq 0$. Similarly (see Exercises 10 and 11 in Section 7.1) three vectors, $\boldsymbol{u}, \boldsymbol{v}$ and $\boldsymbol{w}$ in $\mathbb{R}^3$ form its basis if and only if the volume of the parallelepiped they form is nonzero. We cannot make these statements for the vector space K^n $(n = 2, 3)$ if K is not a subfield of $\mathbb{R}$. For example, the terms "parallelogram" and "area" are meaningless for vectors in $V = K^2$, if K is a finite field. Therefore, we should look for an equivalent formulation of these statements about the bases, which makes sense for any field K of scalars.

We begin with some defining properties of areas of parallelograms in $\mathbb{R}^2$ and of volumes of parallelepipeds in $\mathbb{R}^3$, which do not use the special nature of $\mathbb{R}$, but depend only on the axioms which make $\mathbb{R}$ into a field.

We discuss only the areas of parallelograms. The corresponding facts about the volumes of parallelepipeds in $\mathbb{R}^3$ are similar. After fixing an orientation, let $f(\boldsymbol{u}, \boldsymbol{v})$ denote the area, with appropriate sign, of the oriented parallelogram formed by the ordered set $\{\boldsymbol{u}, \boldsymbol{v}\}$ in $V = \mathbb{R}^2$.

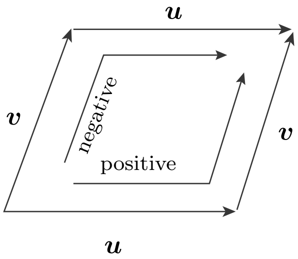


FIGURE 5.1: Orientation of a parallelogram

By this we mean, as Figure 5.1 suggests, that $f(\boldsymbol{u}, \boldsymbol{v}) = -f(\boldsymbol{v}, \boldsymbol{u})$. This function $f : V \times V \to \mathbb{R}$ has the following obvious properties (only part (a) of 1) is a little exercise in geometry);

1) It is *multilinear*, that is, it is linear in each variable. For example, the linearity in the first variable means that

    (a) $f(\boldsymbol{u}_1 + \boldsymbol{u}_2, \boldsymbol{v}) = f(\boldsymbol{u}_1, \boldsymbol{v}) + f(\boldsymbol{u}_2, \boldsymbol{v})$,

    (b) $f(c\boldsymbol{u}, \boldsymbol{v}) = cf(\boldsymbol{u}, \boldsymbol{v})$ for c in $\mathbb{R}$.

2) It is *alternating*, that is $f(\boldsymbol{u}, \boldsymbol{v}) = -f(\boldsymbol{v}, \boldsymbol{u})$.

3) If $\boldsymbol{e}_1 = (1, 0)$, $\boldsymbol{e}_2 = (0, 1)$, then $f(\boldsymbol{e}_1, \boldsymbol{e}_2) = 1$.

It will follow that if $g : V \times V \to \mathbb{R}$ is another function with these three properties, then $g = f$.

This suggests that in the general case of $V = K^n$, where $n > 1$ is any integer and K is a field, we should look for a function $\delta : V^n \to K$, such that it has these properties, and a set $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is a basis of K^n if and only if $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \neq 0$. The following definition of determinant does this. Moreover, most of its properties follow at once from this definition, both algebraically and whenever applicable also geometrically. The discussion of permutations follows right after the definition and remarks.

Definition. Suppose $n \geq 1$, K is a field and $V = K^n$. A function $\delta : V^n \to K$ is called a *determinant function* on V^n if it has the following three properties:

(D-1) δ is *multilinear*, that is, it is linear in each variable.

(D-2) δ is *alternating*, that is, $\delta(\boldsymbol{v}_{\sigma(1)}, \ldots, \boldsymbol{v}_{\sigma(n)}) = -\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$, if σ is a permutation of indices, which switches two indices $i, j (i \neq j)$ and leaves all other fixed.

(D-3) If $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is the standard basis of K^n, then $\delta(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = 1$.

We shall show that such a function exists, and is unique. More importantly, a set $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ of n vectors in V is a basis of V, if and only if $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \neq 0$. Furthermore, if we identify V^n with $M(n, K)$, where the i-th coordinate of a point in V^n is the i-th row (or column) of the corresponding $n \times n$ matrix in $M(n, K)$, then δ is the well-known determinant function on matrices.

Remarks.

1. If $n = 1$, then as a vector space over K, $V^n \cong K$. In this case, by D-1 and D-3, the *determinant* of a 1×1 matrix (a) is clearly a.

2. In (D-2), we assume that K does not contain the field of two elements as a subfield. If that is the case, see the remark after Theorem 5.2.

Permutations

It is assumed that the reader is familiar with the basic properties of permutations. However, for his or her convenience we recall them briefly.

For $n \geq 1$, let X denote the set of n symbols, or indices $1, \ldots, n$. We shall denote the set of all maps $\mu : X \to X$ by X^X. An element σ of X^X is called a *permutation* on X, if it is bijective. A permutation τ is a *transposition* or a *switch* if there are two indices i, j in X with $i \neq j$, such that $\tau(i) = j$ and $\tau(j) = i$, but $\tau(k) = k$ for all other k in X. The set of all permutations is denoted by S_n. Whereas, X^X has n^n elements, its subset S_n has $n!$ elements.

It is well known that:

1) Every permutation σ is composed of transpositions, that is,

$$\sigma = \tau_1 \circ \cdots \circ \tau_r.$$

2) The number r of transpositions σ is composed of is not unique, but whether it is odd or even is uniquely determined by σ. The permutation σ is *odd* or *even*, according as this number r is odd or even. The *sign of a permutation* σ is defined by $\mathrm{sgn}(\sigma) = (-1)^r$.

A practical way to describe a permutation $\sigma : X \to X$ on the set $X = \{1, \ldots, n\}$ of n indices is to write it as

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

The first row of σ lists the elements $1, \ldots, n$ of X in the ascending order. The second row shows the reordering of these indices carried out by σ. Since σ is bijective, every index has to appear in the second row also. For example, if $n = 3$,

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

is the transposition switching 1 and 3. For $n = 5$,

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

is a so-called *cycle of order or length* three. It moves each index of the cycle, abbreviated as $\begin{pmatrix} 1 & 2 & 5 \\ 2 & 5 & 1 \end{pmatrix}$, of σ to the next one and brings the last one to the first. A transposition is a cycle of length two. Two cycles of σ are *disjoint cycles* if their top rows have no index in common. Clearly, every permutation is composed of disjoint cycles. It is easy to see that every cycle is composed of transpositions. For example,

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

This proves that every permutation is composed of transpositions. Note that the indices in the top row of a transposition, cycle or permutation are always in the ascending order, and that we compose maps from right to left.

5.2 Properties of Determinants

We shall identify V^n with $M(n, K)$ via rows and feel free to switch back and forth, whenever convenient. Often, we shall state the theorems for matrices, and give proofs considering determinants as functions from V^n to K. We could have identified the j-th coordinates of points of V^n with the j-th columns of matrices in $M(n, K)$. Hence, whatever we say about the rows is valid, word for word, for columns also. The determinant function (which we shall prove shortly exists and is unique) will be denoted by δ or det, according as it is regarded as a function on V^n or on $M(n, K)$. In this section we prove some of the properties of $\det(A)$. If your field K contains $\mathbb{F}_2$ as a subfield, see the remark below.

Theorem 5.1. *If a row of an $n \times n$ matrix A consists of zeros only, then* $\det(A) = 0$.

Proof. Suppose for example, $\boldsymbol{v}_1 = \mathbf{0}$. By multilinearity of δ in the first variable, $\delta(\mathbf{0}, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = \delta(0\mathbf{0}, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = 0\,\delta(\mathbf{0}, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = 0$. □

Theorem 5.2. *If two rows of an $n \times n$ matrix A are identical, then det*$(A) = 0$.

Proof. We need to show that if for two distinct indices i and j, $\boldsymbol{v}_i = \boldsymbol{v}_j$, then $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = 0$. Let τ be the transposition which switches i and j, $i \neq j$. By (D-2), $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \delta(\boldsymbol{v}_{\tau(1)}, \ldots, \boldsymbol{v}_{\tau(n)}) = -\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. This gives $2\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = 0$ or $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = 0$. □

Remark. If the field K contains the field of two elements as a subfield, we may not conclude from $2\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = 0$ that $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = 0$. In this case, one needs to replace (D-2) with the conclusion of Theorem 5.2.

Theorem 5.3. *If a row (or column) of a matrix is multiplied by a scalar c, its determinant gets multiplied by c.*

Proof. This is just a part of the multilinearity of δ. □

Theorem 5.4. *If a multiple of a row of an $n \times n$ matrix A is added to another row of A, the determinant is unchanged.*

Proof. If we add, for example, $c\boldsymbol{v}_2$ to $\boldsymbol{v}_1$,we need to show that $\delta(c\boldsymbol{v}_2 + \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) = \delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$. By linearity in the first variable,

$$\begin{aligned}\delta(c\boldsymbol{v}_2 + \boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n) &= \delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) + c\delta(\boldsymbol{v}_2, \boldsymbol{v}_2, \boldsymbol{v}_3, \ldots, \boldsymbol{v}_n) \\ &= \delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n),\end{aligned}$$

by Theorem 5.2. □

Theorem 5.5. *If two rows of an $n \times n$ matrix A over K are interchanged, the determinant changes sign.*

Proof. This is nothing but the defining property (D-2) of the determinant function. □

5.3 Existence and Uniqueness of Determinant

Recall that $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is the standard basis of $V = K^n$ and X is the set of n symbols or indices $i = 1, \ldots, n$.

Theorem 5.6. *If δ exists and a function $\mu : X \to X$ is not injective, then $\delta(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)}) = 0$.*

Proof. Suppose $\mu(i) = \mu(j)$ for $i \neq j$. Then $\boldsymbol{e}_{\mu(i)} = \boldsymbol{e}_{\mu(j)}$. Now use Theorem 5.2. □

Theorem 5.7. *If $\delta_1, \delta_2 : V^n \to K$ are two determinant functions, then $\delta_1(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)}) = \delta_2(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)})$ for every map $\mu : X \to X$.*

Proof. If μ is not injective, both are zero by Theorem 5.6. So suppose μ is a permutation. Write $\mu = \tau_1 \circ \ldots \circ \tau_r$ as a product of r transpositions so that $\operatorname{sgn}(\mu) = (-1)^r$. By the defining properties (D-2) and (D-3), we have for $\delta = \delta_1$ and δ_2,

$$\begin{aligned} \delta(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)}) &= (-1)^r \delta(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_r) \\ &= (-1)^r. \end{aligned}$$

□

Theorem 5.8. *The determinant function $\delta : V^n \to K$ exists, and is unique.*

Proof. Uniqueness: Suppose $\delta_1, \delta_2 : V^n \to K$ are two determinant functions, we show that $\delta_1(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \delta_2(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ for every $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ in V^n.

Write each vector

$$\boldsymbol{v}_i = \sum_{j=1}^{n} a_{ij} \boldsymbol{e}_j$$

as a linear combination of the vectors in the standard basis of $V = K^n$. If $\delta = \delta_1$ or δ_2, it is an easy consequence of mutlilinearity that

$$\begin{aligned} \delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) &= \delta\left(\sum_{j=1}^{n} a_{1j} \boldsymbol{e}_j, \ldots, \sum_{j=1}^{n} a_{nj} \boldsymbol{e}_j \right) \\ &= \sum_{\mu \in X^X} a_{1\mu(1)} \ldots a_{n\mu(n)} \cdot \delta(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)}). \end{aligned}$$

If μ is not injective, by Theorem 5.2, $\delta(\boldsymbol{e}_{\mu(1)}, \ldots, \boldsymbol{e}_{\mu(n)}) = 0$. Hence, if you recall the definition of $\operatorname{sgn}(\sigma)$,

$$\begin{aligned} \delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \ldots a_{n\sigma(n)} \delta(\boldsymbol{e}_{\sigma(1)}, \ldots, \boldsymbol{e}_{\sigma(n)}) \\ &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \ldots a_{n\sigma(n)} \operatorname{sgn}(\sigma) \delta(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}, \end{aligned}$$

by (D-3). Hence,

$$\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}. \tag{5.1}$$

This is independent of δ. Hence $\delta_1 = \delta_2$.

Existence: The equation (5.1) explicitly defines the determinant function $\delta(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$, or $\det(A)$, where $\boldsymbol{v}_j$'s are the rows of A, having the desired properties. □

Example. Suppose $n = 2$. There are two permutations on the set X of two indices 1 and 2. These are the identity 1_X and the switch $\sigma(1) = 2, \sigma(2) = 1$. Moreover, sgn($1_X$)=1 and $\operatorname{sgn}(\sigma) = -1$. If $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ is a 2×2 matrix over K, formula (5.1) becomes

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

This justifies our earlier definition of the determinant of a 2×2 matrix

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

as $\det(A) = ad - bc$.

Corollary 5.9. *If $A \in M(2, \mathbb{R})$, the absolute value $|\det(A)|$ is the area of the parallelogram formed by the rows of A, considered as vectors in $\mathbb{R}^2$.*

Proof. The signed area $f(\boldsymbol{u}, \boldsymbol{v})$ satisfies the defining properties (D-1), (D-2), and (D-3) of the determinant function. Hence, by uniqueness $f = \det$. □

Similarly, we have the following fact, which was first proved by Cauchy.

Corollary 5.10. *If $A \in M(3, \mathbb{R})$, then $|\det(A)|$ is the volume of the parallelepiped formed by the rows of A, considered as vectors in $\mathbb{R}^3$.*

In general, for $n \geq 1$, the n-dimensional volume $\mathbb{R}^n$, taken with proper orientation, has properties (D-1), (D-2), and (D-3). Hence, we have the following result.

Theorem 5.11. *For $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ in $\mathbb{R}^n$, the absolute value of the determinant whose rows are $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is the n-dimensional volume of the parallepiped $\{a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n \mid 0 \leq a_j \leq 1\}$.*

Note. The *n-dimensional volume* of a *cube* $a_j \leq x_j \leq b_j$ in $\mathbb{R}^n$ is $(b_1 - a_1) \ldots (b_n - a_n)$. If $n = 1$, it is the length, if $n = 2$, it is the area, for $n = 3$ it is the volume, and so on.

We now prove a fundamental fact about the determinants.

Theorem 5.12. $\det(AB) = \det(A)\det(B)$.

Proof. The i-th row of the $n \times n$ matrix B is $\boldsymbol{e}_i B$. Hence,

$$\det(B) = \delta(\boldsymbol{e}_1 B, \dots, \boldsymbol{e}_n B). \tag{5.2}$$

Since the i-th row of A is $a_{i1}\boldsymbol{e}_1 + \dots + a_{in}\boldsymbol{e}_n$, the i-th row of AB is

$$(a_{i1}\boldsymbol{e}_1 + \dots + a_{in}\boldsymbol{e}_n)B = \sum_{j=1}^{n} a_{ij}\boldsymbol{e}_j B.$$

Hence,

$$\det(AB) = \delta\left(\sum_{j=1}^{n} a_{1j}\boldsymbol{e}_j B, \dots, \sum_{j=1}^{n} a_{nj}\boldsymbol{e}_j B\right).$$

If μ is not injective, $\delta(\boldsymbol{e}_{\mu(1)}B, \dots, \boldsymbol{e}_{\mu(n)}B) = 0$. Therefore, by the multilinearity of δ, this is

$$\begin{aligned}
&= \sum_{\mu \in X^X} a_{1\mu(1)} \dots a_{n\mu(n)} \delta(\boldsymbol{e}_{\mu(1)}B, \dots, \boldsymbol{e}_{\mu(n)}B) \\
&= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} \cdot \delta(\boldsymbol{e}_1 B, \dots, \boldsymbol{e}_n B) \\
&= \det(A)\det(B),
\end{aligned}$$

by equation (5.1). □

Corollary 5.13. *If an $n \times n$ matrix A is invertible, then* $\det(A) \neq 0$ *and* $\det(A^{-1}) = 1/\det(A)$.

Proof. If A is invertible, then $A^{-1}A = I$. By (D-3), $\det(I) = 1$. Hence $\det(A^{-1}A) = \det(A^{-1})\det(A) = 1$, which implies that $\det(A) \neq 0$ and $\det(A^{-1}) = 1/\det(A)$. □

Finally, we return to our starting point and record our discussion as follows:

Theorem 5.14. *Suppose K is a field, $n \geq 1$ and $V = K^n$. A set of n vectors $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ in V is a basis of V if and only if the determinant $\delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \neq 0$.*

Proof. If $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ are linearly dependent, then one of them, say

$$\boldsymbol{v}_1 = c_2\boldsymbol{v}_2 + \dots + c_n\boldsymbol{v}_n$$

is a linear combination of others. Therefore,

$$\begin{aligned}\delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) &= \delta\left(\sum_{j=2}^{n} c_j \boldsymbol{v}_j, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n\right)\\ &= \sum_{j=2}^{n} c_j \delta(\boldsymbol{v}_j, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n) = 0,\end{aligned}$$

because $\delta(\boldsymbol{v}_j, \boldsymbol{v}_2, \dots, \boldsymbol{v}_n) = 0$ for all $j = 2, \dots, n$. Conversely, suppose $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ are linearly independent. We can write

$$\boldsymbol{e}_i = \sum_{j=1}^{n} a_{ij} \boldsymbol{v}_j.$$

Hence,

$$\begin{aligned}1 &= \delta(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)\\ &= \delta\left(\sum_{j=1}^{n} a_{1j}\boldsymbol{v}_j, \dots, \sum_{j=1}^{n} a_{nj}\boldsymbol{v}_j\right)\\ &= \left(\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}\right)\delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n),\end{aligned}$$

which shows that $\delta(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) \neq 0$. □

Corollary 5.15. *A matrix is invertible, if and only if, its rows (columns) are linearly independent.*

Theorem 5.16. *For the transpose A^* of a matrix $A = (a_{ij})$, $\det(A^*) = \det(A)$.*

Proof. The (i, j)-th entry of A^* is the (j, i)-th entry of A. Hence

$$\det(A^*) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

If $i = \sigma^{-1}(j)$, then in the summation above, $a_{\sigma(i)i} = a_{j\sigma^{-1}(j)}$, so that

$$\det(A^*) = \sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}.$$

Now $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$, because if $\sigma = \tau_1 \circ \dots \circ \tau_r$, then $\sigma^{-1} = \tau_r^{-1} \circ \dots \circ \tau_1^{-1}$ (recall the definition of $\operatorname{sgn}(\sigma)$). Therefore,

$$\det(A^*) = \sum_{\sigma} \operatorname{sgn}(\sigma^{-1}) a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}.$$

But up to a rearrangement of terms, the sum on the right is the same as

$$\sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} = \det(A). \qquad \square$$

The following theorem allows one to compute the determinant of a matrix recursively as follows: For an $n \times n$ matrix $A = (a_{ij})$, let A_{ij} denote the matrix obtained from A by deleting its i-th row and j-th column. The determinant $\det(A_{ij})$ is called the (i, j)-th *minor* and $(-1)^{i+j} \det(A_{ij})$ is called the *cofactor* of a_{ij}. A systematic way to get hold on the $n!$ terms of (5.1), in n steps, is by the so-called *expansion of* $\det(A)$ *by i-th row or j-th column*. This is the essence of the following easy to prove theorem.

Theorem 5.17. *Let $A = (a_{ij})$ be an $n \times n$ matrix. Fix i $(1 \le i \le n)$ put*

$$\delta_i(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}). \tag{5.3}$$

Similarly, fix j $(1 \le j \le n)$ and put

$$\delta^j(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}). \tag{5.4}$$

Then δ_i, δ^j both satisfy (D-1), (D-2), and (D-3). Hence (by the uniqueness),

$$\det(A) = \delta_i(A) = \delta^j(A). \tag{5.5}$$

Remark. Equation (5.3) (resp. (5.4)) is the so-called expansion of $\det(A)$ by i-th row (resp. j-th column).

5.4 Computational Definition of Determinant

To summarize the discussion of the previous sections, we now give a computational definition of the determinant of an $n \times n$ matrix A (cf. Theorem 5.17).

Definition. For $n = 1$, $A = (a)$, $\det(A) = a$.

For $n = 2$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and we define $\det(A) = ad - bc$.

For $n > 2$, we define $\det(A)$ of an $n \times n$ matrix $A = (a_{ij})$ recursively as follows:

Let A_{ij} be the $(n-1)\times(n-1)$ matrix obtained from A by deleting its i-th row and j-th column. Then

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \tag{5.6}$$

the *expansion* of $\det(A)$ by its i-th row, or

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \tag{5.7}$$

the *expansion* of $\det(A)$ by its j-th column. Both are independent of the chosen row or column. We leave the proof of this fact as an exercise.

Example. Let

$$A = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

We expand $\det(A)$ by the first row of A.

$$\begin{aligned} &\det(A) = \\ &\quad a_1 \det\begin{pmatrix} b_2 & b_3 \\ c_2 & c_3 \end{pmatrix} - a_2 \det\begin{pmatrix} b_1 & b_3 \\ c_1 & c_3 \end{pmatrix} + a_3 \det\begin{pmatrix} b_1 & b_2 \\ c_1 & c_2 \end{pmatrix} \\ &= a_1(b_2c_3 - b_3c_2) + a_2(b_3c_1 - b_1c_3) + a_3(b_1c_2 - b_2c_1). \end{aligned}$$

Properties of det(A)

We now recall the important properties of the determinant function established in the previous sections. The computational proofs of these properties will be left as exercises, which could be messy if you skipped Section 5.1 through 5.3. Whatever we say about the rows is true for the columns as well.

1. If a row of A consists only of zeros, $\det(A) = 0$ (expand it by that row).
2. If a row of A is multiplied by a constant c, $\det(A)$ gets multiplied by c. (Again expand it by that row.)
3. If two rows of A are interchanged, $\det(A)$ changes sign.
4. If two rows of A are identical, $\det(A) = 0$.
5. If a multiple of a row of A is added to another row of A, $\det(A)$ remains unchanged.

6. The expansion of $\det(A)$ is independent of the choice of a row (or column).

7. If $A = \begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$, $\det(A) = a_{11} \dots a_{nn}$.

   Hint. Expand by the first column and use induction.

8. If B is row equivalent to an upper triangular matrix in 7 above, $\det(B) = a_{11} \dots a_{nn}$.

9. If $\det(A) \neq 0$, then A is invertible.

   Hint. If $\det A \neq 0$, each column of A must have a nonzero entry. Starting with the first column, use this fact first to inductively row reduce A to an upper triangular matrix with all diagonal entries nonzero. Then computing the inverse by row reduction (Section 2.4) shows that A^{-1} exists. For another proof, see Section 5.6.

10. $\det(AB) = \det(A)\det(B)$.

11. If A is invertible, then $\det(A) \neq 0$ and $\det(A^{-1}) = 1/\det(A)$.

12. $\det(A)$ is the same as that of its transpose A^*.

13. The determinant of an $n \times n$ matrix over $\mathbb{R}$ is nonzero if and only if the volume of the n-dimensional parallelepiped formed by its rows is nonzero. [The easiest proof is by using Theorem 5.8.]

The following theorem illustrates the importance of the determinant function. We leave its proof as an exercise.

Theorem 5.18. *Suppose A is an $n \times n$ matrix over K, $V = K^n$ and $T_A : V \to V$ is the corresponding linear transformation given by $T_A(\boldsymbol{x}) = A\boldsymbol{x}$. The following are equivalent.*

1) $\det(A) \neq 0$.

2) A is invertible.

3) The rows of A are linearly independent.

4) The columns of A are linearly independent.

5) $\operatorname{Ker}(T_A) = \{\mathbf{0}\}$.

6) T_A is injective.

7) T_A is surjective.

8) T_A is bijective.

Definition. A matrix satisfying any, and hence all, of the eight conditions of the theorem is called *non-singular*.

EXERCISES

1. For vectors $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$, the *dot product* $\boldsymbol{x} \cdot \boldsymbol{y}$ is the scalar

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n.$$

For two vectors $\boldsymbol{x} = (x_1, x_2, x_3)$, $\boldsymbol{y} = (y_1, y_2, y_3)$ in $\mathbb{R}^3$ (and $\mathbb{R}^3$ only), their *cross product* $\boldsymbol{x} \times \boldsymbol{y}$ is a vector again in $\mathbb{R}^3$ defined by

$$\boldsymbol{x} \times \boldsymbol{y} = (x_2 y_3 - x_3 y_2,\ x_3 y_1 - x_1 y_3,\ x_1 y_2 - x_2 y_1).$$

If $\boldsymbol{a} = (a_1, a_2, a_3)$, $\boldsymbol{b} = (b_1, b_2, b_3)$ and $\boldsymbol{c} = (c_1, c_2, c_3)$, show that $|\boldsymbol{a} \cdot (\boldsymbol{b} \times \boldsymbol{c})|$ is independent of the order in which $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ are taken by showing that for

$$A = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix},$$

$\det(A) = \boldsymbol{a} \cdot (\boldsymbol{b} \times \boldsymbol{c})$.

2. Use the computational definition of $\det(A)$ to prove its properties 3–13 in this section.

5.5 Evaluation of Determinants

The determinant $\det(A)$ of an $n \times n$ matrix $A = (a_{ij})$ is also denoted by

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \\ a_{n1} & \ldots & a_{nn} \end{vmatrix}.$$

The properties 1–12 of $\det(A)$, listed above, make it easy to compute it. Often, no calculation is necessary. For example, if a row of A consists of zeros, or a row is a multiple of another row, $\det(A) = 0$. (The same is true for columns.) If $n = 2$, one can use the definition itself: $\det(A) = a_{11}a_{22} - a_{12}a_{21}$. For $n = 3$, using a row or a column to expand $\det(A)$ is not unmanageable.

For $n \geq 3$, if a row or a column has a large number of zeros, we may use it to expand $\det(A)$, and then work on n determinants of smaller size. In general, we may row reduce A to an upper triangular form, from which we can determine its determinant.

Examples.

1. $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 5 & 7 \end{vmatrix} = 0$, because the rows are linearly dependent – the third row is the sum of the first two.

2. We expand the following determinant using the first row.

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = 1 \cdot \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 2 \cdot \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} + 3 \cdot \begin{vmatrix} 4 & 5 \\ 7 & 8 \end{vmatrix}$$

$= 1(5 \cdot 9 - 8 \cdot 6) - 2(4 \cdot 9 - 7 \cdot 6) + 3(4 \cdot 8 - 7 \cdot 5) = 0$

Let us now compute the same using the second column.

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = -2 \cdot \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} + 5 \cdot \begin{vmatrix} 1 & 3 \\ 7 & 9 \end{vmatrix} - 8 \cdot \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix}$$

$= -2 \cdot (4 \cdot 9 - 7 \cdot 6) + 5(1 \cdot 9 - 7 \cdot 3) - 8(1 \cdot 6 - 4 \cdot 3) = 0.$

3. Let

$$A = \begin{pmatrix} 2 & 4 & 6 \\ 12 & 15 & 18 \\ 28 & 32 & 36 \end{pmatrix}.$$

Taking out the multiples 2, 3 and 4 from the first, second and the third row, respectively,

$$\det(A) = 2 \cdot 3 \cdot 4 \cdot \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = 2 \cdot 3 \cdot 4 \cdot 0 = 0,$$

by Example 2.

EXERCISES

1. Evaluate the following determinants.

(a) by inspection

$$\begin{vmatrix} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & 0 \\ 7 & 8 & 9 & 0 \\ 3 & 2 & 1 & 0 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 1 & 2 & 3 & 4 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \\ 4 & 3 & 2 & 1 \end{vmatrix}.$$

(b) $\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix}$, $\begin{vmatrix} 4 & 3 \\ 2 & 1 \end{vmatrix}$.

(c) $\begin{vmatrix} 1 & i \\ -i & 1 \end{vmatrix}$.

(d) $\begin{vmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{vmatrix}$, $\begin{vmatrix} \frac{-1+\sqrt{-3}}{2} & e \\ \pi & \frac{-1-\sqrt{-3}}{2} \end{vmatrix}$.

(e) $\begin{vmatrix} 2 & -1 & 2 \\ 1 & 3 & 2 \\ 5 & 1 & 4 \end{vmatrix}$, $\begin{vmatrix} 1 & 4 & 6 \\ 5 & 2 & 8 \\ 9 & 7 & 3 \end{vmatrix}$.

(f) $\begin{vmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{vmatrix}$, $\begin{vmatrix} 1 & 2 & 8 & 9 \\ 3 & 4 & 0 & 1 \\ 7 & 0 & 8 & 2 \\ 10 & -1 & -5 & 0 \end{vmatrix}$, $\begin{vmatrix} 3 & 1 & 2 & 1 \\ 2 & 0 & 1 & 2 \\ -1 & 2 & 0 & 3 \\ 4 & 5 & 6 & 4 \end{vmatrix}$.

2. Prove or disprove the following statements:

   (a) $\det(A + B) = \det(A) + \det(B)$.

   (b) If $\det(A) = 0$, then $A = 0$.

   (c) If A is an $n \times n$ matrix and I is the $n \times n$ identity matrix, then $\det(xI - A)$ is a monic polynomial in x of degree n. [A polynomial is *monic* if its leading coefficient is 1.]

3. Suppose $A = \begin{pmatrix} A_{11} & & \dots & A_{1r} \\ \vdots & & & \\ 0 & \dots & 0 & A_{rr} \end{pmatrix}$ is a partition of A with square blocks on the diagonal. Show that i) $\det(A) = \det(A_{11}) \dots \det(A_{rr})$, and ii) A is invertible if and only if each A_j is invertible.

4. Compute the van der Monde (or Vandermonde) determinant, $\begin{vmatrix} 1 & \alpha & \alpha^2 \\ 1 & \beta & \beta^2 \\ 1 & \gamma & \gamma^2 \end{vmatrix}$.

5. Use induction on n to show that the *Vandermonde determinant*

$$\begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & & & \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix} = \Pi_{i<j}(\alpha_i - \alpha_j).$$

6. Show that if A is the $r \times r$ matrix $\begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & & & & \\ 0 & 0 & \dots & 0 & -c_{r-2} \\ 0 & 0 & \dots & 1 & -c_{r-1} \end{pmatrix}$, then the $\det(\lambda I - A) = (-1)^r(c_0 + c_1\lambda + \cdots + c_{r-1}\lambda^{r-1} + \lambda^r)$.

5.6 Adjoint and Cramer's Rule

There are two important and immediate consequences of (5.6) and (5.7) for expanding determinants using a row or column. The first one is the following theorem on computing A^{-1} by the so-called *cofactor method*. The second is Cramer's rule for solving independent systems of n linear equations in n variables. However, it must be pointed out that these are more of a theoretical significance. The row reduction may handle both these tasks more efficiently.

Recall that we have denoted by A_{ij} the $(n-1) \times (n-1)$ matrix obtained from an $n \times n$ matrix A by deleting its i-th row and j-th column.

Theorem 5.19. *Suppose $A = (a_{ij})$ is an $n \times n$ matrix. Let $B = (b_{ij})$ be the $n \times n$ matrix with*

$$b_{ji} = (-1)^{i+j} \det(A_{ij}). \tag{5.8}$$

Then $BA = \det(A)\, I$.

Proof. Suppose $BA = D = (d_{ij})$. By (5.7) and (5.8),

$$d_{jj} = \sum_{i=1}^{n} b_{ji}\, a_{ij} = \sum_{i=1}^{n} a_{ij}(-1)^{i+j} \det(A_{ij}) = \det(A). \tag{5.9}$$

We now show that for $j \neq k$, $d_{jk} = 0$. Replace the j-th column of A by its k-th column, so that the matrix C so obtained has two identical columns.

Since for all i, $C_{ij} = A_{ij}$, on expanding $\det(C)$ by j-th column, we get

$$\begin{aligned} 0 &= \det(C) \\ &= \sum_{i=1}^{n} (-1)^{i+j} a_{ik} \det(C_{ij}) \\ &= \sum_{i=1}^{n} a_{ik} (-1)^{i+j} \det(A_{ij}) \\ &= \sum_{i=1}^{n} b_{ji} a_{ik} \\ &= d_{jk}. \end{aligned}$$

This shows that for $j \neq k$,

$$d_{jk} = 0. \tag{5.10}$$

From (5.9) and (5.10), it follows that $BA = D = \det(A)\, I$. □

Corollary 5.20. (Inverse by Cofactor Method). *If* $\det(A) \neq 0$*, then*

$$A^{-1} = \frac{1}{\det(A)} \left((-1)^{i+j} \det(A_{ij})\right)^{*}.$$

In particular, A is invertible if and only if $\det(A) \neq 0$.

Definition. The transpose $((-1)^{i+j} \det(A_{ji}))$ of the $n \times n$ matrix $((-1)^{i+j} \det(A_{ij}))$ is called the *classical adjoint* of A, and is denoted by $\mathrm{adj}(A)$. Thus, we can write

$$A^{-1} = \frac{1}{\det(A)} \ \mathrm{adj}(A).$$

Cramer's Rule

Consider a system of n linear equations $AX = C$ in n variables with $\det(A) \neq 0$. Multiplying each side of $AX = C$ on the left by $\mathrm{adj}(A)$, we get $(\mathrm{adj}\, A)AX = \mathrm{adj}(A)C$. But $(\mathrm{adj}\, A)AX = ((\mathrm{adj}\, A)A)X = (\det(A)I)X = \det(A)X$. Hence $\det(A)X = \mathrm{adj}(A)C$, that is

$$x_j = \frac{1}{\det(A)} \sum_{i=1}^{n} (-1)^{i+j} c_i \det(A_{ij}). \tag{5.11}$$

Equation (5.11) is called Cramer's rule. It says that

$$x_j = \frac{\det(A_j)}{\det(A)}, \tag{5.12}$$

where A_j is the matrix obtained from A on replacing its j-th column by C.

Examples.

1. We compute the inverse A^{-1} of the 3×3 matrix
$$A = \begin{pmatrix} 1 & 4 & 5 \\ 0 & 2 & 6 \\ 0 & 0 & 3 \end{pmatrix}$$
by the cofactor method.

First note that $\det(A) = 1 \cdot 2 \cdot 3 = 6 \neq 0$. Hence A^{-1} exists. We find the nine *minors* (that is, the cofactors without the sign $(-1)^{i+j}$ of $\det(A_{ij})$). They are

$$|A_{11}| = \begin{vmatrix} 2 & 6 \\ 0 & 3 \end{vmatrix} = 6,\ |A_{12}| = \begin{vmatrix} 0 & 6 \\ 0 & 3 \end{vmatrix} = 0,\ |A_{13}| = \begin{vmatrix} 0 & 2 \\ 0 & 0 \end{vmatrix} = 0,$$

$$|A_{21}| = \begin{vmatrix} 4 & 5 \\ 0 & 3 \end{vmatrix} = 12,\ |A_{22}| = \begin{vmatrix} 1 & 5 \\ 0 & 3 \end{vmatrix} = 3,\ |A_{23}| = \begin{vmatrix} 1 & 4 \\ 0 & 0 \end{vmatrix} = 0,$$

$$|A_{31}| = \begin{vmatrix} 4 & 5 \\ 2 & 6 \end{vmatrix} = 14,\ |A_{32}| = \begin{vmatrix} 1 & 5 \\ 0 & 6 \end{vmatrix} = 6,\ |A_{33}| = \begin{vmatrix} 1 & 4 \\ 0 & 2 \end{vmatrix} = 2.$$

Hence,

$$\operatorname{adj}(A) = ((-1)^{i+j}\det(A_{ij}))^* = \begin{pmatrix} 6 & -12 & 14 \\ 0 & 3 & -6 \\ 0 & 0 & 2 \end{pmatrix}$$

and

$$A^{-1} = \frac{1}{\det(A)}\ \operatorname{adj} A = \begin{pmatrix} 1 & -2 & \frac{7}{3} \\ 0 & \frac{1}{2} & -1 \\ 0 & 0 & \frac{1}{3} \end{pmatrix}.$$

2. We solve, by Cramer's rule, the system

$$\begin{aligned} 3x_1 + x_2 &= 4 \\ 2x_1 + 4x_2 &= 5 \end{aligned} \tag{5.13}$$

of two linear equations in two variables. We write equation (5.13) in the matrix form $AX = C$, with $A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and $C = \begin{pmatrix} 4 \\ 5 \end{pmatrix}$. The matrices A_1, A_2 appearing in equation (5.12) are $A_1 = \begin{pmatrix} 4 & 1 \\ 5 & 4 \end{pmatrix}$, $A_2 = \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}$. Therefore, $\det(A_1) = 16 - 5 = 11$, $\det(A_2) = 15 - 8 = 7$, whereas $\det(A) = 12 - 2 = 10 \neq 0$. By Cramer's rule, the solution of equation (5.13) is

$$x_1 = \frac{\det(A_1)}{\det(A)} = \frac{11}{10},\quad x_2 = \frac{\det(A_2)}{\det(A)} = \frac{7}{10}.$$

EXERCISES

1. Compute $|A|$, $\operatorname{adj} A$, and A^{-1}, if A is

   (a) $\begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$

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

   (c) $\begin{pmatrix} 2 & 5 & 1 \\ 0 & 3 & 7 \\ 0 & 0 & 4 \end{pmatrix}$

   (d) $\begin{pmatrix} 1 & 3 & 2 \\ 4 & 5 & 7 \\ 6 & 8 & 9 \end{pmatrix}$.

2. Use Cramer's Rule to solve

   (a) $$\begin{aligned} 2x_1 + x_2 + x_3 &= 2 \\ x_1 + 3x_2 + x_3 &= 3 \\ -2x_1 + 2x_2 - x_3 &= 5 \end{aligned}$$

   (b) $$\begin{aligned} x + y + z &= 1 \\ 2x - 6y - z &= -1 \\ 3x + 4y + 2z &= 1 \end{aligned}$$

3. Compute the inverse by cofactor method of the matrix A, if A is

   (a) $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ -2 & 2 & -1 \end{pmatrix}$,

   (b) $\begin{pmatrix} 1 & 1 & 1 \\ 2 & -6 & -1 \\ 3 & 4 & 2 \end{pmatrix}$.

4. Use A^{-1} from Problem 3 to solve Problem 2 as $X = A^{-1}C$.

5. If A is an $n \times n$ invertible matrix, show that $\det(\operatorname{adj}(A)) = (\det(A))^{n-1}$.

6

Diagonalization

6.1 Motivation

A linear differential equation

$$y' = ay$$

with solution

$$y = y(t) = e^{at}$$

can be generalized to a system of n linear differential equations

$$Y' = AY$$

with A an $n \times n$ matrix over $\mathbb{R}$ (cf. Chapter 10). Its solutions can again be written formally as

$$Y = Y(t) = e^{At}$$

which requires computing every power A^m of A in the following definition of the exponential function of a matrix:

$$e^A = I + A + \frac{1}{2!}\,A^2 + \frac{1}{3!}\,A^3 + \cdots \tag{6.1}$$

From the right side of equation (6.1), we mean the entry-wise limit,

$$\lim_{m\to\infty}\left(I + A + \frac{1}{2!}\,A^2 + \frac{1}{3!}\,A^3 + \cdots + \frac{1}{m!}\,A^m\right).$$

How can we show that this limit exists and compute the matrix e^A?

The answer lies in the diagonalization. Suppose we can find a non-singular matrix P such that $P^{-1}AP$ is diagonal, say

$$P^{-1}AP = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}. \tag{6.2}$$

Then

$$\begin{pmatrix} \lambda_1^m & & 0 \\ & \ddots & \\ 0 & & \lambda_n^m \end{pmatrix}$$

$$= D^m = (P^{-1}AP)^m = (P^{-1}AP)(P^{-1}AP)\dots(P^{-1}AP) = P^{-1}A^mP,$$

which gives $A^m = PD^mP^{-1}$. Therefore, if we write $A^o = I$,

$$e^A = \sum_{m=0}^{\infty} \frac{1}{m!}A^m = \sum_{m=0}^{\infty} \frac{1}{m!}PD^mP^{-1} = P\left(\sum_{m=0}^{\infty} \frac{1}{m!}D^m\right)P^{-1} =$$

$$P\begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix}P^{-1}.$$

Thus, if we have equation (6.2), the computation of e^A involves multiplying only three, in fact essentially two matrices.

6.2 Eigenvalues and Eigenvectors

How can we find the non-singular matrix P appearing in (6.2)? To answer this question, we recall from earlier chapters some fundamental facts about matrices and linear transformations.

1) The $n \times n$ matrices correspond to linear transformations $T : V \to V$ from an n-dimensional vector space V to itself.
2) This correspondence depends on the choice of ordered basis of V. A change of bases changes the matrix A of T to a similar matrix $B = P^{-1}AP$. Moreover, the matrix P can be computed from the two bases involved.
3) If $\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ is the standard basis of K^n (K being the field of scalars) and $D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ is diagonal, then $D\boldsymbol{e}_j = \lambda_j \boldsymbol{e}_j$.

These properties suggest that in order to *diagonalize* A, i.e., to find P with $P^{-1}AP$ diagonal, we need to find a basis of V consisting of vectors $\boldsymbol{v}$, such that $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$. Note that a basis vector $\boldsymbol{v}$ cannot be zero. This leads to the following terminology.

Definition. Suppose V is a vector space over a field K, not necessarily finite dimensional. A scalar λ in K (or in a larger field containing K as a subfield) is called an *eigenvalue* or a *characteristic root* of the linear transformation $T : V \to V$ if $T(\boldsymbol{v}) = \lambda\boldsymbol{v}$ for a nonzero vector $\boldsymbol{v}$, called an *eigenvector* (or a *characteristic vector*) belonging to the eigenvalue λ.

An $n \times n$ matrix over K represents a linear transformation from $V = K^n$ to itself and the above definition may be reformulated as follows.

Definition. If A is an $n \times n$ matrix over K, a scalar λ is an *eigenvalue* of A, if $A\boldsymbol{v} = \lambda\boldsymbol{v}$ for a nonzero column vector $\boldsymbol{v}$ in K^n. We call $\boldsymbol{v}$ an *eigenvector* for or *belonging to* λ.

Examples.

1. Let $A = \begin{pmatrix} 1 & 6 \\ 5 & 2 \end{pmatrix}$. Since for $\boldsymbol{x} = \binom{1}{1}$, $A\boldsymbol{x} = 7\boldsymbol{x}$, therefore $\lambda = 7$ is an eigenvalue of A and $\boldsymbol{x} = \binom{1}{1}$ is an eigenvector belonging to the eigenvalue $\lambda = 7$ of A.

2. Suppose $T : \mathbb{R}^2 \to \mathbb{R}^2$ is the rotation through $\pi/3$. Then T has no real eigenvalue. (Why?)

3. If $I : V \to V$ is the identity map (or I is the identity matrix), then $\lambda = 1$ is the only eigenvalue of I, but every $\boldsymbol{v} \neq 0$ is an eigenvector of I.

4. Let A be an $n \times n$ diagonal matrix $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$. Then $A\boldsymbol{e}_j = \lambda_j\boldsymbol{e}_j$, where $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ is the standard basis of K^n. Hence $\boldsymbol{e}_j$ is an eigenvector for the eigenvalue λ_j.

5. Let $V = C^\infty(0, 1)$, the vector space of functions $f : (0, 1) \to \mathbb{R}$ having derivatives of all orders. Let $T = \frac{d}{dx} : V \to V$. Every real number α is an eigenvalue of T. An eigenvector for α is $f(x) = e^{\alpha x}$, because $T(f) = \alpha f$. This linear transformation has infinitely many eigenvalues. The linearly independent set $\{e^{\alpha x} \mid \alpha \in \mathbb{R}\}$ has the same cardinality as $\mathbb{R}$.

Characteristic Polynomial

Suppose A is an $n \times n$ matrix. How many eigenvalues can A have and how do we find these eigenvalues and eigenvectors belonging to them? To answer this question, suppose $\boldsymbol{v} \neq 0$ is an eigenvector for an eigenvalue λ of A. By definition,

$$A\boldsymbol{v} = \lambda\boldsymbol{v}, \tag{6.3}$$

for a nonzero column vector

$$\boldsymbol{v} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

We rewrite equation (6.3) as

$$(\lambda I - A)\boldsymbol{v} = \mathbf{0}, \tag{6.4}$$

where I is the $n \times n$ identity matrix. Since $\boldsymbol{v} \neq 0$, $\lambda I - A$ cannot be invertible. Hence

$$\det(\lambda I - A) = 0. \tag{6.5}$$

The equation (6.5) is a polynomial equation

$$\lambda^n + \cdots = 0 \tag{6.6}$$

in λ of degree n. Hence the eigenvalues of A are the roots of the so-called *characteristic polynomial*

$$\chi_A(\lambda) = \det(\lambda I - A) \tag{6.7}$$

of A, which is of degree n. Although $\chi_A(\lambda)$ has real coefficients some of its roots, counted with multiplicity, may be imaginary. One then replaces (see Chapter 9) the field $K = \mathbb{R}$ of scalars by $\mathbb{C}$. We will prove in Chapter 9 that when A is symmetric, all its eigenvalues are real.

Remark. We can write (6.4) also as $(A - \lambda I)\ \boldsymbol{v} = \mathbf{0}$ and define the characteristic polynomial as $\det(A - \lambda I)$. But then for n odd, $\chi_A(\lambda) = -\lambda^n + \cdots$, which is not monic, i.e., the leading coefficient is -1 and not 1.

Theorem 6.1. *If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of an $n \times n$ matrix A, then their*

i) product $\lambda_1, \ldots, \lambda_n = \det(A)$, and

ii) sum $\lambda_1 + \cdots + \lambda_n = \operatorname{tr}(A)$.

Moreover,

$$\chi_A(\lambda) = \lambda^n - \operatorname{tr}(A)\lambda^{n-1} + \cdots + \det(A).$$

Proof. Putting $\lambda = 0$ in

$$\chi_A(\lambda) = \det(\lambda I - A) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n)$$

proves i).

To prove ii), first observe that

$$\begin{aligned}\chi_A(\lambda) &= (\lambda-\lambda_1)\cdots(\lambda-\lambda_n)\\ &= \lambda^n-(\lambda_1+\cdots+\lambda_n)\lambda^{n-1}+\cdots+\lambda_1\cdots\lambda_n.\end{aligned}$$

Then use its first row to expand $|\lambda I - A|$. Denoting the $(n-1)\times(n-1)$ matrix obtained by deleting the i-th row and j-th column of $\lambda I - A$ by M_{ij},

$$|\lambda I - A| = (\lambda - a_{11})\det M_{11} + a_{12}\det(M_{12}) - \cdots .$$

Note that to obtain M_{1j} $(j>1)$, we delete from $\lambda I - A$ its first row with entry $\lambda - a_{11}$ and j-th column with entry $\lambda - a_{jj}$, so $\deg(M_{ij})$ is less than $n-1$ (if $j>1$). Thus the leading two terms of $\chi_A(\lambda)$ come from $(\lambda - a_{11})\det(M_{11})$. Applying the same argument to M_{11} and continuing, we see that the leading two terms of $\chi_A(\lambda)$ come from

$$(\lambda-a_{11})\cdots(\lambda-a_{nn}) = \lambda^n-(a_{11}+\cdots+a_{nn})\lambda^{n-1}+\cdots+\lambda_1\ldots\lambda_n.$$

Comparing the coefficients of λ^{n-1} in the above two calculations for $\chi_A(\lambda)$, proves ii). The last assertion is now obvious. □

Corollary 6.2. *If* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *then* $\chi_A(\lambda) = \lambda^2 - (a+d)\lambda + (ad-bc)$.

Definition. Given A and an eigenvalues λ of A, the *eigenspace* V_λ of λ is the solution space of the homogeneous system in equation (6.4). By construction, V_λ is a subspace of $\mathbb{R}^n$ and contains a nonzero vector, hence $\dim V_\lambda > 0$.

Examples.

1. Let us first look at a trivial example. Suppose $A = I$, the identity matrix of size n. Its characteristic polynomial

$$\chi_A(\lambda) = \det(\lambda I - A) = \begin{vmatrix} \lambda-1 & & 0 \\ & \ddots & \\ 0 & 0 & \lambda-1 \end{vmatrix} = (\lambda-1)^n.$$

So A has only one eigenvalue, $\lambda = 1$ (of multiplicity n) and clearly, its eigenspace is all of $V = K^n$.

2. Now, suppose A is a diagonal matrix

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

with distinct $\lambda_1, \ldots, \lambda_n$. Then $\chi_A(\lambda) = (\lambda-\lambda_1)\ldots(\lambda-\lambda_n)$ and A has n eigenvalues $\lambda_1, \ldots, \lambda_n$. It is easy to show that each eigenspace is one-dimensional.

Diagonalization.

Recall that two $n \times n$ matrices A and B are similar if $B = P^{-1}AP$ for an invertible matrix P.

Definition. We say that an $n \times n$ matrix A is *diagonalizable* if A is similar to a diagonal matrix.

By *diagonalizing* a diagonalizable matrix A, we mean finding P such that PAP^{-1} is diagonal.

Remarks.

1. To be precise, one should say *similar over* K and *diagonalizable over* K to mean P has entries in K. There are examples of matrices in $M(n, \mathbb{R})$ that are diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$. However, this will not concern us in this chapter.

2. We shall see later that not all $n \times n$ matrices A are diagonalizable. In fact, A is diagonalizable if and only if K^n has a basis consisting of eigenvectors of A.

The following fact is obvious from the above discussion. (See Section 4.6)

Theorem 6.3. *Suppose the vector space K^n has a basis consisting of eigenvectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ of A belonging to its eigenvalues $\lambda_1, \ldots, \lambda_n$ and P is the transition matrix from the standard basis of K^n to the basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$. Then*

$$PAP^{-1} = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Moreover, the columns of P are the eigenvectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Examples.

1. To diagonalize the 2×2 matrix

$$A = \begin{pmatrix} 5 & 3 \\ -4 & -2 \end{pmatrix},$$

we find the roots of its characteristic polynomial

$$\chi_A(\lambda) = \begin{vmatrix} \lambda - 5 & -3 \\ 4 & \lambda + 2 \end{vmatrix} = \lambda^2 - 3\lambda + 2 = (\lambda - 1)(\lambda - 2).$$

Hence, the two eigenvalues are $\lambda = 1, 2$. We now find eigenvectors for these eigenvalues.

For $\lambda = 1$, the defining equation $A\boldsymbol{v} = \lambda\boldsymbol{v}$, that is, $(\lambda I - A)\boldsymbol{v} = \mathbf{0}$ is

$$\begin{pmatrix} -4 & -3 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

which is equivalent to the single linear equation

$$4x_1 + 3x_2 = 0.$$

We take $x_1 = -3$, $x_2 = 4$. So an eigenvector for $\lambda = 1$ is the nonzero vector $\boldsymbol{v}_1 = \binom{-3}{4}$.

For $\lambda = 2$, $(\lambda I - A)\boldsymbol{v} = \mathbf{0}$ becomes

$$\begin{pmatrix} -3 & -3 \\ 4 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

or $x_1 + x_2 = 0$.

We take $\boldsymbol{v}_2 = \binom{1}{-1}$ for an eigenvector for $\lambda = 2$.

The transition matrix P is the one that takes the standard basis $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ to the basis consisting of the eigenvectors $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. So P is the matrix whose two columns are $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$, that is,

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

We compute

$$P^{-1} = \begin{pmatrix} 1 & 1 \\ 4 & 3 \end{pmatrix}.$$

Finally, we see that $P^{-1}AP =$

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

is indeed a diagonal matrix with the eigenvalues $\lambda = 1, 2$ of A on its diagonal.

2. Let us diagonalize now the 3×3 matrix

$$A = \begin{pmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{pmatrix}.$$

The characteristic polynomial

$$\chi_A(\lambda) = \begin{vmatrix} \lambda - 5 & 6 & 6 \\ 1 & \lambda - 4 & -2 \\ -3 & 6 & \lambda + 4 \end{vmatrix}$$

$= x^3 - 5x^2 + 8x - 4 = (x-1)(x-2)^2$. The eigenvalues of A are $\lambda = 1, 2, 2$. For $x = 1$ the eigenspace is the solution space of $(1I - A)\boldsymbol{v} = \mathbf{0}$, which is

$$\begin{aligned} -2x + 3y + 3z &= 0 \\ x - 3y - 2z &= 0 \\ -3x + 6y + 5z &= 0. \end{aligned}$$

The last equation is the difference of the first two. Hence, we need only to find a basis for the solution space of

$$\begin{aligned} -2x + 3y + 3z &= 0 \\ x - 3y - 2z &= 0, \end{aligned}$$

which, being the intersection of two planes, is a line. Taking $z = 1$, these two equations become

$$\begin{aligned} -2x + 3y &= -3 \\ x - 3y &= 2. \end{aligned}$$

Solving these, we find that $x = 1$ and $y = \frac{-1}{3}$. So, an eigenvector for $\lambda = 1$ is $\begin{pmatrix} 1 \\ \frac{-1}{3} \\ 1 \end{pmatrix}$ which can be scaled to $\boldsymbol{v}_1 = \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix}$.

For the eigenvalues $\lambda = 2$, $(\lambda I - A)\boldsymbol{v} = \mathbf{0}$ is

$$\begin{aligned} -3x + 6y + 6z &= 0 \\ x - 2y - 2z &= 0 \\ -3x + 6y + 6z &= 0, \end{aligned}$$

which is equivalent to the single equation

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

This equation represents a plane, which is a two dimensional space. We pick a basis

$$\boldsymbol{v}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \boldsymbol{v}_3 = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$$

for the eigenspace for $\lambda = 2$. The matrix P consisting of $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3$ is

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

It may be checked that

$$P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

a diagonal matrix with the eigenvalues 1, 2, 2 on the diagonal.

Remark. As we shall see later, it is no coincidence that the dimension of each eigenspace belonging to an eigenvalue is equal to its multiplicity.

EXERCISES

1. (a) If A, B are similar, show that $\det(A) = \det(B)$ and $\operatorname{tr}(A) = \operatorname{tr}(B)$.

   (b) Show that similar matrices have the same eigenvalues.

2. (a) If λ is an eigenvalue of a linear map $T : V \to V$, show that λ^r is an eigenvalue of T^r for all $r = 1, 2, 3, \ldots$. [In particular, if λ is an eigenvalue of a matrix A, then λ^r is an eigenvalue of A^r for all $r \geq 1$.]

   (b) Show that if $f(x)$ is a polynomial and λ is an eigenvalue of $T : V \to V$, then $f(\lambda)$ is an eigenvalue of $f(T)$.

   (c) Show that if an $n \times n$ matrix A is diagonalizable, then $f(A)$ is diagonalizable.

   (d) If A, B are diagonalizable and $AB = BA$, show that AB is also diagonalizable.

3. Suppose λ is an eigenvalue of an $n \times n$ matrix A.

   (a) Show that the eigenspace $V_\lambda = \{\boldsymbol{v} \in K^n | A\boldsymbol{v} = \lambda\boldsymbol{v}\}$ belonging to the eigenvalue λ of A is indeed a subspace of $V = K^n$.

   (b) Suppose $r =$ the row rank of $\lambda I - A$. Show that $\dim V_\lambda = n - r$.

4. (a) If $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ are eigenvectors belonging to distinct eigenvalues λ_1, λ_2 of A, show that $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ are linearly independent. Generalize it to more than two vectors. [Thus if all the eigenvalues of A are distinct, it is diagonalizable.]

   (b) If all the eigenvalues of A are distinct and λ is one of them, show that $\text{dim}V_\lambda = 1$.

5. If λ is a root of multiplicity m of the characteristic polynomial of a matrix A, we call m the *algebraic multiplicity* of the eigenvalue λ of A, whereas, $\dim V_\lambda$ is called the *geometric multiplicity* of λ.

(a) Show that for every eigenvalue, the algebraic multiplicity $\geq$ geometric multiplicity ≥ 1.

(b) Give examples to show that both equality and inequality can occur.

(c) A matrix is *simple* if its eigenvalues are all distinct. It is *semisimple* if the geometric multiplicity of its every eigenvalue is equal to the algebraic multiplicity. A simple matrix is automatically semisimple. Show that A is diagonalizable if and only if it is semisimple.

6. Use Exercise 5 above to show that $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is not diagonalizable.

7. Show that 2×2 symmetric matrices over $\mathbb{R}$ are diagonalizable.

8. If A is a real matrix, show that (see Section 8.2)

(a) the imaginary eigenvalues occur in pairs λ, $\overline{\lambda}$.

(b) If $\boldsymbol{v} = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ is an eigenvector in $\mathbb{C}^n$ belonging to an imaginary eigenvalue λ, then $\overline{\boldsymbol{v}} = \begin{pmatrix} \overline{z_1} \\ \vdots \\ \overline{z_n} \end{pmatrix}$ is an eigenvector belonging to $\overline{\lambda}$.

9. Show that $A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, $0 \leq \theta < 2\pi$, has no real eigenvalues except for $\theta = 0$ and π. Interpret this geometrically.

10. It is a non-trivial task to find the three roots of a cubic polynomial. Suppose an eigenvector of a 3×3 matrix is known somehow. Explain how we can find all the eigenvalues and the eigenvectors belonging to them.

11. For the following matrices, find eigenvalues, eigenvectors and a matrix P such that PAP^{-1} is diagonal. Check that PAP^{-1} has the eigenvalues of A on the diagonal of PAP^{-1}. Finally compute e^A. The field K of scalars in these problems is $\mathbb{C}$.

(a) $\begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}$, $\begin{pmatrix} -2 & 3 \\ 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 5 & -18 \\ 1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$;

(b) $\begin{pmatrix} 3 & -1 & -1 \\ 2 & 0 & -2 \\ 2 & -1 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}$, $\begin{pmatrix} 2 & 4 & 2 \\ 1 & -1 & -1 \\ 1 & 1 & 3 \end{pmatrix}$.

6.3 Cayley-Hamilton Theorem

We remarked earlier that not every matrix is diagonalizable. (See Exercise 6, Section 6.2.) In this section, we characterize diagonalizable matrices.

The vector space $V = M(n, K)$ of $n \times n$ matrices over a field K has dimension $\dim_K(V) = n^2$. Hence, for any matrix A in V, the $n^2 + 1$ matrices $I, A, A^2, \ldots, A^{n^2}$, viewed as vectors in V, are linearly dependent, that is, there are constants $c_0, c_1, \ldots, c_{n^2}$, not all zero, such that

$$c_0 I + c_1 A + c_2 A^2 + \cdots + c_{n^2} A^{n^2} = 0.$$

Thus every $n \times n$ matrix A in $M(n, K)$ satisfies a nonzero polynomial

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n^2} x^{n^2}$$

of degree at most n^2.

Later in this section, we shall prove the Cayley-Hamilton Theorem, which strengthens this statement and asserts that an $n \times n$ matrix satisfies a polynomial equation of degree at most n.

A nonzero polynomial of the smallest degree satisfied by an $n \times n$ matrix A in $M(n, K)$ is called its *minimal polynomial*. We now show that up to a constant, it is unique. If $f(x)$ and $g(x)$ are two minimal polynomials of A, then $g(x) = cf(x)$ for a constant c. To see this, we write by the division algorithm $g(x) = q(x)f(x) + r(x)$, where deg $r(x) <$ deg $f(x)$. Since $f(A) = g(A) = 0$, $r(A) = 0$. By minimality of the degree of $f(x)$, $r(x) = 0$. This shows that $f(x)$ is a factor of $g(x)$. Similarly, $g(x)$ is a factor of $f(x)$. Hence $g(x) = cf(x)$. If the leading coefficient of $f(x)$ is taken to be 1, then $f(x)$ is unique and is called the *minimal polynomial of the matrix A*.

We now state without proof the following characterization of diagonalizable matrices.

Theorem 6.4. *An $n \times n$ matrix A is diagonalizable over K if and only if its minimal polynomial*

$$m(x) = (x - \lambda_1) \ldots (x - \lambda_r)$$

has distinct roots $\lambda_1, \ldots, \lambda_r$ $(r \leq n)$ in K.

The interested reader can find the proof in [4, p. 200]. Instead, we give some applications of this theorem.

Suppose W is a subspace of a finite dimensional vector space V, invariant under T, that is, $T(W) \subset W$. Let $T_{|W} : W \to W$ be the restriction of T to W. Clearly, $T_{|W}$ is also a linear map. The following proposition relates the characteristic polynomial of $T_{|W}$ to that of T.

Theorem 6.5. *The characteristic polynomial $\chi_{T_{|W}}(\lambda)$ is a factor of $\chi_T(\lambda)$.*

Proof. Suppose $T : V \to V$ is a linear map and $\dim(W) = r \leq n$. If $r = n$, there is nothing to prove. So, let $r < n$. Complete a basis $\mathcal{B}_W = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$ of W to a basis $\mathcal{B}_V = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r, \boldsymbol{w}_{r+1}, \ldots, \boldsymbol{w}_n\}$ of V. The $r \times r$ matrix $A = (a_{ij})$ of $T_{|W}$ relative to $\mathcal{B}_W$ is given by the r equations

$$T(\boldsymbol{w}_j) = \sum_{i=1}^{r} a_{ij}\boldsymbol{w}_i$$

and hence,

$$\chi_{T_{|W}}(\lambda) = \det(\lambda I - A). \tag{6.8}$$

The $n \times n$ matrix of $T : V \to V$ relative to the basis $\mathcal{B}_V$ is of the form $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ which shows that

$$\chi_T(\lambda) = \det(\lambda I - A)\det(\lambda I - C). \tag{6.9}$$

The theorem follows from (6.8) and (6.9). □

Now we state and prove a well-known property of the characteristic polynomials.

Theorem 6.6. (Cayley-Hamilton) *Every $n \times n$ matrix A satisfies its characteristic polynomial $\chi_A(\lambda)$.*

Proof. We need to show that the $n \times n$ matrix $B = \chi_A(A)$ is the zero matrix. For this it is enough to show that $B\boldsymbol{v} = \mathbf{0}$ for every column vector $\boldsymbol{v} \neq \mathbf{0}$ in $V = K^n$.

Let $T : V \to V$ be the linear map $T(\boldsymbol{v}) = A\boldsymbol{v}$, associated with the matrix A. We denote by W the linear span of the set $\{T^j(\boldsymbol{v}) \mid j = 0, 1, 2, \ldots\} = \{\boldsymbol{v}, T(\boldsymbol{v}), T^2(\boldsymbol{v}), \ldots\}$. Clearly, W is invariant under T. The dimension $\dim(W)$ is the largest integer $r \geq 1$ such that $\boldsymbol{v}, T(\boldsymbol{v}), T^2(\boldsymbol{v}), \ldots, T^{r-1}(\boldsymbol{v})$ are linearly independent, because then every subsequent vector $T^j(\boldsymbol{v})$, $j \geq r$, can be expressed as a linear combination of previous ones. In particular,

$$c_0\boldsymbol{v} + c_1T(\boldsymbol{v}) + c_2T^2(\boldsymbol{v}) + \cdots + c_{r-1}T^{r-1}(\boldsymbol{v}) + T^r(\boldsymbol{v}) = \mathbf{0},$$

with not all $c_j = 0$, which shows that the matrix of $T_{|W} : W \to W$ relative to the basis $\mathcal{B}_W = \{\boldsymbol{v}, T(\boldsymbol{v}), T^2(\boldsymbol{v}), \ldots, T^{r-1}(\boldsymbol{v})\}$ is

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & & & & \\ 0 & 0 & \ldots & 0 & -c_{r-2} \\ 0 & 0 & \ldots & 1 & -c_{r-1} \end{pmatrix}.$$

By Exercise 6, Section 5.5, the characteristic polynomial of this matrix, and hence that of $T_{|W}$, is

$$(-1)^r(c_0 + c_1\lambda + \cdots + c_{r-1}\lambda^{r-1} + \lambda^r).$$

On the other hand, the choice of r shows that the minimal polynomial of $T_{|W}$ is $c_0 + c_1\lambda + \cdots + c_r\lambda^r$. Therefore, up to sign, the characteristic polynomial of $T_{|W}$ is also its minimal polynomial, and hence, $\chi_{T_{|W}}(T)(\boldsymbol{v}) = \mathbf{0}$. By Theorem 6.5, $\chi_T(\lambda) = f(\lambda)\chi_{T_{|W}}(\lambda)$ for some $f(\lambda)$, which depends of course on the vector $\boldsymbol{v}$, and we have

$$\chi_T(T)(\boldsymbol{v}) = f(T)\chi_{T_{|W}}(T)(\boldsymbol{v}) = f(T)\mathbf{0} = \mathbf{0}.$$

This proves the Cayley-Hamilton Theorem. □

Example. For the 2×2 matrix

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

its characteristic polynomial $\chi_A(\lambda) = (\lambda - 1)^2$. Therefore, its minimal polynomial, which is a factor of $\chi_A(\lambda)$, is either $\lambda - 1$ or $(\lambda - 1)^2$. But A does not satisfy $\lambda - 1$. Hence the minimal polynomial of A is $(\lambda - 1)^2$. By Theorem 6.4, A is not diagonalizable.

Example. If U is a nonzero $n \times n$ upper triangular matrix, with zeros on the diagonal, its characteristic polynomial $\chi_U(\lambda) = \lambda^n$. Hence, the minimal polynomial $m(\lambda)$ of U is λ^r for some $r \geq 1$. For $r = 1$, $m(U) = U \neq 0$. Hence $r > 1$. But then $m(\lambda) = \lambda^r$ does not have distinct roots. Hence U is not diagonalizable. As a particular case, let $V = P_n$, the vector space of polynomials over $\mathbb{R}$ of degree smaller than n. Relative to the standard basis $\{1, x, \ldots, x^{n-1}\}$ of P_n, the matrix of the linear map $D = \frac{d}{dx} : P_n \to P_n$ is upper diagonal. Hence D is not diagonalizable.

EXERCISES

1. Determine which of the following matrices are diagonalizable.

$$\text{(a)} \begin{pmatrix} 2 & -3 \\ 2 & -5 \end{pmatrix}, \quad \text{(b)} \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}, \quad \text{(c)} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

2. Show that the following matrices are diagonalizable over $\mathbb{C}$ but not over $\mathbb{R}$.

$$\text{(a)} \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}, \quad \text{(b)} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

3. Verify the Cayley-Hamilton Theorem for the following matrices.

$$\text{(a)} \begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix}, \quad \text{(b)} \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}, \quad \text{(c)} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

7

Inner Product Spaces

7.1 Inner Product

Although some notions like distance, angles, parallelism, and perpendicularity make sense only in the Euclidean n-spaces $\mathbb{R}^n$ $(n = 2, 3)$, they can be generalized to more general vector spaces over $K = \mathbb{R}$ or $\mathbb{C}$. Throughout this chapter, unless stated otherwise, we shall have our field of scalars $K = \mathbb{R}$.

Since the concepts like length and angle in $V = \mathbb{R}^n(n = 2, 3)$ can be defined purely in terms of the dot product on V, an immediate generalization would be to $V = \mathbb{R}^n$. For $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$, their dot product $\boldsymbol{x} \cdot \boldsymbol{y}$ is the scalar

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n.$$

It is easy to verify that the dot product has the following basic or defining properties. For all $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ in $\mathbb{R}^n$ and all scalars a,

1) $\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x}$,
2) $(\boldsymbol{x} + \boldsymbol{y}) \cdot \boldsymbol{z} = \boldsymbol{x} \cdot \boldsymbol{z} + \boldsymbol{y} \cdot \boldsymbol{z}$,
3) $(a\boldsymbol{x}) \cdot \boldsymbol{y} = a(\boldsymbol{x} \cdot \boldsymbol{y})$, and
4) $\boldsymbol{x} \cdot \boldsymbol{x} \geq 0$ and $= 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.

To begin with, we restrict ourselves to the case $n = 2$ or 3. Clearly, the length $\|\boldsymbol{x}\|$ of $\boldsymbol{x}$ is $\sqrt{\boldsymbol{x} \cdot \boldsymbol{x}}$. If $\boldsymbol{x}$ and $\boldsymbol{y}$ are two nonzero vectors in $\mathbb{R}^2$, the angle θ between them is determined by their dot product as follows.

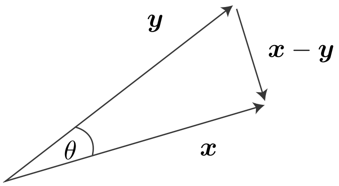


FIGURE 7.1: For the Law of Cosines

By the Law of Cosines (see Figure 7.1),

$$\|\boldsymbol{x}-\boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 - 2\|\boldsymbol{x}\|\,\|\boldsymbol{y}\|\cos\theta. \tag{7.1}$$

But also it follows from the basic properties of the dot product that

$$\begin{aligned}\|\boldsymbol{x}-\boldsymbol{y}\|^2 &= (\boldsymbol{x}-\boldsymbol{y})\cdot(\boldsymbol{x}-\boldsymbol{y})\\ &= \boldsymbol{x}\cdot\boldsymbol{x} - 2\boldsymbol{x}\cdot\boldsymbol{y} + \boldsymbol{y}\cdot\boldsymbol{y}\\ &= \|\boldsymbol{x}\|^2 - 2\boldsymbol{x}\cdot\boldsymbol{y} + \|\boldsymbol{y}\|^2\end{aligned}$$

i.e.,

$$\|\boldsymbol{x}-\boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 - 2\boldsymbol{x}\cdot\boldsymbol{y}. \tag{7.2}$$

Comparing (7.1) and (7.2), we get

$$\boldsymbol{x}\cdot\boldsymbol{y} = \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|\cos\theta. \tag{7.3}$$

If $\boldsymbol{x}$, $\boldsymbol{y} \neq \boldsymbol{0}$, we have

$$\theta = \cos^{-1}\left(\frac{\boldsymbol{x}\cdot\boldsymbol{y}}{\|\boldsymbol{x}\|\,\|\boldsymbol{y}\|}\right).$$

In particular, $\boldsymbol{x}$ is perpendicular (or orthogonal) to $\boldsymbol{y}$ if and only if $\boldsymbol{x}\cdot\boldsymbol{y} = 0$.

For any $n > 1$ and $\boldsymbol{x} = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$, we can certainly define its length as

$$\|\boldsymbol{x}\| = \sqrt{x_1^2 + \cdots + x_n^2} = \sqrt{\boldsymbol{x}\cdot\boldsymbol{x}}.$$

We can even say that given $\boldsymbol{y} = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$, $\boldsymbol{x}$ is orthogonal to $\boldsymbol{y}$, written $\boldsymbol{x} \perp \boldsymbol{y}$, if $\boldsymbol{x}\cdot\boldsymbol{y} = 0$. However, this will not be meaningful unless we first define the angle θ between $\boldsymbol{x}$ and $\boldsymbol{y}$, say by (7.3). But in order to do that, we must have

$$-1 \leq \frac{\boldsymbol{x}\cdot\boldsymbol{y}}{\|\boldsymbol{x}\|\,\|\boldsymbol{y}\|} \leq 1.$$

or

$$|\boldsymbol{x}\cdot\boldsymbol{y}| \leq \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|. \tag{7.4}$$

We shall show that (7.4), called the Cauchy-Schwarz Inequality, follows from the basic properties 1)–4) of the dot products. That is suggested by the fact that in deriving (7.2), we only used the basic properties 1)–4) of the dot product on $\mathbb{R}^n$.

Remark. There is a distinction between "orthogonal" and "perpendicular." The zero vector doesn't make an angle with any other vector $\boldsymbol{x}$. So we say that $\boldsymbol{x}$ is *orthogonal* to $\boldsymbol{y}$ if $\boldsymbol{x}\cdot\boldsymbol{y} = 0$, and $\boldsymbol{x}$ is *perpendicular* to $\boldsymbol{y}$ if $\boldsymbol{x}\cdot\boldsymbol{y} = 0$ with $\boldsymbol{x}$, $\boldsymbol{y} \neq 0$.

Definition. Let V be a vector space over $\mathbb{R}$. An *inner product* on V is a map

$$V \times V \ni (x, y) \to \langle x, y\rangle \in \mathbb{R}$$

satisfying the following (defining) properties of the dot product. For all $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ in V and all c in $\mathbb{R}$,

1) $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{y}, \boldsymbol{x} \rangle$,

2) $\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{z} \rangle + \langle \boldsymbol{y}, \boldsymbol{z} \rangle$,

3) $\langle c\boldsymbol{x}, \boldsymbol{y} \rangle = c\langle \boldsymbol{x}, \boldsymbol{y} \rangle$, and

4) $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \geq 0$ and $= 0$ if and only if $\boldsymbol{x} = \mathbf{0}$.

Definition. An *inner product space* is a vector space V over $\mathbb{R}$ with an inner product $\langle\ ,\ \rangle$ on it.

Examples.

1. $V = \mathbb{R}^n$ with the usual dot product

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n. \tag{1}$$

We shall call $\mathbb{R}^n$ with (1) as the *Euclidean n-space.*

2. Again $V = \mathbb{R}^n$, and choose positive reals $w_j (i \leq j \leq n)$ called the weights. Then

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = w_1 x_1 y_1 + \cdots + w_n x_n y_n$$

defines an inner product on V, called the *weighted inner product.*

3. Let $V = C[0,1]$, the vector space of (real valued) continuous functions $f : [0,1] \to \mathbb{R}$. The following defines an inner product on V.

$$\langle f, g \rangle = \int_0^1 f(x)g(x)dx.$$

Definition. Two inner products $\langle , \rangle_1$, $\langle , \rangle_2$ on a vector space V over $\mathbb{R}$ are *equivalent* if $\langle , \rangle_1 = c\langle , \rangle_2$ for some $c > 0$. Otherwise, they are *inequivalent.*

Example. The inner product $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = x_1 y_1 + 2x_2 y_2 + \cdots + n x_n y_n$ on $\mathbb{R}^n$ is not equivalent to the dot product in Example 1.

Proposition 7.1. *In an inner product space V, for any $\boldsymbol{x}$ in V, $\langle \mathbf{0}, \boldsymbol{x} \rangle = 0$.*

Proof. For every scalar c,

$$c\langle \mathbf{0}, \boldsymbol{x} \rangle = \langle c\,\mathbf{0}, \boldsymbol{x} \rangle = \langle \mathbf{0}, \boldsymbol{x} \rangle,$$

which can be true only if $\langle \mathbf{0}, \boldsymbol{x} \rangle = 0$. □

Definition. The *length* $\|\boldsymbol{x}\|$ of a vector $\boldsymbol{x}$ in an inner product space is the non-negative real number

$$\|\boldsymbol{x}\| = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}.$$

Note that i) $\|\boldsymbol{x}\|$, is well defined and is zero only for the zero vector $\mathbf{0}$, ii) $\|c\,\boldsymbol{x}\| = |c|\,\|\boldsymbol{x}\|$.

Definition. A vector of unit length is called a *unit vector*. Replacing a nonzero vector $\boldsymbol{x}$ by the unit vector $\frac{1}{\|\boldsymbol{x}\|}\boldsymbol{x}$ is called its *normalization*.

Definition. The *distance* $\operatorname{dist}(\boldsymbol{x},\boldsymbol{y})$ between $\boldsymbol{x}$ and $\boldsymbol{y}$ is the non-negative real number $\operatorname{dist}(\boldsymbol{x},\boldsymbol{y}) = \|\boldsymbol{x}-\boldsymbol{y}\|$.

Examples.

1. Take $\mathbb{R}^3$ with the usual dot product. Let $\boldsymbol{x} = (3,0,4)$ and $\boldsymbol{y} = (3,3,0)$. Then $\|\boldsymbol{x}\| = 5$ and since $\boldsymbol{x}-\boldsymbol{y} = (0,-3,4)$, $\operatorname{dist}(\boldsymbol{x},\boldsymbol{y}) = 5$.

2. Let $V = C[0,1]$ with the inner product

$$\langle f, g\rangle = \int_0^1 f(x)g(x)dx.$$

If $f(x) = \cos 2\pi x$, its length

$$\|f\| = \langle f, f\rangle^{1/2} = \left(\int_0^1 \cos^2 2\pi x\, dx\right)^{1/2} = \left(\frac{1}{2\pi}\int_0^{2\pi} \cos^2 u\, du\right)^{1/2}$$

$$= \left(\frac{1}{2\pi}\int_0^{2\pi} \frac{\cos 2u + 1}{2}\, du\right)^{1/2} = \frac{1}{\sqrt{2}}.$$

The following inequality is a fundamental result.

Theorem. (Cauchy-Schwarz Inequality) *If $\boldsymbol{x}$, $\boldsymbol{y}$ are in an inner product space, then*

$$|\langle \boldsymbol{x}, \boldsymbol{y}\rangle| \le \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|. \tag{7.5}$$

Proof. If $\boldsymbol{x} = \boldsymbol{0}$, there is nothing to prove, as both sides of (7.5) are equal to zero.

So let $\boldsymbol{x} \ne \boldsymbol{0}$. Consider the parabola $s = f(t)$ where $f(t) = \|t\boldsymbol{x}+\boldsymbol{y}\|^2 = \langle t\boldsymbol{x}+\boldsymbol{y}, t\boldsymbol{x}+\boldsymbol{y}\rangle = \|\boldsymbol{x}\|^2t^2 + 2\langle \boldsymbol{x}, \boldsymbol{y}\rangle t + \|\boldsymbol{y}\|^2$. Since $\|t\boldsymbol{x}+\boldsymbol{y}\|^2 \ge 0$, the parabola $s = f(t)$ lies above the t-axis, hence the discriminant $d(f)$ of $f(t)$ satisfies

$$d(f) = 4(\langle \boldsymbol{x}, \boldsymbol{y}\rangle^2 - 4\|\boldsymbol{x}\|\,\|\boldsymbol{y}\|) \le 0$$

which gives (7.5).

The Cauchy-Schwarz Inequality allows us to define the angle between two nonzero vectors of an inner product space by

$$\langle \boldsymbol{x}, \boldsymbol{y}\rangle = \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|\cos\theta \tag{7.6}$$

□

Definition. The *angle* θ between two nonzero vectors $\boldsymbol{x}$, $\boldsymbol{y}$ in an inner product space is the number θ in the interval $[0, \pi]$ given by

$$\theta = \cos^{-1}\left(\frac{\langle \boldsymbol{x}, \boldsymbol{y}\rangle}{\|\boldsymbol{x}\|\,\|\boldsymbol{y}\|}\right). \tag{7.7}$$

Definition. Two vectors $\boldsymbol{x}$, $\boldsymbol{y}$ of an inner product space are *orthogonal*, written $\boldsymbol{x} \perp \boldsymbol{y}$, if $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = 0$. Moreover, if $\boldsymbol{x}$, $\boldsymbol{y}$ are both nonzero, we call them *perpendicular*.

Examples.

1. Let $V = \mathbb{R}^4$ with the usual dot product. The vectors $\boldsymbol{x} = (1, -1, 1, -1)$ and $\boldsymbol{y} = (1, 1, 1, 1)$ are orthogonal, because $\boldsymbol{x} \cdot \boldsymbol{y} = 0$. If we take $\boldsymbol{x} = (1, -1, 1, 1)$ and again $\boldsymbol{y} = (1, 1, 1, 1)$, $\langle \boldsymbol{x} \cdot \boldsymbol{y}\rangle = 2$, $\|\boldsymbol{x}\| = \|\boldsymbol{y}\| = 2$, so $\theta = \cos^{-1}\left(\frac{1}{2}\right) = \frac{\pi}{3}$.
2. Let $V = C[0, 1]$ with

$$\langle f, g\rangle = \int_0^1 f(x)g(x)dx.$$

To compute the angle θ between two functions $f(x) = 1$, $g(x) = x$, we have

$$\|f\|^2 = \int_0^1 f(x)f(x)dx = 1,$$

so $\|f\| = 1$, whereas

$$\|g\|^2 = \int_0^1 x^2 dx = \frac{1}{3}$$

gives $\|g\| = \frac{1}{\sqrt{3}}$.

On the other hand,

$$\langle f, g\rangle = \int_0^1 x dx = \frac{1}{2}.$$

Therefore,

$$\theta = \cos^{-1}\left(\frac{\sqrt{3}}{2}\right) = \frac{\pi}{6}.$$

EXERCISES

1. Does $\langle A, B\rangle = \operatorname{tr}(A^*B)$ define an inner product on the vector space $V = M(n, \mathbb{R})$? Justify your answer.

2. Does $\langle f, g\rangle = \int_0^1 (f(x) + g(x))dx$ define an inner product on the vector space of continuous functions $f : [0, 1] \to \mathbb{R}$? Explain!

3. If $\langle\ ,\ \rangle$ is an inner product and $c > 0$, show that $c\langle\ ,\ \rangle$ is also an inner product.

4. Show that two weighted dot products on $\mathbb{R}^n$ with weight vectors $(w_1, \ldots, w_n)$ and $(w'_1, \ldots, w'_n)$ are equivalent if and only if $(w'_1, \ldots, w'_n) = c(w_1, \ldots, w_n)$ for some $c > 0$.

5. Show that the angle between two vectors is the same under equivalent inner products on a given vector space.

6. Define on the vector space of continuous functions $f : \mathbb{R} \to \mathbb{R}$
$$\langle f, g\rangle_j = \int_0^{a_j} f(x)g(x)dx,\ j = (1, 2).$$
Are they inner products? If they are, are they equivalent?

7. Suppose $V = \mathbb{R}^4$ with the usual dot product. Let $\boldsymbol{x} = (1, 2, 3, 4)$. Find a vector $\boldsymbol{y}$ in $\mathbb{R}^4$ with integer coordinates such that the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$ is $\pi/6$.

8. In $\mathbb{R}^3$, define the *cross product* $\boldsymbol{x} \times \boldsymbol{y}$ of $\boldsymbol{x} = (x_1, x_2, x_3)$ and $\boldsymbol{y} = (y_1, y_2, y_3)$ by $\boldsymbol{x} \times \boldsymbol{y} = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$. Show that the length
$$\|\boldsymbol{x} \times \boldsymbol{y}\| = \|\boldsymbol{x}\|\,\|\boldsymbol{y}\|\,\sin\theta,$$
θ is the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$.

   Hint: Use the identity
$$(x_2y_3 - x_3y_2)^2 + (x_3y_1 - x_1y_3)^2 + (x_1y_2 - x_2y_1)^2 =$$
$$(x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) - (x_1y_1 + x_2y_2 + x_3y_3)^2$$
and equation (7.3).

9. Use 8 to show that $\|\boldsymbol{x} \times \boldsymbol{y}\|$ is the area of the parallelogram formed by $\boldsymbol{x}$ and $\boldsymbol{y}$, in particular, the area of the parallelogram formed by the vectors $\boldsymbol{x} = (a, b)$ and $\boldsymbol{y} = (c, d)$ in $\mathbb{R}^2$ is the absolute value of $ad - bc$.

10. Show that for the three vectors $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ in $\mathbb{R}^3$, the volume of the parallelepiped formed by them is $|\boldsymbol{x} \cdot (\boldsymbol{y} \times \boldsymbol{z})|$.

11. Show that the scalar $\boldsymbol{x} \cdot (\boldsymbol{y} \times \boldsymbol{z})$ is the determinant of the 3×3 matrix with rows $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$.

7.2 Fourier Series

If a real valued function $f(x)$ is periodic, of period say 2π (which can always be assumed by rescaling and the shift in the variable x), it is completely determined by its values on $[-\pi, \pi]$. Such periodic functions, if continuous, can be expressed in terms of trigonometric functions sine and cosine. A given periodic $f(x)$ of period 2π is not a (finite) linear combination of these functions, but is an infinite series. This is one of the most important tools in mathematics.

To begin with, let V be the vector space over $\mathbb{R}$ of all continuous functions $f : [-\pi, \pi] \to \mathbb{R}$ with the inner product

$$< f, g >= \int_{-\pi}^{\pi} f(x)g(x)dx.$$

The trigonometric functions alluded to above are

$$1, \cos x, \sin x, \cos 2x, \sin 2x, \ldots$$

The norm $\|1\| = \sqrt{2\pi}$ and $\sqrt{\pi}$ for all other functions (in this inner product). Let $f \in V$. The infinite series

$$a_0 + \sum_{m=1}^{\infty} (a_m \cos mx + b_m \sin mx) \tag{7.8}$$

whose terms are mutually orthogonal (see the Exercises in this section) is called the Fourier series or *Fourier expansion* of $f(x)$. By the theory of inner product spaces, the *Fourier coefficients* a_m, b_m are given by (see Section 7.3)

$$a_0 = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x)dx$$

and for $m > 0$,

$$\left.\begin{aligned} a_m &= \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos mx dx, \\ b_m &= \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin mx dx. \end{aligned}\right\} \tag{7.9}$$

The issue of the convergence of infinite series is beyond the scope of this book, so we shall not say anything more on this topic.

EXERCISES

Suppose m, n are integers and the inner product is as in this section. In 1–3 below, show that

1. $\cos mx \perp \sin nx$ for all m, n,
2. $\cos mx \perp \cos nx$ for $m \neq n$,
3. $\sin mx \perp \sin nx$ for $m \neq n$.
4. Compute $\|\cos mx\|$ for all $m \neq 0$.
5. Compute $\|\sin nx\|$ for all $n \neq 0$.

7.3 Orthogonal and Orthonormal Sets

For the sake of simplicity and motivation, consider the Euclidean plane $V = \mathbb{R}^2$. Any set $\mathcal{B} = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ of two linearly independent vectors in V is a basis of V, so that a vector $\boldsymbol{v}$ in V has a unique representation

$$\boldsymbol{v} = x_1\boldsymbol{v}_1 + x_2\boldsymbol{v}_2,$$

which is abbreviated as $\boldsymbol{v} = (x_1, x_2)_{\mathcal{B}}$. But why do we prefer $\boldsymbol{v}_1 = \boldsymbol{i} = (1,0)$ and $\boldsymbol{v}_2 = \boldsymbol{j} = (0,1)$? It is because $\{\boldsymbol{i}, \boldsymbol{j}\}$ is an "orthonormal" basis (basis vectors are unit and perpendicular to each other). So what? The answer is that in the representation

$$\boldsymbol{v} = x\boldsymbol{i} + y\boldsymbol{j},$$

for $\boldsymbol{v} = (x, y)$, $x = \boldsymbol{v} \cdot \boldsymbol{i}$, $y = \boldsymbol{v} \cdot \boldsymbol{j}$. In other words, the coordinates of $\boldsymbol{v}$ along $\boldsymbol{i}$ and $\boldsymbol{j}$ are just the dot products of $\boldsymbol{v}$ with $\boldsymbol{i}$ and $\boldsymbol{j}$, respectively. This brings us to an important concept in the study of inner product spaces.

Definition. A set of nonzero vectors $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r\}$ in an inner product space V is an *orthogonal set* if $\boldsymbol{v}_i \perp \boldsymbol{v}_j$ for $i \neq j$.

Definition. An orthogonal set is an *orthonormal set* if each vector in it is a unit vector.

Examples.

1. The set $\{(1,1,1,1), (1,-1,1,-1)\}$ is an orthogonal set in $\mathbb{R}^4$ but it is not orthonormal.

2. If $\boldsymbol{e}_1 = (1,0,\ldots,0), \ldots, \boldsymbol{e}_n = (0,\ldots,0,1)$, then $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ is an orthonormal set in $\mathbb{R}^n$ with the usual dot product on it.

3. For any real number θ, $\{(\cos\theta, \sin\theta), (-\sin\theta, \cos\theta)\}$ is an orthonormal set in $\mathbb{R}^2$.

Theorem. (Linear Independence of Orthogonal Vectors) *A set of mutually perpendicular vectors is a linearly independent set.*

Proof. Suppose $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_r$ are mutually perpendicular and

$$c_1\boldsymbol{v}_1 + \cdots + c_r\boldsymbol{v}_r = \mathbf{0}.$$

Then for each $j = 1, \ldots, n$,

$$\begin{aligned} 0 = \langle 0, \boldsymbol{v}_j\rangle &= \langle c_1\boldsymbol{v}_1 + \cdots + c_r\boldsymbol{v}_r, \boldsymbol{v}_j\rangle \\ &= c_1\langle \boldsymbol{v}_1, \boldsymbol{v}_j\rangle + \cdots + c_j\langle \boldsymbol{v}_j, \boldsymbol{v}_j\rangle + \cdots + c_r\langle \boldsymbol{v}_r, \boldsymbol{v}_j\rangle \\ &= c_j\langle \boldsymbol{v}_j, \boldsymbol{v}_j\rangle, \end{aligned}$$

because for $i \neq j$, $\langle \boldsymbol{v}_i, \boldsymbol{v}_j\rangle = 0$. Since $\langle \boldsymbol{v}_j, \boldsymbol{v}_j\rangle \neq 0$, $c_j = 0$. □

Corollary. *An orthogonal set of $n = \dim V$ nonzero vectors in an inner product space V forms a basis of V.*

Definition. A basis consisting of orthogonal (resp. orthonormal) vectors is an *orthogonal basis* (resp. *orthonormal basis*).

Theorem 7.2. *The j-th coordinate of a vector $\boldsymbol{v}$ relative to an orthogonal basis $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is $\frac{\langle \boldsymbol{v}, \boldsymbol{v}_j\rangle}{\langle \boldsymbol{v}_j, \boldsymbol{v}_j\rangle}$. In particular, if $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is orthonormal, then it is $\langle \boldsymbol{v}, \boldsymbol{v}_j\rangle$.*

Proof. If $\boldsymbol{v} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$, then $\langle \boldsymbol{v}, \boldsymbol{v}_j\rangle = \langle c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n, \boldsymbol{v}_j\rangle = c_j\langle \boldsymbol{v}_j, \boldsymbol{v}_j\rangle$, which proves the theorem. □

Now we show that any subspace of a finite dimensional inner product space possesses an orthonormal basis. It is enough to prove that it has an orthogonal basis, because then each basis vector can be normalized. The main idea is the following definition suggested by the fact that in $\mathbb{R}^2$, $x\boldsymbol{i}$ is the orthogonal projection of $\boldsymbol{v} = (x, y)$ on $\boldsymbol{i}$, and that $\boldsymbol{v} - x\boldsymbol{i} = y\boldsymbol{j}$ is orthogonal to $x\boldsymbol{i}$.

Definition. Let $\boldsymbol{v}$ be a nonzero vector in an inner product space V and $\boldsymbol{x} \in V$. The *orthogonal projection* of $\boldsymbol{x}$ on $\boldsymbol{v}$ is the vector

$$\text{proj}_{\boldsymbol{v}}(\boldsymbol{x}) = \frac{\langle \boldsymbol{x}, \boldsymbol{v}\rangle}{\langle \boldsymbol{v}, \boldsymbol{v}\rangle}\,\boldsymbol{v}.$$

In particular for $\boldsymbol{u}$ unit,

$$\text{proj}_{\boldsymbol{u}}(\boldsymbol{x}) = \langle \boldsymbol{x}, \boldsymbol{u}\rangle\boldsymbol{u}.$$

Definition. The scalar $\langle \boldsymbol{x}, \boldsymbol{u} \rangle$ is called the *component* or *coordinate* of $\boldsymbol{x}$ along $\boldsymbol{u}$ and we write it as $\operatorname{comp}_{\boldsymbol{u}}(\boldsymbol{x})$.

Examples.

1. In $\mathbb{R}^3$, $(\boldsymbol{v} \cdot \boldsymbol{i})\, \boldsymbol{i} = x\boldsymbol{i}$ for $\boldsymbol{v} = (x, y, z)$ is the orthogonal projection of $\boldsymbol{v}$ on $\boldsymbol{i}$.

2. Let $V = \mathbb{R}^n$ with the usual dot product, $\boldsymbol{x} = (1, 2, \ldots, n)$, $\boldsymbol{v} = (1, \ldots, 1)$. It is easy to check that

$$\operatorname{proj}_{\boldsymbol{v}}(\boldsymbol{x}) = \frac{n+1}{2}\,(1, \ldots, 1).$$

Theorem 7.3. *If $\boldsymbol{x}$ is not a linear multiple of $\boldsymbol{v} \neq \boldsymbol{0}$, then $\boldsymbol{x} - \operatorname{proj}_{\boldsymbol{v}}(\boldsymbol{x})$ is perpendicular to $\boldsymbol{v}$.*

Proof. $\langle (\boldsymbol{x} - \operatorname{proj}_{\boldsymbol{v}}(\boldsymbol{x})), \boldsymbol{v} \rangle = \langle \boldsymbol{x}, \boldsymbol{v} \rangle - \dfrac{\langle \boldsymbol{x}, \boldsymbol{v} \rangle}{\langle \boldsymbol{v}, \boldsymbol{v} \rangle} \langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0.$ □

Theorem 7.3 leads to an algorithm to produce an orthogonal basis, called the Gram-Schmidt Process.

7.4 Gram-Schmidt Process

The *Gram-Schmidt Process* is an algorithm to obtain an orthonormal basis from a given one.

Let $\mathcal{B} = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ be a given basis of a finite dimensional subspace W of an inner product space V, V not necessarily finite dimensional. Put

$$\begin{aligned}
\boldsymbol{v}_1 &= \boldsymbol{x}_1 \\
\boldsymbol{v}_2 &= \boldsymbol{x}_2 - \frac{\langle \boldsymbol{x}_2, \boldsymbol{v}_1 \rangle}{\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle} \boldsymbol{v}_1, \\
\boldsymbol{v}_3 &= \boldsymbol{x}_3 - \frac{\langle \boldsymbol{x}_3, \boldsymbol{v}_1 \rangle}{\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle} \boldsymbol{v}_1 - \frac{\langle \boldsymbol{x}_3, \boldsymbol{v}_2 \rangle}{\langle \boldsymbol{v}_2, \boldsymbol{v}_2 \rangle} \boldsymbol{v}_2, \\
&\vdots \\
\boldsymbol{v}_n &= \boldsymbol{x}_n - \frac{\langle \boldsymbol{x}_n, \boldsymbol{v}_1 \rangle}{\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle} \boldsymbol{v}_1 - \cdots - \frac{\langle \boldsymbol{x}_n, \boldsymbol{v}_{n-1} \rangle}{\langle \boldsymbol{v}_{n-1}, \boldsymbol{v}_{n-1} \rangle} \boldsymbol{v}_{n-1}.
\end{aligned}$$

It is clear that each $\boldsymbol{v}_j$ is orthogonal to $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{j-1}$. Hence $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ is an orthogonal basis of W. Now normalize each $\boldsymbol{v}_1$ to obtain an orthonormal basis of W.

Examples.

1. $V = \mathbb{R}^3$ with the usual dot product. Let

$$\boldsymbol{x}_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \boldsymbol{x}_2 = \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix}, \boldsymbol{x}_3 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

Then an orthogonal basis of V is

$$\boldsymbol{v}_1 = \boldsymbol{x}_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$\begin{aligned} \boldsymbol{v}_2 &= \boldsymbol{x}_2 - \frac{\boldsymbol{x}_2 \cdot \boldsymbol{v}_1}{\boldsymbol{v}_1 \cdot \boldsymbol{v}_1}\, \boldsymbol{v}_1 \\ &= \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \frac{3}{2} \begin{pmatrix} -1 \\ +1 \\ 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \boldsymbol{v}_3 &= \boldsymbol{x}_3 - \frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_1}{\boldsymbol{v}_1 \cdot \boldsymbol{v}_1}\, \boldsymbol{v}_1 - \frac{\boldsymbol{x}_3 \cdot \boldsymbol{v}_2}{\boldsymbol{v}_2 \cdot \boldsymbol{v}_2}\, \boldsymbol{v}_2 \\ &= \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} - \frac{3}{2} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}. \end{aligned}$$

By normalizing this orthogonal basis, we obtain the following orthonormal basis of V.

$$\boldsymbol{u}_1 = \frac{1}{\|\boldsymbol{v}_1\|} \cdot \boldsymbol{v}_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}, \text{ similarly } \boldsymbol{u}_2 = \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ +\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}, \ \boldsymbol{u}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

2. Let $V = C[0,1]$ with the inner product

$$\langle f, g \rangle = \int_0^1 f(x)g(x)dx.$$

Let W be the span of $f_1(x) = 1$, $f_2(x) = x$. We put $g_1(x) = f_1(x) = 1$.

$$g_2(x) = f_2 - \frac{\langle f_2, g_1 \rangle}{\langle g_1, g_1 \rangle}\, g_1.$$

Now

$$\langle f_2, g_1\rangle = \int_0^1 x\,dx = \frac{1}{2},\ \langle g_1, g_1\rangle = \int_0^1 1\,dx = 1.$$

So $g_2(x) = x - \frac{1}{2}$, and we have an orthogonal basis $\left\{1, x - \frac{1}{2}\right\}$ of W. Again $\|g_1\|^2 = \langle g_1, g_1\rangle = 1$, so $\|g_1\| = 1$, and $\|g_2\|^2 = \int_0^1 \left(x - \frac{1}{2}\right)^2 dx = \frac{1}{12}$, so $\|g_2\| = \sqrt{\frac{1}{12}}$. An orthonormal basis of W is $\{u_1(x), u_2(x)\}$, where $u_1(x) = 1$, $u_2(x) = 2\sqrt{3}\,\left(x - \frac{1}{2}\right)$.

QR Factorization

An immediate consequence of a slight variation of the Gram-Schmidt process is the so-called QR factorization of an $m \times n$ matrix A with linearly independent columns (hence $m \geq n$). One obtains from the linearly independent columns $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ of A, an orthonormal basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ of the column space of A. Since $\boldsymbol{x}_j$ is in span$\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j\}$,

$$\boldsymbol{x}_j = r_{1j}\boldsymbol{u}_1 + \cdots + r_{jj}\boldsymbol{u}_j, \quad j = 1, \ldots, m.$$

If necessary, replacing $\boldsymbol{u}_j$ by $-\boldsymbol{u}_j$, we may assume $r_{jj} \geq 0$. If we put

$$\boldsymbol{r}_j = \begin{pmatrix} r_{1j} \\ \vdots \\ r_{jj} \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

then $\boldsymbol{x}_j = Q\boldsymbol{r}_j$ where Q is the matrix with columns $\boldsymbol{u}_j$. This gives

$$\boxed{A = QR} \tag{7.10}$$

with R the $m \times m$ upper diagonal matrix (r_{ij}). The equation (7.10) is a *QR-factorization* (or *decomposition*) of A.

Example. Take $A = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}$ so that $\boldsymbol{x}_1 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ and $\boldsymbol{x}_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$. By the Gram-Schmidt Process we obtain orthonormal basis vectors

$$\boldsymbol{u}_1 = \begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix} \text{ and } \boldsymbol{u}_2 = \begin{pmatrix} \frac{4}{5} \\ -\frac{3}{5} \end{pmatrix}$$

Now

$$\boldsymbol{x}_1 = 5\boldsymbol{u}_1 + 0\boldsymbol{u}_2,$$

$$\boldsymbol{x}_2 = 2\boldsymbol{u}_1 + 1\boldsymbol{u}_2.$$

Therefore, $R = \begin{pmatrix} 5 & 2 \\ 0 & 1 \end{pmatrix}$. It can be checked that $A = QR$ where $Q = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & -\frac{3}{5} \end{pmatrix}$.

EXERCISES

1. Let $V = R^4$ with the usual dot product. Find an orthogonal set of four vectors in V, each vector with at least three nonzero components. Check your answer.

2. Let V be the (infinite dimensional) vector space of polynomials with real coefficients. Find two non-constant perpendicular polynomials in V, if V is equipped with the inner product

$$\langle f, g \rangle = \int_0^1 f(x)g(x)\,dx.$$

3. Use the Gram-Schmidt Process to obtain an orthonormal basis of $\mathbb{R}^2$ from $\binom{1}{1}$, $\binom{1}{2}$.

4. Give an example of an inner product space having an infinite orthogonal set.

5. Use the Gram-Schmit Process to find an orthonormal basis of the row space of the matrix

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

6. Use the Gram-Schmidt Process to construct an orthonormal basis of the subspace W of $\mathbb{R}^4$ spanned by

$$\begin{pmatrix} 4 \\ -1 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 5 \\ 1 \end{pmatrix}.$$

7. Let V be as in Exercise 2 above. Use the Gram-Schmidt to construct an orthonormal basis of the subspace W of V spanned by $f_1(x) = x$, $f_2(x) = x^3$.

8. Find the QR-decomposition of the matrix A in Exercise 5.

7.5 Orthogonal Projections on Subspaces

We begin with the following:

Definition. Let W be a subspace of an inner product space V. The *orthogonal complement* of W in V is the set

$$W^\perp = \{\boldsymbol{v} \in V \mid \langle \boldsymbol{v}, \boldsymbol{w} \rangle = 0 \text{ for all } \boldsymbol{w} \text{ in } W\}.$$

Examples. Let L be a line and W a plane in $\mathbb{R}^3$ both through the origin O. Then $L^\perp$ is the plane through O with normal L and $W^\perp$ is a line through O perpendicular to W.

Theorem 7.4. *Let V be a finite dimensional inner product space and W a subspace of V. Then*

1) $W^\perp$ is a subspace of V,

2) $W \cap W^\perp = \{\mathbf{0}\}$, and

3) $V = W \oplus W^\perp$.

Remark. Part 3) above is another way of saying that each $\boldsymbol{v}$ in V is a unique sum $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{z}$ with $\boldsymbol{w}$ in W and $\boldsymbol{z}$ in $W^\perp$. We say that V is a *direct sum* of W and $W^\perp$.

Proof.

1) is obvious.

2) If $\boldsymbol{v} \in W \cap W^\perp$, then $\langle \boldsymbol{v}, \boldsymbol{v} \rangle = 0$ implies that $\boldsymbol{v} = \mathbf{0}$.

3) Let $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$ be an orthonormal basis of W. Enlarge it to an orthonormal basis $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n\}$ of V. Given $\boldsymbol{v}$ in V, let $\boldsymbol{v} = c_1\boldsymbol{w}_1 + \cdots + c_n\boldsymbol{w}_n$. Take $\boldsymbol{w} = c_1\boldsymbol{w}_1 + \cdots + c_r\boldsymbol{w}_r$ and $\boldsymbol{z} = c_{r+1}\boldsymbol{w}_{r+1} + \cdots + c_n\boldsymbol{w}_n$.

To prove uniqueness, suppose $\boldsymbol{v} = \boldsymbol{w}_1 + \boldsymbol{z}_1 = \boldsymbol{w}_2 + \boldsymbol{z}_2$ with $\boldsymbol{w}_1$, $\boldsymbol{w}_2$ in W and $\boldsymbol{z}_1$, $\boldsymbol{z}_2$ in $W^\perp$. Then $\boldsymbol{w}_1 - \boldsymbol{w}_2 = \boldsymbol{z}_2 - \boldsymbol{z}_1$ is in both W and $W^\perp$. Hence by 2), $\boldsymbol{w}_1 - \boldsymbol{w}_2 = \boldsymbol{z}_2 - \boldsymbol{z}_1 = 0$, i.e. $\boldsymbol{w}_1 = \boldsymbol{w}_2$ and $\boldsymbol{z}_1 = \boldsymbol{z}_2$. □

Corollary. *If W is a subspace of an inner product space V, then* $\dim V = \dim W + \dim W^\perp$.

Theorem 7.5. *The row rank and the column rank of an $m \times n$ matrix A are equal.*

Proof. If necessary, by adding enough number of rows or columns of zeros at the end, we may assume that $m = n$. Consider $\mathbb{R}^n$ with dot product. We write vectors in $\mathbb{R}^n$ as column vectors. Let W be the row space of A. Then

$W^\perp$ is the solution space of $A\boldsymbol{x} = \boldsymbol{0}$, also called the *null-space* of A. By the corollary, $n =$ row rank of $A + \dim W^\perp$. On the other hand, the image of the linear map $\boldsymbol{x} \to A\boldsymbol{x} = x_1\boldsymbol{c}_1 + \cdots + x_n\boldsymbol{c}_n$, $\boldsymbol{c}_j$ being the j-th column of A, is the column space of A. Therefore, since $W^\perp$ is also the kernel of this map, by Theorem 4.4, $n =$ column rank of $A + \dim W^\perp$. This proves that the row rank of $A =$ the column rank of A. □

Remark. The corollary above may now be rephrased as follows:

If A is an $m \times n$ matrix, its row rank plus nullity is equal to n, the number of its columns. Recall that the nullity of A is the dimension of its null space $\mathrm{Null}(A)$, i.e. the solution space of $A\boldsymbol{x} = \boldsymbol{0}$.

Definition. Let W be a subspace of an inner product space V and $\boldsymbol{v}$ in V. Write $\boldsymbol{v}$ uniquely as $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{z}$ with $\boldsymbol{w}$ in W and $\boldsymbol{z}$ in $W^\perp$. Then $\boldsymbol{w}$ is called the *projection* of $\boldsymbol{v}$ on W, denoted by $\mathrm{proj}_W(\boldsymbol{v})$.

The following is now obvious

Theorem. *If* $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_r\}$ *is an orthogonal basis of* W *and* $\boldsymbol{v} \in V$, *then*

$$\mathrm{proj}_W(\boldsymbol{v}) = \frac{\langle \boldsymbol{v}, \boldsymbol{w}_1 \rangle}{\langle \boldsymbol{w}_1, \boldsymbol{w}_1 \rangle}\,\boldsymbol{w}_1 + \cdots + \frac{\langle \boldsymbol{v}, \boldsymbol{w}_r \rangle}{\langle \boldsymbol{w}_r, \boldsymbol{w}_r \rangle}\,\boldsymbol{w}_r.$$

We now state and prove some facts from high school geometry.

Theorem. (Pythagoras) *Suppose* $\boldsymbol{x}$, $\boldsymbol{y}$ *are two orthogonal vectors in an inner product space* V. *Then*

$$\|\boldsymbol{x} + \boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2.$$

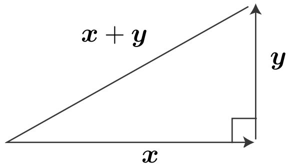


FIGURE 7.2: For Pythagoras' Theorem

Proof. Since $\boldsymbol{x} \perp \boldsymbol{y}$ (cf. Figure 7.2), $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$. Hence

$$\begin{aligned} \|\boldsymbol{x} + \boldsymbol{y}\|^2 &= \langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{y} \rangle \\ &= \langle \boldsymbol{x}, \boldsymbol{x} \rangle + 2\langle \boldsymbol{x}, \boldsymbol{y} \rangle + \langle \boldsymbol{y}, \boldsymbol{y} \rangle \\ &= \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2. \end{aligned}$$ □

Triangle Inequality

Theorem (Triangle Inequality)**.** *For $\boldsymbol{x}$, $\boldsymbol{y}$ in an inner product space,*

$$\|\boldsymbol{x}+\boldsymbol{y}\| \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|.$$

Proof. Considering $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{x}+\boldsymbol{y}$ as the three sides of a triangle (cf. Figure 7.3, we have

$$\begin{aligned}\|\boldsymbol{x}+\boldsymbol{y}\|^2 &= \langle \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}\rangle \\ &= \|\boldsymbol{x}\|^2 + 2\langle \boldsymbol{x}, \boldsymbol{y}\rangle + \|\boldsymbol{y}\|^2 \\ &\leq \|\boldsymbol{x}\|^2 + 2\|\boldsymbol{x}\|\,\|\boldsymbol{y}\| + \|\boldsymbol{y}\|^2 (\text{Cauchy-Schwarz Inequality}) \\ &= (\|\boldsymbol{x}\| + \|\boldsymbol{y}\|)^2.\end{aligned}$$

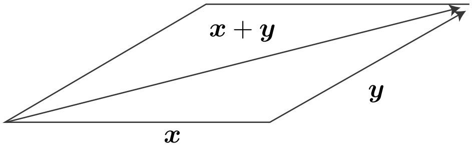


FIGURE 7.3: Cauchy-Schwarz Inequality

□

Theorem 7.6. *Let $\boldsymbol{p} = \text{proj}_W(\boldsymbol{v})$ and $\boldsymbol{w} \in W$. Then $\|\boldsymbol{v}-\boldsymbol{p}\| \leq \|\boldsymbol{w}-\boldsymbol{p}\|$.*

Remark. The theorem says that $\boldsymbol{v}$ is closer to $\boldsymbol{p}$ than to any other vector $\boldsymbol{w}$ in W.

Proof. The vector $\boldsymbol{p}-\boldsymbol{w}$ is in W, whereas $\boldsymbol{v}-\boldsymbol{p}$ is orthogonal to W. Therefore, by Pythagoras' theorem,

$$\begin{aligned}\|\boldsymbol{v}-\boldsymbol{w}\|^2 &= \|(\boldsymbol{v}-\boldsymbol{p}) + (\boldsymbol{p}-\boldsymbol{w})\|^2 \\ &= \|\boldsymbol{v}-\boldsymbol{p}\|^2 + \|\boldsymbol{p}-\boldsymbol{w}\|^2,\end{aligned}$$

which shows that

$$\|\boldsymbol{v}-\boldsymbol{p}\| \leq \|\boldsymbol{v}-\boldsymbol{w}\|.$$

□

Inconsistent Systems of Linear Equations

For an application of the above discussion, we take $V = \mathbb{R}^n$ with the usual dot product. Consider a system

$$A\boldsymbol{x} = \boldsymbol{b} \tag{7.11}$$

of m linear equations in n variables. For randomly chosen A and $\boldsymbol{b}$, (7.11) is usually inconsistent, in which case the next best thing is to find a vector $\hat{\boldsymbol{x}}$ in $\mathbb{R}^n$ such that $A\hat{\boldsymbol{x}}$ is as close to $\boldsymbol{b}$ as possible. In other words, $\|\boldsymbol{b} - A\hat{\boldsymbol{x}}\|$ is as small as possible. If $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n$ are the columns of A, and $\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, then (7.11) can be rewritten as

$$\boldsymbol{b} = x_1\boldsymbol{c}_1 + \cdots + x_n\boldsymbol{c}_n. \tag{7.12}$$

If $W = \operatorname{span}\{\boldsymbol{c}_1, \ldots, \boldsymbol{c}_n\}$, then (7.11) is consistent if and only if $\boldsymbol{b}$ is in W. Otherwise, the best approximation to $\boldsymbol{b}$ in W is the $\operatorname{proj}_W(\boldsymbol{b})$, called the *least squares approximation* (as it involves taking the least sum of squares), for which we need to find a vector $\hat{\boldsymbol{x}}$ in $\mathbb{R}^n$, such that

$$A\hat{\boldsymbol{x}} = \operatorname{proj}_W(\boldsymbol{b}). \tag{7.13}$$

But (7.13) holds $\Leftrightarrow$ $\boldsymbol{b} - A\hat{\boldsymbol{x}}$ is orthogonal to every column of A, i.e.

$$A^*(\boldsymbol{b} - A\hat{\boldsymbol{x}}) = \boldsymbol{0},$$

or

$$A^*A\hat{\boldsymbol{x}} = A^*\boldsymbol{b}. \tag{7.14}$$

Hence $\hat{\boldsymbol{x}}$ is a solution of (7.14) which, by construction always exists.

In many applications, the columns of A are linearly independent, in which case the following result is relevant.

Theorem 7.7. *Suppose A is an $m \times n$ matrix. The columns of A are linearly independent if and only if A^*A is invertible.*

Proof. It is enough to show that

$$A^*A\boldsymbol{x} = \boldsymbol{0} \tag{7.15}$$

has a non-trivial solution if and only if

$$A\boldsymbol{x} = x_1\boldsymbol{c}_1 + \cdots + x_n\boldsymbol{c}_n = \boldsymbol{0}, \tag{7.16}$$

has a non-trivial solution.

If $\boldsymbol{x}$ is a non-trivial solution of $A\boldsymbol{x} = \boldsymbol{0}$, then obviously it is also a non-trivial solution of $A^*A\boldsymbol{x} = \boldsymbol{0}$.

Conversely, a non-trivial solution of $A^*A\boldsymbol{x} = \boldsymbol{0}$ gives

$$\boldsymbol{x}^*A^*A\boldsymbol{x} = \boldsymbol{0}$$

or

$$(A\boldsymbol{x})^*(A\boldsymbol{x}) = \boldsymbol{0},$$

i.e. $\|A\boldsymbol{x}\| = 0$. So $A\boldsymbol{x} = \boldsymbol{0}$, and (7.16) has a non-trivial solution. □

Projection Matrix

Suppose W is a subspace of $\mathbb{R}^m$ with $\dim W = n$. We write the vectors in $\mathbb{R}^m$ as columns. Let $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ be a basis of W. If A is the $m \times n$ matrix with $\boldsymbol{a}_j$ as its columns, then the $n \times n$ matrix A^*A is invertible. For any $\boldsymbol{b}$ in $\mathbb{R}^m$, the projection $\mathrm{proj}_W(\boldsymbol{b})$ of $\boldsymbol{b}$ on W is given by $\mathrm{proj}_W(\boldsymbol{b}) = A\hat{\boldsymbol{x}}$, where $\hat{\boldsymbol{x}}$ is a solution of

$$A^*A\hat{\boldsymbol{x}} = A^*\boldsymbol{b}$$

i.e.

$$\hat{\boldsymbol{x}} = (A^*A)^{-1}A^*\boldsymbol{b}. \tag{7.17}$$

Therefore,

$$\begin{aligned}\mathrm{proj}_W(\boldsymbol{b}) &= A\hat{\boldsymbol{x}} \\ &= A(A^*A)^{-1}A^*\boldsymbol{b}.\end{aligned}$$

Definition. The $m \times m$ matrix $P = A(A^*A)^{-1}A^*$ is the *projection matrix* of $\mathbb{R}^m$ on W.

Example. Let W be the subspace of $\mathbb{R}^3$ spanned by

$$\begin{pmatrix}1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\2\end{pmatrix}.$$

Then one can easily compute that the projection matrix

$$P = A(A^*A)^{-1}A^* = \frac{1}{6}\begin{pmatrix}5 & 2 & -1\\ 2 & 2 & 2\\ -1 & 2 & 5\end{pmatrix}.$$

Check that $P^2 = P$, because the projection of the projection is projection itself.

Example. To find the least squares solution to

$$\begin{aligned} x + y &= 3 \\ -2x + 3y &= 1 \\ 2x - y &= 2 \end{aligned}$$

we have $A = \begin{pmatrix}1 & 1\\ -2 & 3\\ 2 & -1\end{pmatrix}$, $\boldsymbol{b} = \begin{pmatrix}3\\1\\2\end{pmatrix}$. So $A^*A = \begin{pmatrix}9 & -7\\ -7 & 11\end{pmatrix}$, $A^*\boldsymbol{b} = \begin{pmatrix}5\\4\end{pmatrix}$. Solving $A^*A\hat{\boldsymbol{x}} = A^*\boldsymbol{b}$, i.e.

$$\begin{pmatrix}9 & -7\\ -7 & 11\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}5\\4\end{pmatrix},$$

we get $\hat{\boldsymbol{x}} = \begin{pmatrix}83/50\\71/50\end{pmatrix}$.

Least Squares Fit

Given a data (record of an experiment–say, the highest temperatures on different days of a year) of a given quantity against another:

x	x_1	x_2	x_3	$\cdots$	x_m
y	y_1	y_2	y_3	$\cdots$	y_m

we would like to find a polynomial function $y = f(x) = c_0 + c_1 x + \cdots + c_n x^n$, called the *least square fit*, whose graph approximates the data as close as possible. For that we have a system of linear equations

$$\left.\begin{aligned} &c_0 + c_1 x_1 + \cdots + c_n x_1^n = y_1 \\ &c_0 + c_1 x_2 + \cdots + c_n x_2^n = y_2 \\ &\vdots \\ &c_0 + c_1 x_m + \cdots + c_n x_m^n = y_m \end{aligned}\right\} \tag{7.18}$$

or

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & & & & \\ 1 & x_m & x_m^2 & \cdots & x_m^n \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

which we need to solve for $c_0, c_1, \ldots, c_n$ to find $f(x)$. This is just solving the matrix equation

$$A\hat{\boldsymbol{x}} = \boldsymbol{b}.$$

If we assume that $n = \deg f(x) < m$, A has linearly independent columns. This is so because in an experiment, $x_1, \ldots, x_m$ are all distinct, so the first n columns of A are the first n columns of the $m \times m$ van der Monde determinant $\det(x_i^j)$, which is nonzero by our assumption on x_j.

Example. Let the given data be

x	0	1	2	3
y	3	2	4	4

Then for $n = 2$ (quadratic fit) (7.18) is

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 4 \\ 4 \end{pmatrix}.$$

If we write it as $A\hat{\boldsymbol{x}} = \boldsymbol{b}$, then $A^* A\hat{\boldsymbol{x}} = A^*\boldsymbol{b}$ becomes

$$\begin{pmatrix} 4 & 6 & 14 \\ 6 & 14 & 36 \\ 14 & 36 & 98 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 13 \\ 22 \\ 54 \end{pmatrix}.$$

Solving this for c_0, c_1, c_2 we get

$$f(x) = c_0 + c_1 x + c_2 x^2 = \frac{11}{4} - \frac{1}{4}\,x + \frac{1}{4}\,x^2.$$

EXERCISES

1. Find the least squares solution to $A\boldsymbol{x} = \boldsymbol{b}$ if

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \\ -1 & 2 \end{pmatrix}, \quad \boldsymbol{b} = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}.$$

2. Find a least squares fit by a linear function to the data

x	-1	0	1	2
y	0	0	3	9

3. Find a parabolic (or quadratic) least squares fit to the data

x	-3	-2	0	1
y	9	6	2	1

4. Find a parabolic least squares fit to the data

x	2	3	5	6
y	0	-10	-48	-70

5. Find a cubic least squares fit to the data

x	-1	0	1	2	3
y	-14	-5	-4	1	22

6. Show that rank $A^*A = \operatorname{rank} A$.

8

Linear Algebra over the Field of Complex Numbers

Linear algebra over the field of real numbers is not always adequate. For example, we already had to deal with complex numbers while looking for the eigenvalues of the matrix

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

which are the roots of its characteristic polynomial $\chi_{_A}(\lambda) = \lambda^2 + 1$. These are clearly a pair of imaginary numbers i and $-i$. In general, when A is real, its characteristic polynomial has real coefficients. Since the imaginary roots of polynomials with real coefficients occur in pairs, so do the eigenvectors belonging to imaginary eigenvalues. The extra effort involved in working with complex numbers is compensated somewhat by the fact that one needs to find only one member of a pair of complex eigenvectors. The other is given by its complex conjugate. For this chapter it is necessary to have a functional knowledge of complex numbers which, for the reader's convenience, we summarize here.

8.1 Algebra of Complex Numbers

A *complex number* is a number $z = a + ib$, where a, b are real and $i = \sqrt{-1}$ or equivalently, $i^2 = -1$. We call a the real part of z, b the imaginary part of z, and write $a = \mathrm{Re}(z)$, $b = \mathrm{Im}(z)$. The field $\mathbb{C}$ of complex numbers may be viewed as a vector space over $\mathbb{R}$ with $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. As such, it is identified with the Euclidean plane $\mathbb{R}^2$ and is called the *complex plane*. A complex number $z = a+ib$ is then identified with the point (a, b) in $\mathbb{R}^2$. The sum of two complex numbers $a_1 + ib_1$ and $a_2 + ib_2$ is what corresponds to their vector sum in $\mathbb{R}^2$, i.e.

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2).$$

The Euclidean plane $\mathbb{R}^2$ has no multiplicative structure, whereas $\mathbb{C}$ does. The product of $a_1 + ib_1$ and $a_2 + ib_2$ is defined by multiplying them formally and using the fact that $i^2 = -1$, i.e.

$$(a_1 + ib_1) \cdot (a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1).$$

The *absolute value* (*length*, *modulus* or *norm*) of a complex number $z = a+ib$, is its length as a vector in $\mathbb{R}^2$, i.e.

$$|z| = r = \sqrt{a^2 + b^2},$$

whereas for $z \neq 0$, its *argument* $\arg(z)$ is the angle θ it makes with the x-axis (see Figure 8.1).

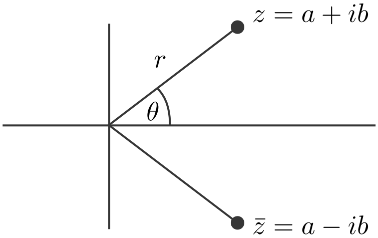


FIGURE 8.1: Complex conjugates

In other words, $\theta = \tan^{-1}\left(\frac{b}{a}\right)$, assuming $a \neq 0$, but we always have $z = r(\cos\theta + i\sin\theta)$.

The *complex conjugate* $\bar{z}$ of $z = a + ib$ is defined by (see Figure 8.1)

$$\bar{z} = a - ib.$$

Note that $\bar{a} = a$ for real a. It is also easy to see that

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \tag{8.1}$$

and

$$\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}\,. \tag{8.2}$$

Since $|z|^2 = z\bar{z}$, it follows that $|z_1z_2| = |z_1|\,|z_2|$. Clearly, $z \cdot \bar{z} = a^2 + b^2 \geq 0$ and $= 0$ if and only if $z = 0$, i.e. $\mathrm{Re}(z) = \mathrm{Im}(z) = 0$. In particular, if $z \neq 0$,

$$\frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\,i.$$

To shorten calculations, it may be convenient to record and remember it as a useful formula: For $z = a + ib \neq 0$,

$$\frac{1}{z} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\,i. \tag{8.3}$$

Roots of Unity

What makes the identification of complex numbers with points of the Euclidean plane indispensable is how the complex numbers z_1, z_2 behave under multiplication. To see this, write

$$\begin{aligned} z_1 &= r_1(\cos\theta_1 + i\sin\theta_1), \\ z_2 &= r_2(\cos\theta_2 + i\sin\theta_2). \end{aligned}$$

Then

$$z_1 z_2 = r_1 r_2[(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1)]$$

or

$$z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \tag{8.4}$$

This shows that

$$|z_1 z_2| = |z_1|\,|z_2| \tag{8.5}$$

$$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2). \tag{8.6}$$

Note that the last equation is true only modulo a multiple of 2π.

As a special case of (8.5), if $|z_1| = |z_2| = 1$, then $|z_1 z_2| = 1$ and $\left|\frac{1}{z}\right| = |1|$, if $|z| = 1$.

Thus, in the language of group theory,

$$G = \{z \in \mathbb{C} \mid |z| = 1\}$$

forms an Abelian group under multiplication of complex numbers.

A special case of (8.4) is the so-called De Moivre's Theorem. We leave the easy proof (by induction) as an exercise.

Definition. Given an integer $n \geq 1$, a complex number ω is an *n-th root of unity* if $\omega^n = 1$.

Theorem. (De Moivre). *For any integer n,*

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta. \tag{8.7}$$

Corollary. *If $n \geq 1$ is an integer and*

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

then

$$1, \omega, \omega^2, \ldots, \omega^{n-1}$$

are all distinct and satisfy the equation

$$z^n = 1,$$

hence are all the n n-th roots of unity.

Note. The n n-th roots of unity are evenly spaced on the unit circle $|z| = 1$ (see Figure 8.2 for $n = 8$).

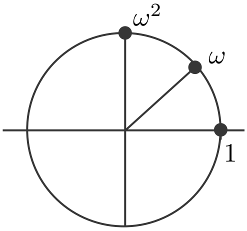


FIGURE 8.2: Roots of unity

8.2 Diagonalization of Matrices with Complex Eigenvalues

We now return to the diagonalization and continue with the example

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

Its eigenvalues are $\lambda = i, -i$.

For $\lambda = i$, an eigenvector is a nonzero solution of

$$(iI - A)\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{0}, \tag{8.8}$$

or

$$(i+1)x - 2y = 0. \tag{8.9}$$

Note that the second equation in (8.8), i.e.

$$x + (i-1)y = 0 \tag{8.10}$$

is just $(i-1)$ multiple of equation (8.9).

So for an eigenvector $\boldsymbol{x}_1$ belonging to $\lambda = i$ we put $y = 1$ in (8.10) to get

$$\boldsymbol{x}_1 = \begin{pmatrix} 1-i \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} - i\begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The eigenvector belonging to $\lambda = -i$ is then its complex conjugate (see Exercise 8, Section 6.2)

$$\boldsymbol{x}_2 = \bar{\boldsymbol{x}}_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} + i\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1+i \\ 1 \end{pmatrix}.$$

We now take

$$P = \begin{pmatrix} 1-i & 1+i \\ 1 & 1 \end{pmatrix}. \tag{8.11}$$

It can be checked that P is invertible and

$$P^{-1}AP = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}. \tag{8.12}$$

EXERCISE

Compute the inverse of P in (8.11) and verify (8.12).

8.3 Matrices over Complex Numbers

For an $m \times n$ matrix $X = (x_{ij})$ with complex entries x_{ij}, we write the $m \times n$ matrix $(\bar{x}_{ij})$ as $\overline{X}$. Then given matrices X and Y of appropriate size,

$$\overline{X+Y} = \overline{X} + \overline{Y},$$
$$\overline{XY} = \overline{X}\,\overline{Y}$$

and for a complex number λ,

$$\overline{\lambda X} = \bar{\lambda}\,\overline{X}.$$

Note that A is a real matrix if and only if

$$\bar{A} = A,$$

and a complex matrix X can be written as

$$X = A + iB$$

with A, B real. In particular, a complex eigenvector belonging to a complex eigenvalue λ may be written as

$$\boldsymbol{x} = \boldsymbol{a} + i\boldsymbol{b}.$$

Now

$$A\boldsymbol{x} = \lambda\boldsymbol{x}$$

for A real implies that

$$A\bar{\boldsymbol{x}} = \bar{\lambda}\bar{\boldsymbol{x}},$$

which shows that $\bar{\boldsymbol{x}}$ is an eigenvector of A belonging to $\bar{\lambda}$.

We show that the eigenvalues of a real symmetric matrix A are all real. Moreover, the eigenvectors belonging to distinct eigenvalues of A are not only linearly independent, but also orthogonal. We will actually prove it for Hermitian matrices, of which the symmetric matrices are a special case.

Hermitian Matrices

The concept of Hermitian matrices (after C. Hermite (1822–1901)) is a generalization of (real) symmetric matrices to the matrices over the field $\mathbb{C}$ of complex numbers. We first generalize the notion of the transpose of a real matrix to that of adjoint of a complex one. To show the two steps (transposing and conjugation) it may be better to temporarily denote the transpose of Z as Z^T.

Definition. The *adjoint* Z^* of a matrix Z over $\mathbb{C}$ is the conjugate of its transpose, i.e. $Z^* = \overline{Z^T} = \overline{Z}^T$.

Clearly, $(XY)^* = Y^*X^*$, $(\lambda Z)^* = \bar{\lambda}Z^*$ and $(Z^*)^* = Z$.

Definition. A matrix A over $\mathbb{C}$ is *Hermitian* (or *self-adjoint*) if $A^* = A$.

Remarks.

1. If A is real, the adjoint of A is its transpose.

2. For A to be Hermitian, it has to be square.

3. A^*A is always Hermitian for every A. So is AA^*, although A^*A and AA^* may be of different sizes.

4. A real matrix A is Hermitian if and only if it is symmetric.

5. The diagonal entries of a Hermitian matrix are real.

Example. The matrix

$$\begin{pmatrix} 2 & 3+3i \\ 3-3i & 5 \end{pmatrix}$$

is Hermitian. However,

$$\begin{pmatrix} 2 & 3+3i \\ 3+3i & 5 \end{pmatrix}$$

is not Hermitian, although it is (complex) symmetric. At first thought, complex symmetric may seem to be a natural generalization of real symmetric, but it is not. It is the concept of a Hermitian matrix that leads to the correct definitions of the dot product, length, and orthogonality in the vector space $V = \mathbb{C}^n$ over the field $\mathbb{C}$.

Definition. The *dot product of complex vectors* $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{C}^n$ is the complex number

$$\boldsymbol{x} \cdot \boldsymbol{y} = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n. \tag{8.13}$$

If the vectors in $\mathbb{C}^n$ are written as columns, then the *dot product* is the matrix product

$$\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y}^*\boldsymbol{x}.$$

This dot product has the following defining properties:

1) $(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{z}=\boldsymbol{x}\cdot\boldsymbol{z}+\boldsymbol{y}\cdot\boldsymbol{z}$,

2) For c in $\mathbb{C}$, $(c\boldsymbol{x})\cdot\boldsymbol{y}=c(\boldsymbol{x}\cdot\boldsymbol{y})$,

3) $\overline{\boldsymbol{x}\cdot\boldsymbol{y}}=\boldsymbol{y}\cdot\boldsymbol{x}$

4) $\boldsymbol{x}\cdot\boldsymbol{x}$ is real and ≥ 0, and $=0$ if and only if $\boldsymbol{x}=\boldsymbol{0}$.

Remark. Analogous to the real inner product spaces, one can also define a complex inner product space, now requiring the complex number $\langle\boldsymbol{x},\boldsymbol{y}\rangle$ to satisfy axioms 1)–4) above.

Property 4) leads to the definition of the length of a vector in $\mathbb{C}^n$.

Definition. Let $\boldsymbol{x}$ be in $\mathbb{C}^n$. Its *length* $\|\boldsymbol{x}\|=\sqrt{\boldsymbol{x}\cdot\boldsymbol{x}}$, the non-negative square root of $\boldsymbol{x}\cdot\boldsymbol{x}$.

A *unit vector* in $\mathbb{C}^n$ is a vector of length one. The *normalization* of a nonzero vector $\boldsymbol{x}$ is its replacement by the unit vector $\boldsymbol{u}=\frac{1}{\|\boldsymbol{x}\|}\cdot\boldsymbol{x}$. Note that we can always do this, because only the zero vector has length zero.

Example. Let $\boldsymbol{x}=(x_1,\ldots,x_n)\in\mathbb{C}^n$. Then

$$\begin{aligned}\boldsymbol{x}\cdot\boldsymbol{x}&=x_1\bar{x}_1+\cdots+x_n\bar{x}_n\\&=|x_1|^2+\cdots+|x_n|^2.\end{aligned}$$

So we can write $\|\boldsymbol{x}\|=\sqrt{|x_1|^2+\cdots+|x_n|^2}$, which coincides with the definition of the length in $\mathbb{R}^n$. As a concrete example, let $\boldsymbol{x}=(1,-1,i,-i)$, a vector in $\mathbb{C}^4$. Its length $\|\boldsymbol{x}\|=\sqrt{|1|^2+|-1|^2+|i|^2+|-i|^2}=2$. The normalization of $\boldsymbol{x}$ is $\boldsymbol{u}=\left(\frac{1}{2},-\frac{1}{2},\frac{i}{2},-\frac{i}{2}\right)$.

Definition. The vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{C}^n$ are *orthogonal* if $\boldsymbol{x}\cdot\boldsymbol{y}=0$. A set $\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_r\}\subseteq\mathbb{C}^n$ is an *orthogonal set* if $\boldsymbol{x}_i\cdot\boldsymbol{x}_j=0$ for every pair i, j with $i\neq j$. An orthogonal set of vectors in $\mathbb{C}^n$ is *orthonormal* if each vector in the set is a unit vector. The definition of an *orthonormal basis* of $\mathbb{C}^n$ is obvious.

Definition. An $n\times n$ matrix U over $\mathbb{C}$ is a *unitary matrix* if $U^*U=UU^*=I$, in other words, if $U^{-1}=U^*$.

It is clear that U is unitary if and only if its columns (equivalently rows) form an orthonormal basis of $\mathbb{C}^n$ with vectors in $\mathbb{C}^n$ written as columns (equivalently rows).

Examples.

1. Any real matrix P with $P^{-1}=P^*$ is automatically unitary (see Section 9.3).

2. The 2×2 matrix

$$U=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}$$

is unitary.

3. The 3×3 matrix

$$U = \begin{pmatrix} 0 & i & 0 \\ i & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is unitary.

Theorem 8.1. *Suppose U is unitary. The map $\boldsymbol{x} \to U\boldsymbol{x}$ is length preserving.*

Proof. $\|U\boldsymbol{x}\|^2 = (U\boldsymbol{x})^*(U\boldsymbol{x}) = \boldsymbol{x}^*(U^*U)\boldsymbol{x} = \boldsymbol{x}^*\boldsymbol{x} = \|\boldsymbol{x}\|^2$. □

Theorem 8.2. *The eigenvalues of a Hermitian (in particular, a real symmetric) matrix A are all real and the eigenvectors belonging to distinct eigenvalues of A are orthogonal.*

Proof. By an *eigenvalue* of a complex matrix A we mean a complex number λ such that

$$A\boldsymbol{x} = \lambda\boldsymbol{x}$$

holds for a nonzero (column) vector $\boldsymbol{x}$ in $\mathbb{C}^n$, called an *eigenvector* belonging to λ.

First we show that the complex number $\boldsymbol{x}^*A\boldsymbol{x}$ is in fact a real number, if A is Hermitian. For this, since $\boldsymbol{x}^T\bar{A}\bar{\boldsymbol{x}}$ is a 1×1 matrix,

$$\overline{\boldsymbol{x}^*A\boldsymbol{x}} = \boldsymbol{x}^T\bar{A}\bar{\boldsymbol{x}} = (\boldsymbol{x}^T\bar{A}\bar{\boldsymbol{x}})^T = \boldsymbol{x}^*A^*\boldsymbol{x} = \boldsymbol{x}^*A\boldsymbol{x},$$

which shows that $\boldsymbol{x}^*A\boldsymbol{x}$ is its own conjugate, hence a real number. Next

$$A\boldsymbol{x} = \lambda\boldsymbol{x} \quad (\boldsymbol{x} \neq \boldsymbol{0})$$

implies that

$$\boldsymbol{x}^*A\boldsymbol{x} = \boldsymbol{x}^*\lambda\boldsymbol{x} = \lambda\boldsymbol{x}^*\boldsymbol{x} = \lambda\|\boldsymbol{x}\|^2.$$

Hence

$$\lambda = \frac{\boldsymbol{x}^*A\boldsymbol{x}}{\|\boldsymbol{x}\|^2}$$

is real.

To prove the last statement, suppose λ_1, λ_2 are two distinct eigenvalues of A and that $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ are eigenvectors belonging to λ_1, λ_2 respectively. Since λ_1, λ_2 are real,

$$\begin{aligned} \lambda_1\boldsymbol{x}_1^*\boldsymbol{x}_2 &= (\lambda_1\boldsymbol{x}_1)^*\boldsymbol{x}_2 = (A\boldsymbol{x}_1)^*\boldsymbol{x}_2 \\ &= \boldsymbol{x}_1^*A^*\boldsymbol{x}_2 = \boldsymbol{x}_1^*A\boldsymbol{x}_2 = \boldsymbol{x}_1^*\lambda_2\boldsymbol{x}_2 \\ &= \lambda_2\boldsymbol{x}_1^*\boldsymbol{x}_2, \end{aligned}$$

which gives

$$(\lambda_1 - \lambda_2)\boldsymbol{x}_1^*\boldsymbol{x}_2 = 0.$$

Since $\lambda_1 - \lambda_2 \neq 0$, $\boldsymbol{x}_1^*\boldsymbol{x}_2 = 0$. □

Without delving much into complex inner product spaces, we just recall the definition and some examples.

Definition. A *complex inner product space* is a vector space V over $\mathbb{C}$ together with a map $V \times V \ni (\boldsymbol{x}, \boldsymbol{y}) \to \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{C}$, called an *inner product* on V such that for all $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ in V, and all c in $\mathbb{C}$,

1) $\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{x}, \boldsymbol{z} \rangle + \langle \boldsymbol{y}, \boldsymbol{z} \rangle$,
2) For a scalar c, $\langle c\boldsymbol{x}, \boldsymbol{y} \rangle = c\langle \boldsymbol{x}, \boldsymbol{y} \rangle$,
3) $\overline{\langle \boldsymbol{x}, \boldsymbol{y} \rangle} = \langle \boldsymbol{y}, \boldsymbol{x} \rangle$, and
4) $\langle \boldsymbol{x}, \boldsymbol{x} \rangle \geq 0$ and $= 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.

Examples.

1. We already have the standard inner product $\boldsymbol{x} \cdot \boldsymbol{y}$ on $\mathbb{C}^n$ defined by (8.13).

2. Choose any real diagonal $n \times n$ matrix D with diagonal entries all positive. On $V = \mathbb{C}^n$,

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{y}^* D \boldsymbol{x}$$

defines an inner product.

3. Let V be the vector space of all complex valued continuous functions on the unit interval $I = [0, 1]$. Then

$$\langle f, g \rangle = \int_0^1 f(t)\,\overline{g(t)}\,dt$$

is an inner product on V. The vectors $f(t) = e^{2\pi i t}$ and $g(t) = e^{-2\pi i t}$ are orthogonal in V, meaning $\langle f, g \rangle = 0$.

Finally, we remark that everything like orthogonal complements, orthogonal projections, the Gram-Schmidt Process, as well as most of what we shall do in the next chapter (symmetric matrices and real quadratic forms) carries over to the matrices and vector spaces over the field $\mathbb{C}$. We leave the details and verification for the reader to check.

EXERCISES

1. Find the length of the vector $(i, 2 + i, 3 - i)$.

2. If possible, diagonalize the matrices

   i) $\begin{pmatrix} 0 & 1-i \\ 1+i & 1 \end{pmatrix}$,

   ii) $\begin{pmatrix} 0 & -1+i \\ 1+i & i \end{pmatrix}$,

   iii) $\begin{pmatrix} 1 & 1-i \\ 1+i & -1 \end{pmatrix}$, and

   iv) $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

3. Show that the products and inverses of unitary matrices are unitary. [In other words, the set of unitary matrices of a given size forms a group.]

4. Show that the inverse of a Hermitian matrix is Hermitian.

5. Show that the determinant of a Hermitian matrix is real.

6. What is the relation between the spectrum of A (the set of eigenvalues of A) and that of A^*?

7. Let $\boldsymbol{u}$ be a (column) vector in $\mathbb{C}^n$. If $\boldsymbol{u}^*\boldsymbol{u} = 1$, show that $I - 2\boldsymbol{u}\boldsymbol{u}^*$ is Hermitian and unitary.

8. Prove or disprove the following:

   (a) If A is an $n \times n$ real matrix, then $iI + A$ is invertible.

   (b) If A is Hermitian, then $iI + A$ is invertible.

   (c) If U is unitary, then $iI + U$ is invertible.

9. Show that $\langle A, B \rangle =$ the trace $\operatorname{tr}(A^*B)$ defines an inner product on the vector space $M(n, \mathbb{C})$ of $n \times n$ matrices over $\mathbb{C}$.

9

Orthonormal Diagonalization

9.1 Motivational Introduction

If we write at random a degree two equation

$$ax^2 + by^2 + cxy + dx + \cdots = 0$$

we know it represents a conic section, but to know exactly which one requires some work. By completing the squares, equivalently by shifting the origin, we can reduce the above equation to one of the form

$$a_1x^2 + b_1y^2 + c_1xy = \text{const.}$$

(We omit the easy cases, e.g. when only one variable appears in the degree two terms.) We still need to work on the quadratic form $a_1x^2 + b_1y^2 + c_1xy$, if $c_1 \neq 0$ to determine the nature of the conic section. To be precise, making a linear substitution, equivalently, using an appropriate linear map we need to get rid of the mixed term c_1xy to reduce it further to the form $a_2x^2 + b_2y^2$. We can then infer the nature of our conic section by looking at the signs of a_2, b_2. In order to preserve the distinction between a circle and an ellipse, the linear map has to be length preserving, equivalently, its matrix to be orthonormal.

Another application of the above discussion is in the multivariable calculus. The quadratic term in the Taylor expansion of a multivariable function at a critical point (which may be, by shifting the origin, assumed to be the origin) determines the nature of the critical point. If we can reduce it to $\lambda_1x_1^2 + \cdots + \lambda_nx_n^2$, we can infer the nature of the critical point by looking at the signs of $\lambda_1, \ldots, \lambda_n$.

Quadratic Forms

A *quadratic form* is a homogeneous polynomial $q(x_1, \ldots, x_n)$ of degree two in n variables $x_1, \ldots, x_n$. If $n = 2$, it is called a *binary quadratic form*, for $n = 3$, it is a *ternary quadratic form*, and so on. Recall that a polynomial

$q(x_1,\ldots,x_n)$ is a *homogeneous polynomial* of degree $d \geq 1$ if for a parameter t,

$$q(tx_1,\ldots,tx_n) = t^d q(x_1,\ldots,x_n).$$

The polynomial

$$q(x,y) = 3x^2 + 2xy + 3y^2$$

is a binary quadratic form, whereas

$$q(x,y,z) = x^2 + 2y^2 + 3z^2 + 4xy + 6yz + 8xz$$

is a ternary quadratic form.

Although, as remarked at the end of Chapter 8, we could have done everything in more generality by taking our field of scalars to be $\mathbb{C}$, we restrict ourselves to $\mathbb{R}$. This is because for applications, $\mathbb{R}$ is the most interesting case. One particular example is the study of real valued multivariable functions $f(x_1,\ldots,x_n)$ or just $f(\boldsymbol{x})$ which are analytic, i.e. have partial derivatives of every order. Such a function can be represented by its Taylor expansion at a given point $\boldsymbol{x} = \boldsymbol{a}$. By moving the origin to $\boldsymbol{a}$, we may take $\boldsymbol{a} = \boldsymbol{0}$, so that the *Taylor expansions* of $f(\boldsymbol{x})$ at $\boldsymbol{a} = \boldsymbol{0}$ is

$$f(\boldsymbol{x}) = f(\boldsymbol{0}) + \ell(\boldsymbol{x}) + q(\boldsymbol{x}) + \text{higher degree terms.} \tag{9.1}$$

The linear term $\ell(\boldsymbol{x})$ is a homogeneous polynomial of degree one, $q(\boldsymbol{x})$ is a quadratic form and so on. If $n = 1$, we have the usual Taylor expansion

$$f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \cdots . \tag{9.2}$$

If $x = a = 0$ is a critical point, $f'(a) = 0$ (by definition), so $\ell(x) = 0$. The behavior of the critical point (whether it is a local maximum or minimum) is determined by quadratic term $\frac{f''(a)}{2!}x^2$. If $f''(a) < 0$, $f(a)$ is a local maximum and for $f''(a) > 0$, $f(a)$ is a local minimum. This is so because near a, the contribution of the higher terms is negligible compared to that of the quadratic term. This is not the case when $f''(a) = 0$, so in this case the second derivative test fails.

For $n > 1$, one replaces $f'(x) = 0$ by $\frac{\partial f}{\partial x_1}(\boldsymbol{x}) = \cdots = \frac{\partial f}{\partial x_n}(\boldsymbol{x}) = 0$ for the critical point $\boldsymbol{a}$ so that in (9.1), $\ell(\boldsymbol{x}) = 0$. If $\boldsymbol{a} = \boldsymbol{0}$, the quadratic form $q(\boldsymbol{x}) = \frac{1}{2}\sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_i \partial x_j}(\boldsymbol{0})x_i x_j$. Thus i) if $q(\boldsymbol{x}) > 0$ for all $\boldsymbol{x}$, $f(\boldsymbol{a})$ is a local minimum, ii) if $q(\boldsymbol{x}) < 0$ for all $\boldsymbol{x}$, $f(\boldsymbol{a})$ is a local maximum, and iii) if $q(\boldsymbol{x}) > 0$ for some $\boldsymbol{x}$ and < 0 for other values of $\boldsymbol{x}$, $f(\boldsymbol{a})$ is a *saddle point*. Finally, if $q(\boldsymbol{x})$ is identically equal to zero, the second derivative test fails. The cases i), ii), and iii) are referred to as *positive definite*, *negative definite*, and *indefinite*, respectively. Now we show how to find out which case it is.

9.2 Matrix Representation of a Quadratic Form

Let

$$q(\boldsymbol{x}) = \sum_{i \le j} b_{ij} x_i x_j$$

be a quadratic form. Then

$$q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$$

where $A = (a_{ij})$ is symmetric with $a_{ij} = \begin{cases} \frac{b_{ij}}{2} & \text{if } i \neq j \\ b_{ii} & \text{if } i = j. \end{cases}$

What we have done is to split the mixed terms $x_i x_j$ $(i < j)$ half and half to be put symmetrically off the diagonal in A, whereas the coefficients a_{jj} of x_j^2 appear on the diagonal.

Examples.

1. If $q(x, y) = 3x^2 + 2xy + 3y^2$, then for

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

it is easy to verify that

$$q(x, y) = \begin{pmatrix} x & y \end{pmatrix} A \begin{pmatrix} x \\ y \end{pmatrix}.$$

2. If $q(x, y, z) = x^2 + 2y^2 + 3z^2 + 4xy + 6yz + 8xz$, then

$$q(x, y, z) = \begin{pmatrix} x & y & z \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

with

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

Our goal is to determine if a given quadratic form $q(\boldsymbol{x})$ over $\mathbb{R}$ is positive definite, negative definite or indefinite. This is obvious if $q(\boldsymbol{x})$ has no mixed terms. In fact, then $q(\boldsymbol{x})$ is positive definite if all $a_{jj} > 0$, negative definite if all $a_{jj} < 0$ and indefinite when some $a_{jj} > 0$ and some other $a_{jj} < 0$. This suggests we diagonalize symmetric matrices, in order to get rid of the mixed terms. We begin with an example.

Example. Let

$$q(x_1, x_2) = 3x_1^2 + 2x_1x_2 + 3x^2.$$

Its (symmetric) matrix

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix},$$

whose characteristic polynomial $\chi_A(\lambda) = (\lambda - 2)(\lambda - 4)$. The eigenvalues $\lambda = 2$, 4 of A are real. This is no surprise – the eigenvalues of symmetric matrices are all real. By solving

$$(\lambda I - A)\boldsymbol{v} = \mathbf{0}$$

we find eigenvectors, $\boldsymbol{v}_1 = \binom{1}{-1}$ and $\boldsymbol{v}_2 = \binom{1}{1}$ belonging to $\lambda_1 = 2$ and $\lambda_2 = 4$. It can be checked that if $\boldsymbol{u}_1$, $\boldsymbol{u}_2$ are the normalizations of $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ respectively, the matrix P whose columns are $\boldsymbol{u}_1$, $\boldsymbol{u}_2$ orthonormally diagonalizes A. In other words,

$$P^*AP = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}.$$

Now let $\boldsymbol{x} = P\boldsymbol{y}$. Then $q(x_1, x_2) = \boldsymbol{x}^*A\boldsymbol{x} = \boldsymbol{y}^*(P^*AP)\boldsymbol{y}$

$$(y_1 y_2) \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 2y_1^2 + 4y_2^2.$$

This will be called an orthonormal diagonalization of A. By getting rid of the mixed term by linear substitution $\boldsymbol{x} = P\boldsymbol{y}$ we can say that $q(x_1, x_2)$ is positive definite. [Recall that $\boldsymbol{y} \to P\boldsymbol{y}$ is a bijection from $\mathbb{R}^2$ to itself.]

EXERCISES

Find the matrices of the following quadratic forms:

1. $q(\boldsymbol{x}) = 2x_1^2 + 3x_2^2 + 4x_1x_2$.
2. $q(\boldsymbol{x}) = 2x_1^2 + 3x_2^2 + 5x_3^2 + 4x_1x_2 + 6x_2x_3 + 8x_1x_3$.
3. (a) Write the quadratic form $q(x_1, x_2) = x_1^2 - 8x_1x_2 - 5x_2^2$ as $\boldsymbol{x}^*A\boldsymbol{x}$ with A symmetric.

   (b) Orthonormally diagonalize A in (a).

   (c) Write the transformed quadratic form without mixed terms.
4. Repeat 3 above for $5x_1^2 - 4x_1x_2 + 5x_2^2$.

9.3 Spectral Decomposition

Definition. A real matrix P is *orthonormal* if $P^*P = PP^* = I$, in other words, if $P^{-1} = P^*$.

Remark. An orthonormal matrix A is unitary, hence by Theorem 8.1, the map $\boldsymbol{x} \to A\boldsymbol{x}$ is length preserving, hence a shape preserving rigid motion of axes.

Definition. A square matrix A over $\mathbb{R}$ is *orthonormally diagonalizable* if $P^*AP = D$, with D diagonal, for an orthonormal matrix P. One says that P *orthonormally diagonalizes* A.

Remark. It is more accurate to use the terms orthonormal matrix and orthonormally diagonalizable matrix rather than the traditional "orthogonal" and "orthogonally diagonalizable."

Example. The matrix

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

is orthonormally diagonalizable. In fact,

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

orthonormally diagonalizes A. Note that our A is symmetric.

Recall that (Theorem 8.2) if A is a real symmetric matrix, then

i) the eigenvalues of A are real,

ii) the eigenspaces $V_\lambda = \{\boldsymbol{x} \in \mathbb{R}^n \mid A\boldsymbol{x} = \lambda\boldsymbol{x}\}$ belonging to distinct eigenvalues are mutually orthogonal.

We now use these results to prove the following fact:

Theorem (Criterion for Diagonalizability)**.** *An $n \times n$ real matrix A is orthonormally diagonalizable if and only if A is symmetric.*

Proof. Suppose A is orthonormally diagonalizable. Then $P^*AP = D$ for some diagonal D and orthonormal P. Taking the transpose of each side of this equation, we get $P^*A^*P = D$. These two equations now imply that $A^* = A$.

Conversely, suppose A is symmetric. We show that A is diagonalizable.

The proof is by induction on n. If $n = 1$, there is nothing to prove. For $n > 1$, let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of A and let $\boldsymbol{u}_1$ be a unit eigenvector belonging to λ_1. Obtain by the Gram-Schmidt Process an orthonormal basis of $\mathbb{R}^n$ with $\boldsymbol{u}_1$ as its first vector. Take P_1 to be the matrix whose j-th column is the j-th vector of this orthonormal basis. Then

$$P_1^* A P_1 = \left(\begin{array}{c|c} \lambda_1 & 0 \\ \hline 0 & B \end{array}\right).$$

Since B is also symmetric, by the induction hypothesis, Q^*BQ is diagonal for an orthonormal matrix Q. If $P = P_1 Q_1$, where

$$Q_1 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & Q \end{array}\right),$$

then P orthonormally diagonalizes A. □

Remark. By similar arguments, we can prove the following variant of the above theorem, called Schur's Lemma.

Theorem (Schur)**.** *If A is an $n \times n$ matrix over $\mathbb{C}$, there is a unitary matrix U such that U^*AU is upper triangular with the eigenvalues of A appearing on the diagonal.*

Corollary. *The rank of an $n \times n$ matrix is equal to the number of its non-zero eigenvalues.*

Spectral Decomposition of Symmetric Matrices

The *spectrum* of an $n \times n$ matrix is the set of its n eigenvalues. Let P be an orthonormnal matrix with columns $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ that diagonalizes a given symmetric matrix A, i.e.

$$P^*AP = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

or

$$A = PDP^*, \tag{9.3}$$

λ_j being the eigenvalues of A. Then

$$A = PDP^* = (\boldsymbol{u}_1 \cdots \boldsymbol{u}_n) \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \begin{pmatrix} \boldsymbol{u}_1^* \\ \vdots \\ \boldsymbol{u}_n^* \end{pmatrix}$$

or

$$A = \lambda_1 \boldsymbol{u}_1 \boldsymbol{u}_1^* + \cdots + \lambda_n \boldsymbol{u}_n \boldsymbol{u}_n^* \tag{9.4}$$

Equation (9.4) is called the *spectral decomposition* of A, because it involves only the spectrum of A and the corresponding unit eigenvectors of A.

Example. Let

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

Its eigenvalues are $\lambda = 2, 4$ and the corresponding unit vectors are

$$\boldsymbol{u}_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \text{ and } \boldsymbol{u}_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Therefore,

$$\boldsymbol{u}_1\boldsymbol{u}_1^* = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

and

$$\boldsymbol{u}_2\boldsymbol{u}_2^* = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

So

$$\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} = 2 \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} + 4 \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

is the spectral decomposition of A.

Remark. The criterion for diagonalizability is also called the *Principal Axes Theorem* for the following reason: Suppose $q(x_1, x_2)$ is a quadratic form, e.g.

$$q(x_1, x_2) = 3x_1^2 + 2x_1x_2 + 3x_2^2 = \boldsymbol{x}^* A \boldsymbol{x}$$

with

$$A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}.$$

Unless $q(\boldsymbol{x})$ is negative definite, the equation $q(\boldsymbol{x}) = c$ ($c > 0$ a constant) defines a conic section. The orthogonal substitution $\boldsymbol{x} = P\boldsymbol{y}$ with

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

transforms the equation

$$3x_1^2 + 2x_1x_2 + 3x_2^2 = 1$$

to

$$2y_1^2 + 4y_2^2 = 1.$$

This is an ellipse with its principal axes determined by the eigenvectors of A. We couldn't say this if the substitution wasn't orthonormal, i.e. didn't preserve lengths and angles. An ellipse could have become a circle. If for a different A the two eigenvalues of A have opposite sign, then

$$\boldsymbol{x}^* A \boldsymbol{x} = 1$$

will be a hyperbola.

In the definition below, we assume the quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ is *non-singular*, meaning the matrix A is non-singular (equivalently, the eigenvalues of A are all nonzero).

Definition. (Classification of Quadratic Forms) A real quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ is

i) *positive definite* if $q(\boldsymbol{x}) > 0$ for all $\boldsymbol{x} \neq \boldsymbol{0}$,

ii) *negative definite* if $q(\boldsymbol{x}) < 0$ for all $\boldsymbol{x} \neq \boldsymbol{0}$.

iii) *indefinite* if $q(\boldsymbol{x})$ takes both positive and negative values.

The following is obvious.

Theorem 9.1. *A quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ with A symmetric is*

i) positive definite if and only if all the eigenvalues of A are positive,

ii) negative definite if and only if all the eigenvalues of A are negative, and

iii) indefinite if and only if neither i) nor ii) holds.

In multivariable calculus of two variables, the following is often referred to as the second derivative test:

Theorem 9.2. *Let A be a 2×2 invertible real symmetric matrix*

$$A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

Then

i) A is indefinite if $\det(A) < 0$.

ii) For $\det(A) > 0$*, A is positive/negative definite accordingly as a is positive/negative.*

Remark. In ii), a can be replaced by c.

Proof. Let λ_1, λ_2 be the two real eigenvalues of A. Then $\det(A) = \lambda_1\lambda_2 < 0$ implies λ_1, λ_2 have opposite signs. This proves i).

ii) Suppose $\det(A) = ac - b^2 > 0$. Then a and c have the same sign. Also $\det(A) = \lambda_1\lambda_2 > 0$ implies that λ_1 and λ_2 have the same sign as well. Therefore, since $\operatorname{tr}(A) = a + c = \lambda_1 + \lambda_2$, A is positive definite $\Leftrightarrow \lambda_1, \lambda_2 > 0 \Leftrightarrow a$, or c (hence both) > 0. This proves ii). □

Remark. The case $\det(A) = 0$ corresponds to the case when the quadratic term in the Taylor expansion fails to give complete information about the nature of the function at its critical points (i.e. whether they are local maxima, local minima, or saddle points).

EXERCISES

1. Classify (positive definite, negative definite, or indefinite, etc.) the quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ if $A =$

$$\text{(a)} \begin{pmatrix} 2 & 3 \\ 3 & -6 \end{pmatrix} \quad \text{(b)} \begin{pmatrix} 9 & -4 \\ -4 & 3 \end{pmatrix} \quad \text{(c)} \begin{pmatrix} -5 & 2 \\ 2 & -2 \end{pmatrix} \quad \text{(d)} \begin{pmatrix} 3 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

2. Write the spectral decomposition $A = PDP^*$ if

$$\text{(a) } A = \begin{pmatrix} 3 & -2 & 4 \\ -2 & 6 & 2 \\ 4 & 2 & 3 \end{pmatrix} \qquad \text{(b)} \begin{pmatrix} 6 & -2 & -1 \\ -2 & 6 & -1 \\ -1 & -1 & 5 \end{pmatrix}$$

3. If A is invertible, show that all eigenvalues of A^*A are positive.

4. If A and B are $n \times n$ symmetric matrices with all eigenvalues positive, show that all eigenvalues of $A + B$ are also positive.

5. For a nonempty set X, let $\mathcal{P}_r(X)$ be the set of all subsets Y of X with cardinality $|Y| = r$ $(r \geq 0)$. A *graph* G consists of a finite nonempty set $V = V(G)$ of *vertices* of G and a set $E = E(G) \subseteq \mathcal{P}_2(V)$. If $\{u, v\} \in E(G)$, we call $\{u, v\}$ an *edge* of G and u, v *adjacent* to each other. Note that no u is adjacent to itself. The *adjacency matrix* $A = A(G)$ of a graph G is defined as follows:

Let $V = V(G) = \{v_1, \ldots, v_n\}$ and $A = A(G) = (a_{ij})$. Then

$$a_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \in E(G) \\ 0 & \text{otherwise.} \end{cases}$$

Show that the sum of the eigenvalues of $A(G)$ is zero.

Note. The study of the spectra of the adjacency matrices of graphs is an important part of graph theory (cf. [17]).

6. Fix an order $V(G) = \{v_1, \ldots, v_n\}$ on the set of vertices of a graph G. If $P(f)$ is the permutation matrix of a permutation $f : V(G) \to V(G)$ and B is the adjacency matrix of G relative to the reordering $\{f(v_1), \ldots f(v_n)\}$ of $V(G)$, show that $B = P(f)^* A P(f)$.

7. The *degree of a vertex* v of a graph G is the cardinality

$$\deg(v) = |\{u \in V(G) \mid u \text{ is adjacent to } v\}|.$$

Put $\Delta(G) = \max\limits_{v \in V(G)} \deg(v)$. If λ is an eigenvalue of the adjacency matrix $A(G)$ of a graph G, show that $|\lambda| \leq \Delta(G)$.

8. For $k \geq 0$, a graph G is *k-regular* if $\deg(v) = k$ for all v in $V(G)$. Show that $\lambda = k$ is an eigenvalue of the adjacency matrix $A(G)$ of a k-regular graph G.

9. Show that if A is an $m \times n$ matrix, then $A^* A$ is positive semi-definite (that is all its eigenvalues are non-negative).

10. If $q_1(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ is positive definite, show that $q_2(\boldsymbol{x}) = \boldsymbol{x}^* A^{-1} \boldsymbol{x}$ is also positive definite.

11. Prove or disprove:

(a) An invertible matrix is orthonormally diagonalizable.

(b) The inverse of a symmetric matrix is symmetric.

(c) If A is an $n \times n$ positive definite symmetric matrix, then there is also such a matrix B with $A = B^* B$.

(d) An orthonormal matrix is orthonormally diagonalizable.

(e) If A, B are orthonormally diagonalizable and $AB = BA$, then AB is orthonormally diagonalizable.

9.4 Constrained Optimization – Extrema of Spectrum

The values of a quadratic form as a function from $\mathbb{R}^n$ to $\mathbb{R}$ are unbounded unless its domain is restricted or constrained.

The eigenvalues of a real symmetric matrix are all real. Suppose M, m are the largest and the smallest eigenvalues of A. We call the subset

$$S = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\| = 1\}$$

the *unit sphere* (*circle* if $n = 2$). We now show that M and m have something to do with the values of the quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A\boldsymbol{x}$ for $\boldsymbol{x}$ in S.

Theorem 9.3. *Suppose A is an $n \times n$ real symmetric matrix whose smallest eigenvalue is m and the largest is M. Let $q(\boldsymbol{x}) = \boldsymbol{x}^* A\boldsymbol{x}$. Then*

$$M \geq q(\boldsymbol{x}) \geq m$$

for all $\boldsymbol{x}$ in S and with both bounds m and M attained for $\boldsymbol{x}$ in S.

Proof. Suppose $M = \lambda_1 \geq \cdots \geq \lambda_n = m$ are the eigenvalues of A. If $A = PDP^*$ is a spectral decomposition of A, then $P^*AP = D$, with say

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Under the orthonormal substitution $\boldsymbol{x} = P\boldsymbol{y}$, the quadratic form $q(\boldsymbol{x}) = \boldsymbol{x}^* A\boldsymbol{x}$ becomes $f(\boldsymbol{y}) = \lambda_1 y_1^2 + \cdots + \lambda_n y_n^2$. Since $\|\boldsymbol{x}\|^2 = \|P\boldsymbol{y}\|^2 = \boldsymbol{y}^*(P^*P)\boldsymbol{y} = \boldsymbol{y}^* \cdot \boldsymbol{y} = \|\boldsymbol{y}\|^2$ and P is invertible,

$$\{q(\boldsymbol{x}) \mid \boldsymbol{x} \in S\} = \{f(\boldsymbol{y}) \mid \boldsymbol{y} \in S\}.$$

Therefore for $\boldsymbol{y}$ in S,

$$\lambda_1 = \lambda_1(y_1^2 + \cdots + y_n^n) \geq \lambda_1 y_1^2 + \cdots + \lambda_n y_n^2$$

$$= f(\boldsymbol{y}) \geq \lambda_n(y_1^2 + \cdots + y_n^2) = \lambda_n$$

and $M = \lambda_1 = f((1, 0, \ldots, 0))$ and $m = \lambda_n = f((0, \ldots, 0, 1))$. □

Remark. The *Rayleigh quotient* of a symmetric matrix A is the ratio

$$R(A, \boldsymbol{x}) = \frac{\boldsymbol{x}^* A\boldsymbol{x}}{\boldsymbol{x}^*\boldsymbol{x}}$$

for $\boldsymbol{x} \neq \boldsymbol{0}$. We may rephrase Theorem 9.3 as follows:

$$m \leq R(A, \boldsymbol{x}) \leq M.$$

EXERCISES

1. Find the maximum and minimum values M and m, respectively of $q(\boldsymbol{x}) = \boldsymbol{x}^*A\boldsymbol{x}$ for $\boldsymbol{x}$ in S if $A =$

   (a) $\begin{pmatrix} -5 & 2 \\ 2 & -2 \end{pmatrix}$ (b) $\begin{pmatrix} 3 & 2 & 0 \\ 2 & 2 & 2 \\ 0 & 2 & 1 \end{pmatrix}$.

2. Find unit vectors $\boldsymbol{x}$ at which M and m are attained by $q(\boldsymbol{x})$ of (a) and (b).

3. Suppose λ is an eigenvalue of a real symmetric matrix A and $q(\boldsymbol{x}) = \boldsymbol{x}^*A\boldsymbol{x}$. Show that $\lambda = q(\boldsymbol{x})$ for some $\boldsymbol{x}$ with $\|\boldsymbol{x}\| = 1$.

9.5 Singular Value Decomposition (SVD)

We know that the eigenvalues $\lambda_1, \ldots, \lambda_n$ of a real symmetric matrix A are all real and that A can be orthonormally diagonalized, i.e.

$$V^*AV = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \tag{9.5}$$

for V orthonormal. Equivalently we can write (9.5) as

$$A = VDV^* \tag{9.6}$$

and call (9.6) a spectral (or eigenvalue) decomposition of A.

Now given a non-symmetric, or even a non-square $m \times n$ real matrix, how close can we get to a decomposition of it like (9.6)? Of course, if $m \neq n$, (9.6) makes no sense. The best we can expect on the left of (9.5) is U^*AV for U an $m \times m$ orthonormal and V and $n \times n$ orthonormal. On the right of (9.5), we should expect an $m \times n$ matrix of zeros except a block of diagonal matrix D on its upper left corner. That this can always be done is the essence of the singular value decomposition or just SVD of any real matrix.

An $n \times n$ matrix A is non-singular if and only if $\lambda_j \neq 0$ for all $j = 1, \ldots, n$. The more the number of $\lambda_j = 0$, the further the matrix A from being non-singular. The signs of nonzero λ_j have no relevance in this context. Hence, we may call the absolute values of the eigenvalues of A its singular values.

To extend this notion to an arbitrary $m \times n$ real matrix, first note that for a real symmetric matrix A, the eigenvalues of $A^*A = A^2$ are non-negative. So the singular values of A are the square roots of those of A^*A. Therefore, for an arbitrary $m \times n$ real matrix, we should be able to obtain a singular value decomposition of A in this manner from that of the real symmetric matrix A^*A, provided the eigenvalues of A^*A are all non-negative.

Theorem 9.4. *Given an $m \times n$ real matrix A, all the eigenvalues of A^*A are non-negative.*

Proof. Let $\boldsymbol{v}$ be a unit eigenvector of A^*A belonging to a given eigenvalue λ of A^*A. Then

$$\begin{aligned}\|A\boldsymbol{v}\|^2 &= (A\boldsymbol{v})^*A\boldsymbol{v} = \boldsymbol{v}^*A^*A\boldsymbol{v} = \lambda\boldsymbol{v}^*\boldsymbol{v} \\ &= \lambda\|\boldsymbol{v}\|^2 = \lambda.\end{aligned}$$

Therefore $\lambda = \|A\boldsymbol{v}\|^2 \geq 0$. □

For a symmetric matrix, the number of its nonzero eigenvalues is its rank. To obtain a similar result for the rank of an $m \times n$ matrix A, not necessarily square, we arrange the eigenvalues of A^*A as

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

Theorem 9.5. *Let r be the largest index such that $\lambda_r > 0$. Then r is the rank of A. In fact, let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ be an orthonormal basis of $\mathbb{R}^n$ consisting of eigenvectors of A^*A belonging to the eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$. Then $\{A\boldsymbol{v}_1, \ldots A\boldsymbol{v}_r\}$ is an orthogonal basis for the column span of A.*

Proof. Clearly $A\boldsymbol{v}_1, \ldots, A\boldsymbol{v}_r$ are in the column space of A. We show that they form an orthogonal basis for the column space of A. Suppose $\boldsymbol{v}$ is a unit eigenvector belonging to any eigenvalue λ of A^*A. Then

$$\|A\boldsymbol{v}\|^2 = \lambda, \text{ so } A\boldsymbol{v} = 0 \Leftrightarrow \lambda = 0.$$

For $i \neq j$, $1 \leq i, j \leq r$,

$$(A\boldsymbol{v}_i) \cdot (A\boldsymbol{v}_j) = \boldsymbol{v}_j^*A^*A\boldsymbol{v}_i = \lambda_i\boldsymbol{v}_j^*\boldsymbol{v}_i = 0.$$

So $A\boldsymbol{v}_i$ and $A\boldsymbol{v}_j$ are orthogonal. All that remains to be proved now is that $A\boldsymbol{v}_1, \ldots, A\boldsymbol{v}_r$ span the column space of A.

So let $\boldsymbol{y} = A\boldsymbol{x}$ be any vector in the column space of A. We can certainly write

$$\boldsymbol{x} = c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n$$

as a linear combination of the (orthonormal) basis vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ of $\mathbb{R}^n$. Therefore,

$$\boldsymbol{y} = A\boldsymbol{x} = c_1A\boldsymbol{v}_1 + \cdots + c_rA\boldsymbol{v}_r$$

as $A\boldsymbol{v}_j = \lambda_j\boldsymbol{v}_j = 0$ for $j > r$.

We can now complete the proof the following important facts: □

Theorem 9.6. *Suppose A is an $m \times n$ real matrix. Then*

> *i) The eigenvalues of the $n \times n$ symmetric matrix A^*A are all non-negative. Let them be*
>
> $$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0. \tag{9.7}$$
>
> *If r is the largest index such that $\lambda_r > 0$, then r is the rank of A.*
>
> *ii) Let $\sigma_j = \sqrt{\lambda_j}$, $j = 1, \ldots, r$ and D the diagonal matrix*
>
> $$D = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_r \end{pmatrix}.$$
>
> *Let S be the $m \times n$ matrix with D as its upper left $r \times r$ block and all other entries zeros. There are orthonormal matrices U and V, U in $M(m, \mathbb{R})$, V in $M(n, \mathbb{R})$ such that*
>
> $$U^*AV = S \tag{9.8}$$
>
> *or equivalently*
>
> $$A = USV^*. \tag{9.9}$$

Proof. Let $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ be an orthonormal basis of $\mathbb{R}^n$ consisting of eigenvectors of A^*A with $\boldsymbol{v}_j$ belonging to λ_j, where λ_j is as in (9.7). Let V be the orthonormal matrix with $\boldsymbol{v}_j$ as its j-th column.

To construct U, put $\boldsymbol{u}_j = \frac{1}{\sigma_j} A\boldsymbol{v}_j$ or

$$A\boldsymbol{v}_j = \sigma_j \boldsymbol{u}_j \tag{9.10}$$

for $j = 1, \ldots, r$. Then $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r\}$ is an orthonormal set in $\mathbb{R}^m$. Extend it to an orthonormal basis $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_m\}$ of $\mathbb{R}^m$. Take U to be the orthonormal matrix with $\boldsymbol{u}_j$ as its j-th column. Then

$$\begin{aligned} AV &= (A\boldsymbol{v}_1 \ldots A\boldsymbol{v}_r A\boldsymbol{v}_{r+1} \ldots A\boldsymbol{v}_n) \\ &= (\sigma_1 \boldsymbol{u}_1 \ldots \sigma_r \boldsymbol{u}_r \mathbf{0} \ldots \mathbf{0}). \end{aligned}$$

On the other hand,

$$\begin{aligned} US &= (\boldsymbol{u}_1 \ldots \boldsymbol{u}_m) \left(\begin{array}{c|c} \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_r \end{pmatrix} & 0 \\ \hline 0 & 0 \end{array} \right) \\ &= (\sigma_1 \boldsymbol{u}_1 \ldots \sigma_r \boldsymbol{u}_r \mathbf{0} \ldots \mathbf{0}). \end{aligned}$$

So $US = AV$ or

$$U^*AV = S, \tag{9.11}$$

equivalently,

$$A = USV^*. \tag{9.12}$$

□

Definition. The *singular values* of a real $m \times n$ matrix A are the square roots σ of the positive eigenvalues λ of A^*A.

Corollary (Singular Value Decomposition)**.** *The equation* (9.12) *can be written as*

$$A = \sigma_1 \boldsymbol{u}_1 \boldsymbol{v}_1^* + \cdots + \sigma_r \boldsymbol{u}_r \boldsymbol{v}_r^*, \tag{9.13}$$

called the singular value decomposition (or SVD) of A.

The following summary of the proof also provides an algorithm to obtain an SVD of an $m \times n$ real matrix A. Note that by construction U and V are not unique, especially if an eigenvalue of A^*A repeats. However, the matrix S is unique.

Step 1. Find the eigenvalues

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$$

of A^*A. Put $\sigma_j = \sqrt{\lambda_j}$ for $j = 1, \ldots, r$ (r the largest index with $\lambda_j > 0$). Take

$$D = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_r \end{pmatrix}$$

and extend D to an $m \times n$ matrix S with the block D at its upper left corner, zeros elsewhere.

Step 2. Find an orthonormal basis $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ of $\mathbb{R}^n$ consisting of unit eigenvectors $\boldsymbol{v}_j$ belonging to λ_j. Take V to be the $n \times n$ (orthonormal) matrix with $\boldsymbol{v}_j$ as its j-th column.

Step 3. For $j = 1, \ldots, r$, put $\boldsymbol{u}_j = \frac{1}{\sigma_j} A\boldsymbol{v}_j$. Then $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r\}$ is an orthonormal set in $\boldsymbol{R}^m$. Extend it to an orthonormal basis $\{\boldsymbol{u}_1, \ldots \boldsymbol{u}_m\}$ of $\mathbb{R}^m$. Take U to be the $m \times m$ orthogonal matrix with $\boldsymbol{u}_j$ as its j-th column.

Step 4. Check that

$$USV^* = A.$$

Examples.

1. The matrix

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

is square but not symmetric.

Step 1. $A^*A = \begin{pmatrix} 5 & -3 \\ -3 & 5 \end{pmatrix}$. The eigenvalues of A^*A are 8 and 2, so its singular values are $2\sqrt{2}$ and $\sqrt{2}$ and

$$S = \begin{pmatrix} 2\sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

Step 2. Unit vectors of A^*A belonging to the eigenvalues 8 and 2 are

$$\boldsymbol{v}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \ \boldsymbol{v}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

So

$$V = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Step 3. $\boldsymbol{u}_1 = \frac{1}{\sigma_1}A\boldsymbol{v}_1 = \frac{1}{2\sqrt{2}}\begin{pmatrix} 2 & -2 \\ 1 & 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$. Similarly, $\boldsymbol{u}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Hence

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

Step 4. Check if we got the SVD of A:

$$\begin{aligned} USV^* &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2\sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -2 \\ 1 & 1 \end{pmatrix} = A. \end{aligned}$$

2. We now take a non-square matrix

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

Step 1. $A^*A = 9\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ and the eigenvalues of A^*A are 9 times that of $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ which are 2 and 0. (Why?) So the singular values of A are $\sqrt{18} = 3\sqrt{2}$ and 0, and

$$S = \begin{pmatrix} 3\sqrt{2} & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Step 2. Unit eigenvectors belonging to the eigenvalues 18 and 0 of A^*A are

$$\boldsymbol{v}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \ \boldsymbol{v}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

So

$$V = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Step 3. The first column of U is

$$\boldsymbol{u}_1 = \frac{1}{\sigma_1} A\boldsymbol{v}_1 = \frac{1}{3\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -2 & 2 \\ 2 & -2 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

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

To extend $\boldsymbol{u}_1$ to an orthonormal basis of $\mathbb{R}^3$, we pick any orthonormal basis $\boldsymbol{u}_2$, $\boldsymbol{u}_3$ of the orthogonal complement of $\boldsymbol{u}_1$, i.e. the solution space of

$$\boldsymbol{u}_1^* \cdot \boldsymbol{x} = \mathbf{0}$$

or

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

For that, start with any two linearly independent solutions, say $\boldsymbol{w}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ and $\boldsymbol{w}_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ so $\boldsymbol{u}_2 = \frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$.

For $\boldsymbol{u}_3$ we normalize $\boldsymbol{w}_3 - (\boldsymbol{w}_3 \cdot \boldsymbol{u}_2)\boldsymbol{u}_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \frac{1}{5}\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -\frac{2}{5} \\ \frac{4}{5} \\ 1 \end{pmatrix}$.

So $\boldsymbol{u}_3 = \frac{5}{\sqrt{45}}\begin{pmatrix} -\frac{2}{5} \\ \frac{4}{5} \\ 1 \end{pmatrix} = \frac{1}{\sqrt{45}}\begin{pmatrix} -2 \\ 4 \\ 5 \end{pmatrix}$, hence

$$U = \begin{pmatrix} -\dfrac{1}{3} & \dfrac{2}{\sqrt{5}} & -\dfrac{2}{\sqrt{45}} \\ -\dfrac{2}{3} & \dfrac{1}{\sqrt{5}} & \dfrac{4}{\sqrt{45}} \\ \dfrac{2}{3} & 0 & \dfrac{5}{\sqrt{45}} \end{pmatrix}.$$

Step 4. **Check** that $USV^* = A$. (Exercise!)

Application to Data Compression

It often becomes necessary to compress a large amount of data when the space available for its storage or transmission is limited. The *low-rank approximation* to an $m \times n$ matrix A provided by the singular value decomposition enables one to do that.

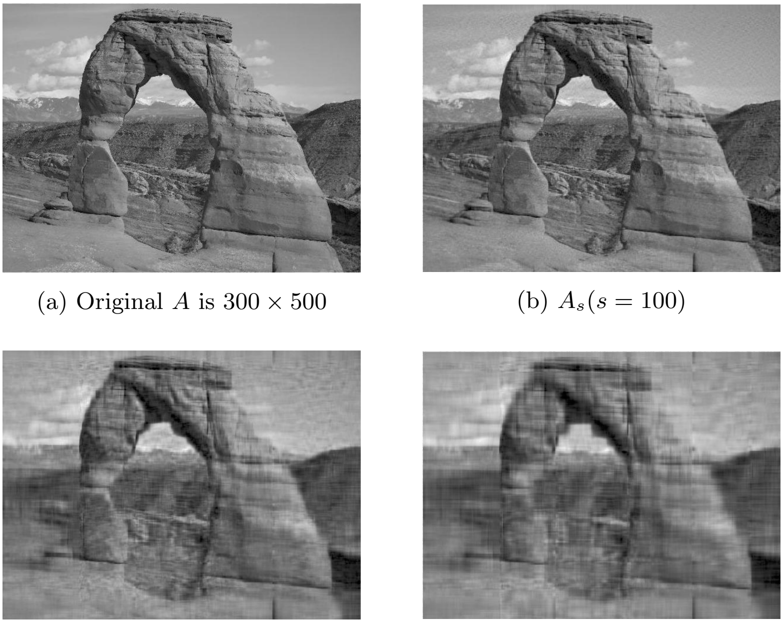
A black and white photograph can be scanned and stored as an $m \times n$ matrix A, giving each entry (pixel) a value, say a number between 0 (white) and 9 (black), depending on the shade of gray of that pixel. This requires mn numbers to be stored. However, using the singular value decomposition,

$$A = \sigma_1 \boldsymbol{u}_1 \boldsymbol{v}_1^* + \cdots + \sigma_r \boldsymbol{u}_r \boldsymbol{v}_r^*$$

of A, the matrix A can be recovered from its r singular values $\sigma_1, \dots, \sigma_r$ and the $2r$ vectors $\boldsymbol{u}_1, \dots, \boldsymbol{u}_r$ in $\mathbb{R}^m$ and $\boldsymbol{v}_1, \dots, \boldsymbol{v}_r$ in $\mathbb{R}^n$, needing only $r(m+n+1)$ entries to be stored. Moreover, if $\{\sigma_1, \dots, \sigma_s\}$ is a dominant set of singular values of A (meaning the remaining are small enough to be ignored), A can be approximated by its *s-rank approximation*

$$A_s = \sigma_1 \boldsymbol{u}_1 \boldsymbol{v}_1^* + \cdots + \sigma_s \boldsymbol{u}_s \boldsymbol{v}_s^*.$$

Recall that we follow the convention $\sigma_1 \geq \cdots \geq \sigma_r > 0$.



(a) Original A is 300×500

(b) $A_s(s = 100)$

(c) $A_s(s = 25)$

(d) $A_s(s = 15)$

FIGURE 9.1: Often the image constructed using A_s is hardly distinguishable from the original one, but the saving on the storage space is huge. For example, suppose the rank of a 300×500 matrix A that represents a 3×5 photograph is 100, but only the first 10 of its singular values are significant. The space needed to store $10(300 + 500 + 1) = 8010$ entries for A_{10} is minuscule compared to 150000 of A. Figure 9.1 illustrates this phenomenon. Note that (a) and (b) are indistinguishable, but (c) is not too bad either. Data compression comparison. Author's photographs of Delicate Arch, Moab, Utah.

EXERCISES

1. If A is square, show that $|\det A|$ is the product of its singular values.
2. If A is invertible, what is the singular value decomposition of A^{-1}?
3. Find the SVD of the following matrices and check your answer:

(a) $\begin{pmatrix} 3 & 5 \\ 4 & 0 \end{pmatrix}$ (b) $\begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & -2 \end{pmatrix}$ (c) $\begin{pmatrix} 7 & 1 \\ 0 & 0 \\ 5 & 5 \end{pmatrix}$ (d) $\begin{pmatrix} 2 & 5 & 4 \\ 6 & 3 & 0 \\ 6 & 3 & 0 \\ 2 & 5 & 4 \end{pmatrix}$

10

Selected Applications of Linear Algebra

Linear algebra appears almost everywhere in mathematics, so it will be a futile task even to list all its applications. In this chapter, we discuss a few of its standard and nonstandard, but non-trivial applications in computer science, engineering, physics, as well as mathematics itself.

10.1 System of First Order Linear Differential Equations

In Section 4.7 we saw that solving the linear differential equation $Ly = 0$ is the same as finding a basis of the vector space $V = \operatorname{Ker}(L)$, the kernel of the linear map L.

A linear differential equation $Ly = 0$ of order n is a special case of a system of first order linear differential equations

$$\begin{aligned} x_1'(t) &= a_{11}x_1(t) + \cdots + a_{1n}x_n(t) \\ &\vdots \\ x_n'(t) &= a_{n1}x_1(t) + \cdots + a_{nn}x_n(t) \end{aligned}$$

which has a matrix representation

$$X' = AX \tag{10.1}$$

with

$$X = \begin{pmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{pmatrix}, \ X' = \begin{pmatrix} x_1'(t) \\ \vdots \\ x_n'(t) \end{pmatrix} \text{ and } A = (a_{ij}).$$

To write the order n linear differential equation

$$x^{(n)} + a_{n-1}x^{(n-1)} + \cdots + a_1x' + a_0x = 0$$

we put $x = x_1$ and

$$\begin{aligned} x_1' &= x_2 \\ x_2' &= x_3 \\ &\vdots \\ x_{n-1}' &= x_n \\ x_n' &= -a_0x_1 - a_1x_2 - \cdots - a_{n-1}x_n. \end{aligned}$$

Note that the solution of (10.1) is the kernel of a linear map, and hence a vector space. Thus to find a general solution is the same as finding a basis for this vector space. The following theorem translates the formal solution $X(t) = e^{At}$ of (10.1) into the following algorithm. For the sake of simplicity in stating the theorem, we assume that all the eigenvalues of the matrix A are real and distinct. The case of repeated roots (real or imaginary) is analogous. For details, see a book on differential equations.

Theorem 10.1. *Let all the eigenvalues $\lambda_1, \ldots, \lambda_n$ of the $n \times n$ real matrix A be real and distinct and $\boldsymbol{E}_1, \ldots, \boldsymbol{E}_n$ are eigenvectors belonging to $\lambda_1, \ldots, \lambda_n$ respectively. Then a general solution of* (10.1) *is*

$$X(t) = c_1e^{\lambda_1 t}\boldsymbol{E}_1 + \cdots + c_ne^{\lambda_n t}\boldsymbol{E}_n,$$

$c_1, \ldots, c_n$ being arbitrary constants,

For a proof, see a book on differential equations.

Example. To solve

$$\begin{aligned} x_1' &= x_1 + 3x_2 \\ x_2' &= x_1 - x_2, \end{aligned}$$

we compute the eigenvalues λ_1, λ_2 of the matrix

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

which are $\lambda_1 = 2$, $\lambda_2 = -2$. Corresponding eigenvectors belonging to $\lambda_1 = 2$, $\lambda_2 = -2$ are $\boldsymbol{E}_1 = \binom{3}{1}$, $\boldsymbol{E}_2 = \binom{-1}{1}$. So a general solution of this system of first order linear differential equations is

$$X(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} = c_1e^{2t}\begin{pmatrix} 3 \\ 1 \end{pmatrix} + c_2e^{-2t}\begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

which can be rewritten as

$$\begin{aligned} x_1(t) &= 3c_1e^{2t} - c_2e^{-2t} \\ x_2(t) &= c_1e^{2t} + c_2e^{-2t}. \end{aligned}$$

EXERCISES

Solve the following systems of first order linear differential equations.

1) $x_1' = x_1 + 6x_2$

$x_2' = 5x_1 + 2x_2,$

2) $x_1' = x_1 - 2x_2$

$x_2' = x_1 - x_2.$

3) $x_1' = x_1 - x_2 + 4x_3$

$x_2' = 3x_1 + 2x_2 - x_3$

$x_3' = 2x_1 + x_2 - x_3$

10.2 Multivariable Calculus

We now apply the theory of quadratic forms we have learned to determine the nature of a critical point of a multivariable function $f(\boldsymbol{x}) = f(x_1, \ldots, x_n)$ of n variables $x_1, \ldots, x_n$. For this we first explain how to write its Taylor series at a point $\boldsymbol{a} = (a_1, \ldots, a_n)$ of the domain where $f(\boldsymbol{x})$ is *completely smooth*, i.e. all partial derivatives of every order exist. To do so in a neat and compact way, we use the following notion.

For an n-tuple $\boldsymbol{j} = (j_1, \ldots, j_n)$ of non-negative integers and $\boldsymbol{x} = (x_1, \ldots, x_n)$, we put

i) $|\boldsymbol{j}| = j_1 + \cdots + j_n$

ii) $\boldsymbol{j}! = j_1! \cdots j_n!$

iii) $\boldsymbol{x}^{\boldsymbol{j}} = x_1^{j_1} \ldots x_n^{j_n}$

vi) $\frac{\partial^{|\boldsymbol{j}|} f}{\boldsymbol{x}^{\boldsymbol{j}}} = \frac{\partial^{|\boldsymbol{j}|} f}{\partial x_1^{j_1} \ldots \partial x_n^{j_n}}.$

The *Taylor expansion* of $f(\boldsymbol{x})$ centered at $\boldsymbol{x} = \boldsymbol{a}$ is then the power series (which looks similar to the one variable case)

$$f(\boldsymbol{x}) = f(\boldsymbol{a}) + \sum_{|\boldsymbol{j}|>0} \frac{1}{\boldsymbol{j}!} \frac{\partial^{|\boldsymbol{j}|} f}{\partial \boldsymbol{x}^{\boldsymbol{j}}} (\boldsymbol{a})(\boldsymbol{x} - \boldsymbol{a})^{\boldsymbol{j}}. \tag{10.2}$$

In case $\boldsymbol{a} = \mathbf{0}$, (10.2) is called the *Maclaurin series* of $f(\boldsymbol{x})$ and has a simpler form

$$f(\boldsymbol{x}) = f(\mathbf{0}) + \sum_{|\boldsymbol{j}|>0} \frac{1}{\boldsymbol{j}!} \frac{\partial^{|\boldsymbol{j}|} f}{\partial \boldsymbol{x}^{\boldsymbol{j}}} (\mathbf{0}) \boldsymbol{x}^{\boldsymbol{j}}. \tag{10.3}$$

The linear term in (10.2) is

$$\frac{\partial f}{\partial x_1}(\boldsymbol{a})(x_1 - a_1) + \cdots + \frac{\partial f}{\partial x_n}(\boldsymbol{a})(x_n - a_n).$$

If $\boldsymbol{a} = \mathbf{0}$, twice the quadratic term in (10.3) is the quadratic form

$$Q(\boldsymbol{x}) = \sum_{i,j=1}^{n} \frac{\partial^2 f}{\partial x_i \partial x_j}(\mathbf{0}) x_i x_j.$$

It (or its matrix) is called the *Hessian* of f (at $\boldsymbol{x} = \mathbf{0}$) and denoted by $H(f)(\boldsymbol{x})$, or simply by $H(f)$.

Since moving the origin to $\boldsymbol{a}$ does not change the nature of a critical point $\boldsymbol{a}$ of $f(\boldsymbol{x})$, there is no loss of generality in assuming that the given critical point is indeed $\boldsymbol{a} = \mathbf{0}$. Then by definition, there is no linear term in the Maclaurin expansion (10.3) of $f(\boldsymbol{x})$, so that

$$f(\boldsymbol{x}) = f(\mathbf{0}) + \frac{1}{2} H(f) + \text{ higher order terms.} \tag{10.4}$$

Near the origin, the contribution of higher order terms in (10.4) to $f(\boldsymbol{x})$ is negligible and the nature of the critical point $\boldsymbol{a} = \mathbf{0}$ of $f(\boldsymbol{x})$ is determined by the Hessian $H(f)$.

Unless $\boldsymbol{a} = \mathbf{0}$, the quadratic terms in (10.2) are not a quadratic form. To avoid moving $\boldsymbol{a}$ to $\mathbf{0}$, define the *Hessian* of f at $\boldsymbol{x} = \boldsymbol{a}$ as the matrix $A = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right)_{|\boldsymbol{x}=\boldsymbol{a}}$, which is invariant under $\boldsymbol{x} \to \boldsymbol{x} - \boldsymbol{a}$. Then in the next theorem, we need not assume that the critical point $\boldsymbol{a} = \mathbf{0}$. Just go to the Hessian matrix of f at $\boldsymbol{a}$.

Theorem. *If $\boldsymbol{a} = \mathbf{0}$ is a critical point of $f(\boldsymbol{x})$, then it is a local minimum, a local maximum, or a saddle point according as the quadratic form $H(f)$ is positive definite, negative definite, or indefinite.*

Recall that a quadratic form is by definition

i) *positive definite* if $Q(\boldsymbol{x}) > 0$ for all $\boldsymbol{x} \neq \mathbf{0}$,

ii) *negative definite* if $Q(\boldsymbol{x}) < 0$ for all $\boldsymbol{x} \neq \mathbf{0}$, and

iii) *indefinite* if $Q(\boldsymbol{x}) > 0$ for the same $\boldsymbol{x}$ and < 0 for the some other $\boldsymbol{x}$.

If we write $Q(\boldsymbol{x}) = \boldsymbol{x}^* A \boldsymbol{x}$ with A $n \times n$ symmetric matrix, then $Q(\boldsymbol{x})$ is

i) *positive definite* if all the eigenvalues of A are positive,

ii) *negative definite* if all the eigenvalues of A are negative,

iii) *indefinite* if A has positive as well as negative eigenvalues.

Example. Consider the function

$$f(x_1,x_2) = x_1^2 - 5x_2^2 - 8x_1x_2 - 14x_1 - 28x_2 - 35$$

It is easy to check that $x_1 = -1$ and $x_2 = -2$ is a critical point of $f(x_1,x_2)$, i.e. a solution of $\frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = 0$. The Hessian

$$H(f) = \left.\begin{pmatrix} \dfrac{\partial^2 f}{\partial x_1^2} & \dfrac{\partial^2 f}{\partial x_1 \partial x_2} \\[2ex] \dfrac{\partial^2 f}{\partial x_2 \partial x_1} & \dfrac{\partial^2 f}{\partial x_2^2} \end{pmatrix}\right|_{(-1,-2)}$$
$$= \begin{pmatrix} 1 & -4 \\ -4 & -5 \end{pmatrix}.$$

The two eigenvalues of the matrix $H(f)$ are 3 and -7. Hence $x_1 = -1$, $x_2 = -2$ is a saddle point of $f(x_1,x_2)$.

Note. We may also use Theorem 9.2. However, Theorem 9.2 is applicable only to functions of two variables, whereas going to the eigenvalues works for the functions of any number of variables.

EXERCISES

1. Show that i) (0,0) is a critical point of $f(x_1,x_2) = e^{x_1^2 - 2\sqrt{3}x_1x_2 - x_2^2}$, and ii) find the nature of this critical point.

2. Check that i) (1,0) is a critical point of $f(x_1,x_2) = \ln(1 + 9x_1^2 + 3x_2^2 - 8x_1x_2 - 18x_1 + 8x_2 + 10)$, and ii) find the nature of this critical point.

10.3 Special Theory of Relativity

In this section, we study a special linear map $L : \mathbb{R}^4 \to \mathbb{R}^4$ to prove the assertion of Einstein's theory of relativity about the time contraction when objects are moving at speeds commensurable with that of light.

If you are driving at 40 miles/hour into wind blowing directly toward you at 60 miles/hour, it will hit you at 100 miles/hour. On the other hand, if you are driving away from it at the same speed, you will feel it coming at a speed of 20 miles/hour. The speed of light is $186,000$ miles/second. So if you are traveling with a speed of 100,000 miles/second toward an incoming beam of light, you would expect it to be traveling toward you at 286,000 miles/second, and only at 86,000 miles/second if you are running away from it with the same speed. During the late nineteenth century, it was established by various experiments, most notably by the Michelson-Morley experiment of 1887 that this is not so. The speed of light was measured to be the same 186,000 miles/second whether the measuring instrument was traveling toward or away from an incoming beam of light.

Soon thereafter, in 1905 this led Albert Einstein to publish his special theory of relativity (see [6]) using which he showed that this fact about the speed of light has some astonishing consequences. For example, suppose a cosmonaut blasts off from Earth in 2020 at 99% the speed of light to visit a star 49.5 light years away (this is the distance traveled by light in 49.5 years). As soon as she reaches the star, she turns around and heads back to Earth at the same speed. After a 100-year journey, when she is back on Earth in 2120, her clock shows that the journey took her only about 14 years. How is this possible?

Linear algebra can be used to capture the essence of Einstein's special theory of relativity, at least to prove this curious phenomenon. His revolutionary idea is that time is not absolute. The time of an event depends on its location.

The special theory of relativity establishes a correspondence between events as observed on two inertial (non-accelerating) coordinate systems which are in motion relative to each other with a constant velocity, under the assumption the speed of light measured on either system is the same.

An *event* (e.g. a flash of light) observed at a point (x, y, z) in space relative to a given choice of coordinate axes at a time t, measured by a clock stationary relative to these axes, can be represented by a vector (x, y, z, t) in $\mathbb{R}^4$, called the *space-time coordinates*, of the event. So if (x, y, z, t) and (x', y', z', t') are the space-time coordinates of the same event as observed in two coordinate systems there is a map

$$(x', y', z', t') = L(x, y, z, t), \tag{10.5}$$

called the *Lorentz transformation*, which describes this correspondence. One of the postulates of the special theory of relativity is that the map L is a length preserving bijective linear transformation from $\mathbb{R}^4$ to $\mathbb{R}^4$. Moreover, if the coordinates axes in the two bases are aligned properly, L has no effect on the x- and y-coordinates of the event (x, y, z, t). All the information about L is contained in its action on the other two coordinates of the event.

Any linear map $L : V \to W$ of finite dimensional vector spaces is given by a matrix P, once we have chosen our coordinate systems, i.e. a pair of ordered bases $\mathcal{B}_V$ and $\mathcal{B}_W$ of V and W, respectively. In particular, if $V = W = \mathbb{R}^4$ and the chosen basis for $\mathbb{R}^4$ is the standard basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_4$ with $\boldsymbol{e}_1 = (1,0,0,0), \ldots, \boldsymbol{e}_4 = (0,0,0,1)$, then the j-th column of P is $L\boldsymbol{e}_j, j = 1, \ldots, 4$.

Let W_1 be the subspace of $\mathbb{R}^4$ spanned by $\boldsymbol{e}_1, \boldsymbol{e}_2$ and $W_2 = \operatorname{span}\{\boldsymbol{e}_3, e_4\}$. We regard $\mathbb{R}^4$ as an inner product space under the dot product. Then W_1 and W_2 are orthogonal complements of each other. Moreover $\mathbb{R}^4$ is a direct sum $\mathbb{R}^4 = W_1 \oplus W_2$, in other words, every $\boldsymbol{w}$ in $\mathbb{R}^4$ is a unique sum $\boldsymbol{w} = \boldsymbol{w}_1 + \boldsymbol{w}_2$ with $\boldsymbol{w}_j$ in W_j, $j = 1, 2$. Each subspace W_j is *invariant* under L, i.e. $L(\boldsymbol{w}_j)$ is in W_j for all $\boldsymbol{w}_j$ in W_j $(j = 1, 2)$.

Now suppose we have two frames of reference, that is, two coordinate systems or bases $\mathcal{B}$ and $\mathcal{B}'$ to represent the space-time coordinates (x, y, z, t) and (x', y', z', t') of an event. By this we mean $\mathcal{B}$ (similarly $\mathcal{B}'$) consists of coordinate axes: x-axis, y-axis, and z-axis to locate the position (x, y, z) and a clock C placed at a fixed point (x_0, y_0, z_0) to register the time t of the event. It is assumed that initially, i.e. at the time $t = 0$, both the clocks C and C' register time $t' = t = 0$, x'-axis coincides with x-axis, y'-axis coincides with y-axis, and z'-axis coincides with z-axis. The system B' is in motion relative to $\mathcal{B}$ along the positive direction of z-axis at a constant speed v, while the other two axes of the two systems stay parallel (see Figure 10.1).

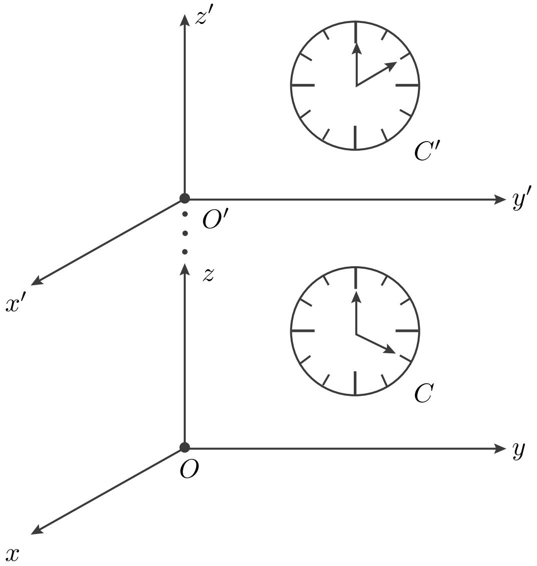


FIGURE 10.1: Clocks in motion relative to each other

It is assumed there is a symmetry between $\mathcal{B}$ and $\mathcal{B}'$. To be precise, $\mathcal{B}'$ is moving relative to $\mathcal{B}$ with velocity v in the positive direction of z-axis if and only if $\mathcal{B}$ is moving relative to $\mathcal{B}'$ with velocity v in the negative direction of z'-axis. Einstein made the following two postulates on which to base his special theory of relativity.

Postulate 1 (The Principle of Relativity) The laws of physics are the same in all inertial frames of reference.

Postulate 2 (The consistency of the speed of light.) The speed of light is the same in all inertial systems.

Our unit of time is 1 second and the unit of length the distance traveled by light in 1 second. Thus the speed of light is 1/second. Under this set up, we rephrase for our purpose the postulates of the special theory of relativity as follows:

Postulate 1 The correspondence in equation (10.5) is a length preserving bijective linear map $L : \mathbb{R}^4 \to \mathbb{R}^4$ such that

i) its restriction $L_{|W_1}$, is the identity map on W_1, and

ii) W_2 is invariant under L.

Postulate 2 The speed of light is 1/sec. whether observed in the frame of reference $\mathcal{B}$ or $\mathcal{B}'$.

We show that those postulates determine L uniquely. The map L is called the *Lorentz transformation*. In fact, the matrix P of L with respect to the standard basis of $\mathbb{R}^4$ is

$$P = \left(\begin{array}{c|c} I & O \\ \hline O & B \end{array}\right),$$

where each block of P is a 2×2 matrix and

$$B = \begin{pmatrix} 1/\sqrt{1-v^2} & -v/\sqrt{1-v^2} \\ -v/\sqrt{1-v^2} & 1/\sqrt{1-v^2} \end{pmatrix}.$$

Computing the Matrix of the Lorentz Transformation

1. Basic Lemmas

In view of our set up and the postulates of the special theory of relativity, the only thing that needs to be proved is the assertion about the block B in the matrix P.

Let E be the set of events whose space-time coordinates are (x, y, z, t) relative to $\mathcal{B}$. Since the speed of light is 1/sec., the points at which an event is observed at a time t (say $t \geq 0$), are at a distance $t \cdot 1 = t$ from the origin O of the coordinate axis of $\mathcal{B}$ (assuming the same event was observed initially (meaning $t = 0$) at the origin when $\mathcal{B}$ and $\mathcal{B}'$ overlapped). Therefore, their space-time coordinates satisfy the equation

$$x^2 + y^2 + z^2 - t^2 = 0. \tag{10.6}$$

By Postulate 2, the space-time coordinates (x', y', z', t') of the same event in $\mathcal{B}'$ satisfy

$$x'^2 + y'^2 + z'^2 - t'^2 = 0. \tag{10.7}$$

Thus (10.6) will hold if and only if (10.7) holds.

For a real matrix P, we denote its transpose by P^*. In our discussion, a crucial role is played by the matrix

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

Lemma 10.2. *For $\boldsymbol{w}$ in $\mathbb{R}^4$, written as a column vector, $A\boldsymbol{w}$ is orthogonal to $\boldsymbol{w}$ if and only if $P^*AP\boldsymbol{w}$ is orthogonal to $\boldsymbol{w}$.*

Proof. The vector

$$\boldsymbol{w} = \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}$$

in $\mathbb{R}^4$ is orthogonal to $A\boldsymbol{w}$ if $A\boldsymbol{w} \cdot \boldsymbol{w} = 0$ which is the same as equation (10.6). By assumption, the map $\boldsymbol{w} \to P\boldsymbol{w}$ is length preserving, equivalently P is orthonormal ($P^*P = I$). So $P^*AP\boldsymbol{w}$ is orthogonal to $\boldsymbol{w} \Leftrightarrow P^*AP\boldsymbol{w} \cdot \boldsymbol{w} = 0 \Leftrightarrow PP^*AP\boldsymbol{w} \cdot P\boldsymbol{w} = 0 \Leftrightarrow AP\boldsymbol{w} \cdot P\boldsymbol{w} = 0 \Leftrightarrow$ (10.7) holds since

$$P\boldsymbol{w} = \begin{pmatrix} x' \\ y' \\ z' \\ t' \end{pmatrix}.$$

Since (10.6) and (10.7) are equivalent, we are done. □

The vectors

$$\boldsymbol{w}_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \quad \boldsymbol{w}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$$

form an orthogonal basis of W_2. They are special in the following way.

Lemma 10.3.

$$\text{i) } P^*AP\boldsymbol{w}_1 = a\boldsymbol{w}_2,$$
$$\text{ii) } P^*AP\boldsymbol{w}_2 = b\boldsymbol{w}_1$$

for nonzero scalars a and b.

Proof. Because $A\boldsymbol{w}_1 \cdot \boldsymbol{w}_1 = 0$, we get by Lemma 10.2, $P^*AP\boldsymbol{w}_1 \cdot \boldsymbol{w}_1 = 0$. Therefore by the invariance of W_2 under P, if $P^*AP\boldsymbol{w}_1$ is orthogonal to $\boldsymbol{w}_1$ it must be a nonzero multiple of $\boldsymbol{w}_2$. This proves i). Part ii) follows at once from Part i) on multiplying each side on the left by P^*AP. □

Lemma 10.4. $P^*AP = A$.

Proof. We write P^*AP block by block as

$$P^*AP = \left(\begin{array}{c|c} I & O \\ \hline O & C \end{array}\right),$$

each block being a 2×2 matrix. By Lemma 10.3, the first and second columns of C are

$$C\begin{pmatrix}1\\0\end{pmatrix} = C\,\frac{1}{2}\left(\begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}1\\-1\end{pmatrix}\right) = \frac{1}{2}\left[C\begin{pmatrix}1\\1\end{pmatrix} + C\begin{pmatrix}1\\-1\end{pmatrix}\right]$$
$$= \frac{1}{2}\left[\begin{pmatrix}a\\-a\end{pmatrix} + \begin{pmatrix}b\\b\end{pmatrix}\right] = \begin{pmatrix}\dfrac{a+b}{2}\\ -\dfrac{a-b}{2}\end{pmatrix}$$

and similarly,

$$C\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\dfrac{a-b}{2}\\ -\dfrac{a+b}{2}\end{pmatrix}.$$

Since C is symmetric, it follows that $a = b$. Hence

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

which proves the lemma. □

Computing the matrix P

To compute P, consider the situation 1 second after the origins O and O' of $\mathcal{B}$ and $\mathcal{B}'$ have coincided as measured by the clock C of $\mathcal{B}$. Since O' is moving in the positive direction of z-axis with constant velocity v; its space-time coordinates relative to $\mathcal{B}$ are $(0, 0, v, 1)$, whereas, its space-time coordinates relative to $\mathcal{B}'$ are $(0, 0, 0, t')$ for some $t' > 0$, measured by the clock C'. By Lemma 10.4,

$$P^*AP \begin{pmatrix}0\\0\\v\\1\end{pmatrix} \cdot \begin{pmatrix}0\\0\\v\\1\end{pmatrix} = A \begin{pmatrix}0\\0\\v\\1\end{pmatrix} \cdot \begin{pmatrix}0\\0\\v\\1\end{pmatrix} = v^2 - 1. \tag{10.8}$$

On the other hand, since the matrix P^*AP is orthonormal,

$$P^*AP \begin{pmatrix}0\\0\\v\\1\end{pmatrix} \cdot \begin{pmatrix}0\\0\\v\\1\end{pmatrix} = AP \begin{pmatrix}0\\0\\v\\1\end{pmatrix} \cdot P \begin{pmatrix}0\\0\\v\\1\end{pmatrix} = A \begin{pmatrix}0\\0\\0\\t'\end{pmatrix} \cdot \begin{pmatrix}0\\0\\0\\t'\end{pmatrix} = -t'^2. \tag{10.9}$$

From (10.8) and (10.9), we get the following fundamental relationship - the dependence of t' on v.

$$\boxed{t' = \sqrt{1 - v^2}}. \tag{10.10}$$

This gives

$$P \begin{pmatrix}0\\0\\v\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\\sqrt{1-v^2}\end{pmatrix}. \tag{10.11}$$

Next, by the symmetry between $\mathcal{B}$ and $\mathcal{B}'$, 1 second (measured by the clock C) after O and O' have coincided, the space-time coordinates of O relative $\mathcal{B}'$ are

$$\begin{pmatrix}0\\0\\-vt''\\t''\end{pmatrix}$$

for some t'' (measured by the clock C'). Thus

$$\begin{pmatrix}0\\0\\-vt''\\t''\end{pmatrix} = P \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Now on one hand,

$$P^*AP\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\cdot\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = AP\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\cdot P\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

$$= A\begin{pmatrix}0\\0\\-vt''\\t''\end{pmatrix}\cdot\begin{pmatrix}0\\0\\-vt''\\t''\end{pmatrix} = t''^2(v^2-1). \tag{10.12}$$

But on the other hand, by Lemma 10.4, we have

$$P^*AP\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\cdot\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = A\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\cdot\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = -1. \tag{10.13}$$

Therefore by (10.12) and (10.13),

$$t'' = 1/\sqrt{1-v^2},$$

so that

$$P\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\-v/\sqrt{1-v^2}\\1/\sqrt{1-v^2}\end{pmatrix}. \tag{10.14}$$

We now return to

$$P = \left(\begin{array}{c|c} I & O \\ \hline O & B\end{array}\right). \tag{10.15}$$

In the standard basis of $\mathbb{R}^4$, (10.14) is the last column of P. Therefore the last column of B is

$$\begin{pmatrix}\dfrac{-v}{\sqrt{1-v^2}}\\ \dfrac{1}{\sqrt{1-v^2}}\end{pmatrix}.$$

Finally, by (10.11) and (10.14), the third column of P is $P\boldsymbol{e}_3 =$

$$P\frac{1}{v}\left(\begin{pmatrix}0\\0\\v\\1\end{pmatrix}-\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right)=\frac{1}{v}\left(P\begin{pmatrix}0\\0\\v\\1\end{pmatrix}-P\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right)$$

$$=\frac{1}{v}\left(\begin{pmatrix}0\\0\\0\\\sqrt{1-v^2}\end{pmatrix}-\begin{pmatrix}0\\0\\-v/\sqrt{1-v^2}\\1/\sqrt{1-v^2}\end{pmatrix}\right)$$

$$=\begin{pmatrix}0\\0\\1/\sqrt{1-v^2}\\-v/\sqrt{1-v^2}\end{pmatrix}.$$

Therefore

$$B=\begin{pmatrix}\dfrac{1}{\sqrt{1-v^2}} & \dfrac{-v}{\sqrt{1-v^2}}\\ -\dfrac{v}{\sqrt{1-v^2}} & \dfrac{1}{\sqrt{1-v^2}}\end{pmatrix}. \tag{10.16}$$

Theorem 10.5. *The matrix P with respect to the standard basis of $\mathbb{R}^4$ of the Lorentz transformation $L:\mathbb{R}^4\to\mathbb{R}^4$ is as in* (10.15) *where B is given by* (10.16)*.*

2. Time Contraction

We now derive, as an easy consequence of Theorem 10.5, one of the main conclusions of the special theory of relativity.

Suppose the origin O of $\mathcal{B}$, is a cosmodrome somewhere on the globe and O' is the spaceship that blasts off the Earth from this cosmodrome carrying the cosmonaut for a trip to a distant star with velocity v. As viewed from the cosmodrome the space-time coordinates of the spaceship at a time $t>0$ (registered by the clock in the cosmodrome) are $(0,0,vt,t)$ whereas as observed by the cosmonaut, her space-time coordinates are $(0,0,0,t')$. Since the two are the space-time coordinates of the same event relative to $\mathcal{B}$ and $\mathcal{B}'$,

$$\begin{pmatrix}0\\0\\0\\t'\end{pmatrix}=P\begin{pmatrix}0\\0\\vt\\t\end{pmatrix}. \tag{10.17}$$

Since P is given by Theorem 10.5, it follows from (10.17) that

$$\boxed{t' = t\sqrt{1-v^2}}. \tag{10.18}$$

The factor $\sqrt{1-v^2}$ is called the *time contraction.*

Now, if the star is 49.5 light years away, and the velocity of the spaceship is .99/sec, i.e. 99% of the speed of light, according to the calendar kept at the cosmodrome, the round trip to the star by the spaceship will take 100 years. So $t = 100$, whereas the time t' measured by the clock C' on the spaceship, is only $t' = 100\sqrt{1-.99^2} = 14.14$ years. So according to her own clock, only 14.14 years have passed since the cosmonaut left the cosmodrome.

Remarks.

1. In order to simplify our calculations, we have taken the unit of length to be the distance traveled in 1 second by a beam of light. Physicists however like to take it to be the traditional one, for example, in the USA, it is $c = 186,000$ miles/second. Then v is also in miles/second. So v has to be replaced by v/c everywhere in our discussion. For example, equation (10.18) becomes

$$t' = t\sqrt{1-\frac{v^2}{c^2}}\,. \tag{10.19}$$

2. If $v = c$, $t' = 0$, so the clock C' stops running.

3. According to the special theory of relativity, nothing can travel faster than the speed of light, because we cannot take the square-root of the negative quality $1-\frac{v^2}{c^2}$ in equation (10.19).

4. *Length contraction.* The quantity $\gamma(v) = \sqrt{1-\frac{v^2}{c^2}}$ is called the *Lorentz factor*. It is easy to see that if a rod of length ℓ is moving in a straight line (with its two ends staying on the line of motion) on which an observer is located, to him the rod will appear to be only $\ell\cdot\gamma(v)$ long. In other words, the lengths of moving rods contract by the factor $\gamma(v)$. If $v = c$, the rod disappears from sight.

10.4 Cryptography

In this section, we use the linear map $\boldsymbol{x} \to A\boldsymbol{x}$ combined with a shift, over (the rings of) finitely many scalars as an introduction to cryptography.

Cryptography is the science of sending a message in disguise so that only the intended recipient should be able to read it. The scrambling of the message at the source is called *encryption*, the scrambled message is called the *ciphertext*. The process of recovering the original message or the *plaintext* from the ciphertext is called *decryption*. This is a very old science. Julius Caesar used to move every letter in his message to third down in the alphabet in a circular order so that A goes to D, B goes to $E, \ldots, X$ goes to A, Y to B, and Z to C. For example, he would send the message

ATTACKATMIDNIGHT

as

DWWDFNDWPLGQLJKW.

Only his generals had the key to recover the message.

We can formulate the basic idea of cryptography as follows. First, we have an alphabet, which is a set $\aleph$ consisting of letters A, B, C,...; the punctuation signs, comma, period, etc.; the ten digits $0, 1, \ldots, 9$; arithmetic symbols $+, \times, \ldots$; and so on. An encryption is a permutation on $\aleph$, whose elements are called letters, symbols, or characters. A *message* is a string $x_1 \ldots x_r$ of elements of $\aleph$. If the encryption is the permutation $\sigma : \aleph \to \aleph$, the ciphertext is the string $y_1 \ldots y_r$, where $y_j = \sigma(x_j)$. Since the recipient also knows which σ is being used, he or she can recover the message as $\sigma^{-1}(y_1) \ldots \sigma^{-1}(y_r)$. The whole set up is called a *cryptosystem*.

Breaking the code means figuring out which σ is being used by the sender and hence σ^{-1} by the recipient. For example, to break a Caesar-like or *Caesarean encryption*, with his three hops replaced by say, a shift to the fourth place down the alphabet, one does the "frequency analysis." The most frequent letter in English is e. Hence in this ciphertext, the most frequent letter will be i, from which one can figure out this code.

A slightly improved cryptosystem is the "Vigenère cipher" (named after Blaise de Vigenère), which had been in use for several centuries. The mathematical way to explain it (in fact, all cryptosystems) is to assign each letter of the alphabet a numerical value, usually zero to A, one to B, ..., twenty-five to Z. The addition and multiplication are "modular" modulo 26. The sum (or product) of two letters is the letter that corresponds to the remainder of the sum (or product) of their numerical values under division by 26. For example, X + Y = 23 + 24 = 47, which is 21 modulo 26. Hence X + Y = V. Similarly, H · E = 7 · 4 = 28, which is 2 mod 26. So H · E = C. The same way, −Q = K, because K + Q = 26 is zero mod 26, J^{-1} = D as J · D is one mod 26.

In the *Vigenère cipher*, one chooses a favorite word of desired length, say BLUE of length four and groups the plaintext into blocks of four letters, e.g. *ATTA CKAT MIDN IGHT*. The first letter in each block is moved to the right by one (the numerical value of B), the second letter by eleven (the numerical value of L), and so on. Thus

ATTACKATMIDNIGHT

will be sent as

BENEDVUXNTXRJRBX.

To recover the original message one has to reverse the process.

It is not too hard to break the Vigenère cipher by doing the frequency analysis on corresponding letters of blocks provided one can find out somehow the length of the sender's favorite word.

Affine Cryptosystems

Caesarean and Vigenère ciphers are special cases of more complex cryptosystems, which are harder to break. These are called *affine cryptosystems*. In these systems one first decides the dimension $d \geq 1$ for the system and then chooses a $d \times d$ matrix A, a column vector $\boldsymbol{b}$ with d components, the entries of A, $\boldsymbol{b}$ taken from the numerical values given to the letters of the alphabet $\aleph$. It is required that $\det(A)$ has no common factor larger than one with the number of letters in $\aleph$. For example, if $\aleph$ is the usual alphabet A–Z, $\det(A)$ must be an odd number other than 13. This guarantees that A is invertible with entries of A^{-1} also in $\aleph$.

The plaintext is grouped into blocks of d letters and each block is written as a column vector $\boldsymbol{x}$ with d components. In case $d = 2$, $\boldsymbol{x}$ is called a *digraph.* An affine cryptosystem is the map

$$\boldsymbol{y} = A\boldsymbol{x} + \boldsymbol{b} \tag{10.20}$$

applied to each block $\boldsymbol{x}$ of the plaintext. It is a linear map if and only if $\boldsymbol{b} = \mathbf{0}$. Note that the inverse

$$\boldsymbol{x} = A^{-1}\boldsymbol{y} - A^{-1}\boldsymbol{b} \tag{10.21}$$

of (10.20) is also affine. An affine cryptosytem is harder to break even if the dimension $d = 1$. Note that one has only to know one encryption key (A and $\boldsymbol{b}$) or decryption key (A^{-1} and $A^{-1}\boldsymbol{b}$) in order to know the other.

Example. Let us pretend to have only nine letters A–I in our alphabet $\aleph$, so that $\aleph = \{0, 1, \ldots, 8\}$ with A as $0, \ldots, I$ as 8. We choose the dimension $d = 2$ and

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

[Note the perversity of having to use the letter A also as a 2×2 matrix consisting of letters from our alphabet A–Z.] Then $\det(A) = 2$, which is invertible mod 9. In fact, its inverse $(\det(A))^{-1}$ (mod 9) is 5, because 2 times 5 is 1 (mod 9). Hence, by modular arithmetic mod 9,

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

$$= \begin{pmatrix} 10 & 25 \\ 40 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 7 \\ 4 & 6 \end{pmatrix}.$$

We check that

$$\begin{pmatrix} 1 & 7 \\ 4 & 6 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

In the Affine cryptosystem (10.20) we also choose

$$\boldsymbol{b} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Suppose in the plaintext, there is a word ACID. We write ACID as

$$\boldsymbol{x}_1 = \begin{pmatrix} \text{A} \\ \text{C} \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \; \boldsymbol{x}_2 = \begin{pmatrix} \text{I} \\ \text{D} \end{pmatrix} = \begin{pmatrix} 8 \\ 3 \end{pmatrix}.$$

With A and $\boldsymbol{b}$ as above,

$$\boldsymbol{y}_1 = A\boldsymbol{x}_1 + \boldsymbol{b} = \begin{pmatrix} 1 \\ 7 \end{pmatrix} = \begin{pmatrix} \text{B} \\ \text{H} \end{pmatrix}$$

$$y_2 = A\boldsymbol{x}_2 + \boldsymbol{b} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} \text{C} \\ \text{B} \end{pmatrix}.$$

Therefore the plaintext ACID is encrypted as BHCD.

We leave it as an exercise to use (10.21) to recover the original message ACID.

Breaking an Affine Cryptosystem

Suppose we know our enemy is using the affine encryption (10.20) on digraphs (blocks of 2 letters from our usual alphabet A–Z of 26 letters). To break the code, we must find out A and $\boldsymbol{b}$ in (10.20). To do that we need to know somehow three digraph pairs, i.e. three digraphs $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3$ in the plaintext and the corresponding $\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3$ in the ciphertext. In other words

$$\boldsymbol{y}_j = A\boldsymbol{x}_j + \boldsymbol{b} \quad (j = 1, 2, 3).$$

That will give

$$\left.\begin{aligned} \boldsymbol{y}_3 - \boldsymbol{y}_1 &= A(\boldsymbol{x}_3 - \boldsymbol{x}_1) \\ \text{and} \qquad \\ \boldsymbol{y}_3 - \boldsymbol{y}_2 &= A(\boldsymbol{x}_3 - \boldsymbol{x}_2) \end{aligned}\right\}. \tag{10.22}$$

We can write (10.22) as a simple matrix equation

$$Z = AC$$

where C is the matrix with columns $\boldsymbol{c}_1 = \boldsymbol{x}_3 - \boldsymbol{x}_1$, $\boldsymbol{c}_2 = \boldsymbol{x}_3 - \boldsymbol{x}_2$ and Z with columns $\boldsymbol{z}_1 = \boldsymbol{y}_3 - \boldsymbol{y}_1$, $\boldsymbol{z}_2 = \boldsymbol{y}_3 - \boldsymbol{y}_2$. Suppose C is invertible. Then

$$A = ZC^{-1}$$

and

$$\boldsymbol{b} = \boldsymbol{y}_j - A\boldsymbol{x}_j.$$

Example. Suppose we know that the last six letters NXJOUU in the ciphertext stand for the signature ALBERT of our enemy. Thus we write ALBERT as

$$\boldsymbol{x}_1 = \begin{pmatrix} 0 \\ 11 \end{pmatrix}, \ \boldsymbol{x}_2 = \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \ \boldsymbol{x}_3 = \begin{pmatrix} 17 \\ 19 \end{pmatrix}$$

and NXJOUU as

$$\boldsymbol{y}_1 = \begin{pmatrix} 13 \\ 23 \end{pmatrix}, \ \boldsymbol{y}_2 = \begin{pmatrix} 9 \\ 14 \end{pmatrix}, \ \boldsymbol{y}_3 = \begin{pmatrix} 20 \\ 20 \end{pmatrix}.$$

We are lucky that $C = \begin{pmatrix} 17 & 16 \\ 8 & 15 \end{pmatrix}$ is invertible $\pmod{26}$ and

$$\begin{aligned} A = ZC^{-1} &= \begin{pmatrix} 7 & 11 \\ 23 & 6 \end{pmatrix} \begin{pmatrix} 21 & 14 \\ 20 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \boldsymbol{b} &= \boldsymbol{y}_2 - A\boldsymbol{x}_2 \\ &= \begin{pmatrix} 9 \\ 14 \end{pmatrix} - \begin{pmatrix} 7 \\ 13 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}. \end{aligned}$$

EXERCISES

1. In Example 1, we recover the plaintext.

2. Let the alphabet $\aleph$ consists of $p = 29$ symbols: 26 letters, A, B, C, … and three punctuation signs. Identify $\aleph$ with the finite field $\mathbb{F}_p$ by letting A, B, C, … be $0, 1, 2, \ldots$, blank space with 26, period with 27, and the question mark ? with 28.

   (a) Suppose you want to arrange a clandestine meeting: Use the encryption
   $$y = \sigma(x) = 5x + 7 \tag{10.23}$$
   to send the following message to your accomplice.

   WHERE IN PEEWAUKEE SHALL WE MEET?

   (b) Break the code (10.23), i.e., find σ^{-1}, using frequency analysis of the ciphertext in (a).

   (c) Suppose $d = 3$ and A the non-singular matrix
   $$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 2 & 3 & 5 \end{pmatrix}$$
   over $\mathbb{F}_p$ $(p = 29)$. Encrypt the message in (a) using blocks $\boldsymbol{x}$ of three letters on the plaintext and $\boldsymbol{y} = A\boldsymbol{x}$.

   (d) How can one break the code in (c)?

3. Let $\aleph$ be the alphabet A–Z with zero assigned to A, …, 25 to Z. Let (mod 26)
   $$A = \begin{pmatrix} 9 & 2 \\ 11 & 3 \end{pmatrix}, \; \boldsymbol{b} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$
   In arithmetic modulo 26,

   (a) Compute A^{-1}.

   (b) Encrypt and decrypt the message

   ATTACKATMIDNIGHT

   in the affine cryptosystem $\boldsymbol{y} = A\boldsymbol{x} + \boldsymbol{b}$.

   (c) Suppose the last 6 letters HEPLMI in the ciphertext stand for the signature JOSEPH of our adversary. We know that he is using the affine cryptosystem on digraphs on the 26-letter alphabet A-Z with the usual numerical values 0–25 given to these letters. Compute A and $\boldsymbol{b}$. Check your answer by encrypting JOSEPH.

10.5 Solving Famous Problems from Greek Geometry

In this section, we will use a special property of the vector spaces of polynomials of bounded degrees to show that it is impossible, using a straightedge and a compass only, to trisect angles and duplicate cubes.

It took two millennia to settle those problems (see [18]). It is beyond linear algebra alone to tackle the third famous problem from Greek geometry. However, we shall go as far as possible to show what goes into proving the impossibility of squaring a circle. We highly recommend the great classics by Emil Artin [1] and Felix Klein [12] cited in the Bibliography. In this section, all fields considered are subfields of the field $\mathbb{C}$ of complex numbers.

10.5.1 Vector Spaces of Polynomials

Besides high school algebra, all we need to prove the impossibility of these geometric constructions is a special feature of the n-dimensional vector space $P_n(k)$ of polynomials of degree less than n over a field of k. If we think of these polynomials as remainders under (long) divisions of polynomials when divided by a fixed irreducible polynomial of degree n, the same kind of modular arithmetic that we used in cryptography turns the vector space $P_n(k)$ into a field K. The same can be repeated with $P_m(K)$, the vector space of polynomials of degree less than m over K to obtain a field L. Clearly L is a vector space over k. The crucial ingredient in our proofs is the following lemma.

Lemma 10.6. *Suppose k is a subfield of K, and K a subfield of L. Then as vector spaces,*

$$\dim_k L = \dim_k K \cdot \dim_K L.$$

The proof is straightforward. If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L over K and $\{\beta_1, \ldots, \beta_m\}$ that of K over k, then it can be checked easily that $\{\alpha_i\beta_j \mid i = 1, \ldots, n; j = 1, \ldots, m\}$ is a basis of L over k. An immediate consequence of the lemma is the following fact.

Theorem 10.7. *If we have an ascending chain*

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

of fields and as vector spaces $\dim_{K_{i-1}} K_i = d_i$, then $\dim_{K_0} K_r = d_1 \ldots d_r$.

Our first task is to explain the modular arithmetic for polynomials.

The integers and the polynomials have strikingly similar arithmetic. Suppose k is a subfield of $\mathbb{C}$. Then $\mathbb{Q} \subseteq k \subseteq \mathbb{C}$. A *polynomial over k* is a formal expression

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

with coefficients a_j in k. The symbol $f(x) \in k[x]$ means that $f(x)$ is a polynomial over k. If $a_n \neq 0$, we call n the *degree* of $f(x)$. We write $n = \deg f(x)$. If $a_n = 1$, we call $f(x)$ *monic*.

We take it for granted that the reader knows how to add and multiply polynomials. It is also assumed that he or she knows how to perform the "long division" to get the quotient and the remainder. Note that if $f(x)$, $g(x) \in k[x]$, then $f(x)+g(x)$ and $f(x)g(x)$ are also in $k[x]$. If $f(x)$, $g(x) \in k[x]$ and $\deg f(x) > 0$ we write under long division,

$$g(x) = q(x)f(x) + r(x) \tag{10.24}$$

with $\deg r(x) < \deg f(x)$. The *quotient* $q(x)$ and the *remainder* $r(x)$ are also in $k[x]$. If the *remainder* $r(x)$ in (10.24) is zero, we say that $f(x)$ *divides* $g(x)$ or $f(x)$ is a *factor* of $g(x)$, or that $g(x)$ is a *multiple* of $f(x)$. We call $f(x)$ *irreducible over* k or *prime* (like prime numbers) if it has no non-trivial factor, from which we mean a factor of positive degree less than that of $f(x)$. If the field k is clear from the context, we shall call $f(x)$ *irreducible*. Clearly, polynomials of degree 1 are irreducible.

Given nonzero $f(x)$, $g(x)$ in $k[x]$, a common factor $d(x)$ in $k[x]$ of $f(x)$ and $g(x)$ of the largest degree is called their *greatest common divisor*. If we require $d(x)$ to be monic, it is unique and is written as the g.c.d. $(f(x), g(x))$. We call two nonzero polynomials in $k[x]$ *coprime* if the g.c.d. $(f(x), g(x)) = 1$.

For integers, one learns in high school (otherwise, see [3, p. 7]) and it is the same for polynomials, to compute $d(x) =$ g.c.d. $(f(x), g(x))$ by the so-called Euclidean algorithm. By this algorithm, one can also express

$$d(x) = a(x)f(x) + b(x)g(x)$$

as a linear combination of $f(x)$ and $g(x)$ with $a(x)$, $b(x)$ in $k[x]$.

Example. Let $k = \mathbb{Q}$ and $f(x) = x^4 + x^3 + x^2 + x + 1$, $g(x) = x^2 - 1$. Performing long divisions, we write

$$f(x) = (x^2 + x + 2)g(x) + 2x + 3$$

$$g(x) = \left(\frac{1}{2}x - \frac{3}{4}\right)(2x + 3) + \frac{5}{4}.$$

Hence to obtain the g.c.d.$(f(x), g(x)) = 1$ as a linear combination of $f(x)$ and $g(x)$, we write

$$\begin{aligned}\frac{5}{4} &= g(x) - \left(\frac{1}{2}\,x - \frac{3}{4}\right)(2x+3)\\ &= g(x) - \left(\frac{1}{2}\,x - \frac{3}{4}\right)[f(x) - (x^2+x+2)g(x)]\\ &= -\left(\frac{1}{2}x - \frac{3}{4}\right) f(x) + \left(\left(\frac{1}{2}\,x - \frac{3}{4}\right)(x^2+x+2)+1\right) g(x).\end{aligned}$$

This gives

$$1 = \left(-\frac{2}{5}\,x + \frac{3}{5}\right) f(x) + \left(\frac{2}{5}\,x^3 - \frac{1}{5}\,x^2 + \frac{1}{5}\,x - \frac{2}{5}\right) g(x).$$

Thus $(g(x))^{-1}$ in $K = \mathbb{Q}[x]/(f(x))$ is $\frac{2}{5}\,x^3 - \frac{1}{5}\,x^2 + \frac{1}{5}\,x - \frac{2}{5}$.

EXERCISES

1. Write the g.c.d. $(f(x), g(x)) = a(x)f(x)+b(x)g(x)$ for $f(x) = 8x^3 - 6x - 1$ and $g(x) = x^2 - 3$ with $a(x)$, $b(x)$ in $\mathbb{Q}[x]$ to compute the multiplicative inverse of $g(x)$ in $K = \mathbb{Q}[x]/(f(x))$.
2. Repeat 1 with $f(x) = x^4 + x^3 + x^2 + x + 1$ and $g(x) = 8x^3 - 6x - 1$.

10.5.2 Roots of Polynomials

We now assemble the tools necessary to prove the impossibility of the aforementioned endeavors. We take k to be an arbitrary but fixed subfield of $\mathbb{C}$.

Definition. A complex number α is a *root* of a polynomial

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \;\; (a_j \text{ in } k)$$

of degree n, if $f(\alpha) = 0$, that is if

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Every complex number is a root of the zero polynomial. Therefore from now on, even if it is not explicitly stated, we shall consider only the roots of nonzero polynomials. If α is a root of $f(x)$, we also say that α *satisfies* $f(x)$.

Definition. A complex number α is *algebraic over* k, if it is a root of a nonzero polynomial with coefficients in k.

Suppose α is algebraic over k. Among all the polynomials over k satisfied by α, there is one, say $f(x)$ of the smallest degree. We call $\deg f(x)$ the *degree of α over k* and write it as $\deg_k(\alpha)$. It is obvious that the elements of k are precisely the complex numbers α with $\deg_k(\alpha) = 1$. They are the roots of the polynomials $x - \alpha$ with α in k.

Definition. A complex number is an *algebraic number*, or simply *algebraic*, if it is algebraic over the smallest subfield $\mathbb{Q}$ of $\mathbb{C}$. Otherwise it is *transcendental.*

Example. The real numbers $\sqrt{3}$, $\sqrt[3]{2}$ and the imaginary number i are algebraic numbers, being roots of $x^2 - 3$, $x^3 - 2$ and $x^2 + 1$, respectively. So is $\alpha = \frac{-1+\sqrt{-3}}{2}$. It is one of the complex roots of $x^3 - 1 = (x-1)(x^2 + x + 1)$. Clearly, α satisfies $x^3 - 1$, as well as $x^2 + x + 1$. If α satisfies a polynomial of degree 1, then it has to be a rational number, which it is not. Hence $\deg_{\mathbb{Q}}(\alpha) = 2$.

Suppose α is algebraic over k and $f(x)$, $g(x)$ are two polynomials over k of minimal degree satisfied by α. Then they must divide each other. Otherwise, writing

$$g(x) = q(x)f(x) + r(x) \tag{10.25}$$

with $\deg r(x) < \deg f(x)$ and putting $x = \alpha$ in (10.25), α would be a root of $r(x)$, a polynomial of degree less than that of $f(x)$, contradicting the minimality of $f(x)$. Hence, if we require $f(x)$ to be monic, it is unique. We call it the *minimal polynomial* of α over k. It is necessarily irreducible, because otherwise α would be a root of one of its factor, again contradicting the minimality of $\deg f(x)$.

Now suppose α is algebraic over k with the minimal polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

with its coefficients a_j in k. The vector space

$$K = P_n(k) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_j \in k\}$$

is a subfield of $\mathbb{C}$ with k as its subfield. To see this, note that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0$$

implies that for all $j \geq 0$,

$$\alpha^{n+j} = -a_{n-1}\alpha^{n+j-1} - \ldots - a_0\alpha^j.$$

Hence the powers of α higher than $n-1$ can be replaced by lower ones, and thus are linear combinations of $1, \alpha, \ldots, \alpha^{n-1}$. This shows that the products of elements of K are again in K. On the other hand, given $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \neq 0$ in K, and $f(x)$ being irreducible, the polynomial $g(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ is coprime with $f(x)$. Hence by the Euclidean Algorithm, for some $r(x)$ and $s(x)$ in $k[x]$,

$$f(x)r(x) + g(x)s(x) = 1. \tag{10.26}$$

Putting $x = \alpha$ in (10.26), we get $g(\alpha)s(\alpha) = 1$. As said above, we may take $s(\alpha) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$. This proves that $g(\alpha)$ has a multiplicative inverse $s(\alpha)$ in K.

The field K is the smallest subfield of $\mathbb{C}$ containing both k and α and is denoted by $k(\alpha)$. We say that $k(\alpha)$ has been *obtained by adjoining* α to k. We now summarize this discussion for our record.

Theorem 10.8. *Suppose α is algebraic of degree n over k. Then the vector space*

$$K = k(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \mid c_j \in k\}$$

over k is the smallest subfield of $\mathbb{C}$ containing both α and k. As a vector space over k, $\dim_k(K) = \deg_k(\alpha)$.

Proof. The only thing that remains to be shown is that $\dim_k(K) = n$. It is clear that $\dim_k(K) \leq n$. On the other hand, $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over k by the definition of $\deg_k(\alpha)$. Thus $\dim_k(K) \geq n$. □

Theorem 10.9. *Suppose k is a subfield of K with $\dim_k K$ finite and $\alpha \in K$. Then α is algebraic over k and $\deg_k \alpha$ is a factor of $\dim_k(K)$.*

Proof. Suppose $\dim_k(K) = n$. Then the $n+1$ vectors $1, \alpha, \ldots, \alpha^n$ are linearly dependent over k, hence satisfy a non-trivial relation

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

This shows that α is algebraic over k with $\deg_k(\alpha) \leq n$. Since $k \subseteq k(\alpha) \subseteq K$, the rest of our claim follows from $\dim_k(K) = \dim_k(k(\alpha)) \cdot \dim_{k(\alpha)}(K)$. □

Examples. For proving the impossibility of trisecting angles and duplicating cubes, we need to study two special polynomials over $\mathbb{Q}$. These are

1. $x^3 - 2$ and
2. $8x^3 - 6x - 1$.

What concerns us are the real roots $\alpha = \sqrt[3]{2}$ of $x^3 - 2$ and $\beta = \cos 20°$ of $8x^3 - 6x - 1$. To show that β is a root of $8x^3 - 6x - 1$, recall the trigonometric identity

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta. \tag{10.27}$$

In (10.27), if we put $\theta = 20°$, we get $8\beta^3 - 6\beta - 1 = 0$.

In order to prove that it is impossible to duplicate cubes and trisect angles, the phrases to be explained shortly, we show that α and β have wrong degree for this to be possible. Since an irreducible polynomial is also a constant multiple of the minimal polynomial of its roots, we show that $\deg_{\mathbb{Q}}(\alpha) = \deg_{\mathbb{Q}}(\beta) = 3$ by showing that $x^3 - 2$ and $8x^3 - 6x - 1$ are irreducible over $\mathbb{Q}$.

For a polynomial of degree three to be reducible over $\mathbb{Q}$, at least one of its factors has to be of degree one. This factor, say $ax - b$, with a, b in $\mathbb{Q}$ has a rational root b/a. Thus to show that $x^3 - 2$ and $8x^3 - 6x - 1$ are irreducible over $\mathbb{Q}$, it suffices to show that they have no rational root. For this, we need the following elementary fact from high school algebra.

Theorem 10.10. *Suppose*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad (a_0 a_n \neq 0)$$

is a polynomial with integer coefficients and c/d is a rational root, in the reduced form, of $f(x)$. Then c is a factor of a_0 and d is a factor of a_n.

Proof. The hypothesis means that

$$f\left(\frac{c}{d}\right) = a_0 + a_1\left(\frac{c}{d}\right) + \ldots + a_n\left(\frac{c}{d}\right)^n = 0.$$

Clearing the denominators, this gives

$$a_0 d^n = -c(a_1 d^{n-1} + \cdots + a_n c^{n-1}).$$

Since c and d have no common factor > 1, c must be a factor of a_0. Similarly, d is a factor of a_n. □

The theorem implies that the only possible rational roots of $x^3 - 2$ are ± 1 and ± 2, but obviously, they are not. The only possible rational roots of $8x^3 - 6x - 1$ are $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. We leave it as an easy exercise, by plugging in, to show that none of these satisfies $8x^3 - 6x - 1$. We now record this conclusion for a ready reference.

Theorem 10.11. $\deg_{\mathbb{Q}}(\sqrt[3]{2}) = \deg_{\mathbb{Q}}(\cos 20°) = 3.$

EXERCISES

1. Prove that a rational number is an algebraic number. Moreover, the rational numbers are precisely the algebraic numbers α with $\deg_{\mathbb{Q}}(\alpha) = 1$.
2. If α, β are algebraic, show that their sum $\alpha + \beta$ and product $\alpha\beta$ are also algebraic.

10.5.3 Straightedge and Compass

More than two millennia ago, the Greek mathematician, Euclid laid the ground rules for what we now call pure mathematics. This can be found in Euclid's

Elements. First, one makes the mathematical terms precise by defining them. Then, starting from a minimal set of axioms and postulates, one draws conclusions, called theorems.

The Greeks also considered various kinds of geometric constructions, depending on the sets of tools that were permissible. The most famous are the geometric constructions of plane geometry using straightedge and compass only. This means that one is allowed to

1) join two points by a straightedge, and

2) using a compass, draw a circle of a given radius with a given center.

Of course, one can extend existing lines and choose points at random in the plane and join them, by a straightedge, to points we already have.

We declare, once and for all, that we are only allowed to use a straightedge and compass. In Book 1 of Euclid's *Elements*, one finds procedures to bisect a given line segment, and to draw a perpendicular from a given point to a given line, on or off this given line. For example, to bisect a line segment AB (see Figure 10.2), first using a compass, one draws circles of radius AB with A and B as their centers. Then joining points C and D of their intersection by a straightedge, one obtains the midpoint M of AB. In Book 1 of the *Elements*, one also finds ways to bisect an angle and to draw a line through a given point which is parallel to a given line.

Line segments can be added and subtracted in an obvious way. As a matter of convenience, we define a new word.

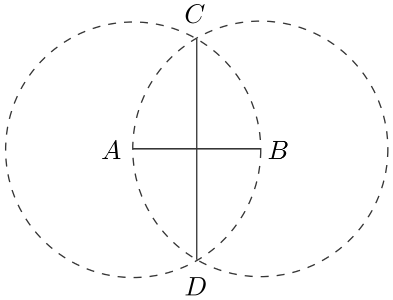


FIGURE 10.2: Bisecting lines

Definition. A real number α is *constructible*, if starting from a line segment of unit length, one can construct in a finite number of steps, using a straightedge and a compass only, a line segment of length α.

If α is constructible, so is $-\alpha$, because if AB has length α then BA is of length $-\alpha$. Obviously, every integer m in $\mathbb{Z}$ is constructible. If $n \geq 1$ is an integer, any line segment AB can be divided into n equal parts. [Draw a line AC making, say an acute angle with AB. Choose a point P_1, on AC and with the help of a compass, mark $n-1$ points $P_2, \ldots, P_n$ on AC with lengths $|AP_1| = |P_1P_2| = \cdots = |P_{n-1}P_n|$. Join P_n to B and through $P_1, \ldots, P_{n-1}$, draw lines parallel to P_nB.]

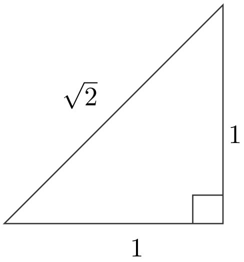


FIGURE 10.3: Constructing $\sqrt{2}$

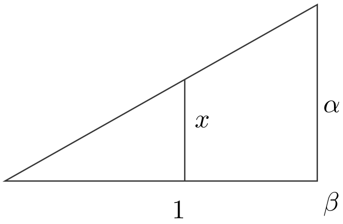


FIGURE 10.4: Constructing α/β

Thus every rational number m/n is constructible. This is not all. Some irrational numbers like $\sqrt{2}$ (see Figure 10.3) are also constructible. In fact, it is not hard to see that if $m \geq 1$ is an integer, then $\sqrt{m}$ is constructible. [Inductively, use 1 and $\sqrt{m-1}$ and the Pythagorean theorem to construct $\sqrt{m}$.]

EXERCISE

Show that the set of constructible numbers is a subfield of $\mathbb{R}$.

[Hint: If α, β are constructible, use for example, Figure 10.4 to show that $x = x/1 = \alpha/\beta$ is constructible.]

10.5.4 Intersecting Lines and Circles

Suppose k is a subfield of $\mathbb{R}$. A point $P = (x, y)$ in the Euclidean plane $\mathbb{R}^2$ is called a *k-rational point*, or simply a *k-point* if $x, y \in k$. A circle in $\mathbb{R}^2$ is *k-rational* or simply a *k-circle* if its radius $r \in k$ and its center is a k-point. A straight line is a *k-line* if it has an equation

$$ax + by + c = 0 \tag{10.28}$$

with a, b, c in k.

It is easy to check that the intersection of k-lines is a k-point, and that (after a change of coordinates) a k-circle has an equation

$$x^2 + y^2 = r^2 \tag{10.29}$$

with r in k. To find the intersection of a k-line with a k-circle, one eliminates a variable from (10.28) and (10.29) and solves a quadratic equation

$$f(x) = Ax^2 + Bx + C = 0.$$

Thus the coordinates of the points of intersection of (10.28) and (10.29) are in k if and only if the square root of the discriminant $d = B^2 - 4AC$ of $f(x)$ is in k. Otherwise, they are in the quadratic extension $K = k(\sqrt{d})$ of k. [By definition, K/k is a *quadratic extension* if k is a subfield of K and $\dim_k(K) = 2$.] It is easy to see that two k-circles intersect in K-points with $K = k$ or a quadratic extension of k.

10.5.5 Degrees of Constructible Numbers

It is now clear that for α to be constructible, it must lie in a field K obtained from $\mathbb{Q}$ by a finite sequence of quadratic extensions k_j/k_{j-1} with

$$\mathbb{Q} = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_n = K.$$

By Theorem 10.7, $\dim_{\mathbb{Q}}(K) = 2^r$ for some $r \geq 0$. Since $\deg_{\mathbb{Q}}(\alpha)$ is a factor of $\dim_{\mathbb{Q}}(K) = 2^r$, $\deg_{\mathbb{Q}}(\alpha) = 2^m$ for some $m \leq r$. We have now proved the following fact.

Theorem 10.12. *If α is constructible, then α is algebraic of degree 2^m over $\mathbb{Q}$ for some $m \geq 0$.*

10.5.6 Solutions of the Famous Problems

By *trisection of an angle*, we mean to divide it, using a straightedge and compass only, into three equal parts. *Duplicating a cube* is to construct, starting from the edge of a given cube, the edge of another one of twice the volume. Algebraically, it means to construct the real root $\sqrt[3]{2v}$ of $x^3 - 2v$, v being the volume of the given cube.

It was only in 1836 that the French mathematician, M. L. Wantzel settled two of the three famous problems from Greek geometry (see [18]). Someone else might have done it too, but it is as an exercise for the reader to find out.

Corollary 10.13. *It is impossible to duplicate cubes.*

Proof. We show that a cube of volume $v = 1$ cannot be duplicated. If possible, then by Theorems 10.11 and 10.12, $\deg_{\mathbb{Q}}(\sqrt[3]{2}) = 3 = 2^m$ for an integer $m \geq 0$. This is impossible. □

Corollary 10.14. *It is impossible to trisect angles.*

Proof. We show that a $60°$ angle cannot be trisected. With $\theta = 60°$, $\alpha = \cos\frac{\theta}{3}$ is a root of $8x^3 - 6x - 1$. So for a $20°$ angle to be constructible, $\deg_{\mathbb{Q}}(\alpha) = 3$ has to be a power of 2, which is again impossible. This proves that $60°$ angle cannot be trisected. □

By squaring the circle we mean constructing the length of a side of the square whose area equals to that of a unit circle, i.e. the circle of radius 1. This amounts to constructing a line segment of length $\sqrt{\pi}$. Therefore $\sqrt{\pi}$ and hence π must be an algebraic number. Thus to show that squaring the circle is impossible one needs to show that π is not an algebraic number, i.e. π is transcendental. This was done by German mathematician Ferdinand Lindemann in 1882.

Theorem 10.15. *(Lindemann) π is transcendental.*

For a proof, see [2], p. 5. For an easier proof, see New Testament, John 20:29.

Answers to Selected Numerical Problems

Chapter 2

Section 2.1.1

1. $\begin{pmatrix} -32 & 3 & 30 \\ 23 & 17 & 7 \\ -7 & 47 & 5 \end{pmatrix}$

Section 2.1.2

1. (a) $\begin{pmatrix} -4 & 26 \\ 13 & 1 \end{pmatrix}$

   (b) $\begin{pmatrix} 22 & 57 & -29 \\ 28 & -15 & -29 \end{pmatrix}$

   (c) $\begin{pmatrix} 2x - 5y + 4z \\ 3x + y + 10z \end{pmatrix}$

2. $\begin{pmatrix} 6 & 7 \\ 1 & 4 \end{pmatrix}$

3. b)

4. $\begin{pmatrix} 4 \\ 8 \end{pmatrix}$

Section 2.2

2. (a) $\begin{pmatrix} 4 & -1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \end{pmatrix}$

(b) $\begin{pmatrix} 3 & 2 & -1 \\ -3 & -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 \\ -2 \\ 3 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 1 & -1 \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$

3. (a) and (b) are consistent, (c) and (d) are not.

Section 2.3

1. (a) $x_1 = \frac{5}{6}$, $x_2 = -\frac{7}{9}$

   (b) $x = \frac{9}{11}$, $y = \frac{17}{11}$, $z = \frac{10}{11}$

2. $x = \frac{1}{52} + \frac{25\sqrt{3}}{52} + i\left(\frac{5}{52} - \frac{5\sqrt{3}}{52}\right)$,

   $y = -\frac{1}{13} + \frac{\sqrt{3}}{13} + i\left(-\frac{5}{13} + \frac{5\sqrt{3}}{13}\right)$

3. (a) $x = 2$, $y = 4$

   (b) Some of the solutions are $(x, y, z) = (1, 4, 2)$, $(3, 1, 5)$.

   (c) 5 and 7.

5. $x = 2$, $y = 3$.

7. (a) $\begin{pmatrix} 1 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix}$.

   (b) $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

   (c) $\begin{pmatrix} 1 & 2 & 1 & -3 & -1 \\ 0 & 1 & 1 & -3 & -3 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

Section 2.4

7. $A^{-1} = \begin{pmatrix} \frac{3}{11} & \frac{1}{11} \\ -\frac{5}{11} & \frac{2}{11} \end{pmatrix}, \quad X = \begin{pmatrix} \frac{4}{11} \\ -\frac{3}{11} \end{pmatrix}$

8. $A^{-1} = \begin{pmatrix} \frac{3}{13} & \frac{2}{13} \\ \frac{2}{13} & -\frac{3}{13} \end{pmatrix}, \quad X = \begin{pmatrix} \frac{1}{13} \\ \frac{5}{13} \end{pmatrix}$

9. $A^{-1} = \begin{pmatrix} 1 & -2 & \frac{7}{3} \\ 0 & \frac{1}{2} & -1 \\ 0 & 0 & \frac{1}{3} \end{pmatrix}, \quad X = \begin{pmatrix} 12 \\ -5 \\ 3 \end{pmatrix}$

10. $A^{-1} = \begin{pmatrix} -1 & -3 & 3 \\ 2 & 6 & 1 \\ 3 & 8 & 3 \end{pmatrix}, \quad X = \begin{pmatrix} \frac{-13}{7} \\ \frac{6}{7} \\ \frac{4}{7} \end{pmatrix}$

11. $A^{-1} = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & -1 \\ 0 & -2 & 2 & 1 \\ -1 & 2 & -2 & 0 \end{pmatrix}, \quad X = \begin{pmatrix} 6 \\ -7 \\ 9 \\ -15 \end{pmatrix}$

12. $A^{-1} = \begin{pmatrix} -3 & 2 & 2 & -\frac{1}{2} \\ 8 & -2 & -7 & 2 \\ -10 & 0 & 11 & -\frac{7}{2} \\ 0 & 1 & -1 & \frac{1}{2} \end{pmatrix}, \quad X = \begin{pmatrix} \frac{13}{2} \\ -11 \\ \frac{21}{2} \\ \frac{3}{2} \end{pmatrix}$

Section 2.5

1. $\boldsymbol{x} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \;\; \boldsymbol{b} = -\boldsymbol{c}_1 + \boldsymbol{c}_2$

2. $\boldsymbol{x} = \begin{pmatrix} \frac{25}{17} \\ -\frac{18}{17} \\ \frac{13}{17} \end{pmatrix}, \;\; \boldsymbol{b} = \dfrac{25}{17}\,\boldsymbol{c}_1 - \dfrac{18}{17}\,\boldsymbol{c}_2 + \dfrac{13}{17}\,\boldsymbol{c}_3$

Section 2.6.5

1. $\boldsymbol{x} = \begin{pmatrix} 1919 \\ 1297 \end{pmatrix}$

2. $\boldsymbol{x} = \begin{pmatrix} 45,142.9 \\ 31,035.7 \\ 31,035.7 \end{pmatrix}$

Chapter 3

Section 3.4

2, 4, 6 linearly independent,

1, 3, 5 linearly dependent

Section 3.6

1. $P = \begin{pmatrix} 8 & 3 & 1 \\ 10 & 4 & 1 \\ \frac{7}{2} & \frac{3}{2} & \frac{1}{2} \end{pmatrix}$

2. $P = \begin{pmatrix} 40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & 1 \end{pmatrix}$

Section 3.7

1. (a) 1 (b) 3 (c) 3 (d) 3 (e) 4

Chapter 4

Section 4.1

1. (b)

Section 4.3

6. i) $\begin{pmatrix} \frac{7}{3} & \frac{8}{3} \\ \frac{16}{3} & \frac{17}{3} \end{pmatrix}$, ii) $\begin{pmatrix} \frac{5}{3} & -\frac{1}{3} \\ \frac{11}{3} & -\frac{1}{3} \end{pmatrix}$, iii) $\begin{pmatrix} \frac{23}{2} & \frac{25}{2} \\ -\frac{3}{2} & -\frac{3}{2} \end{pmatrix}$,

   iv) $\begin{pmatrix} 8 & -1 \\ -1 & 0 \end{pmatrix}$

Section 4.6

1. (a) $P = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ -1 & -1 \end{pmatrix}$

   (b) $P = \begin{pmatrix} 23 & 16 \\ 5 & 3 \end{pmatrix}$

2. $P = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & -\frac{1}{2} & 1 \\ \frac{1}{2} & -\frac{1}{2} & -1 \end{pmatrix}$

3. (a) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$

   (b) $\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & \frac{5}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 1 \\ 0 & 0 & \frac{3}{2} & -\frac{3}{2} \end{pmatrix}$

   (c) $P = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$

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

Section 4.7

1. $y = c_1 e^x + c_2 e^{2x}$
2. $y = c_1 e^{3x} + c_2 x e^{3x}$
3. $y = c_1 e^x + c_2 e^{-x} + c_3 \cos x + c_4 \sin x$

Chapter 5

Section 5.5

1. (b) -2, -2

   (c) 0

   (d) 1, $1 - e\pi$

   (e) -14, 280

   (f) 0, -3506, 34

Section 5.6

1. (a) $|A| = -1$, $\operatorname{adj} A = \begin{pmatrix} 5 & -2 \\ -3 & 1 \end{pmatrix} \quad A^{-1} - \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}.$

   (b) $|A| = ad - bc$, $\operatorname{adj} A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \quad A^{-1} - \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$

   (c) $$|A| = 24, \operatorname{adj} A = \begin{pmatrix} 12 & -20 & 32 \\ 0 & 8 & -14 \\ 0 & 0 & 6 \end{pmatrix}, A^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{5}{6} & \frac{4}{3} \\ 0 & \frac{1}{3} & -\frac{7}{12} \\ 0 & 0 & \frac{1}{4} \end{pmatrix}.$$

   (d) $$|A| = 11, \operatorname{adj} A = \begin{pmatrix} -11 & -11 & 11 \\ 6 & -3 & 1 \\ 2 & 10 & -7 \end{pmatrix}, A^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ \frac{6}{11} & -\frac{3}{11} & \frac{1}{11} \\ \frac{2}{11} & \frac{10}{11} & \frac{-7}{11} \end{pmatrix}.$$

2. (a) $x_1 = \dfrac{11}{3}$, $x_2 = \dfrac{7}{3}$, $x_3 = \dfrac{-23}{3}$

   (b) $x = \dfrac{-5}{11}$, $y = \dfrac{-3}{11}$, $z = \dfrac{19}{11}$

3. (a) $$\begin{pmatrix} \frac{5}{3} & -1 & \frac{2}{3} \\ \frac{1}{3} & - & \frac{1}{3} \\ -\frac{8}{3} & 2 & -\frac{5}{3} \end{pmatrix}$$

(b) $\begin{pmatrix} -\frac{8}{11} & \frac{2}{11} & \frac{5}{11} \\ -\frac{7}{11} & -\frac{1}{11} & \frac{3}{11} \\ \frac{26}{11} & -\frac{1}{11} & -\frac{8}{11} \end{pmatrix}$

Chapter 6

Section 6.2

11. (a) $\lambda = 5,\ -1;\ \boldsymbol{x} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ \begin{pmatrix} -1 \\ 2 \end{pmatrix};\ P = \dfrac{1}{3}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix},$

$\lambda = 4,\ -3;\ \boldsymbol{x} = \begin{pmatrix} 1 \\ 2 \end{pmatrix},\ \begin{pmatrix} -3 \\ 1 \end{pmatrix};\ P = \dfrac{1}{7}\begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix},$

$\lambda = 2 \pm 3i;\ \boldsymbol{x} = \begin{pmatrix} 3 \pm 3i \\ 1 \end{pmatrix},\ P = \dfrac{1}{6}\begin{pmatrix} -i & 3+3i \\ i & 3-3i \end{pmatrix},$

$\lambda = 1 \pm 2i;\ \boldsymbol{x} = \begin{pmatrix} \mp i \\ 1 \end{pmatrix},\ P = \dfrac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix}.$

(b) $\lambda = 2, 1, -1;\ \boldsymbol{x} = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix},\ \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix},\ \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix},$

$P = \dfrac{1}{6}\begin{pmatrix} 4 & -2 & 0 \\ 0 & 3 & -3 \\ -2 & 1 & 3 \end{pmatrix},$

$\lambda = 4, -2, -2;\ \boldsymbol{x} = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix},\ \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix},\ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$

$P = \dfrac{1}{6}\begin{pmatrix} 1 & -1 & 1 \\ -2 & 2 & 0 \\ -1 & 3 & -1 \end{pmatrix},$

$\lambda = 4, 2, -2;\ \boldsymbol{x} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},\ \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix},\ \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix},$

$$P = \frac{1}{4}\begin{pmatrix} 2 & 2 & 2 \\ -1 & -1 & -1 \\ -1 & 3 & 1 \end{pmatrix},$$

Section 6.3

1. Diagonalizable: (a), (c).

2. (a) $P = \frac{1}{2}\begin{pmatrix} i & 1+i \\ i & 1-i \end{pmatrix},$

$$P\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}\ P^{-1} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

(b) $P = \frac{1}{2}\begin{pmatrix} i & 1 \\ -i & 1 \end{pmatrix},$

$$P\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\ P^{-1} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

3. (a) $A^2 - 4A + 7I = \begin{pmatrix} 5 & -8 \\ 8 & -3 \end{pmatrix} - 4\begin{pmatrix} 3 & -2 \\ 2 & 1 \end{pmatrix} + 7I = 0,$

(b) $A^2 - 9A - I = \begin{pmatrix} 19 & 27 \\ 45 & 65 \end{pmatrix} - 9\begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} - I = 0,$

(c) $$\begin{aligned} -A^2 + 15A^2 + 18A &= \begin{pmatrix} 468 & 576 & 684 \\ 1062 & 1305 & 1548 \\ 1656 & 2034 & 2412 \end{pmatrix} \\ &\quad +15\begin{pmatrix} 30 & 36 & 42 \\ 66 & 81 & 96 \\ 102 & 126 & 160 \end{pmatrix} + 18\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \\ &= 0. \end{aligned}$$

Chapter 7

Section 7.4

3. $\left\{\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}, \begin{pmatrix}-\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\right\}.$

5. $\begin{pmatrix}\frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}}\\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{6}} & \frac{2}{\sqrt{6}} & -\frac{1}{\sqrt{6}}\end{pmatrix}.$

6. $\left\{\begin{pmatrix}\frac{4}{3\sqrt{3}}\\ \frac{-1}{3\sqrt{3}}\\ \frac{1}{\sqrt{3}}\\ \frac{1}{3\sqrt{3}}\end{pmatrix}, \begin{pmatrix}\frac{-5}{3\sqrt{19}}\\ \frac{8}{3\sqrt{19}}\\ \frac{3}{\sqrt{19}}\\ \frac{1}{3\sqrt{19}}\end{pmatrix}\right\}.$

Section 7.5

1. $\begin{pmatrix}\frac{1}{5}\\ \frac{3}{5}\end{pmatrix}$

3. $y = 2 - \dfrac{4}{3}\,x + \dfrac{1}{3}\,x^2$

4. $y = \dfrac{1}{11}\,(10 + 31x - 27x^2)$

5. $y = -5 + 3x - 4x^2 + 2x^3.$

Chapter 8

Section 8.3

1. 4

2. i) $\begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$, ii) $\begin{pmatrix} 2i & 0 \\ 0 & -i \end{pmatrix}$, iii) $\begin{pmatrix} -\sqrt{3} & 0 \\ 0 & \sqrt{3} \end{pmatrix}$,

   iv) $\begin{pmatrix} \cos\theta + i\sin\theta & 0 \\ 0 & \cos\theta - i\sin\theta \end{pmatrix}$

Chapter 9

Section 9.2

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

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

3. (b) $\begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{-2}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \end{pmatrix}$

   (c) $7y_1^2 - 3y_2^2$.

   (d) $7y_1^2 + 3y_2^2$.

Section 9.3

1. (a) indefinite (b) positive definite (c) negative definite

   (d) indefinite

2. (a) $P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{3\sqrt{2}} & -\frac{2}{3} \\ 0 & \frac{2\sqrt{2}}{3} & -\frac{1}{3} \\ \frac{1}{\sqrt{2}} & \frac{1}{3\sqrt{2}} & \frac{2}{3} \end{pmatrix}$

   $D = \begin{pmatrix} 7 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & -2 \end{pmatrix}$

(b) $P = \begin{pmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} \end{pmatrix}$

$D = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

Section 9.4

1. (a) min -6, max -1

   (b) min -1, max 5

Section 9.5

3. i) $U = \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{-2}{\sqrt{5}} \end{pmatrix}$, $S = \begin{pmatrix} 2\sqrt{10} & 0 \\ 0 & \sqrt{10} \end{pmatrix}$, $V = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$

   iv) $U = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$, $S = \begin{pmatrix} 12 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $V = \frac{1}{3}\begin{pmatrix} 2 & -2 & 1 \\ 2 & 1 & -2 \\ 1 & 2 & 2 \end{pmatrix}$

Chapter 10

Section 10.1

1. $X = c_1 e^{-4t}\begin{pmatrix} 6 \\ -5 \end{pmatrix} + c_2 e^{7t}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$

3. $x_1 = -c_1 e^t + c_2 e^{-2t} + c_3 e^{3t}$

   $x_2 = 4c_1 e^t - c_2 e^{-2t} + 2c_3 e^{3t}$

   $x_3 = c_1 e^t - c_2 e^{-2t} + c_3 e^{3t}$

Notation

$\mathbb{N}$: the set of natural numbers $1, 2, 3, \ldots$

$\mathbb{Z}$: the set of integers (i.e. whole numbers) $0, \pm 1, \pm 2, \ldots$

$\mathbb{Q}$: the field of rational numbers a/b with a, b in $\mathbb{Z}$, $b \neq 0$.

$\mathbb{R}$: the field of real numbers.

$\mathbb{R}^+$: the set of positive reals.

$\mathbb{C}$: the field of complex numbers.

e^{s+it}: the complex number $e^s(\cos t + i \sin t)$.

K, k: fields with k a subfield of K.

$\mathbb{F}_p$: the field of prime p elements.

$A \subseteq B$: A is a subset of B, possibly with $A = B$.

$A \subsetneqq B$: A is a proper subset of B.

$A \cup B$: the union of sets A and B.

$A \cap B$: the intersection of sets A and B.

$f : A \to B$: f is a function or map with domain A and codomain B.

$f_{|A}$: the restriction of a function f to a subset A of its domain.

$g \circ f$: the composition of maps g and f.

f^{-1}: the inverse of a bijective map f.

A^S: the set of functions from S to A.

$M(m \times n, K)$: the vector space of $m \times n$ matrices over K.

$M(n, K)$: the algebra of $n \times n$ matrices over K.

$\mathbb{R}^n$: the Euclidean n shape.

$k[x]$: the polynomials over a field k.

$P_n(k)$: polynomials over k of degree $< n$.

$\dim_k(V)$: the dimension of a vector space V over k.

span(S): the span of a set S of vectors.

Ker(T): the kernel of a linear map T.

$W_1 \oplus W_2$: the direct sum of subspaces W_1 and W_2.

$\mathrm{Hom}_K(V, W)$: the vector space of linear maps $T : V \to W$ over K.

$\tau_{\mathcal{B}_V, \mathcal{B}_W}(T)$: the matrix of T relative to bases $\mathcal{B}_V$ and $\mathcal{B}_W$ of V and W.

$|c|$: the absolute value of c in $\mathbb{R}$ or length of c in $\mathbb{C}$.

$\det(A)$: the determinant of A.

$\mathrm{tr}(A)$: the trace of A.

A^*: the transpose of a (real) matrix A.

Z^*: the adjoint of a complex matrix Z over $\mathbb{C}$.

$\mathrm{adj}(A)$: the classical adjoint of a square matrix A.

$\chi_A(\lambda)$: the characteristic polynomial of a square matrix A.

$|\boldsymbol{a}|$: length of a vector $\boldsymbol{a}$.

$\mathrm{proj}_{\boldsymbol{b}}(\boldsymbol{a})$: projection of a vector $\boldsymbol{a}$ on a nonzero vector $\boldsymbol{b}$.

$\mathrm{comp}_{\boldsymbol{b}}(\boldsymbol{a})$: component of a vector $\boldsymbol{a}$ along a nonzero vector $\boldsymbol{b}$.

$\mathrm{proj}_W(\boldsymbol{a})$: the projection of a vector $\boldsymbol{a}$ on a subspace $W \neq \{\mathbf{0}\}$.

$W^\perp$: the orthogonal complement of a subspace W.

δ_{ij}: the Kronecker's deltas.

$\mathrm{sgn}(\sigma)$: the sign of a permutation σ.

$\deg(f)$: the degree of a polynomial $f(x)$.

$H(f)$: the Hessian of a multivariable function $f(x_1, \ldots, x_n)$.

$\Rightarrow$: implies

$\Leftrightarrow$: implies and is implied by, i.e. if and only if.

Bibliography

[1] E. Artin. *Galois Theory.* Dover, 1998.

[2] A. Baker. *Transcendental Number Theory.* Cambridge University Press, 1979.

[3] J. S. Chahal. *Topics in Number Theory.* Plenum, 1988.

[4] C. W. Curtis. *Linear Algebra.* Springer, 1984.

[5] A. Einstein. *The Principle of Relativity.* Dover, 1952.

[6] Euclid. *Book 1, The Elements.* Dover, 1956.

[7] R. Horn and C. Johnson. *Matrix Analysis.* Cambridge University Press, 1985.

[8] P. R. Halmos. *Naïve Set Theory.* Springer, 1974

[9] P. R. Halmos. *Finite Dimensional Vector Spaces.* Van Nostrand (1960) and Springer UTM, 1974

[10] K. Hoffman and R. Kunze. *Linear Algebra.* Prentice Hall, 1961.

[11] S. H. Friedberg, A. J. Insel, L. E. Spence. *Linear Algebra.* Prentice Hall, 1997.

[12] F. Klein. *Famous Problems of Elementary Geometry.* Dover, 1956.

[13] N. Koblitz. *A Course in Number Theory and Cryptography.* Springer, 1987.

[14] W. Leontief. *Input-Output Economics.* Oxford University Press, 1986.

[15] M. Ram Murty. *Ramanujan Graphs. J. Ramanujan Math. Soc.*, 18:1–20, 2003.

[16] G. Shilov. *Linear Algebra.* Dover, 1977.

[17] G. Strang. *Introduction to Linear Algebra.* Wellesley–Cambridge Press, 2009.

[18] M. L. Wantzel. Recherches sur les moyens de reconnoitre, si un problème de géométre peut se résoudre avec la règle et le compas. *J. Math. Pures Appliq.*, 1:366–372, 1836.

Index

This book on linear algebra and its applications in economics, engineering, physics, and in mathematics itself, is somewhat different from other books on the subject. Rather than present linear algebra as a collection of seemingly unrelated topics, it aims to combine them into a single theme - the study of linear maps in full generality. The vector spaces are merely their domains and codomains. The matrices are a convenient tool to represent and keep track of them when their domains and codomains are finite dimensional.

Some unusual definitions have been adopted to either eliminates entirely the need for some theorems or make their proofs very short. For example, the dimension of a vector space is defined by borrowing ideas from algebraic geometry and commutative algebra. Not only it is a more natural definition, the replacement theorem is no longer needed. It is a trivial consequence of this definition that any two bases of a finite dimensional vector space have the same number of vectors. Moreover, being more general, this definition works equally well when the geometric objects are nonlinear.

By following more conceptual and less computational approach the book has, in less than 250 pages, achieved a more comprehensive coverage of the subject and its applications than books with more than twice as many pages. A wide range of applications discussed herein should convince students majoring in various disciplines of the utility of linear algebra. The reader lacking the knowledge of prerequisite material will find it in Chapter 1