Titu Andreescu

Essential Linear Algebra with Applications

A Problem-Solving Approach

Birkhäuser

Titu Andreescu

Essential Linear Algebra with Applications

A Problem-Solving Approach

Birkhäuser

Titu Andreescu
Natural Sciences and Mathematics
University of Texas at Dallas
Richardson, TX, USA

ISBN 978-0-8176-4360-7 ISBN 978-0-8176-4636-3 (eBook)
DOI 10.1007/978-0-8176-4636-3
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2014948201

Mathematics Subject Classification (2010): 15, 12, 08

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.birkhauser-science.com)

Preface

This textbook is intended for an introductory followed by an advanced course in linear algebra, with emphasis on its interactions with other topics in mathematics, such as calculus, geometry, and combinatorics. We took a straightforward path to the most important topic, linear maps between vector spaces, most of the time finite dimensional. However, since these concepts are fairly abstract and not necessarily natural at first sight, we included a few chapters with explicit examples of vector spaces such as the standard n-dimensional vector space over a field and spaces of matrices. We believe that it is fundamental for the student to be very familiar with these spaces before dealing with more abstract theory. In order to maximize the clarity of the concepts discussed, we included a rather lengthy chapter on 2×2 matrices and their applications, including the theory of Pell's equations. This will help the student manipulate matrices and vectors in a concrete way before delving into the abstract and very powerful approach to linear algebra through the study of vector spaces and linear maps.

The first few chapters deal with elementary properties of vectors and matrices and the basic operations that one can perform on them. A special emphasis is placed on the Gaussian Reduction algorithm and its applications. This algorithm provides efficient ways of computing some of the objects that appear naturally in abstract linear algebra such as kernels and images of linear maps, dimensions of vector spaces, and solutions to linear systems of equation. A student mastering this algorithm and its applications will therefore have a much better chance of understanding many of the key notions and results introduced in subsequent chapters.

The bulk of the book contains a comprehensive study of vector spaces and linear maps between them. We introduce and develop the necessary tools along the way, by discussing the many examples and problems proposed to the student. We offer a thorough exposition of central concepts in linear algebra through a problem-based approach. This is more challenging for the students, since they have to spend time trying to solve the proposed problems after reading and digesting the theoretical

material. In order to assist with the comprehension of the material, we provided solutions to all problems posed in the theoretical part. On the other hand, at the end of each chapter, the student will find a rather long list of proposed problems, for which no solution is offered. This is because they are similar to the problems discussed in the theoretical part and thus should not cause difficulties to a reader who understood the theory.

We truly hope that you will have a wonderful experience in your linear algebra journey.

Richardson, TX, USA Titu Andreescu

Contents

Chapter 1
Matrix Algebra

Abstract This chapter deals with matrices and the basic operations associated with them in a concrete way, paving the path to a more advanced study in later chapters. The emphasis is on special types of matrices and their stability under the described operations.

Keywords Matrices • Operations • Invertible • Transpose • Orthogonal • Symmetric matrices

Before dealing with the abstract setup of vector spaces and linear maps between them, we find it convenient to discuss some properties of matrices. Matrices are a very handy way of describing linear phenomena while being very concrete objects. The goal of this chapter is to define these objects as well as some basic operations on them.

Roughly, a matrix is a collection of "numbers" displayed in some rectangular board. We call these "numbers" the entries of the matrix. Very often, these "numbers" are simply rational, real, or more generally complex numbers. However, these choices are not always adapted to our needs: in combinatorics and computer science, one works very often with matrices whose entries are residue classes of integers modulo prime numbers (especially modulo 2 in computer science), while other areas of mathematics work with matrices whose entries are polynomials, rational functions, or more generally continuous, differentiable, or integrable functions. There are rules allowing to add and multiply matrices (if suitable conditions on the size of the matrices are satisfied), if the set containing the entries of these matrices is stable under these operations. Fields are algebraic structures specially designed to have such properties (and more...), and from this point of view they are excellent choices for the sets containing the entries of the matrices we want to study.

The theory of fields is extremely beautiful and one can write a whole series of books on it. Even the basics can be fairly difficult to digest by a reader without some serious abstract algebra prerequisites. However, the purpose of this introductory book is not to deal with subtleties related to the theory of fields, so we decided to take the following rather pragmatic approach: we will only work with a very explicit set of fields in this book (we will say which ones in the next paragraphs), so the reader not familiar with abstract algebra will **not** need to know the subtleties of

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_1

the theory of fields in the sequel. Of course, the reader familiar with this theory will realize that all the general results described in this book work over general fields.

In most introductory books of linear algebra, one works exclusively over the fields **R** and **C** of real numbers and complex numbers, respectively. They are indeed sufficient for essentially all applications of matrices to analysis and geometry, but they are not sufficient for some interesting applications in computer science and combinatorics. We will introduce one more field that will be used from time to time in this book. This is the **field $\mathbf{F}_2$ with two elements** 0 **and** 1. It is endowed with addition and multiplication rules as follows:

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0$$

and

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

We do not limit ourselves exclusively to **R** and **C** since a certain number of issues arise from time to time when working with general fields, and this field $\mathbf{F}_2$ allows us to make a series of remarks about this issues. From this point of view, one can see $\mathbf{F}_2$ as a test object for some subtle issues arising in linear algebra over general fields.

Important convention: in the remainder of this book, we will work exclusively with one of the following fields:

- **the field Q of rational numbers**
- **the field R of real numbers**.
- **the field C of complex numbers**.
- **The field with two elements $\mathbf{F}_2$ with addition and multiplication rules described as above**.

We will assume familiarity with each of the sets **Q**, **R** and **C** as well as the basic operations that can be done with rational, real, or complex numbers (such as addition, multiplication, or division by nonzero numbers).

We will reserve the letter F for one of these fields (if we do not want to specify which one of the previous fields we are working with, we will simply say "Let F be a field").

The even more pragmatic reader can take an even more practical approach and simply assume that F will stand for **R** or **C** in the sequel.

1.1 Vectors, Matrices, and Basic Operations on Them

Consider a field F. Its elements will be called **scalars**.

Definition 1.1. Let n be a positive integer. We denote by F^n the set of n-tuples of elements of F. The elements of F^n are called **vectors** and are denoted either in row-form $X = (x_1, \ldots, x_n)$ or in column-form

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

The scalar x_i is called the ith **coordinate** of X (be it written in row or column form).

The previous definition requires quite a few clarifications. First of all, note that if we want to be completely precise we should call an element of F^n an n-vector or n-dimensional vector, to make it apparent that it lives in a set which depends on n. This would make a lot of statements fairly cumbersome, so we simply call the elements of F^n vectors, without any reference to n. So (1) is a vector in F^1, while $(1, 2)$ is a vector in F^2. There is no relation whatsoever between the two exhibited vectors, as they live in completely different sets a priori.

While the abuse of notation discussed in the previous paragraph is rather easy to understand and accept, the convention about writing vectors either in row or in column form seems strange at first sight. It is easily understood once we introduce matrices and basic operations on them, as well as the link between matrices and vectors, so we advise the reader to take it simply as a convention for now and make no distinction between the vector $(v_1, \ldots, v_n)$ and the vector $\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$. We will see later on that from the point of view of linear algebra the column notation is more useful.

The **zero vector** in F^n is denoted simply 0 and it is the vector whose coordinates are all equal to 0. Note that the notation 0 is again slightly abusive, since it does not make apparent the dependency on n: the 0 vector in F^2 is definitely not the same object as the zero vector in F^3. However, this will (hopefully) not create any confusion, since in the sequel the context will always make it clear which zero vector we consider.

Definition 1.2. Let m, n be positive integers. An $m \times n$ **matrix with entries in** F is a rectangular array

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

The scalar $a_{ij} \in F$ is called the (i, j)**-entry** of A. The column-vector

$$C_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

is called the j**th column of** A and the row-vector

$$L_i = [a_{i1}, a_{i2}, \dots, a_{in}]$$

is called the i**th row of** A. We denote by $M_{m,n}(F)$ the set of all $m \times n$ matrices with entries in F.

Definition 1.3. A **square matrix of order** n with entries in F is a matrix $A \in M_{n,n}(F)$. We denote by $M_n(F)$ the set $M_{n,n}(F)$ of square matrices of order n.

We can already give an explanation for our choice of denoting vectors in two different ways: a $m \times n$ matrix can be seen as a family of vectors, namely its rows. But it can also be seen as a family of vectors given by its columns. It is rather natural to denote rows of A in row-form and columns of A in column-form. Note that a row-vector in F^n can be thought of as a $1 \times n$ matrix, while a column-vector in F^n can be thought of as a $n \times 1$ matrix. From now on, whenever we write a vector as a row vector, we think of it as a matrix with one row, while when we write it in column form, we think of it as a matrix with one column.

Remark 1.4. If $F_1 \subset F$ are fields, then we have a natural inclusion $M_{m,n}(F_1) \subset M_{m,n}(F)$: any matrix with entries in F_1 is naturally a matrix with entries in F. For instance the inclusions $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$, induce inclusions of the corresponding sets of matrices, i.e.

$$M_{m,n}(\mathbf{Q}) \subset M_{m,n}(\mathbf{R}) \subset M_{m,n}(\mathbf{C}).$$

Whenever it is convenient, matrices in $M_{m,n}(F)$ will be denoted symbolically by capital letters $A, B, C, \dots$ or by $[a_{ij}], [b_{ij}], [c_{ij}], \dots$ where $a_{ij}, b_{ij}, c_{ij}, \dots$ respectively, represent the entries of the matrices.

Example 1.5. a) The matrix $[a_{ij}] \in M_{2,3}(\mathbf{Q})$, where $a_{ij} = i^2 + j$ is given by

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 5 & 6 & 7 \end{bmatrix}.$$

b) The matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{bmatrix}$$

can also be written as the matrix $A = [a_{ij}] \in M_4(\mathbf{Q})$ with $a_{ij} = i + j - 1$.

Remark 1.6. Two matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ are equal if and only if they have **the same size** (i.e., the same number of columns and rows) **and** $a_{ij} = b_{ij}$ for all pairs (i, j).

A certain number of matrices will appear rather constantly throughout the book and we would like to make a list of them. First of all, we have the **zero** $m \times n$ **matrix**, that is the matrix all of whose entries are equal to 0. Equivalently, it is the matrix all of whose rows are the zero vector in F^n, or the matrix all of whose columns are the zero vector in F^m. This matrix is denoted $O_{m,n}$ or, if the context is clear, simply 0 (in this case, the context will make it clear that 0 is the zero matrix and not the element $0 \in F$).

Another extremely important matrix is the **unit (or identity) matrix** $I_n \in M_n(F)$, defined by

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

with entries

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

Among the special but important classes of matrices that we will have to deal with quite often in the sequel, we mention:

- The **diagonal matrices**. These are square matrices $A = [a_{ij}]$ such that $a_{ij} = 0$ unless $i = j$. The typical shape of a diagonal matrix is therefore

$$\begin{bmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_n \end{bmatrix}.$$

- The **upper-triangular matrices**. These are square matrices $A = [a_{ij}]$ whose entries below the main diagonal are zero, that is $a_{ij} = 0$ whenever $i > j$. Hence the typical shape of an upper-triangular matrix is

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}.$$

  Of course, one can also define lower-triangular matrices as those square matrices whose entries above the main diagonal are zero.

We will deal now with the basic operations on matrices. Two matrices of **the same size** $m \times n$ can be added together to produce another matrix of the same size. The addition is done component-wise. The re-scaling of a matrix by a scalar is done by multiplying each entry by that scalar. The obtained matrix has the same size as the original one. More formally:

Definition 1.7. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be matrices in $M_{m,n}(F)$ and let $c \in F$ be a scalar.

a) The **sum** $A + B$ of the matrices A and B is the matrix

$$A + B = [a_{ij} + b_{ij}].$$

In fully expanded form

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1n} \\ b_{21} & b_{22} & b_{23} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & b_{m3} & \dots & b_{mn} \end{bmatrix} =$$

$$\begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} & a_{13} + b_{13} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & a_{23} + b_{23} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & a_{m3} + b_{m3} & \dots & a_{mn} + b_{mn} \end{bmatrix}.$$

b) The **re-scaling** of A by c is the matrix

$$cA = [ca_{ij}].$$

Remark 1.8. a) **We insist on the fact that it does not make sense to add two matrices if they do not have the same size.**

b) We also write $-A$ instead of $(-1)A$, thus we write $A - B$ instead of $A + (-1)B$, if A and B have the same size.

Example 1.9. We have

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 & 3 \\ 1 & 3 & 4 & 4 \\ 2 & 3 & 5 & 6 \end{bmatrix}$$

but

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} + I_3$$

does not make sense.

As another example, we have

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

in $M_{3,4}(\mathbf{R})$.

On the other hand, we have the following equality in $M_{3,4}(\mathbf{F}_2)$

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

As we observed in the previous section, we can think of column-vectors in F^n as $n \times 1$ matrices, thus we can define addition and re-scaling for vectors by using the above definition for matrices. Explicitly, we have

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} := \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}$$

and for a scalar $c \in F$

$$c \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} cx_1 \\ cx_2 \\ \vdots \\ cx_n \end{bmatrix}.$$

Similarly, we can define operations on row-vectors by thinking of them as matrices with only one row.

Remark 1.10. a) **Again, it makes sense to add two vectors if and only if they have the same number of coordinates.** So it is nonsense to add a vector in F^2 and a vector in F^3.

b) Similarly, we let $-X$ be the vector $(-1)X$ and, if $X, Y \in F^n$, we let $X - Y = X + (-Y)$.

The following result follows from the basic properties of addition and multiplication rules in a field. We leave the formal proof to the reader.

Proposition 1.11. *For any matrices $A, B, C \in M_{m,n}(F)$ and any scalars $\alpha, \beta \in F$ we have*

(A1) $(A + B) + C = A + (B + C)$ *(associativity of the addition);*
(A2) $A + B = B + A$ *(commutativity of the addition);*
(A3) $A + O_{m,n} = O_{m,n} + A = A$ *(neutrality of $O_{m,n}$);*
(A4) $A + (-A) = (-A) + A = O_{m,n}$ *(cancellation with the opposite matrix).*
(S1) $(\alpha + \beta)A = \alpha A + \beta A$ *(distributivity of the re-scaling over scalar sums);*
(S2) $\alpha(A + B) = \alpha A + \alpha B$ *(distributivity of the re-scaling over matrix sums);*
(S3) $\alpha(\beta A) = (\alpha\beta)A$ *(homogeneity of the scalar product);*
(S4) $1A = A$ *(neutrality of 1).*

Since vectors in F^n are the same thing as $n \times 1$ matrices (or $1 \times n$ matrices, according to our convention of representing vectors), the previous proposition implies that the properties (A1)–(A4) and (S1)–(S4) are also satisfied by vectors in F^n. Of course, this can also be checked directly from the definitions.

Definition 1.12. The **canonical basis** (or **standard basis**) of F^n is the n-tuple of vectors $(e_1, \ldots, e_n)$, where

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Thus e_i is the vector in F^n whose ith coordinate equals 1 and all other coordinates are equal to 0.

Remark 1.13. Observe that the meaning of e_i depends on the context. For example, if we think of e_1 as the first standard basis vector in F^2 then $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, but if we think of it as the first standard basis vector in F^3 then $e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$. It is customary not

to introduce extra notation to distinguish such situations but to rely on the context in deciding on the meaning of e_i.

The following result follows directly by unwinding definitions:

Proposition 1.14. *Any vector $v \in F^n$ can be uniquely written as*

$$v = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n$$

for some scalars $x_1, \ldots, x_n \in F$. In fact, $x_1, \ldots, x_n$ are precisely the coordinates of v.

Proof. If $x_1, \ldots, x_n$ are scalars, then by definition

$$x_1 e_1 + x_2 e_2 + \ldots + x_n e_n = \begin{bmatrix} x_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ x_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \ldots + \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}.$$

The result follows. □

We have similar results for matrices:

Definition 1.15. Let m, n be positive integers. For $1 \leq i \leq m$ and $1 \leq j \leq n$ consider the matrix $E_{ij} \in M_{m,n}(F)$ whose (i, j)-entry equals 1 and all other entries are 0.

The mn-tuple $(E_{11}, \ldots, E_{1n}, E_{21}, \ldots, E_{2n}, \ldots, E_{m1}, \ldots, E_{mn})$ is called the **canonical basis** (or **standard basis**) of $M_{m,n}(F)$.

Proposition 1.16. *Any matrix $A \in M_{m,n}(F)$ can be uniquely expressed as*

$$A = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij}$$

for some scalars a_{ij}. In fact, a_{ij} is the (i, j)-entry of A.

Proof. As in the proof of Proposition 1.14, one checks that for any scalars $x_{ij} \in F$ we have

$$\sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} E_{ij} = \begin{bmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \ldots & x_{mn} \end{bmatrix},$$

which yields the desired result. □

Example 1.17. Let us express the matrix $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 \end{bmatrix}$ in terms of the canonical basis. We have

$$A = E_{11} + E_{12} + E_{22} + E_{23} + 2E_{33} + 2E_{34}.$$

1.1.1 Problems for Practice

1. Write down explicitly the entries of the matrix $A = [a_{ij}] \in M_{2,3}(\mathbf{R})$ in each of the following cases:
   a) $a_{ij} = \frac{1}{i+j-1}$.
   b) $a_{ij} = i + 2j$.
   c) $a_{ij} = ij$.
2. For each of the following pairs of matrices (A, B) explain which of the matrices $A + B$ and $A - 2B$ make sense and compute these matrices whenever they do make sense:
   a) $A = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \end{bmatrix}$.
   b) $A = \begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$.
   c) $A = \begin{bmatrix} 3 & 1 & 0 \\ -1 & -1 & 1 \\ 2 & 0 & 5 \end{bmatrix}$ and $B = \begin{bmatrix} -2 & 1 & 0 \\ 4 & -1 & 1 \\ 6 & 4 & 3 \end{bmatrix}$.
3. Consider the vectors
$$v_1 = \begin{bmatrix} 1 \\ -2 \\ 3 \\ 1 \\ 4 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 2 \\ 2 \\ -1 \\ 4 \\ 3 \end{bmatrix}.$$
   What are the coordinates of the vector $v_1 + 2v_2$?
4. Express the matrix $A = \begin{bmatrix} 3 & 1 & 0 & -4 \\ 7 & -1 & 1 & -2 \\ 8 & 9 & 5 & -3 \end{bmatrix}$ in terms of the canonical basis of $M_{3,4}(\mathbf{R})$.
5. Let $(E_{ij})_{1 \le i \le 2, 1 \le j \le 3}$ be the canonical basis of $M_{2,3}(\mathbf{R})$. Describe the entries of the matrix $E_{11} - 3E_{12} + 4E_{23}$.

6. Let F be a field.
   a) Prove that if $A, B \in M_n(F)$ are diagonal matrices, then $A + cB$ is a diagonal matrix for any $c \in F$.
   b) Prove that the same result holds if we replace diagonal with upper-triangular.
   c) Prove that any matrix $A \in M_n(F)$ can be written as the sum of an upper-triangular matrix and of a lower-triangular matrix. Is there a unique such writing?
7. a) How many distinct matrices are there in $M_{m,n}(\mathbf{F}_2)$?
   b) How many of these matrices are diagonal?
   c) How many of these matrices are upper-triangular?

1.2 Matrices as Linear Maps

In this section we will explain how to see a matrix as a map on vectors. Let F be a field and let $A \in M_{m,n}(F)$ be a matrix with entries a_{ij}. To each vector $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in F^n$ we associate a new vector $AX \in F^m$ defined by

$$AX = \begin{bmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{bmatrix}.$$

We obtain therefore a map $F^n \to F^m$ which sends X to AX.

Example 1.18. The map associated with the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \in M_{3,4}(\mathbf{R})$$

is the map $f : \mathbf{R}^4 \to \mathbf{R}^3$ defined by

$$f\left(\begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix}\right) = A \cdot \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} x + y \\ x + y + z \\ z + t \end{bmatrix}.$$

In terms of row-vectors we have

$$f(x, y, z, t) = (x + y, x + y + z, z + t).$$

Remark 1.19. Consider the canonical basis $e_1, \ldots, e_n$ of F^n. Then by definition for all $1 \leq i \leq n$

$$Ae_i = C_i = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{mi} \end{bmatrix},$$

the ith column of A. In general, if $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in F^n$ is any vector, then

$$AX = x_1C_1 + x_2C_2 + \ldots + x_nC_n,$$

as follows directly from the definition of AX.

The key properties of this correspondence are summarized in the following:

Theorem 1.20. *For all matrices $A, B \in M_{m,n}(F)$, all vectors $X, Y \in F^n$ and all scalars $\alpha, \beta \in F$ we have*

a) $A(\alpha X + \beta Y) = \alpha AX + \beta AY$.
b) $(\alpha A + \beta B)X = \alpha AX + \beta BX$.
c) If $AX = BX$ for all $X \in F^n$, then $A = B$.

Proof. Writing $A = [a_{ij}]$, $B = [b_{ij}]$, and $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, $Y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$, we have

$\alpha A + \beta B = [\alpha a_{ij} + \beta b_{ij}]$ and $\alpha X + \beta Y = \begin{bmatrix} \alpha x_1 + \beta y_1 \\ \alpha x_2 + \beta y_2 \\ \vdots \\ \alpha x_n + \beta y_n \end{bmatrix}$.

a) By definition, the ith coordinate of $A(\alpha X + \beta Y)$ is

$$\sum_{j=1}^{n} a_{ij}(\alpha x_j + \beta y_j) = \alpha \sum_{j=1}^{n} a_{ij}x_j + \beta \sum_{j=1}^{n} a_{ij}y_j.$$

The right-hand side is the ith coordinate of $\alpha AX + \beta AY$, giving the desired result.

b) The argument is identical: the equality is equivalent to

$$\sum_{j=1}^{n}(\alpha a_{ij} + \beta b_{ij})x_j = \alpha \sum_{j=1}^{n} a_{ij}x_j + \beta \sum_{j=1}^{n} b_{ij}x_j$$

which is clear.

c) By hypothesis we have $Ae_i = Be_i$, where $e_1, \ldots, e_n$ is the canonical basis of F^n. Then Remark 1.19 shows that the ith column of A equals the ith column of B for $1 \leq i \leq n$, which is enough to conclude that $A = B$. □

We obtain therefore an injective map $A \mapsto (X \mapsto AX)$ from $M_{m,n}(F)$ to the set of maps $\varphi : F^n \to F^m$ which satisfy

$$\varphi(\alpha X + \beta Y) = \alpha\varphi(X) + \beta\varphi(Y)$$

for all $X, Y \in F^n$ and $\alpha, \beta \in F$. Such a map $\varphi : F^n \to F^m$ is called **linear**. Note that a linear map necessarily satisfies $\varphi(0) = 0$ (take $\alpha = \beta = 0$ in the previous relation), hence this notion is different from the convention used in some other areas of mathematics (in linear algebra a map $\varphi(X) = aX + b$ is usually referred to as an **affine map**).

The following result shows that we obtain all linear maps by the previous procedure:

Theorem 1.21. *Let $\varphi : F^n \to F^m$ be a linear map. There is a unique matrix $A \in M_{m,n}(F)$ such that $\varphi(X) = AX$ for all $X \in F^n$.*

Proof. The uniqueness assertion is exactly part c) of the previous theorem, so let us focus on the existence issue. Let $\varphi : F^n \to F^m$ be a linear map and let $e_1, \ldots, e_n$ be the canonical basis of F^n. Consider the matrix A whose ith column C_i equals the vector $\varphi(e_i) \in F^m$. By Remark 1.19 we have $Ae_i = C_i = \varphi(e_i)$ for all $1 \leq i \leq n$. If $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in F^n$ is an arbitrary vector, then $X = x_1e_1 + \ldots + x_ne_n$, thus since φ is linear, we have

$$\varphi(X) = \varphi(x_1e_1 + \ldots + x_ne_n) = x_1\varphi(e_1) + \ldots + x_n\varphi(e_n) =$$
$$x_1C_1 + \ldots + x_nC_n = AX,$$

the last equality being again a consequence of Remark 1.19. Thus $\varphi(X) = AX$ for all $X \in F^n$ and the theorem is proved. □

We obtain therefore a bijection between matrices in $M_{m,n}(F)$ and linear maps $F^n \to F^m$.

Example 1.22. Let us consider the map $f : \mathbf{R}^4 \to \mathbf{R}^3$ defined by

$$f(x, y, z, t) = (x - 2y + z, 2x - 3z + t, t - x).$$

What is the matrix $A \in M_{3,4}(\mathbf{R})$ corresponding to this linear map? By Remark 1.19, we must have $f(e_i) = C_i$, where e_1, e_2, e_3, e_4 is the canonical basis of $\mathbf{R}^4$ and C_1, C_2, C_3, C_4 are the successive columns of A. Thus, in order to find A, it suffices to compute the vectors $f(e_1), \ldots, f(e_4)$. We have

$$f(e_1) = f(1, 0, 0, 0) = (1, 2, -1), \quad f(e_2) = f(0, 1, 0, 0) = (-2, 0, 0),$$
$$f(e_3) = f(0, 0, 1, 0) = (1, -3, 0), \quad f(e_4) = f(0, 0, 0, 1) = (0, 1, 1).$$

Hence

$$A = \begin{bmatrix} 1 & -2 & 1 & 0 \\ 2 & 0 & -3 & 1 \\ -1 & 0 & 0 & 1 \end{bmatrix}.$$

In practice, one can avoid computing $f(e_1), \ldots, f(e_4)$ as we did before: we look at the first coordinate of the vector $f(x, y, z, t)$, that is $x - 2y + z$. We write it as $1 \cdot x + (-2) \cdot y + 1 \cdot z + 0 \cdot t$ and this gives us the first row of A, namely $\begin{bmatrix} 1 & -2 & 1 & 0 \end{bmatrix}$. Next, we look at the second coordinate of $f(x, y, z, t)$ and write it as $2 \cdot x + 0 \cdot y + (-3) \cdot z + 1 \cdot t$, which gives the second row $\begin{bmatrix} 2 & 0 & -3 & 1 \end{bmatrix}$ of A. We proceed similarly with the last row.

1.2.1 Problems for Practice

1. Describe the linear maps associated with the matrices

$$\begin{bmatrix} 1 & -3 & 2 & 0 \\ 2 & 1 & 4 & 1 \\ -1 & 5 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 3 & 1 \\ -2 & 4 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 2 & -3 & 2 & 5 \end{bmatrix}.$$

2. Consider the map $f : \mathbf{R}^3 \to \mathbf{R}^4$ defined by

$$f(x, y, z) = (x - 2y + 2z, y - z + x, x, z).$$

Prove that f is linear and describe the matrix associated with f.

3. a) Consider the map $f : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

$$f(x, y) = (x^2, y^2).$$

Is this map linear?

b) Answer the same question with the field $\mathbf{R}$ replaced with $\mathbf{F}_2$.

4. Consider the map $f : \mathbf{R}^2 \to \mathbf{R}^2$ defined by

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

Is the map f linear?

5. Consider the matrix $A = \begin{bmatrix} 1 & -2 & 2 & 0 \\ 2 & 0 & 4 & 1 \\ -1 & 1 & 0 & 1 \end{bmatrix}$. Describe the image of the vector $v = \begin{bmatrix} 1 \\ 1 \\ 2 \\ 2 \end{bmatrix}$ through the linear map attached to A.

6. Give an example of a map $f : \mathbf{R}^2 \to \mathbf{R}$ which is **not** linear and for which

$$f(av) = af(v)$$

for all $a \in \mathbf{R}$ and all $v \in \mathbf{R}^2$.

1.3 Matrix Multiplication

Let us consider now three positive integers m, n, p and $A \in M_{m,n}(F)$, $B \in M_{n,p}(F)$. We insist on the fact that **the number of columns n of A equals the number of rows n of B**. We saw in the previous section that A and B define natural maps

$$\varphi_A : F^n \to F^m, \quad \varphi_B : F^p \to F^n,$$

sending $X \in F^n$ to $AX \in F^m$ and $Y \in F^p$ to $BY \in F^n$.

Let us consider the composite map

$$\varphi_A \circ \varphi_B : F^p \to F^m, \quad (\varphi_A \circ \varphi_B)(X) = \varphi_A(\varphi_B(X)).$$

Since φ_A and φ_B are linear, it is not difficult to see that $\varphi_A \circ \varphi_B$ is also linear. Thus by Theorem 1.21 there is a unique matrix $C \in M_{m,p}(F)$ such that

$$\varphi_A \circ \varphi_B = \varphi_C.$$

Let us summarize this discussion in the following fundamental:

Definition 1.23. The product of two matrices $A \in M_{m,n}(F)$ and $B \in M_{n,p}(F)$ (such that the number of columns n of A equals the number of rows n of B) is the unique matrix $AB \in M_{m,p}(F)$ such that

$$A(BX) = (AB)X$$

for all $X \in F^p$.

Remark 1.24. Here is a funny thing, which shows that the theory developed so far is coherent: consider a matrix $A \in M_{m,n}(F)$ and a vector $X \in F^n$, written in column-form. As we said, we can think of X as a matrix with one column, i.e., a matrix $\tilde{X} \in M_{n,1}(F)$. Then we can consider the product $A\tilde{X} \in M_{m,1}(F)$. Identifying again $M_{m,1}(F)$ with column-vectors of length m, i.e., with F^m, $A\tilde{X}$ becomes identified with AX, the image of X through the linear map canonically attached to A. In other words, when writing AX we can either think of the image of X through the canonical map attached to A (and we strongly encourage the reader to do so) or as the product of the matrix A and of a matrix in $M_{n,1}(F)$. The result is the same, modulo the natural identification between column-vectors and matrices with one column.

The previous definition is a little bit abstract, so let us try to **compute explicitly the entries of AB in terms of the entries a_{ij} of A and b_{ij} of B**. Let $e_1, \ldots, e_p$ be the canonical basis of F^p. Then $(AB)e_j$ is the jth column of AB by Remark 1.19. Let $C_1(A), \ldots, C_n(A)$ and $C_1(B), \ldots, C_p(B)$ be the columns of A and B respectively. Using again Remark 1.19, we can write

$$A(Be_j) = AC_j(B) = b_{1j}C_1(A) + b_{2j}C_2(A) + \ldots + b_{nj}C_n(A).$$

Since by definition $A(Be_j) = (AB)e_j = C_j(AB)$, we obtain

$$C_j(AB) = b_{1j}C_1(A) + b_{2j}C_2(A) + \ldots + b_{nj}C_n(A) \tag{1.1}$$

We conclude that

$$(AB)_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj} \tag{1.2}$$

and so we have established the following

Theorem 1.25 (Product Rule). *Let $A = [a_{ij}] \in M_{m,n}(F)$ and $B = [b_{ij}] \in M_{n,p}(F)$. Then the (i, j)-entry of the matrix AB is*

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

Of course, one could also take the previous theorem as a definition of the product of two matrices. But it is definitely not apparent why one should define the product

in such a complicated way: for instance a very natural way of defining the product would be component-wise (i.e., the (i, j)-entry of the product should be the product of the (i, j)-entries in A and B), but this naive definition is not useful for the purposes of linear algebra. The key point to be kept in mind is that **for the purposes of linear algebra (and not only), matrices should be thought of as linear maps, and the product should correspond to the composition of linear maps.**

Example 1.26. a) If $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ are matrices in $M_2(F)$, then AB exists and

$$AB = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}.$$

b) If

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

then the product AB is defined and it is the 3×2 matrix

$$AB = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \\ a_{31}b_{11} + a_{32}b_{21} & a_{31}b_{12} + a_{32}b_{22} \end{bmatrix}$$

The product BA is not defined since $B \in M_{2,2}(F)$ and $A \in M_{3,2}(F)$.

c) Considering

$$A = \begin{bmatrix} 1 & -1 \\ 2 & 0 \\ -1 & 3 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -1 & 2 \\ -3 & 1 \end{bmatrix}$$

we get

$$AB = \begin{bmatrix} 2 & 1 \\ -2 & 4 \\ -8 & 1 \end{bmatrix}$$

d) Take $A, B \in M_2(\mathbf{C})$, where

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}$$

Then, both products AB and BA are defined and we have

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O_2 \quad \text{and} \quad BA = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}.$$

This last example shows two important things:

- multiplication of matrices (even in $M_2(F)$) is **not commutative**, i.e., generally $AB \neq BA$ when AB and BA both make sense (this is the case if $A, B \in M_n(F)$, for instance).
- There are nonzero matrices A, B whose product is 0: for instance in this example we have $A \neq O_2$, $B \neq O_2$, but $AB = O_2$.

Definition 1.27. Two matrices $A, B \in M_n(F)$ **commute** if

$$AB = BA.$$

One has to be very careful when using algebraic operations on matrices, since multiplication is not commutative in general. For instance, one uses quite often identities such as

$$(a+b)^2 = a^2 + 2ab + b^2, \quad (a+b)(a-b) = a^2 - b^2$$

for elements of a field F. Such identities are (in general) no longer true if a, b are matrices and they should be replaced by the following correct identities

$$(A+B)^2 = A^2 + AB + BA + B^2, \quad (A+B)(A-B) = A^2 - AB + BA - B^2.$$

We see that the previous identities (which hold for elements of a field) hold for A and B if and only if A and B commute.

Matrix multiplication obeys many of the familiar arithmetical laws apart from the commutativity property. More precisely, we have the following:

Proposition 1.28. *Multiplication of matrices has the following properties*

1) Associativity: we have $(AB)C = A(BC)$ for all matrices $A \in M_{m,n}(F)$, $B \in M_{n,p}(F)$, $C \in M_{p,q}(F)$.
2) Compatibility with scalar multiplication: we have $\alpha(AB) = (\alpha A)B = A(\alpha B)$ if $\alpha \in F$, $A \in M_{m,n}(F)$ and $B \in M_{n,p}(F)$
3) Distributivity with respect to addition: we have

$$(A+B)C = AC + BC \quad \text{if} \quad A, B \in M_{m,n}(F) \quad \text{and} \quad C \in M_{n,p}(F),$$

and

$$D(A+B) = DA + DB \quad \text{if} \quad A, B \in M_{m,n}(F) \quad \text{and} \quad D \in M_{p,m}(F).$$

All these properties follow quite easily from Definition 1.23 or Theorem 1.25. Let us prove for instance the associativity property (which would be the most painful to check by bare hands if we took Theorem 1.25 as a definition). It suffices (by Theorem 1.21) to check that for all $X \in F^q$ we have

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

But by definition of the product we have

$$((AB)C)X = (AB)(CX) = A(B(CX))$$

and

$$(A(BC))X = A((BC)X) = A(B(CX)),$$

and the result follows. One could also use Theorem 1.25 and check by a rather painful computation that the (i, j)-entry in $(AB)C$ equals the (i, j)-entry in $A(BC)$, by showing that they are both equal to

$$\sum_{k,l} a_{ik} b_{kl} c_{lj}.$$

All other properties of multiplication stated in the previous proposition are proved in exactly the same way and we leave it to the reader to fill in the details.

Remark 1.29. Because of the associativity property we can simply write $ABCD$ instead of the cumbersome $((AB)C)D$, which also equals $(A(BC))D$ or $A(B(CD))$. Similarly, we define the product of any number of matrices. When these matrices are all equal we use the notation

$$A^n = A \times A \times \ldots \times A,$$

with n factors in the right-hand side. This is the nth power of the matrix A. Note that it only make sense to define the powers of a **square** matrix! By construction we have

$$A^n = A \cdot A^{n-1}.$$

We make the natural convention that $A^0 = I_n$ for any $A \in M_n(F)$. The reader will have no difficulty in checking that I_n is a unit for matrix multiplication, in the sense that

$$A \cdot I_n = A \quad \text{and} \quad I_m \cdot A = A \quad \text{if} \quad A \in M_{m,n}(F).$$

We end this section with a long list of problems which illustrate the concepts introduced so far.

Problem 1.30. Let $A(x) \in M_3(\mathbf{R})$ be the matrix defined by

$$A(x) = \begin{bmatrix} 1 & x & x^2 \\ 0 & 1 & 2x \\ 0 & 0 & 1 \end{bmatrix}.$$

Prove that $A(x_1)A(x_2) = A(x_1 + x_2)$ for all $x_1, x_2 \in \mathbf{R}$.

Solution. Using the product rule given by Theorem 1.25, we obtain

$$A(x_1)A(x_2) = \begin{bmatrix} 1 & x_1 & x_1^2 \\ 0 & 1 & 2x_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x_2 & x_2^2 \\ 0 & 1 & 2x_2 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x_2 + x_1 & x_2^2 + 2x_1x_2 + x_1^2 \\ 0 & 1 & 2x_2 + 2x_1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x_1 + x_2 & (x_1 + x_2)^2 \\ 0 & 1 & 2(x_1 + x_2) \\ 0 & 0 & 1 \end{bmatrix}.$$

By definition, the last matrix is simply $A(x_1 + x_2)$. □

The result established in the following problem is very useful and constantly used in practice:

Problem 1.31. a) Prove that the product of two diagonal matrices is a diagonal matrix.

b) Prove that the product of two upper-triangular matrices is upper-triangular.

c) Prove that in both cases the diagonal entries of the product are the product of the corresponding diagonal entries.

Solution. a) Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two diagonal matrices in $M_n(F)$. Let $i \neq j \in \{1, \ldots, n\}$. Using the product rule, we obtain

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

We claim that $a_{ik}b_{kj} = 0$ for all $k \in \{1, 2, \ldots, n\}$, thus $(AB)_{ij} = 0$ for all $i \neq j$ and AB is diagonal. To prove the claim, note that since $i \neq j$, we have $i \neq k$ or $j \neq k$. Thus either $a_{ik} = 0$ (since A is diagonal) or $b_{kj} = 0$ (since B is diagonal), thus in all cases $a_{ik}b_{kj} = 0$ and the claim is proved.

b) Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be upper-triangular matrices in $M_n(F)$. We want to prove that $(AB)_{ij} = 0$ for all $i > j$. By the product rule,

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj},$$

thus it suffices to prove that for all $i > j$ and all $k \in \{1, 2, \ldots, n\}$ we have $a_{ik}b_{kj} = 0$. Fix $i > j$ and $k \in \{1, 2, \ldots, n\}$ and suppose that $a_{ik}b_{kj} \neq 0$, thus $a_{ik} \neq 0$ and $b_{kj} \neq 0$. Since A and B are upper-triangular, we deduce that $i \leq k$ and $k \leq j$, thus $i \leq j$, a contradiction.

c) Again, using the product rule we compute

$$(AB)_{ii} = \sum_{k=1}^{n} a_{ik}b_{ki}.$$

Assume that A and B are upper-triangular (which includes the case when they are both diagonal). If $a_{ik}b_{ki}$ is nonzero for some $k \in \{1, 2, \ldots, n\}$, then $i \leq k$ and $k \leq i$, thus $k = i$. We conclude that

$$(AB)_{ii} = a_{ii}b_{ii}$$

and the result follows. □

Problem 1.32. A matrix $A \in M_n(\mathbf{R})$ is called **right stochastic** if all entries are nonnegative real numbers and the sum of the entries in each row equals 1. We define the concept of **left stochastic** matrix similarly by replacing the word row with column. Finally, a matrix is called **doubly stochastic** if it is simultaneously left and right stochastic.

a) Prove that the product of two left stochastic matrices is a left stochastic matrix.
b) Prove that the product of two right stochastic matrices is a right stochastic matrix.
c) Prove that the product of two doubly stochastic matrices is a doubly stochastic matrix.

Solution. Note that c) is just the combination of a) and b). The argument for proving b) is identical to the one used to prove a), thus we will only prove part a) and leave the details for part b) to the reader. Consider thus two left stochastic matrices $A, B \in M_n(\mathbf{R})$, say $A = [a_{ij}]$ and $B = [b_{ij}]$. Thus $a_{ij} \geq 0$, $b_{ij} \geq 0$ for all $i, j \in \{1, 2, \ldots, n\}$ and moreover the sum of the entries in each column of A or B is 1, which can be written as

$$\sum_{k=1}^{n} a_{ki} = 1, \quad \sum_{k=1}^{n} b_{ki} = 1$$

for $i \in \{1, 2, \ldots, n\}$. Note that by the product rule

$$(AB)_{ij} = \sum_{l=1}^{n} a_{il}b_{lj}$$

is nonnegative for all $i, j \in \{1, 2, \ldots, n\}$. Moreover, the sum of the entries of AB in the ith column is

$$\sum_{k=1}^{n}(AB)_{ki} = \sum_{k=1}^{n}\left(\sum_{j=1}^{n} a_{kj}b_{ji}\right) = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} a_{kj}b_{ji}\right)$$
$$= \sum_{j=1}^{n} b_{ji}\cdot\left(\sum_{k=1}^{n} a_{kj}\right) = \sum_{j=1}^{n} b_{ji}\cdot 1 = \sum_{j=1}^{n} b_{ji} = 1,$$

where we used once the fact that A is left stochastic (so that $\sum_{k=1}^{n} a_{kj} = 1$ for all j) and once the fact that B is stochastic (hence $\sum_{j=1}^{n} b_{ji} = 1$ for all i). The result follows. □

Problem 1.33. Let $(E_{ij})_{1\le i,j\le n}$ be the canonical basis of $M_n(F)$. Prove that if $i, j, k, l \in \{1, 2, \ldots, n\}$, then

$$E_{ij}E_{kl} = \delta_{jk}E_{il},$$

where δ_{jk} equals 1 if $j = k$ and 0 otherwise.

Solution. We use the product rule: let $u, v \in \{1, 2, \ldots, n\}$, then

$$(E_{ij}E_{kl})_{uv} = \sum_{w=1}^{n}(E_{ij})_{uw}(E_{kl})_{wv}.$$

Now $(E_{ab})_{cd}$ is zero unless $a = c$ and $b = d$, and it is equal to 1 if the previous two equalities are satisfied. Thus $(E_{ij})_{uw}(E_{kl})_{wv}$ is zero unless $i = u$, $j = w$ and $k = w$, $l = v$. The last equalities can never happen if $j \neq k$, so if $j \neq k$, then $(E_{ij}E_{kl})_{uv} = 0$ for all $u, v \in \{1, 2, \ldots, n\}$. We conclude that $E_{ij}E_{kl} = 0$ when $j \neq k$.

Assuming now that $j = k$, the previous discussion yields $(E_{ij}E_{kl})_{uv} = 1$ if $u = i$ and $v = l$, and it equals 0 otherwise. In other words,

$$(E_{ij}E_{kl})_{uv} = (E_{il})_{uv}$$

for all $u, v \in \{1, 2, \ldots, n\}$. Thus $E_{ij}E_{kl} = E_{il}$ in this case, as desired. □

Problem 1.34. Let $(E_{ij})_{1\le i,j\le n}$ be the canonical basis of $M_n(F)$. Let $i, j \in \{1, 2, \ldots, n\}$ and consider a matrix $A = [a_{ij}] \in M_n(F)$.

a) Prove that

$$AE_{ij} = \begin{bmatrix} 0 & 0 & \ldots & a_{1i} & 0 & \ldots & 0 \\ 0 & 0 & \ldots & a_{2i} & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & 0 & \ldots & a_{ni} & 0 & \ldots & 0 \end{bmatrix},$$

the only possibly nonzero entries being in the jth column.

b) Prove that

$$E_{ij}A = \begin{bmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix},$$

the only possibly nonzero entries being in the ith row.

Solution. a) Write

$$A = \sum_{k,l=1}^{n} a_{kl} E_{k,l}.$$

Using Problem 1.33, we can write

$$AE_{i,j} = \sum_{k,l=1}^{n} a_{kl} E_{k,l} E_{i,j} = \sum_{k,l=1}^{n} a_{kl} \delta_{i,l} E_{k,j}$$

$$= \sum_{k=1}^{n} a_{ki} E_{k,j} = a_{1i} E_{1,j} + a_{2i} E_{2,j} + \ldots + a_{ni} E_{n,j}.$$

Coming back to the definition of the matrices $E_{1j}, \ldots, E_{n,j}$, the result follows.
b) The proof is identical and left to the reader.

□

Problem 1.35. Prove that a matrix $A \in M_n(F)$ commutes with all matrices in $M_n(F)$ if and only if $A = cI_n$ for some scalar $c \in F$.

Solution. If $A = cI_n$ for some scalar $c \in F$, then $AB = cB$ and $BA = cB$ for all $B \in M_n(F)$, hence $AB = BA$ for all matrices $B \in M_n(F)$. Conversely, suppose that A commutes with all matrices $B \in M_n(F)$. Then A commutes with E_{ij} for all $i, j \in \{1, 2, \ldots, n\}$. Using Problem 1.34 we obtain the equality

$$\begin{bmatrix} 0\,0\,\dots\,a_{1i}\,0\,\dots\,0 \\ 0\,0\,\dots\,a_{2i}\,0\,\dots\,0 \\ \vdots\,\vdots\,\vdots\,\vdots \\ 0\,0\,\dots\,a_{ni}\,0\,\dots\,0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

If $i \neq j$, considering the (j, j)-entry in both matrices appearing in the previous equality yields $a_{ji} = 0$, thus $a_{ij} = 0$ for $i \neq j$ and A is diagonal. Contemplating again the previous equality yields $a_{ii} = a_{jj}$ for all i, j and so all diagonal entries of A are equal. We conclude that $A = a_{11} I_n$ and the problem is solved. □

Problem 1.36. Find all matrices $A \in M_3(\mathbf{C})$ which commute with the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Solution. Let $B = [b_{ij}]$ be a matrix commuting with A. Using the product rule, we obtain

$$AB = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 2b_{21} & 2b_{22} & 2b_{23} \\ 3b_{31} & 3b_{32} & 3b_{33} \end{bmatrix}$$

and

$$BA = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} b_{11} & 2b_{12} & 3b_{13} \\ b_{21} & 2b_{22} & 3b_{23} \\ b_{31} & 2b_{32} & 3b_{33} \end{bmatrix}.$$

Comparing the equality $AB = BA$ yields

$$b_{12} = b_{13} = b_{21} = b_{23} = b_{31} = b_{32} = 0$$

and conversely if these equalities are satisfied, then $AB = BA$. We conclude that the solutions of the problem are the matrices of the form $B = \begin{bmatrix} b_{11} & 0 & 0 \\ 0 & b_{22} & 0 \\ 0 & 0 & b_{33} \end{bmatrix}$, that is the diagonal matrices. □

Problem 1.37. A 3×3 matrix $A \in M_3(\mathbf{R})$ is called **circulant** if there are real numbers a, b, c such that

$$A = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}.$$

a) Prove that the sum and product of two circulant matrices is a circulant matrix.
b) Prove that any two circulant matrices commute.

Solution. Let $A = \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$ and $B = \begin{bmatrix} x & y & z \\ z & x & y \\ y & z & x \end{bmatrix}$ be two circulant matrices.

a) Note that

$$A + B = \begin{bmatrix} a+x & b+y & c+z \\ c+z & a+x & b+y \\ b+y & c+z & a+x \end{bmatrix}$$

is a circulant matrix. Using the product rule we compute

$$AB = \begin{bmatrix} u & v & w \\ w & u & v \\ v & w & u \end{bmatrix},$$

where

$$u = ax + bz + cy, \quad v = ay + bx + cz, \quad w = az + by + cx.$$

Thus AB is also a circulant matrix.

b) Similarly, using the product rule we check that

$$BA = \begin{bmatrix} u & v & w \\ w & u & v \\ v & w & u \end{bmatrix} = AB.$$

□

Problem 1.38. If $A, B \in M_n(\mathbf{C})$ are matrices satisfying

$$A^2 = B^2 = (AB)^2 = I_n,$$

prove that A and B commute.

Solution. Multiplying the relation $ABAB = I_n$ by A on the left and by B on the right, we obtain

$$A^2BAB^2 = AB.$$

By assumption, the left-hand side equals $I_nBAI_n = BA$, thus $BA = AB$. □

1.3.1 Problems for Practice

1. Consider the matrices

$$A = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix}.$$

Which of the products AB and BA make sense? For each product which makes sense, compute the entries of the product.

2. Consider the matrices

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

in $M_3(\mathbf{F}_2)$. Compute AB and BA.

3. Consider the matrices

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 3 & -1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 2 & -1 \\ 1 & 0 \end{bmatrix}.$$

Which of the products A^2, AB, BA, B^2 makes sense? Compute all products that make sense.

4. Let $A = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$.

   a) Find all matrices $B \in M_2(\mathbf{C})$ which commute with A.
   b) Find all matrices $B \in M_2(\mathbf{C})$ for which $AB + BA$ is the zero matrix.

5. Determine all matrices $A \in M_2(\mathbf{R})$ commuting with the matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

6. Let G be the set of matrices of the form $\frac{1}{\sqrt{1-x^2}} \begin{bmatrix} 1 & x \\ x & 1 \end{bmatrix}$ with $x \in (-1, 1)$. Prove that the product of two elements of G is an element of G.

7. (matrix representation of $\mathbf{C}$) Let G be the set of matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ with $a, b \in \mathbf{R}$.

   a) Prove that the sum and product of two elements of G is in G.

b) Consider the map $f : G \to \mathbf{C}$ defined by

$$f\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a + ib.$$

Prove that f is a bijective map satisfying $f(A + B) = f(A) + f(B)$ and $f(AB) = f(A)f(B)$ for all $A, B \in G$.

c) Use this to compute the nth power of the matrix $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

8. For any real number x let

$$A(x) = \begin{bmatrix} 1-x & 0 & x \\ 0 & 1 & 0 \\ x & 0 & 1-x \end{bmatrix}.$$

a) Prove that for all real numbers a, b we have

$$A(a)A(b) = A(a + b - 2ab).$$

b) Given a real number x, compute $A(x)^n$.

9. Compute A^{20}, where

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

10. a) Give a detailed proof, by induction on k, for the **binomial formula**: if $A, B \in M_n(F)$ **commute** then

$$(A + B)^k = \sum_{j=0}^{k} \binom{k}{j} A^{k-j} B^j.$$

b) Give a counterexample to the binomial formula if we drop the hypothesis that A and B commute.

11. a) Let

$$B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Prove that $B^3 = O_3$.

b) Let a be a real number. Using part a) and the binomial formula, compute A^n where

$$A = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & -a \\ a & a & 1 \end{bmatrix}.$$

12. Let

$$A = \begin{bmatrix} 1 & 0 & 1 \\ -1 & 1 & \frac{1}{2} \\ 0 & 0 & 1 \end{bmatrix}.$$

a) Prove that $(A - I_3)^3 = O_3$.
b) Compute A^n for all positive integers n, by using part a) and the binomial formula.

13. a) Prove that the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

satisfies $(A - I_3)^3 = O_3$.
b) Compute A^n for all positive integers n.

14. a) Prove that the matrix

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 4 & 2 & 0 \\ -3 & 0 & 2 \end{bmatrix}$$

satisfies $(A - 2I_3)^3 = O_3$.
b) Compute A^n for all positive integers n.

15. Suppose that $A \in M_n(\mathbf{C})$ is a diagonal matrix whose diagonal entries are pairwise distinct. Let $B \in M_n(\mathbf{C})$ be a matrix such that $AB = BA$. Prove that B is diagonal.
16. A matrix $A \in M_n(\mathbf{R})$ is called a **permutation matrix** if each row and column of A has an entry equal to 1 and all other entries equal to 0. Prove that the product of two permutation matrices is a permutation matrix.
17. Consider a permutation σ of $1, 2, \ldots, n$, that is a bijective map

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

We define the associated permutation matrix P_σ as follows: the (i, j)-entry of P_σ is equal to 1 if $i = \sigma(j)$ and 0 otherwise.

a) Prove that any permutation matrix is of the form P_σ for a unique permutation σ.
b) Deduce that there are $n!$ permutation matrices.
c) Prove that

$$P_{\sigma_1} \cdot P_{\sigma_2} = P_{\sigma_1 \circ \sigma_2}$$

for all permutations σ_1, σ_2.
d) Given a matrix $B \in M_n(F)$, describe the matrices $P_\sigma B$ and BP_σ in terms of B and of the permutation σ.

1.4 Block Matrices

A **sub-matrix** of a matrix $A \in M_{m,n}(F)$ is a matrix obtained from A by deleting rows and/or columns of A (note that A itself is a sub-matrix of A). A matrix can be partitioned into sub-matrices by drawing horizontal or vertical lines between some of its rows or columns. We call such a matrix a **block (or partitioned) matrix** and we call the corresponding sub-matrices **blocks**.

Here are a few examples of partitioned matrices:

$$\left[\begin{array}{c|cc} 1 & 2 & 3 \\ \hline 0 & 1 & 2 \\ 0 & 0 & 1 \end{array}\right], \quad \left[\begin{array}{c|c} 1 & 2 \\ \hline 3 & 4 \end{array}\right], \quad \left[\begin{array}{ccc|c} 0 & 1 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 \end{array}\right].$$

We can see a partitioned matrix as a "matrix of matrices": the typical shape of a partitioned matrix A of size $m \times n$ is

$$A = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1k} \\ A_{21} & A_{22} & \dots & A_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_{l1} & A_{l2} & \dots & A_{lk} \end{bmatrix},$$

where A_{ij} is a matrix of size $m_i \times n_j$ for some positive integers $m_1, \dots, m_l$ and $n_1, \dots, n_k$ with $m_1 + m_2 + \dots + m_l = m$ and $n_1 + n_2 + \dots + n_k = n$. If $l = k$, we call the blocks $A_{11}, \dots, A_{kk}$ the **diagonal blocks** and we say that A is **block diagonal** if all blocks of A but the diagonal ones are zero. Thus a block diagonal matrix is of the form

$$A = \begin{bmatrix} A_{11} & 0 & \dots & 0 \\ 0 & A_{22} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & A_{kk} \end{bmatrix}.$$

An important advantage is given by the following rules for addition and multiplication of block matrices (which follow directly from the rules of addition and multiplication by matrices; we warn however the reader that the proof of the multiplication rule is quite involved from a notational point of view!):

- If

$$A = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1k} \\ A_{21} & A_{22} & \dots & A_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_{l1} & A_{l2} & \dots & A_{lk} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} B_{11} & B_{12} & \dots & B_{1k} \\ B_{21} & B_{22} & \dots & B_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ B_{l1} & B_{l2} & \dots & B_{lk} \end{bmatrix}$$

with A_{ij} and B_{ij} of the same size for all i, j (so the rows and columns of B and A are partitioned in the same way), then

$$A + B = \begin{bmatrix} A_{11} + B_{11} & A_{12} + B_{12} & \dots & A_{1k} + B_{1k} \\ A_{21} + B_{21} & A_{22} + B_{22} & \dots & A_{2k} + B_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_{l1} + B_{l1} & A_{l2} + B_{l2} & \dots & A_{lk} + B_{lk} \end{bmatrix}.$$

- If

$$A = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1k} \\ A_{21} & A_{22} & \dots & A_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ A_{l1} & A_{l2} & \dots & A_{lk} \end{bmatrix}, \quad B = \begin{bmatrix} B_{11} & B_{12} & \dots & B_{1r} \\ B_{21} & B_{22} & \dots & B_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ B_{k1} & B_{k2} & \dots & B_{kr} \end{bmatrix}$$

are $m \times n$, respectively $n \times p$ partitioned matrices, with A_{ij} of size $m_i \times n_j$ and B_{ij} of size $n_i \times p_j$, then

$$AB = \begin{bmatrix} C_{11} & C_{12} & \dots & C_{1r} \\ C_{21} & C_{22} & \dots & C_{2r} \\ \vdots & \vdots & \vdots & \vdots \\ C_{l1} & C_{l2} & \dots & C_{lr} \end{bmatrix},$$

where

$$C_{ij} = \sum_{u=1}^{k} A_{iu} B_{uj}.$$

1.4.1 Problems for Practice

If $A = [a_{ij}] \in M_{m_1,n_1}(F)$ and $B \in M_{m_2,n_2}(F)$ are matrices, the **Kronecker product** or **tensor product** of A and B is the matrix $A \otimes B \in M_{m_1 m_2, n_1 n_2}(F)$ defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1,n_1}B \\ a_{21}B & a_{22}B & \dots & a_{2,n_1}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m_1,1}B & a_{m_1,2}B & \dots & a_{m_1,n_1}B \end{bmatrix}.$$

1. Compute the Kronecker product of the matrices

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 2 & 1 \\ 1 & -1 \end{bmatrix}.$$

2. Do we always have $A \otimes B = B \otimes A$?
3. Check that $I_m \otimes I_n = I_{mn}$.
4. Prove that if $A_1 \in M_{m_1,n_1}(F)$, $A_2 \in M_{n_1,r_1}(F)$, $B_1 \in M_{m_2,n_2}(F)$ and $B_2 \in M_{n_2,r_2}(F)$, then

$$(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) = (A_1 A_2) \otimes (B_1 B_2).$$

5. Prove that if $A \in M_m(F)$ and $B \in M_n(F)$ then

$$A \otimes B = (A \otimes I_n) \cdot (I_m \otimes B).$$

1.5 Invertible Matrices

Let n be a positive integer. We say that a matrix $A \in M_n(F)$ is **invertible or non-singular** if there is a matrix $B \in M_n(F)$ such that

$$AB = BA = I_n.$$

Such a matrix B is then necessarily unique, for if C is another matrix with the same properties, we obtain

$$C = I_n \cdot C = (BA)C = B(AC) = BI_n = B.$$

The matrix B is called the **inverse of** A and denoted A^{-1}.

Let us establish a few basic properties of invertible matrices:

Proposition 1.39. *a) If c is a nonzero scalar, then cI_n is invertible.*
b) If A is invertible, then so is A^{-1}, and $(A^{-1})^{-1} = A$.
c) If $A, B \in M_n(F)$ are invertible, then so is AB and

$$(AB)^{-1} = B^{-1}A^{-1}.$$

Proof. a) The matrix $c^{-1}I_n$ is an inverse of the matrix cI_n.
b) Let $B = A^{-1}$, then $BA = AB = I_n$, showing that B is invertible, with inverse A.
c) By assumption A^{-1} and B^{-1} exist, so the matrix $C = B^{-1}A^{-1}$ makes sense. We compute

$$(AB)C = ABB^{-1}A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

and similarly

$$C(AB) = B^{-1}A^{-1}AB = B^{-1}I_nB = B^{-1}B = I_n,$$

showing that AB is invertible, with inverse C.

□

Remark 1.40. a) One should be careful when computing inverses of products of matrices, for **the formula $(AB)^{-1} = A^{-1}B^{-1}$ is not correct, unless A and B commute.** We will have

$$(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$$

and not $A^{-1}B^{-1}C^{-1}$ in general. Thus the inverse of the product equals the product of the inverses **in the reverse order**.

b) By the proposition, invertible matrices are stable under product, but they are definitely not stable under addition: the matrices I_n and $-I_n$ are invertible, but their sum O_n is not invertible (as $O_nA = O_n \neq I_n$ for any matrix $A \in M_n(F)$).

The set of invertible matrices plays an extremely important role in linear algebra, so it deserves a definition and a special notation:

Definition 1.41. The set of invertible matrices $A \in M_n(F)$ is called the **general linear group** and denoted $\mathrm{GL}_n(F)$.

Unfortunately, with the tools introduced so far it is illusory to hope to understand the fine properties of the general linear group $\mathrm{GL}_n(F)$. Once we develop the theory of linear algebra from the point of view of vector spaces and linear transformations, we will have a much more powerful theory that will make it easier to understand invertible matrices. Just to give a hint of the difficulty of the theory, try to prove by bare hands that if $A, B \in M_n(F)$ satisfy $AB = I_n$, then A is invertible. The key point is proving that this equality forces $BA = I_n$, but this is definitely not trivial simply by coming back to the multiplication of matrices! In subsequent chapters we will develop a theory of determinants which allows a much cleaner characterization of invertible matrices. Also, in subsequent chapters we will describe an algorithm, based on operations on the rows of a matrix, which gives an efficient way of solving the following problem: given a square matrix A, decide whether A is invertible and compute its inverse if A is invertible. This problem is not easy to solve with the tools we have introduced so far.

Problem 1.42. Consider the matrix $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Is the matrix A invertible? If this is case, compute A^{-1}.

Solution. Since we don't have any strong tools at our disposal for the moment, let us use brute force and look for a matrix $\begin{bmatrix} a & b & c \\ x & y & z \\ u & v & w \end{bmatrix}$ such that

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b & c \\ x & y & z \\ u & v & w \end{bmatrix} = I_3.$$

The left-hand side equals $\begin{bmatrix} x & y & z \\ a & b & c \\ u & v & w \end{bmatrix}$, so this last matrix should be equal to I_3. This gives a unique solution $x = b = w = 1$ and all other variables are equal to 0. We conclude that A is invertible and

$$A^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

□

It is clear that the method used to find the inverse of A in the previous problem is not efficient and quickly becomes very painful even for 3×3 matrices. We will see later on a much more powerful approach, but we would like to present yet another

method, which can be fairly useful in some situations (especially when the matrix has some nice symmetry properties or if it has many zeros).

Consider a matrix $A \in M_n(F)$ and a vector $b \in F^n$. Assume that we can always solve the system $AX = b$ with $X \in F^n$ and that it has a unique solution. Then one can prove (we will see this in a later chapter, so we will take it for granted in this chapter) that A is invertible and so the solution of the system is given by $X = A^{-1}b$ (multiply the relation $AX = b$ by A^{-1}). On the other hand, assume that we are able to solve the system by hand, then we have a description of X in terms of the coordinates of b. Thus we will know explicitly $A^{-1}b$ for all vectors $b \in F^n$ and this is enough to find A^{-1}. In practice, the resolution of the system will show that

$$A^{-1}b = \begin{bmatrix} c_{11}b_1 + c_{12}b_2 + \ldots + c_{1n}b_n \\ c_{21}b_1 + c_{22}b_2 + \ldots + c_{2n}b_n \\ \vdots \\ c_{n1}b_1 + c_{22}b_2 + \ldots + c_{nn}b_n \end{bmatrix}$$

for some scalars c_{ij}, independent of $b_1, \ldots, b_n$. Letting b be the ith vector of the canonical basis of F^n, the left-hand side $A^{-1}b$ is simply the ith column of A^{-1}, while the right-hand side is the ith column of the matrix $[c_{ij}]$. Since the two sides are equal and this for all i, we conclude that

$$A^{-1} = [c_{ij}].$$

Note that once the system is solved, it is very easy to write the matrix A^{-1} directly by looking at the expression of $A^{-1}b$. Namely, if the first coordinate of $A^{-1}b$ is $c_{11}b_1 + c_{12}b_2 + \ldots + c_{1n}b_n$, then the first row of A^{-1} is $(c_{11}, c_{12}, \ldots, c_{1n})$. Of course, the key part of the argument is the resolution of the linear system $AX = b$, and this will be discussed in a subsequent chapter. We will limit therefore ourselves in this chapter to rather simple systems, which can be solved by hand without any further theory.

Let us see a few concrete examples:

Problem 1.43. Compute the inverse of the matrix A in the previous problem using the method we have just described.

Solution. Given a vector $b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \in F^3$, we try to solve the system $AX = b$, with $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$. The system can be written as

$$x_2 = b_1, \quad x_1 = b_2, \quad x_3 = b_3,$$

or equivalently

$$x_1 = b_2, \quad x_2 = b_1, \quad x_3 = b_3.$$

Since this system has a solution for all $b \in F^3$, we deduce that A is invertible and that for all $b \in F^3$ we have

$$A^{-1}b = X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} b_2 \\ b_1 \\ b_3 \end{bmatrix}.$$

The first coordinate of $A^{-1}b$ is b_2, thus the first row of A^{-1} is $(0, 1, 0)$, the second coordinate of $A^{-1}b$ is b_1 so the second row of A^{-1} is $(1, 0, 0)$. Finally, the third coordinate of $A^{-1}b$ is b_3, so the third row of A^{-1} is $(0, 0, 1)$. We conclude that

$$A^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

□

Problem 1.44. Consider the matrix

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

Prove that A is invertible and compute A^{-1}.

Solution. Again, given a vector $b = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} \in F^4$ we try to solve the system $AX = b$ with $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$. The system can be written

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = b_1 \\ x_2 + x_3 + x_4 = b_2 \\ x_3 + x_4 = b_3 \\ x_4 = b_4 \end{cases}$$

and can be solved rather easily: the last equation gives $x_4 = b_4$. Subtracting the last equation from the third one yields $x_3 = b_3 - b_4$, then subtracting the third equation from the second one yields $x_2 = b_2 - b_3$ and finally $x_1 = b_1 - b_2$. Thus the system always has solutions and so A is invertible, with

$$A^{-1}b = X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} b_1 - b_2 \\ b_2 - b_3 \\ b_3 - b_4 \\ b_4 \end{bmatrix}.$$

The first coordinate of $A^{-1}b$ being $b_1 - b_2$, we deduce that the first row of A is $\begin{bmatrix} 1 & -1 & 0 & 0 \end{bmatrix}$. Similarly, the coordinate $b_2 - b_3$ gives the second row of A namely $\begin{bmatrix} 0 & 1 & -1 & 0 \end{bmatrix}$, and so on. We end up with

$$A^{-1} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

□

Problem 1.45. Let n be a positive integer. Find the inverse of the matrix

$$\begin{bmatrix} 1 & 2 & 3 & \dots & n \\ 0 & 1 & 2 & \dots & n-1 \\ 0 & 0 & 1 & \dots & n-2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Solution. Let A be the matrix whose inverse we are trying to compute. Given a vector $b \in \mathbf{R}^n$ with coordinates $b_1, b_2, \dots, b_n$, let us try to solve the system $AX = b$. This system is equivalent to

$$\begin{cases} x_1 + 2x_2 + 3x_3 + \dots + nx_n = b_1 \\ x_2 + 2x_3 + \dots + (n-1)x_n = b_2 \\ \vdots \\ x_{n-1} + 2x_n = b_{n-1} \\ x_n = b_n \end{cases}$$

In principle one can easily solve it by starting with the last equation and successively determining $x_n, x_{n-1}, \dots, x_1$ from the equations of the system. To make our life simpler, we subtract the second equation from the first, the third equation from the second,..., the nth equation from the $n-1$th equation. We end

up with the equivalent system

$$\begin{cases} x_1 + x_2 + x_3 + \ldots + x_n = b_1 - b_2 \\ \quad x_2 + x_3 + \ldots + x_n = b_2 - b_3 \\ \qquad\qquad \vdots \\ \quad x_{n-1} + x_n = b_{n-1} - b_n \\ \qquad x_n = b_n. \end{cases}$$

Subtracting again consecutive equations yields

$$x_1 = b_1 - 2b_2 + b_3, \quad x_2 = b_2 - 2b_3 + b_4, \ldots, x_{n-1} = b_{n-1} - 2b_n, \quad x_n = b_n.$$

Since the system $AX = b$ always has solutions, we deduce that A is invertible. Moreover, the system is equivalent to $A^{-1}b = X$ and the expressions of $x_1, x_2, \ldots, x_n$ give us the rows of A^{-1}: $x_1 = b_1 - 2b_2 + b_3$ shows that the first row of A^{-1} equals $(1, -2, 1, 0, \ldots, 0)$,..., $x_{n-1} = b_{n-1} - 2b_n$ shows that the next-to-last row is $(0, 0, \ldots, 0, 1, -2)$ and finally the last row of A^{-1} is $(0, 0, \ldots, 1)$. Thus

$$A^{-1} = \begin{bmatrix} 1 & -2 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & -2 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 & -2 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \end{bmatrix}.$$

□

Problem 1.46. Let $A, B \in M_n(F)$ be matrices such that $AB = BA$. Prove that if A is invertible, then $A^{-1}B = BA^{-1}$.

Solution. Multiply the relation $AB = BA$ on the left by A^{-1} and on the right by A^{-1}. We obtain

$$A^{-1}ABA^{-1} = A^{-1}BAA^{-1}.$$

Since $A^{-1}A = I_n$, the left-hand side equals BA^{-1}. Since $AA^{-1} = I_n$, the right-hand side equals $A^{-1}B$. Thus $A^{-1}B = BA^{-1}$, as desired. □

Problem 1.47. Prove that a diagonal matrix $A \in M_n(F)$ is invertible if and only if all its diagonal entries are nonzero. Moreover, if this is the case, then A^{-1} is also diagonal.

Solution. Let $A = [a_{ij}] \in M_n(F)$ be a diagonal matrix. If $B = [b_{ij}] \in M_n(F)$ is an arbitrary matrix, let us compute AB. Using the product rule, we have

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

We have $a_{ik} = 0$ for $k \neq i$, since A is diagonal. Thus

$$(AB)_{ij} = a_{ii} b_{ij}$$

and similarly

$$(BA)_{ij} = a_{jj} b_{ij}.$$

Suppose now that $a_{ii} \neq 0$ for all $i \in \{1, 2, \ldots, n\}$ and consider the diagonal matrix B with diagonal entries $b_{ii} = \frac{1}{a_{ii}}$. Then the formulae in the previous paragraph yield $AB = BA = I_n$, thus A is invertible and $A^{-1} = B$ is diagonal.

Conversely, suppose that A is invertible and diagonal, thus we can find a matrix B such that $AB = BA = I_n$. Thus for all $i \in \{1, \ldots, n\}$ we have

$$1 = (I_n)_{ii} = (AB)_{ii} = a_{ii} b_{ii},$$

hence $a_{ii} \neq 0$ for all i and so all diagonal entries of A are nonzero. □

Sometimes, it can be very easy to prove that a matrix A is invertible and to compute its inverse, if we know that A satisfies some algebraic equation. For instance, imagine that we knew that

$$A^3 + 3A + I_n = O_n.$$

Then $A^3 + 3A = -I_n$, which can be written as

$$A \cdot (-A^2 - 3I_n) = I_n.$$

On the other hand, we also have

$$(-A^2 - 3I_n) \cdot A = -A^3 - 3A = I_n,$$

thus A is invertible and $A^{-1} = -A^2 - 3I_n$. In general, a similar argument shows that if $A \in M_n(\mathbf{C})$ satisfies an equation of the form

$$a_d A^d + a_{d-1} A^{d-1} + \ldots + a_0 I_n = 0$$

for some complex numbers $a_0, \ldots, a_d$ with $a_0 \neq 0$, then A is invertible and

$$A^{-1} = -\left(\frac{a_d}{a_0}A^{d-1} + \frac{a_{d-1}}{a_0}A^{d-2} + \ldots + \frac{a_1}{a_0}I_n\right).$$

Of course, it is totally mysterious how to find such an algebraic equation satisfied by A in general, but we will see much later how to naturally create such equations (this will already require a lot of nontrivial theory!).

We discuss below two more such examples.

Problem 1.48. Consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 3 & 0 & -1 \end{bmatrix}.$$

a) Check that

$$A^3 - A^2 - 8A - 18I_3 = O_3.$$

b) Deduce that A is invertible and compute A^{-1}.

Solution. a) We compute brutally, using the product rule

$$A^2 = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 3 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 3 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 8 & 4 & 6 \\ 13 & 5 & 2 \\ 0 & 6 & 4 \end{bmatrix}$$

and

$$A^3 = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \\ 3 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 8 & 4 & 6 \\ 13 & 5 & 2 \\ 0 & 6 & 4 \end{bmatrix} = \begin{bmatrix} 34 & 20 & 14 \\ 29 & 31 & 26 \\ 24 & 6 & 14 \end{bmatrix}.$$

It follows that

$$A^3 - A^2 - 18I_3 = \begin{bmatrix} 8 & 16 & 8 \\ 16 & 8 & 24 \\ 24 & 0 & -8 \end{bmatrix} = 8A$$

and the result follows.

b) We can write the identity in a) as follows:

$$A(A^2 - A - 8I_3) = 18I_3$$

or equivalently

$$A \cdot \frac{1}{18}(A^2 - A - 8I_3) = I_3.$$

Similarly, we obtain

$$\frac{1}{18}(A^2 - A - 8I_3) \cdot A = I_3$$

and this shows that A is invertible and

$$A^{-1} = \frac{1}{18}(A^2 - A - 8I_3) = \frac{1}{18}\begin{bmatrix} -1 & 2 & 5 \\ 11 & -4 & -1 \\ -3 & 6 & -3 \end{bmatrix}.$$

□

Problem 1.49. Let $n > 1$ be an integer and let

$$\zeta = e^{\frac{2i\pi}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Let F_n be the **Fourier matrix of order** n, whose (j,k)-entry is $\zeta^{(j-1)(k-1)}$ for $1 \leq j,k \leq n$.

a) Let $\overline{F_n}$ be the matrix whose (j,k)-entry is the complex conjugate of the (j,k)-entry of F_n. Prove that

$$F_n \cdot \overline{F_n} = \overline{F_n} \cdot F_n = nI_n.$$

b) Deduce that F_n is invertible and compute its inverse.

Solution. a) Let $j,k \in \{1,2,\ldots,n\}$ and let us use the product rule to compute

$$(F_n \cdot \overline{F_n})_{jk} = \sum_{l=1}^{n} (F_n)_{jl} \cdot (\overline{F_n})_{lk} =$$

$$\sum_{l=1}^{n} \zeta^{(j-1)(l-1)} \cdot \overline{\zeta^{(l-1)(k-1)}} = \sum_{l=1}^{n} \zeta^{(j-1)(l-1)-(l-1)(k-1)},$$

the last equality being a consequence of the fact that $\overline{\zeta} = \zeta^{-1}$. Thus

$$(F_n \cdot \overline{F_n})_{jk} = \sum_{l=1}^{n} \zeta^{(l-1)(j-k)} = \sum_{l=0}^{n-1} (\zeta^{j-k})^l.$$

The last sum is the sum of a geometric progression with ratio ζ^{j-k}. If $j = k$, then $\zeta^{j-k} = 1$, so the sum equals n, since each term is equal to 1 in this case. If $j \neq k$, then $\zeta^{j-k} \neq 1$ and we have

$$\sum_{l=0}^{n-1} (\zeta^{j-k})^l = \frac{1 - (\zeta^{j-k})^n}{1 - \zeta^{j-k}} = \frac{1 - (\zeta^n)^{j-k}}{1 - \zeta^{j-k}} = 0,$$

the last equality being a consequence of the formula $\zeta^n = 1$. We conclude that $(F_n \cdot \overline{F_n})_{jk}$ equals n when $j = k$ and equals 0 otherwise. It follows that

$$F_n \cdot \overline{F_n} = nI_n.$$

The equality $\overline{F_n} \cdot F_n = nI_n$ is proved is exactly the same way and we leave the details to the reader.

b) By part a) we can write

$$F_n \cdot \frac{1}{n}\overline{F_n} = \frac{1}{n}\overline{F_n} = I_n,$$

which plainly shows that F_n is invertible and

$$F_n^{-1} = \frac{1}{n}\overline{F_n}.$$ □

1.5.1 Problems for Practice

1. Find the inverse of the matrix

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

2. For which real numbers x is the matrix

$$A = \begin{bmatrix} 1 & x \\ 2 & 3 \end{bmatrix}$$

invertible? For each such x, compute the inverse of A.

3. Is the matrix

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \in M_3(\mathbf{F}_2)$$

invertible? If so, compute its inverse.

4. Same problem with the matrix

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in M_3(\mathbf{F}_2).$$

5. Consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in M_5(\mathbf{R}).$$

Prove that A is invertible and compute its inverse.

6. Consider the matrix

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

a) Compute the inverse of A by solving, for each $b \in \mathbf{R}^4$, the system $AX = b$.
b) Prove that $A^2 = 3I_4 + 2A$. Deduce a new way of computing A^{-1}.

7. Let A be the matrix

$$A = \begin{bmatrix} 3 & -1 & 2 \\ 5 & -2 & 3 \\ -1 & 0 & -1 \end{bmatrix}.$$

a) Check that $A^3 = O_3$.
b) Compute $(I_3 + A)^{-1}$.

8. Let n be a positive integer. Find the inverse of the $n \times n$ matrix A whose entries on or above the main diagonal are equal to 1 and whose entries (strictly) below the main diagonal are zero.
9. Consider the matrices

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

and

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

and let $\mathcal{H}$ be the set of all matrices of the form $aA + bB + cC + dI_4$, with a, b, c, d real numbers.

a) Prove that $A^2 = B^2 = C^2 = -I_4$ and

$$BC = -CB = A, \quad CA = -AC = B, \quad AB = -BA = C.$$

b) Prove that the sum and product of two elements of $\mathcal{H}$ is an element of $\mathcal{H}$.
c) Prove that all nonzero elements of $\mathcal{H}$ are invertible.

10. Let $A, B \in M_n(\mathbf{R})$ such that

$$A + B = I_n \quad \text{and} \quad A^2 + B^2 = O_n.$$

Prove that A and B are invertible and that

$$(A^{-1} + B^{-1})^n = 2^n I_n$$

for all positive integers n.
11. Let $A \in M_n(\mathbf{R})$ be an invertible matrix such that

$$A^{-1} = I_n - A.$$

Prove that

$$A^6 - I_n = O_n.$$

12. Let $A \in M_n(\mathbf{R})$ be a matrix such that $A^2 = \mu A$, where μ is a real number with $\mu \neq -1$. Prove that

$$(I_n + A)^{-1} = I_n - \frac{1}{\mu + 1} A.$$

13. Recall that a permutation matrix is a matrix $A \in M_n(\mathbf{C})$ such that every row and column of A contains one entry equal to 1 and all other entries are 0. Prove that a permutation matrix is invertible and that its inverse is also a permutation matrix.
14. Suppose that an upper-triangular matrix $A \in M_n(\mathbf{C})$ is invertible. Prove that A^{-1} is also upper-triangular.
15. Let a, b, c be positive real numbers, not all of them equal and consider the matrix

$$A = \begin{bmatrix} a & 0 & b & 0 & c & 0 \\ 0 & a & 0 & c & 0 & b \\ c & 0 & a & 0 & b & 0 \\ 0 & b & 0 & a & 0 & c \\ b & 0 & c & 0 & a & 0 \\ 0 & c & 0 & b & 0 & a \end{bmatrix}.$$

Prove that A is invertible. Hint: A^{-1} is a matrix of the same form as A (with a, b, c replaced by suitable real numbers x, y, z).

1.6 The Transpose of a Matrix

Let $A \in M_{m,n}(F)$ be a $m \times n$ matrix. The **transpose** of A is the matrix ${}^tA$ (also denoted as A^T) obtained by interchanging the rows and columns of A. Consequently ${}^tA$ is a $n \times m$ matrix, i.e., ${}^tA \in M_{n,m}(F)$. It is clear that ${}^tI_n = I_n$. Note that if $A = [a_{ij}]$, then ${}^tA = [a_{ji}]$, that is

$$({}^tA)_{ij} = A_{ji} \tag{1.3}$$

Example 1.50. a) The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 3 & 4 & 5 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 0 & 3 \\ 2 & -1 & 4 \\ 3 & -2 & 5 \end{bmatrix}$.

b) The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 0 \\ 2 & 1 \\ 3 & 2 \\ 4 & 3 \end{bmatrix}$.

The following proposition summarizes the basic properties of the operation $A \to {}^tA$ on $M_{m,n}(F)$.

Proposition 1.51. *The transpose operation has the following properties:*

1) ${}^t({}^tA) = A$ *for all* $A \in M_{m,n}(F)$.
2) ${}^t(A + B) = {}^tA + {}^tB$ *for all* $A, B \in M_{m,n}(F)$;
3) ${}^t(cA) = c\,{}^tA$ *if* $c \in F$ *is a scalar and* $A \in M_{m,n}(F)$.
4) ${}^t(AB) = {}^tB\,{}^tA$ *if* $A \in M_{m,n}(F)$ *and* $B \in M_{n,p}(F)$;
5) ${}^t(A^k) = ({}^tA)^k$ *if* $A \in M_n(F)$ *and* k *is a positive integer;*
6) If the matrix A *is invertible, then* ${}^tA$ *is also invertible and*

$$({}^tA)^{-1} = {}^t(A^{-1});$$

Proof. Properties 1), 2), and 3) are immediate from the definition of the transpose of a matrix (more precisely from relation (1.3)). Let us prove (4). First, note that ${}^tB \in M_{p,n}(F)$ and ${}^tA \in M_{n,m}(F)$, thus ${}^tB \cdot {}^tA$ makes sense. Next, if $A = [a_{ij}]$ and $B = [b_{jk}]$, we have

$$({}^t(AB))_{ki} = (AB)_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} = \sum_{j=1}^{n} ({}^tB)_{kj} ({}^tA)_{ji} = ({}^tB\,{}^tA)_{ki},$$

thus ${}^t(AB) = {}^tB\,{}^tA$.

Property 5) follows by induction on k, using property 4. Finally, property 6) also follows from 4), since

$$I_n = {}^tI_n = {}^t(A \cdot A^{-1}) = {}^t(A^{-1})\,{}^tA$$

and similarly ${}^tA \cdot {}^t(A^{-1}) = I_n$. □

It follows from the previous proposition that the transpose operation leaves the general linear group $\mathrm{GL}_n(F)$ invariant, that is ${}^tA \in \mathrm{GL}_n(F)$ whenever $A \in \mathrm{GL}_n(F)$.

Problem 1.52. Let $X \in F^n$ be a vector with coordinates $x_1, \ldots, x_n$, considered as a matrix in $M_{n,1}(F)$. Prove that for any matrix $A \in M_n(F)$ we have

$${}^tX({}^tA \cdot A)X = \sum_{i=1}^{n} (a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n)^2.$$

Solution. First of all, we use Proposition 1.51 to obtain

$$ {}^tX({}^tA \cdot A)X = {}^tX\,{}^tAAX = {}^t(AX) \cdot AX. $$

Write now

$$ Y = AX = \begin{bmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ a_{21}x_1 + \ldots + a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + \ldots + a_{nn}x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}. $$

Then

$$ {}^tY \cdot Y = \begin{bmatrix} y_1 & y_2 & \ldots & y_n \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} $$

and using the product rule for matrices, we obtain that the last quantity equals $y_1^2 + \ldots + y_n^2$. We conclude that

$$ {}^tX({}^tA \cdot A)X = {}^tY \cdot Y = y_1^2 + \ldots + y_n^2 = \sum_{i=1}^{n} (a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n)^2. $$

□

There are three types of special matrices that play a fundamental role in linear algebra and that are related to the transpose operation:

- The **symmetric matrices**. These are matrices $A \in M_n(F)$ for which ${}^tA = A$ or equivalently $a_{ij} = a_{ji}$ for all i, j. They play a crucial role in the theory of quadratic forms and euclidean spaces (for the latter one choose $F = \mathbf{R}$), and a whole chapter will be devoted to their subtle properties. For example, all symmetric matrices of order 2 and 3 are of the form

$$ \begin{bmatrix} a & b \\ b & c \end{bmatrix}, \quad a, b, c \in F \quad \text{and} \quad \begin{bmatrix} a & b & c \\ b & d & e \\ c & e & f \end{bmatrix}, \quad a, b, c, d, e, f \in F. $$

- The **orthogonal matrices**. These are matrices $A \in \mathrm{GL}_n(F)$ for which

$$ A^{-1} = {}^tA. $$

They also play a fundamental role in the theory of euclidean spaces, since these matrices correspond to isometries of such spaces. They will also be extensively studied in the last chapter of the book.

- The **skew-symmetric** (or **antisymmetric**) matrices. These are matrices for which

$$A + {}^tA = O_n,$$

that is ${}^tA = -A$. These matrices are related to alternating forms. They satisfy $a_{ij} = -a_{ji}$ for all i, j. Thus $2a_{ii} = 0$. If $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$, then this last equality forces $a_{ii} = 0$ for all i. Thus the diagonal elements of a skew-symmetric matrix are in this case equal to 0. On the other hand, over a field F such as $\mathbf{F}_2$ (the field with two elements), the condition $2a_{ii} = 0$ does not give any information about the element a_{ii}, since for any $x \in \mathbf{F}_2$ we have $2x = 0$. Actually, over such a field there is no difference between symmetric and skew-symmetric matrices! All skew-symmetric matrices of order 2 and 3 over the field $\mathbf{C}$ of complex numbers are of the following form:

$$\begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}, \quad a \in \mathbf{C} \quad \text{and} \quad \begin{bmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{bmatrix}, \quad a, b, c \in \mathbf{C}.$$

Proposition 1.53. *All matrices in the following statements are square matrices of the same size. Prove that*

1) The sum of a matrix and its transpose is a symmetric matrix. The difference of a matrix and its transpose is a skew-symmetric matrix.
2) The product of a matrix and its transpose is a symmetric matrix.
3) Any power of a symmetric matrix is symmetric.
4) An even power of a skew-symmetric matrix is symmetric. An odd power of a skew-symmetric matrix is skew-symmetric.
5) If A is invertible and symmetric, then A^{-1} is symmetric.
6) If A is invertible and skew-symmetric, then A^{-1} is skew-symmetric.

Proof. 1) If A is a matrix, then ${}^t(A +^t A) = {}^tA +^t ({}^tA) = {}^tA + A = A +^t A$, thus $A +^t A$ is symmetric. Similarly, ${}^t(A -^t A) = {}^tA - A = -(A -^t A)$, thus $A -^t A$ is skew-symmetric.
2) We have ${}^t(A^tA) = {}^t({}^tA)^tA = A^tA$, thus A^tA is symmetric.
3) and 4) follow from the equality $({}^tA)^n = {}^t(A^n)$, valid for any matrix A and any $n \geq 1$.
5) and 6) follow from the equality ${}^t(A^{-1}) = ({}^tA)^{-1}$, valid for any invertible matrix A. □

We end this section with a rather long list of problems that illustrate the ideas introduced in this section.

Problem 1.54. Describe the symmetric matrices $A \in M_n(F)$ which are simultaneously upper-triangular.

Solution. Let $A = [a_{ij}]$ be a symmetric and upper-triangular matrix. By definition $a_{ij} = 0$ whenever $i > j$ (since A is upper-triangular) and moreover $a_{ij} = a_{ji}$ for all $i, j \in \{1, 2, \ldots, n\}$. We conclude that $a_{ij} = 0$ whenever $i \neq j$, that is A is diagonal. Conversely, any diagonal matrix is clearly symmetric and upper-triangular. Thus the answer of the problem is: the diagonal matrices. □

Problem 1.55. How many symmetric matrices are there in $M_n(\mathbf{F}_2)$?

Solution. By definition, each entry of a matrix $A = [a_{ij}] \in M_n(\mathbf{F}_2)$ is equal to 0 or 1, and A is symmetric if and only if $a_{ij} = a_{ji}$ for all $i, j \in \{1, 2, \ldots, n\}$. Thus a symmetric matrix A is entirely determined by the choice of the entries above or on the main diagonal, that is the entries a_{ij} with $1 \leq i \leq j \leq n$. Moreover, for any choice of these entries, we can construct a symmetric matrix by defining $a_{ij} = a_{ji}$ for $i > j$. For each pair (i, j) with $1 \leq i \leq j \leq n$ we have two choices for the entry a_{ij} (either 0 or 1). Since there are $n + \binom{n}{2} = \frac{n(n+1)}{2}$ such pairs (i, j) (n pairs with $i = j$ and $\binom{n}{2} = \frac{n(n-1)}{2}$ pairs with $i < j$) and since the choices are independent, we deduce that the number of symmetric matrices in $M_n(\mathbf{F}_2)$ is $2^{\frac{n(n+1)}{2}}$. □

Problem 1.56. a) Describe the diagonal matrices $A \in M_n(\mathbf{R})$ which are skew-symmetric.

b) Same question, but replacing $\mathbf{R}$ with $\mathbf{F}_2$.

Solution. a) Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a diagonal skew-symmetric matrix. Since A is diagonal, all entries away from the main diagonal are zero. Also, since $A + {}^tA = 0$, we have

$$a_{ii} + a_{ii} = 0$$

for all $i \in \{1, 2, \ldots, n\}$, by noticing that A and ${}^tA$ have the same diagonal entries. We conclude that $2a_{ii} = 0$ and so $a_{ii} = 0$ for all $i \in \{1, 2, \ldots, n\}$. Thus $A = O_n$ is the unique diagonal skew-symmetric matrix in $M_n(\mathbf{R})$.

b) As in part a), a matrix $A = [a_{ij}] \in M_n(\mathbf{F}_2)$ is diagonal and skew-symmetric if and only if it is diagonal and its diagonal entries a_{ii} (for $1 \leq i \leq n$) satisfy $2a_{ii} = 0$. However, any element x of $\mathbf{F}_2$ satisfies $2x = 0$, thus the condition $2a_{ii} = 0$ is automatic. We conclude that **any** diagonal matrix $A \in M_n(\mathbf{F}_2)$ is skew-symmetric! □

Problem 1.57. A matrix $A \in M_n(\mathbf{R})$ has a unique nonzero entry in each row and column, and that entry equals 1 or -1. Prove that A is orthogonal.

Solution. Let $A = [a_{ij}]$. We need to prove that $A^{-1} = {}^tA$, that is $A \cdot {}^tA = I_n$ and ${}^tA \cdot A = I_n$. Fix $i, j \in \{1, 2, \ldots, n\}$. Then the (i, j)-entry of $A \cdot {}^tA$ is

$$(A \cdot {}^tA)_{ij} = \sum_{k=1}^{n} a_{ik} a_{jk}.$$

Assume that $a_{ik}a_{jk}$ is nonzero for some $k \in \{1, 2, \ldots, n\}$, thus both a_{ik} and a_{jk} are nonzero. If $i \neq j$, this means that A has at least two nonzero entries in column k, which is impossible. Thus if $i \neq j$, then $a_{ik}a_{jk} = 0$ for all $k \in \{1, 2, \ldots, n\}$ and consequently the (i, j)-entry of $A \cdot {}^tA$ is 0.

On the other hand, if $i = j$, then

$$(A \cdot {}^tA)_{ij} = \sum_{k=1}^{n} a_{ik}^2.$$

Now, by assumption the ith row of A consists of one entry equal to 1 or -1, and all other entries are 0. Since $\sum_{k=1}^{n} a_{ik}^2$ is simply the sum of squares of the entries in the ith row, we deduce that $\sum_{k=1}^{n} a_{ik}^2 = 1$ and so $(A \cdot {}^tA)_{ij} = 1$ for $i = j$. We conclude that $A \cdot {}^tA = I_n$. The reader will have no problem adapting this argument in order to prove the equality ${}^tA \cdot A = I_n$. □

Remark 1.58. In particular all such matrices are invertible, a fact which is definitely not obvious. Moreover, it is very easy to compute the inverse of such a matrix: simply take its transpose!

Problem 1.59. Prove that any matrix $A \in M_n(\mathbf{C})$ can be expressed in a unique way as $B + C$, where B is symmetric and C is skew-symmetric.

Solution. If $A = B + C$ with B symmetric and C skew-symmetric, then necessarily ${}^tA = B - C$, thus

$$B = \frac{1}{2}(A + {}^tA) \quad \text{and} \quad C = \frac{1}{2}(A - {}^tA).$$

Conversely, choosing B and C as in the previous relation, they are symmetric, respectively skew-symmetric (by the previous proposition) and they add up to A. □

Problem 1.60. The matrix $A = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}$ is the difference of a symmetric matrix B and of a skew-symmetric matrix C. Find B.

Solution. By assumption we have $A = B - C$ with ${}^tB = B$ and ${}^tC = -C$. Thus

$${}^tA = {}^t(B - C) = {}^tB - {}^tC = B + C.$$

We conclude that

$$A + {}^tA = (B - C) + (B + C) = 2B$$

and so

$$B = \frac{1}{2}(A + {}^tA) = \frac{1}{2}\left(\begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}\right)$$
$$= \frac{1}{2}\begin{bmatrix} 2 & 5 \\ 5 & 4 \end{bmatrix} = \begin{bmatrix} 1 & \frac{5}{2} \\ \frac{5}{2} & 2 \end{bmatrix}.$$

□

Problem 1.61. a) Let $A \in M_n(\mathbf{R})$ be a matrix such that ${}^tA \cdot A = O_n$. Prove that $A = O_n$.

b) Does the result in part a) hold if we replace $\mathbf{R}$ with $\mathbf{C}$?

Solution. a) Let $A = [A_{ij}]$. By the product rule for matrices, the (i,i)-entry of ${}^tA \cdot A$ is

$$({}^tA \cdot A)_{ii} = \sum_{k=1}^{n} ({}^tA)_{ik} A_{ki} = \sum_{k=1}^{n} A_{ki}^2.$$

Since ${}^tA \cdot A = O_n$, we conclude that for all $i \in \{1, 2, \ldots, n\}$ we have

$$\sum_{k=1}^{n} A_{ki}^2 = 0.$$

Since the square of a real number is nonnegative, the last equality forces $A_{ki} = 0$ for all $k \in \{1, 2, \ldots, n\}$. Since i was arbitrary, we conclude that $A = 0$.

b) The result does no longer hold. Let us look for a symmetric matrix $A \in M_2(\mathbf{C})$ such that ${}^tA \cdot A = O_2$, that is $A^2 = O_2$. Since A is symmetric, we can write

$$A = \begin{bmatrix} a & b \\ b & d \end{bmatrix}$$

for some complex numbers a, b, d. Now

$$A^2 = \begin{bmatrix} a & b \\ b & d \end{bmatrix} \cdot \begin{bmatrix} a & b \\ b & d \end{bmatrix} = \begin{bmatrix} a^2 + b^2 & b(a+d) \\ b(a+d) & b^2 + d^2 \end{bmatrix}.$$

So we look for complex numbers a, b, d which are not all equal to 0 and for which

$$a^2 + b^2 = 0, \quad b(a+d) = 0, \quad b^2 + d^2 = 0.$$

It suffices to ensure that $a + d = 0$ and $a^2 + b^2 = 0$. For instance, one can take $a = i, b = 1, d = -i$.

□

Remark 1.62. We could have also used Problem 1.52 in order to solve part a). Indeed, for any $X \in \mathbf{R}^n$ we have ${}^tX({}^tA \cdot A)X = 0$ and so

$$\sum_{i=1}^{n}(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n)^2 = 0$$

for any choice of real numbers $x_1, \ldots, x_n$. Since the sum of squares of real numbers equals 0 if and only if all these numbers are equal to 0, we deduce that

$$a_{i1}x_1 + \ldots + a_{in} = 0$$

for all $i \in \{1, 2, \ldots, n\}$ and all real numbers $x_1, \ldots, x_n$. Thus $AX = 0$ for all $X \in \mathbf{R}^n$ and then $A = O_n$.

1.6.1 Problems for Practice

1. Consider the matrices

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

Compute each of the following matrices:

a) $A \cdot {}^tB$.
b) $B \cdot {}^tA$.
c) $(A + 2{}^tB)(B + 2{}^tA)$.

2. Let $\theta \in \mathbf{R}$ and let

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

a) Prove that A is orthogonal.
b) Find all values of θ for which A is symmetric.
c) Find all values of θ for which A is skew-symmetric.

3. Which matrices $A \in M_n(\mathbf{F}_2)$ are the sum of a symmetric matrix and of a skew-symmetric matrix?

4. Write the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{bmatrix}$$

as the sum of a symmetric matrix and of a skew-symmetric matrix with real entries.

5. All matrices in the following statements are square matrices of the same size. Prove that

   a) The product of two symmetric matrices is a symmetric matrix if and only if the two matrices commute.
   b) The product of two antisymmetric matrices is a symmetric matrix if and only if the two matrices commute.
   c) The product of a symmetric and a skew-symmetric matrix is skew-symmetric if and only if the two matrices commute.

6. We have seen that the square of a symmetric matrix $A \in M_n(\mathbf{R})$ is symmetric. Is it true that if the square of a matrix $A \in M_n(\mathbf{R})$ is symmetric, then A is symmetric?

7. Consider the map $\varphi : M_3(\mathbf{R}) \to M_3(\mathbf{R})$ defined by

$$\varphi(A) = {}^tA + 2A.$$

Prove that φ is linear, that is

$$\varphi(cA + B) = c\varphi(A) + \varphi(B)$$

for all $A, B \in M_3(\mathbf{R})$ and all $c \in \mathbf{R}$.

8. Let $A \in M_n(\mathbf{R})$ be a matrix such that $A \cdot {}^tA = O_n$. Prove that $A = O_n$.

9. Find the skew-symmetric matrices $A \in M_n(\mathbf{R})$ such that $A^2 = O_n$.

10. Let $A_1, \ldots, A_k \in M_n(\mathbf{R})$ be matrices such that

$${}^tA_1 \cdot A_1 + \ldots + {}^tA_k \cdot A_k = O_n.$$

Prove that $A_1 = \ldots = A_k = O_n$.

11. a) Let $A \in M_3(\mathbf{R})$ be a skew-symmetric matrix. Prove that there exists a nonzero vector $X \in \mathbf{R}^3$ such that $AX = 0$.
    b) Does the result in part a) remain true if we replace $M_3(\mathbf{R})$ with $M_2(\mathbf{R})$?

12. Describe all upper-triangular matrices $A \in M_n(\mathbf{R})$ such that

$$A \cdot {}^tA = {}^tA \cdot A.$$

Chapter 2
Square Matrices of Order 2

Abstract The main topic of this chapter is a detailed study of 2×2 matrices and their applications, for instance to linear recursive sequences and Pell's equations. The key ingredient is the Cayley–Hamilton theorem, which is systematically used in analyzing the properties of these matrices. Many of these properties will be proved in subsequent chapters by more advanced methods.

Keywords Cayley–Hamilton • Trace • Determinant • Pell's equation • Binomial equation

In this chapter we will study some specific problems involving matrices of order two and to make things even more concrete, we will work exclusively with matrices whose entries are real or complex numbers. The reason for doing this is that in this case one can actually perform explicit computations which might help the reader become more familiar with the material introduced in the previous chapter. Also, many of the results discussed in this chapter in a very special context will later on be generalized (very often with completely different methods and tools!). We should however warn the reader from the very beginning: studying square matrices of order 2 is very far from being trivial, even though it might be tempting to believe the contrary.

A matrix $A \in M_2(\mathbf{C})$ is **scalar** if it is of the form zI_2 for some complex number z. One can define the notion of scalar matrix in full generality: if F is a field and $n \geq 1$, the scalar matrices are precisely the matrices of the form cI_n, where $c \in F$ is a scalar.

2.1 The Trace and the Determinant Maps

We introduce now two fundamental invariants of a 2×2 matrix, which will be generalized and extensively studied in subsequent chapters for $n \times n$ matrices:

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_2

Definition 2.1. Consider a matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in M_2(\mathbf{C})$. We define

- the **trace** of A as

$$\mathrm{Tr}(A) = a_{11} + a_{22}.$$

- the **determinant** of A as

$$\det A = a_{11}a_{22} - a_{12}a_{21}.$$

We also write

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

for the determinant of A.

We obtain in this way two maps

$$\mathrm{Tr}, \det : M_2(\mathbf{C}) \to \mathbf{C}$$

which essentially govern the theory of 2×2 matrices. The following proposition summarizes the main properties of the trace map. The second property is absolutely fundamental. Recall that ${}^tA$ is the transpose of the matrix A.

Proposition 2.2. *For all matrices $A, B \in M_2(\mathbf{C})$ and all complex numbers $z \in \mathbf{C}$ we have*

(a) $\mathrm{Tr}(A + zB) = \mathrm{Tr}(A) + z\mathrm{Tr}(B)$.
(b) $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.
(c) $\mathrm{Tr}({}^tA) = \mathrm{Tr}(A)$.

Proof. Properties (a) and (c) are readily checked, so let us focus on property (b). Write

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}$$

and

$$BA = \begin{bmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22}. \end{bmatrix}.$$

Thus

$$\mathrm{Tr}(AB) = a_{11}b_{11} + a_{22}b_{22} + a_{12}b_{21} + a_{21}b_{12} = \mathrm{Tr}(BA).$$

□

Remark 2.3. The map $\mathrm{Tr} : M_2(\mathbf{C}) \to \mathbf{C}$ is not multiplicative, i.e., generally $\mathrm{Tr}(AB) \neq \mathrm{Tr}(A)\mathrm{Tr}(B)$. For instance $\mathrm{Tr}(I_2 \cdot I_2) = \mathrm{Tr}(I_2) = 2$ and $\mathrm{Tr}(I_2) \cdot \mathrm{Tr}(I_2) = 2 \cdot 2 = 4 \neq 2$.

Let us turn now to properties of the determinant map:

Proposition 2.4. *For all matrices $A, B \in M_2(\mathbf{C})$ and all complex numbers α we have*

(1) $\det(AB) = \det A \cdot \det B$;
(2) $\det {}^tA = \det A$;
(3) $\det(\alpha A) = \alpha^2 \det A$.

Proof. Properties (2) and (3) follow readily from the definition of a determinant. Property (1) will be checked by a painful direct computation. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} x & y \\ z & t \end{bmatrix}.$$

Then

$$AB = \begin{bmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{bmatrix}$$

and so

$$\det(AB) = (ax + bz)(cy + dt) - (cx + dz)(ay + bt) =$$

$$acxy + adxt + bcyz + bdzt - acxy - bcxt - adyz - bdzt =$$

$$xt(ad - bc) - yz(ad - bc) = (ad - bc)(xt - yz) = \det A \cdot \det B,$$

as desired. □

Problem 2.5. Let $A \in M_2(\mathbf{R})$ such that

$$\det(A + 2I_2) = \det(A - I_2).$$

Prove that

$$\det(A + I_2) = \det(A).$$

Solution. Write $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. The condition becomes

$$\begin{vmatrix} a+2 & b \\ c & d+2 \end{vmatrix} = \begin{vmatrix} a-1 & b \\ c & d-1 \end{vmatrix}$$

or equivalently

$$(a+2)(d+2) - bc = (a-1)(d-1) - bc.$$

Expanding and canceling similar terms, we obtain the equivalent relation $a+d=-1$. Using similar arguments, the equality $\det(A + I_2) = \det A$ is equivalent to $(a + 1)(d + 1) - bc = ad - bc$, or $a + d = -1$.The result follows. □

2.1.1 Problems for Practice

1. Compute the trace and the determinant of the following matrices

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} -3 & 6 \\ 2 & -4 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

2. Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. Compute the determinant of A^7.
3. The trace of $A \in M_2(\mathbf{C})$ equals 0. Prove that the trace of A^3 also equals 0.
4. Prove that for all matrices $A \in M_2(\mathbf{C})$ we have

$$\det A = \frac{(\mathrm{Tr}(A))^2 - \mathrm{Tr}(A^2)}{2}.$$

5. Prove that for all matrices $A, B \in M_2(\mathbf{C})$ we have

$$\det(A + B) = \det A + \det B + \mathrm{Tr}(A) \cdot \mathrm{Tr}(B) - \mathrm{Tr}(AB).$$

6. Let $f : M_2(\mathbf{C}) \to \mathbf{C}$ be a map with the property that for all matrices $A, B \in M_2(\mathbf{C})$ and all complex numbers z we have

$$f(A + zB) = f(A) + zf(B) \quad \text{and} \quad f(AB) = f(BA).$$

(a) Consider the matrices

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

and define $x_{ij} = f(E_{ij})$. Check that $E_{12}E_{21} = E_{11}$ and $E_{21}E_{12} = E_{22}$, and deduce that $x_{11} = x_{22}$.

(b) Check that $E_{11}E_{12} = E_{12}$ and $E_{12}E_{11} = O_2$, and deduce that $x_{12} = 0$. Using a similar argument, prove that $x_{21} = 0$.

(c) Conclude that there is a complex number c such that

$$f(A) = c \cdot \mathrm{Tr}(A)$$

for all matrices A.

2.2 The Characteristic Polynomial and the Cayley–Hamilton Theorem

Let $A \in M_2(\mathbf{C})$. The **characteristic polynomial** of A is by definition the polynomial denoted $\det(XI_2 - A)$ and defined by

$$\det(XI_2 - A) = X^2 - \mathrm{Tr}(A)X + \det A.$$

We note straight away that AB and BA have the same characteristic polynomial for all matrices $A, B \in M_2(\mathbf{C})$, since AB and BA have the same trace and the same determinant, by results established in the previous section. In particular, if P is invertible, then A and PAP^{-1} have the same characteristic polynomial.

The notation $\det(XI_2 - A)$ is rather suggestive, and it is indeed coherent, in the sense that for any complex number z, if we evaluate the characteristic polynomial of A at z, we obtain precisely the determinant of the matrix $zI_2 - A$. More generally, we have the following very useful:

Problem 2.6. For any two matrices $A, B \in M_2(\mathbf{C})$ there is a complex number u such that

$$\det(A + zB) = \det A + uz + \det B \cdot z^2$$

for all complex numbers z. If A, B have integer/rational/real entries, then u is integer/rational/real.

Solution. Write $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$. Then

$$\det(A + zB) = \begin{vmatrix} a + z\alpha & b + z\beta \\ c + z\gamma & d + z\delta \end{vmatrix} =$$

$$(a+z\alpha)(d+z\delta)-(b+z\beta)(c+z\gamma) = z^2(\alpha\delta-\beta\gamma)+z(a\delta+d\alpha-\beta c-\gamma b)+ad-bc.$$

Since $\alpha\delta - \beta\gamma = \det B$ and $ad - bc = \det A$, the result follows. □

In other words, for any two matrices $A, B \in M_2(\mathbf{C})$ we can define a quadratic polynomial $\det(A + XB)$ which evaluated at any complex number z gives $\det(A + zB)$. Moreover, $\det(A + XB)$ has constant term $\det A$ and leading term B, and if A, B have rational/integer/real entries, then this polynomial has rational/integer/real coefficients. Before moving on, let us practice some problems to better digest these ideas.

Problem 2.7. Let $U, V \in M_2(\mathbf{R})$. Using the polynomial $\det(U + XV)$, prove that

$$\det(U + V) + \det(U - V) = 2\det U + 2\det V.$$

Solution. Write

$$f(X) = \det(XV + U) = \det V \cdot X^2 + mX + \det U,$$

for some $m \in \mathbf{R}$. Then

$$\det(U + V) + \det(U - V) = f(1) + f(-1) =$$

$$(\det V + m + \det U) + (\det V - m + \det U) = 2(\det U + \det V).$$

□

Problem 2.8. Let $A, B \in M_2(\mathbf{R})$. Using the previous problem, prove that

$$\det(A^2 + B^2) + \det(AB + BA) \geq 0.$$

Solution. As suggested, we use the identity

$$\det(U + V) + \det(U - V) = 2\det U + 2\det V.$$

from Problem 2.7, and take $U = A^2 + B^2$, $V = AB + BA$. Thus

$$\det(A^2 + B^2 + AB + BA) + \det(A^2 + B^2 - AB - BA)$$
$$= 2\det(A^2 + B^2) + 2\det(AB + BA).$$

As $A^2 + B^2 + AB + BA = (A + B)^2$ and $A^2 + B^2 - AB - BA = (A - B)^2$, we obtain

$$2\det(A^2 + B^2) + 2\det(AB + BA) = \det(A + B)^2 + \det(A - B)^2 \geq 0.$$

□

Problem 2.9. Let $A, B \in M_2(\mathbf{R})$. Using the polynomial

$$f(X) = \det(I_2 + AB + x(BA - AB)),$$

prove that

$$\det\left(I_2 + \frac{2AB + 3BA}{5}\right) = \det\left(I_2 + \frac{3AB + 2BA}{5}\right).$$

Solution. As suggested, consider the polynomial of degree at most 2

$$f(X) = \det(I_2 + AB + x(BA - AB)).$$

We need to prove that $f\left(\frac{2}{5}\right) = f\left(\frac{3}{5}\right)$. We claim that $f(X) = f(1 - X)$, which clearly implies the desired result. The polynomial $g(X) = f(X) - f(1 - X)$ has degree at most 1 and satisfies $g(0) = g(1) = 0$. Indeed, we have

$$g(0) = f(0) - f(1) = \det(I_2 + AB) - \det(I_2 + BA) = 0,$$

since AB and BA have the same characteristic polynomial. Also, $g(1) = f(1) - f(0) = 0$. Thus g must be the zero polynomial and the result follows. □

We introduce now another crucial tool in the theory of matrices, which will be vastly generalized in subsequent chapters to $n \times n$ matrices (using completely different ideas and techniques).

Definition 2.10. The *eigenvalues* of a matrix $A \in M_2(\mathbf{C})$ are the roots of its characteristic polynomial, in other words they are the complex solutions λ_1, λ_2 of the equation

$$\det(tI_2 - A) = t^2 - \mathrm{Tr}(A)t + \det A = 0.$$

Note that

$$\lambda_1 + \lambda_2 = \mathrm{Tr}(A) \quad \text{and} \quad \lambda_1\lambda_2 = \det A,$$

i.e., **the trace is the sum of the eigenvalues and the determinant is the product of the eigenvalues**. Indeed, by definition of λ_1 and λ_2 the characteristic polynomial

is $(X-\lambda_1)(X-\lambda_2)$, and identifying the coefficients of X and $X^0=1$ yields the desired relations.

The following result is **absolutely fundamental for the study of square matrices of order 2.**

Theorem 2.11 (Cayley–Hamilton). *For any $A \in M_2(\mathbf{C})$ we have*

$$A^2 - \mathrm{Tr}(A)\cdot A + (\det A)\cdot I_2 = O_2.$$

Proof. Write $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then a direct computation shows that

$$A^2 = \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{bmatrix}.$$

Letting $x = \mathrm{Tr}(A)$, we obtain

$$A^2 - \mathrm{Tr}(A)\cdot A + (\det A)\cdot I_2 = \begin{bmatrix} a^2+bc & bx \\ cx & d^2+bc \end{bmatrix} - \begin{bmatrix} ax & bx \\ cx & dx \end{bmatrix}$$

$$+\begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = \begin{bmatrix} a^2+ad-ax & 0 \\ 0 & d^2+ad-dx \end{bmatrix} = 0,$$

since $a^2+ad-ax=a(a+d-x)=0$ and similarly $d^2+ad-dx=d(a+d-x)=0$. □

Remark 2.12. (a) In other words, the matrix A is a solution of the characteristic equation

$$\det(tI_2 - A) = t^2 - \mathrm{Tr}(A)t + \det A = 0.$$

(b) Expressed in terms of the eigenvalues λ_1 and λ_2 of A, the Cayley–Hamilton theorem can be written either

$$A^2 - (\lambda_1+\lambda_2)A + \lambda_1\lambda_2\cdot I_2 = O_2 \tag{2.1}$$

or equivalently

$$(A-\lambda_1\cdot I_2)(A-\lambda_2\cdot I_2) = O_2. \tag{2.2}$$

Both relations are extremely useful when dealing with square matrices of order 2, and we will see many applications in subsequent sections.

Problem 2.13. Let $A \in M_2(\mathbf{C})$ have eigenvalues λ_1 and λ_2. Prove that for all $n \geq 1$ we have

$$\mathrm{Tr}(A^n) = \lambda_1^n + \lambda_2^n.$$

Deduce that λ_1^n and λ_2^n are the eigenvalues of A^n.

Solution. Let $x_n = \mathrm{Tr}(A^n)$. Multiplying relation (2.1) by A^n and taking the trace yields

$$x_{n+2} - (\lambda_1 + \lambda_2)x_{n+1} + \lambda_1\lambda_2 x_n = 0.$$

Since $x_0 = 2$ and $x_1 = \mathrm{Tr}(A) = \lambda_1 + \lambda_2$, an immediate induction shows that $x_n = \lambda_1^n + \lambda_2^n$ for all n.

For the second part, let z_1, z_2 be the eigenvalues of A^n. By definition, they are the solutions of the equation $t^2 - \mathrm{Tr}(A^n)t + \det(A^n) = 0$. Since $\det(A^n) = (\det A)^n = \lambda_1^n\lambda_2^n$ and $\mathrm{Tr}(A^n) = \lambda_1^n + \lambda_2^n$, the previous equation is equivalent to

$$t^2 - (\lambda_1^n + \lambda_2^n)t + \lambda_1^n\lambda_2^n = 0 \quad \text{or} \quad (t - \lambda_1^n)(t - \lambda_2^n) = 0.$$

The result follows. □

Problem 2.14. Let $A \in M_2(\mathbf{C})$ be a matrix with $\mathrm{Tr}(A) \neq 0$. Prove that a matrix $B \in M_2(\mathbf{C})$ commutes with A if and only if B commutes with A^2.

Solution. Clearly, if $BA = AB$, then $BA^2 = A^2B$, so assume conversely that $BA^2 = A^2B$. Using the Cayley–Hamilton theorem, we can write this relation as

$$B(\mathrm{Tr}(A)A - \det A \cdot I_2) = (\mathrm{Tr}(A)A - \det A \cdot I_2)B$$

or

$$\mathrm{Tr}(A)(BA - AB) = O_2.$$

Since $\mathrm{Tr}(A) \neq 0$, we obtain $BA = AB$, as desired. □

Problem 2.15. Prove that for any matrices $A, B \in M_2(\mathbf{R})$ there is a real number α such that $(AB - BA)^2 = \alpha I_2$.

Solution. Let $X = AB - BA$. Since $\mathrm{Tr}(X) = \mathrm{Tr}(AB) - \mathrm{Tr}(BA) = 0$, the Cayley–Hamilton theorem yields $X^2 = -\det X I_2$ and so we can take $\alpha = -\det X$. □

Problem 2.16. Let $X \in M_2(\mathbf{R})$ be a matrix such that $\det(X^2 + I_2) = 0$. Prove that $X^2 + I_2 = O_2$.

Solution. We have $\det(X + iI_2) = 0$ or $\det(X - iI_2) = 0$, and since $\det(X - iI_2) = \overline{\det(X + iI_2)}$, we deduce that $\det(X + iI_2) = 0 = \det(X - iI_2)$. If $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$,

the relation $\det(X + iI_2) = 0$ is equivalent to $(a + i)(d + i) - bc = 0$, i.e., $ad - bc = 1$ and $a + d = 0$. Thus $\det X = 1$ and $Tr(X) = 0$ and we conclude using the Cayley–Hamilton theorem. □

An important consequence of the Cayley–Hamilton theorem is the following result (which can of course be proved directly by hand).

Theorem 2.17. *A matrix $A \in M_2(\mathbf{C})$ is invertible if and only if* $\det A \neq 0$. *If this is the case, then*

$$A^{-1} = \frac{1}{\det A}(\mathrm{Tr}(A) \cdot I_2 - A).$$

Proof. Suppose that A is invertible. Then taking the determinant in the equality $A \cdot A^{-1} = I_2$ we obtain

$$\det A \cdot \det A^{-1} = \det I_2 = 1,$$

thus $\det A \neq 0$.

Conversely, suppose that $\det A \neq 0$ and define

$$B = \frac{1}{\det A}(\mathrm{Tr}(A) \cdot I_2 - A).$$

Then using the Cayley–Hamilton theorem we obtain

$$AB = \frac{1}{\det A}(\mathrm{Tr}(A) \cdot A - A^2) = \frac{1}{\det A} \cdot \det A I_2 = I_2$$

and similarly $BA = I_2$. Thus A is invertible and $A^{-1} = B$. □

Remark 2.18. One can also check directly that if $\det A \neq 0$, then A is invertible, its inverse being given by

$$A^{-1} = \frac{1}{\det A}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}.$$

Problem 2.19. Let $A, B \in M_2(\mathbf{C})$ be two matrices such that $AB = I_2$. Then A is invertible and $B = A^{-1}$. In particular, we have $BA = I_2$.

Solution. Since $AB = I_2$, we have $\det A \cdot \det B = \det(AB) = 1$, thus $\det A \neq 0$. The previous theorem shows that A is invertible. Multiplying the equality $AB = I_2$ by A^{-1} on the left, we obtain $B = A^{-1}$. Finally, $BA = A^{-1}A = I_2$. □

A very important consequence of the previous theorem is the following characterization of eigenvalues:

Theorem 2.20. *If $A \in M_2(\mathbf{C})$ and $z \in \mathbf{C}$, then the following assertions are equivalent:*

(a) z is an eigenvalue of A;
(b) $\det(zI_2 - A) = 0$.
(c) There is a nonzero vector $v \in \mathbf{C}^2$ such that $Av = zv$.

Proof. By definition of eigenvalues, (a) implies (b). Suppose that (b) holds and let $B = A - zI_2$. The assumption implies that $\det B = 0$ and so $b_{11}b_{22} = b_{12}b_{21}$. We need to prove that we can find $x_1, x_2 \in \mathbf{C}$ not both zero and such that

$$b_{11}x_1 + b_{12}x_2 = 0 \quad \text{and} \quad b_{21}x_1 + b_{22}x_2 = 0.$$

If $b_{11} \neq 0$ or $b_{12} \neq 0$, choose $x_2 = b_{11}$ and $x_1 = -b_{12}$, so suppose that $b_{11} = 0 = b_{12}$. If one of b_{21}, b_{22} is nonzero, choose $x_1 = -b_{22}$ and $x_2 = b_{21}$, otherwise choose $x_1 = x_2 = 1$. Thus (b) implies (c).

Suppose now that (c) holds. Then $A^2v = zAv = z^2v$ and using relation (2.1) we obtain

$$(z^2 - \operatorname{Tr}(A)z + \det A)v = 0.$$

Since $v \neq 0$, this forces $z^2 - \operatorname{Tr}(A)z + \det A = 0$ and so z is an eigenvalue of A. Thus (c) implies (a) and the theorem is proved. □

Problem 2.21. Let $A \in M_2(\mathbf{C})$ have two distinct eigenvalues λ_1, λ_2. Prove that we can find an invertible matrix $P \in \mathrm{GL}_2(\mathbf{C})$ such that

$$A = P \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} P^{-1}.$$

Solution. By the previous theorem, we can find two nonzero vectors $X_1 = \begin{bmatrix} x_{11} \\ x_{21} \end{bmatrix}$ and $X_2 = \begin{bmatrix} x_{12} \\ x_{22} \end{bmatrix}$ such that $AX_i = \lambda_i X_i$.

Consider the matrix $P = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ whose columns are X_1, X_2. A simple computation shows that the columns of AP are $\lambda_1 X_1$ and $\lambda_2 X_2$, which are the columns of $P \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$, thus $AP = P \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$. It remains to see that if $\lambda_1 \neq \lambda_2$, then P is invertible (we haven't used so far the hypothesis $\lambda_1 \neq \lambda_2$).

Suppose that $\det P = 0$, thus $x_{11}x_{22} = x_{21}x_{12}$. This easily implies that the columns of P are proportional, say the second column X_2 is α times the first column, X_1. Thus $X_2 = \alpha X_1$. Then

$$\lambda_2 X_2 = AX_2 = \alpha AX_1 = \alpha\lambda_1 X_1 = \lambda_1 X_2,$$

forcing $(\lambda_1 - \lambda_2)X_2 = 0$. This is impossible as both $\lambda_1 - \lambda_2$ and X_2 are nonzero. The problem is solved. □

Problem 2.22. Solve in $M_2(\mathbf{C})$ the following equations

(a) $A^2 = O_2$.
(b) $A^2 = I_2$.
(c) $A^2 = A$.

Solution. (a) Let A be a solution of the problem. Then $\det A = 0$ and the Cayley–Hamilton relation reduces to $\mathrm{Tr}(A)A = 0$. Taking the trace yields $\mathrm{Tr}(A)^2 = 0$, thus $\mathrm{Tr}(A) = 0$. Conversely, if $\det A = 0$ and $\mathrm{Tr}(A) = 0$, then the Cayley–Hamilton theorem shows that $A^2 = O_2$. Thus the solutions of the problem are the matrices

$$A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}, \quad \text{with} \quad a, b, c \in \mathbf{C} \quad \text{and} \quad a^2 + bc = 0.$$

(b) We must have $\det A = \pm 1$ and, by the Cayley–Hamilton theorem, $I_2 - \mathrm{Tr}(A)A + \det A I_2 = O_2$. If $\det A = 1$, then $\mathrm{Tr}(A)A = 2I_2$ and taking the trace yields $\mathrm{Tr}(A)^2 = 4$, thus $\mathrm{Tr}(A) = \pm 2$. This yields two solutions, $A = \pm I_2$. Suppose that $\det A = -1$. Then $\mathrm{Tr}(A)A = O_2$ and taking the trace gives $\mathrm{Tr}(A) = 0$. Conversely, any matrix A with $\mathrm{Tr}(A) = 0$ and $\det A = -1$ is a solution of the problem (again by Cayley–Hamilton). Thus the solutions of the equation are

$$\pm I_2 \quad \text{and} \quad A = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}, \quad a, b, c \in \mathbf{C}, \quad a^2 + bc = 1.$$

(c) If $\det A \neq 0$, then multiplying by A^{-1} yields $A = I_2$. So suppose that $\det A = 0$. The Cayley–Hamilton theorem yields $A - \mathrm{Tr}(A)A = O_2$. If $\mathrm{Tr}(A) \neq 1$, this forces $A = O_2$, which is a solution of the problem. Thus if $A \neq O_2, I_2$, then $\det A = 0$ and $\mathrm{Tr}(A) = 1$. Conversely, all such matrices are solutions of the problem (again by Cayley–Hamilton). Thus the solutions of the problem are

$$O_2, \quad I_2 \quad \text{and} \quad A = \begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}, \quad a, b, c \in \mathbf{C}, \quad a^2 + bc = a.$$

□

Problem 2.23. Let $A \in M_2(\mathbf{C})$ be a matrix. Prove that the following statements are equivalent:

(a) $\mathrm{Tr}(A) = \det A = 0$.
(b) $A^2 = O_2$.
(c) $\mathrm{Tr}(A) = \mathrm{Tr}(A^2) = 0$.
(d) There exists $n \geq 2$ such that $A^n = O_2$.

Solution. Taking the trace of the Cayley–Hamilton theorem, we see that $\mathrm{Tr}(A^2) = \mathrm{Tr}(A)^2 - 2\det A$. From this it is clear that (a) and (c) are equivalent.

The implication (a) implies (b) is just an application of the Cayley–Hamilton theorem. The implication (b) implies (d) is obvious. Thus we need only show (d) implies (a). If $A^n = O_2$ for some $n \geq 2$, then clearly $\det A = 0$. Thus the Cayley–Hamilton theorem reads $A^2 = \mathrm{Tr}(A)A$. Iterating this an immediate induction gives $A^n = \mathrm{Tr}(A)^{n-1}A$, hence $O_2 = \mathrm{Tr}(A)^{n-1}A$. Taking the trace of this identity gives $0 = \mathrm{Tr}(A)^n$ and hence $\mathrm{Tr}(A) = 0$. □

Problem 2.24. Find all matrices $X \in M_2(\mathbf{R})$ such that $X^3 = I_2$.

Solution. We must have $(\det X)^3 = 1$ and so $\det X = 1$ (since $\det X \in \mathbf{R}$). Letting $t = \mathrm{Tr}(X)$, the Cayley–Hamilton theorem and the given equation yield

$$I_2 = X^3 = X(tX - I_2) = t(tX - I_2) - X = (t^2 - 1)X - tI_2.$$

If $t^2 \neq 1$, then the previous relation shows that X is scalar and since $X^3 = I_2$, we must have $X = I_2$. If $t^2 = 1$, then the previous relation gives $t = -1$. Conversely, any matrix $X \in M_2(\mathbf{R})$ with $\mathrm{Tr}(X) = -1$ and $\det X = 1$ satisfies $X^2 + X + I_2 = O_2$ and so also $X^3 = I_2$. We conclude that the solutions of the problem are

$$I_2 \quad \text{and} \quad \begin{bmatrix} a & b \\ c & -1-a \end{bmatrix}, \quad a, b, c \in \mathbf{R}, \quad a^2 + a + bc = -1.$$

□

2.2.1 Problems for Practice

1. Let $A, B \in M_2(\mathbf{R})$ be commuting matrices. Prove that

$$\det(A^2 + B^2) \geq 0.$$

   Hint: check that $A^2 + B^2 = (A + iB)(A - iB)$.
2. Let $A, B \in M_2(\mathbf{R})$ be such that $AB = BA$ and $\det(A^2 + B^2) = 0$. Prove that $\det A = \det B$. Hint: use the hint of the previous problem and consider the polynomial $\det(A + XB)$.
3. Let $A, B, C \in M_2(\mathbf{R})$ be pairwise commuting matrices and let

$$f(X) = \det(A^2 + B^2 + C^2 + x(AB + BA + CA)).$$

   (a) Prove that $f(2) \geq 0$. Hint: check that

$$A^2 + B^2 + C^2 + 2(AB + BA + CA) = (A + B + C)^2.$$

(b) Prove that $f(-1) \geq 0$. Hint: denote $X = A - B$ and $Y = B - C$ and check that

$$A^2 + B^2 + C^2 - (AB + BC + CA) = \left(X + \frac{1}{2}Y\right)^2 + \left(\frac{\sqrt{3}}{2}Y\right)^2.$$

Next use the first problem.

(c) Deduce that

$$\det(A^2 + B^2 + C^2) + 2\det(AB + BC + CA) \geq 0.$$

4. Let $A, B \in M_2(\mathbf{C})$ be matrices with $\mathrm{Tr}(AB) = 0$. Prove that $(AB)^2 = (BA)^2$. Hint: use the Cayley–Hamilton theorem.
5. Let A be a 2×2 matrix with rational entries with the property that

$$\det(A^2 - 2I_2) = 0.$$

Prove that $A^2 = 2I_2$ and $\det A = -2$. Hint: use the fact that $A^2 - 2I_2 = (A - \sqrt{2}I_2)(A + \sqrt{2}I_2)$ and consider the characteristic polynomial of A.
6. Let x be a positive real number and let $A \in M_2(\mathbf{R})$ be a matrix such that $\det(A^2 + xI_2) = 0$. Prove that

$$\det(A^2 + A + xI_2) = x.$$

7. Let $A, B \in M_2(\mathbf{R})$ be such that $\det(AB - BA) \leq 0$. Consider the polynomial

$$f(X) = \det(I_2 + (1 - X)AB + XBA).$$

(a) Prove that $f(0) = f(1)$.

(b) Deduce that

$$\det(I_2 + AB) \leq \det\left(I_2 + \frac{1}{2}(AB + BA)\right).$$

8. Let $n \geq 3$ be an integer. Let $X \in M_2(\mathbf{R})$ be such that

$$X^n + X^{n-2} = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

(a) Prove that $\det X = 0$. Hint: show that $\det(X^2 + I_2) = 0$.

(b) Let t be the trace of X. Prove that

$$t^n + t^{n-2} = 2.$$

(c) Find all possible matrices X satisfying the original equation.

9. Let $n \geq 2$ be a positive integer and let $A, B \in M_2(\mathbf{C})$ be two matrices such that $AB \neq BA$ and $(AB)^n = (BA)^n$. Prove that $(AB)^n = \alpha I_2$ for some complex number α.
10. Let $A, B \in M_2(\mathbf{R})$ and let $n \geq 1$ be an integer such that $C^n = I_2$, where $C = AB - BA$. Prove that n is even and $C^4 = I_2$. Hint: use Problem 2.15.

2.3 The Powers of a Square Matrix of Order 2

In this section we will use the Cayley–Hamilton theorem to compute the powers of a given matrix $A \in M_2(\mathbf{C})$. Let λ_1 and λ_2 be the eigenvalues of A. The discussion and the final result will be very different according to whether λ_1 and λ_2 are different or not.

Let us start with the case $\lambda_1 = \lambda_2$ and consider the matrix $B = A - \lambda_1 I_2$. Then the Cayley–Hamilton theorem in the form of relation (2.2) yields $B^2 = O_2$, thus $B^k = O_2$ for $k \geq 2$. Using the binomial formula we obtain

$$A^n = (B + \lambda_1 I_2)^n = \sum_{k=0}^{n} \binom{n}{k} \lambda_1^{n-k} B^k = \lambda_1^n I_2 + n\lambda_1^{n-1} B.$$

Let us assume now that $\lambda_1 \neq \lambda_2$ and consider the matrices

$$B = A - \lambda_1 I_2 \quad \text{and} \quad C = A - \lambda_2 I_2.$$

Relation (2.2) becomes $BC = O_2$, or equivalently $B(A - \lambda_2 I_2) = O_2$. Thus $BA = \lambda_2 B$, which yields $BA^2 = \lambda_2 BA = \lambda_2^2 B$ and by an immediate induction $BA^n = \lambda_2^n B$ for all n. Similarly, the relation $BC = O_2$ yields $CA^n = \lambda_1^n C$ for all n. Taking advantage of the relation $C - B = (\lambda_1 - \lambda_2) I_2$, we obtain

$$(\lambda_1 - \lambda_2) A^n = (C - B) A^n = CA^n - BA^n = \lambda_1^n C - \lambda_2^n B.$$

Thus

$$A^n = \frac{1}{\lambda_1 - \lambda_2} (\lambda_1^n C - \lambda_2^n B).$$

All in all, we proved the following useful result, in which we change notations:

Theorem 2.25. *Let $A \in M_2(\mathbf{C})$ and let λ_1, λ_2 be its eigenvalues.*

(a) If $\lambda_1 \neq \lambda_2$, then for all $n \geq 1$ we have $A^n = \lambda_1^n B + \lambda_2^n C$, where

$$B = \frac{1}{\lambda_1 - \lambda_2}(A - \lambda_2 I_2) \text{ and } C = \frac{1}{\lambda_2 - \lambda_1}(A - \lambda_1 I_2).$$

(b) If $\lambda_1 = \lambda_2$, then for all $n \geq 1$ we have $A^n = \lambda_1^n B + n\lambda_1^{n-1} C$, where $B = I_2$ and $C = A - \lambda_1 I_2$.

Problem 2.26. Compute A^n, where $A = \begin{bmatrix} 1 & 3 \\ -3 & -5 \end{bmatrix}$.

Solution. As $\mathrm{Tr}(A) = -4$ and $\det A = 4$, the eigenvalues of A are solutions of the equation $t^2 + 4t + 4 = 0$, thus $\lambda_1 = \lambda_2 = -2$ are the eigenvalues of A. Using the previous theorem, we conclude that for any $n \geq 1$ we have

$$A^n = (-2)^n I_2 + n(-2)^{n-1}(A + 2I_2) = (-2)^{n-1} \begin{bmatrix} 3n - 2 & 3n \\ -3n & -3n - 2 \end{bmatrix}.$$

□

Though the exact statement of the previous theorem is a little cumbersome, the basic idea is very simple. If one learns this idea, then one can compute A^n easily. Keep in mind that when computing powers of a 2×2 matrix, one starts by computing the eigenvalues of the matrix (this comes down to solving the quadratic equation $t^2 - \mathrm{Tr}(A)t + \det A = 0$). If the eigenvalues are equal, say both equal to λ, then $B := A - \lambda I_2$ satisfies $B^2 = O_2$ and so one computes A^n by writing $A = B + \lambda I_2$ and using the binomial formula. On the other hand, if the eigenvalues are different, say λ_1 and λ_2, then there are two matrices B, C such that for all n we have

$$A^n = \lambda_1^n B + \lambda_2^n C.$$

One can easily find these matrices without having to learn the formulae by heart: if the previous relation holds for all $n \geq 0$, then it certainly holds for $n = 0$ and $n = 1$. Thus

$$I_2 = B + C, \quad A = \lambda_1 B + \lambda_2 C.$$

This immediately yields the matrices B and C in terms of I_2, A and λ_1, λ_2. Moreover, we see that they are of the form $xI_2 + yA$ for some complex numbers x, y. Combining this observation with Theorem 2.25 yields the following useful

Corollary 2.27. *For any matrix $A \in M_2(\mathbf{C})$ there are sequences $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$ of complex numbers such that*

$$A^n = x_n A + y_n I_2$$

for all $n \geq 0$.

One has to be careful that the sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ in the previous corollary are definitely not always characterized by the equality $A^n = x_n A + y_n I_2$ (this is however the case if A is not scalar). On the other hand, Theorem 2.25 shows that we can take

$$x_n = \frac{\lambda_1^n - \lambda_2^n}{\lambda_1 - \lambda_2} \text{ and } y_n = \frac{\lambda_1\lambda_2^n - \lambda_2\lambda_1^n}{\lambda_1 - \lambda_2}$$

when $\lambda_1 \neq \lambda_2$, and, when $\lambda_1 = \lambda_2$

$$x_n = n\lambda_1^{n-1} \text{ and } y_n = -(n-1)\lambda_1^n.$$

Problem 2.28. Let m, n be positive integers and let $A, B \in M_2(\mathbf{C})$ be two matrices such that $A^m B^n = B^n A^m$. If A^m and B^n are not scalar, prove that $AB = BA$.

Solution. From Corollary 2.27 we have

$$A^k = x_k A + y_k I_2 \text{ and } B^k = u_k B + v_k I_2, \quad k \geq 0,$$

where $(x_k)_{k\geq 0}$, $(y_k)_{k\geq 0}$, $(u_k)_{k\geq 0}$, $(v_k)_{k\geq 0}$ are sequences of complex numbers. Since A^m and B^n are not scalar matrices it follows that $x_m \neq 0$ and $u_n \neq 0$. The relation $A^m B^n = B^n A^m$ is equivalent to

$$(x_m A + y_m I_2)(u_n B + v_n I_2) = (u_n B + v_n I_2)(x_m A + y_m I_2)$$

i.e.

$$x_m u_n (AB - BA) = O_2.$$

Hence $AB = BA$. □

Problem 2.29. Let $t \in \mathbf{R}$ and let

$$A_t = \begin{bmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{bmatrix}.$$

Compute A_t^n for $n \geq 1$.

Solution. We offer three ways to solve this problem. The first is to follow the usual procedure: compute the eigenvalues of A_t and then use the general Theorem 2.25. Here the eigenvalues are e^{it} and e^{-it} and it is not difficult to deduce that

$$A_t^n = \begin{bmatrix} \cos nt & -\sin nt \\ \sin nt & \cos nt \end{bmatrix}.$$

Another argument is as follows: an explicit computation shows that $A_{t_1+t_2} = A_{t_1}A_{t_2}$, thus

$$A_t^n = A_t \cdot A_t \cdot \ldots \cdot A_t = A_{t+t+\ldots+t} = A_{nt}.$$

Finally, one can also argue geometrically: A_t is the matrix of a rotation of angle t, thus A_t^n is the matrix of a rotation of angle nt. □

2.3.1 *Problems for Practice*

1. Consider the matrix

$$A = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}.$$

   (a) Let n be a positive integer. Prove the existence of a unique pair of integers (x_n, y_n) such that

$$A^n = x_n A + y_n I_2.$$

   (b) Compute $\lim_{n\to\infty} \frac{x_n}{y_n}$.

2. Given a positive integer n, compute the nth power of the matrix

$$A = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}.$$

3. Let a, b be real numbers and let n be a positive integer. Compute the nth power of the matrix $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$.
4. Let x be a real number and let

$$A = \begin{bmatrix} \cos x + \sin x & 2\sin x \\ -\sin x & \cos x - \sin x \end{bmatrix}.$$

   Compute A^n for all positive integers n.

2.4 Application to Linear Recurrences

In this section we present two classical applications of the theory developed in the previous section. Let a, b, c, d, x_0, y_0 be complex numbers and consider two sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ recursively defined by

$$\begin{cases} x_{n+1} = ax_n + by_n \\ y_{n+1} = cx_n + dy_n, \quad n \geq 0 \end{cases} \tag{2.3}$$

We would like to find the general terms of the two sequences in terms of the initial data a, b, c, d, x_0, y_0 and n.

The key observation is that the system can be written in matrix form as follows

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \text{ i.e. } \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix}, \quad n \geq 0,$$

where $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the matrix of coefficients. An immediate induction yields

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}, \quad n \geq 0, \tag{2.4}$$

and so the problem is reduced to the computation of A^n, which is solved by Theorem 2.25.

Let us consider a slightly different problem, also very classical. It concerns second order linear recurrences with constant coefficients. More precisely, we fix complex numbers a, b, x_0, x_1 and look for the general term of the sequence $(x_n)_{n\geq 0}$ defined recursively by

$$x_{n+1} = ax_n + bx_{n-1}, \quad n \geq 1, \tag{2.5}$$

We can easily reduce this problem to the previous one by denoting $y_n = x_{n-1}$ for $n \geq 1$ and $y_0 = \dfrac{1}{b}(x_1 - ax_0)$ if $b \neq 0$ (which we will assume from now on, since otherwise the problem is very simple from the very beginning). Indeed, relation (2.5) is equivalent to the following system

$$\begin{cases} x_{n+1} = ax_n + by_n \\ y_{n+1} = x_n \end{cases}, \quad n \geq 0.$$

As we have already seen, finding x_n and y_n (or equivalently x_n) comes down to computing the powers of the matrix of coefficients

$$A = \begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix}.$$

The characteristic equation of this matrix is $\lambda^2 - a\lambda - b = 0$. If λ_1 and λ_2 are the roots of this equation, then Theorem 2.25 yields the following:

• If $\lambda_1 \neq \lambda_2$, then we can find constants u, v such that

$$x_n = u\lambda_1^n + v\lambda_2^n$$

for all n. These two constants are easily determined by imposing

$$x_0 = u + v \quad \text{and} \quad x_1 = u\lambda_1 + v\lambda_2$$

and solving this linear system in the unknowns u, v.

• If $\lambda_1 = \lambda_2$, then we can find constants u, v such that for all $n \geq 0$

$$x_n = (un + v)\lambda_1^n,$$

and u and v are found from the initial conditions by solving $x_0 = v$ and $x_1 = (u + v)\lambda_1$.

Problem 2.30. Find the general terms of $(x_n)_{n\geq 0}$, $(y_n)_{n\geq 0}$ if

$$\begin{cases} x_{n+1} = x_n + 2y_n \\ y_{n+1} = -2x_n + 5y_n, \quad n \geq 0, \end{cases}$$

and $x_0 = 1$, $y_0 = 2$.

Solution. The matrix of coefficients is $A = \begin{bmatrix} 1 & 2 \\ -2 & 5 \end{bmatrix}$, with characteristic equation $\lambda^2 - 6\lambda + 9 = 0$ and solutions $\lambda_1 = \lambda_2 = 3$. Theorem 2.25 yields (after a simple computation)

$$A^n = 3^n I_2 + n3^{n-1}\begin{bmatrix} -2 & 2 \\ -2 & 2 \end{bmatrix} = \begin{bmatrix} (3-2n)3^{n-1} & 2n3^{n-1} \\ -2n3^{n-1} & (3+2n)3^{n-1} \end{bmatrix}$$

Combined with $x_0 = 1$ and $y_0 = 2$, we obtain

$$x_n = (2n + 3)3^{n-1} \text{ and } y_n = 2(n + 3)3^{n-1}, \quad n \geq 0.$$

□

Problem 2.31. Find the limits of sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$, where

$$\begin{cases} x_{n+1} = (1-\alpha)x_n + \alpha y_n \\ y_{n+1} = \beta x_n + (1-\beta)y_n, \end{cases}$$

and α, β are complex numbers with $|1 - \alpha - \beta| < 1$.

Solution. The matrix of coefficients is

$$A = \begin{bmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{bmatrix}$$

and one easily checks that its eigenvalues are $\lambda_1 = 1$ and $\lambda_2 = 1-\alpha-\beta$. Note that $|\lambda_2| < 1$, in particular $\lambda_2 \neq 1$. Letting

$$B = \frac{1}{\lambda_1 - \lambda_2}(A - \lambda_2 I_2) = \frac{1}{\alpha+\beta}\begin{bmatrix} \beta & \alpha \\ \beta & \alpha \end{bmatrix},$$

Theorem 2.25 gives the existence of an explicit matrix C such that

$$A^n = \lambda_1^n B + \lambda_2^n C = B + \lambda_2^n C.$$

Since $|\lambda_2| < 1$, we have $\lim_{n\to\infty} \lambda_2^n = 0$ and the previous relation shows that $\lim_{n\to\infty} A^n = B$.

Since $\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$, we conclude that x_n and y_n are convergent sequences, and if l_1, l_2 are their limits, then

$$\begin{bmatrix} l_1 \\ l_2 \end{bmatrix} = B \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}.$$

Taking into account the explicit form of B, we obtain

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n = \frac{\beta x_0 + \alpha y_0}{\alpha+\beta}.$$

□

2.4.1 *Problems for Practice*

1. Find the general term of the sequence $(x_n)_{n\geq 0}$ defined by $x_1 = 1$, $x_2 = 0$ and for all $n \geq 1$

$$x_{n+2} = 4x_{n+1} - x_n.$$

2. Consider the sequence $(x_n)_{n\geq 0}$ defined by $x_0 = 1$, $x_1 = 2$ and for all $n \geq 0$

$$x_{n+2} = x_{n+1} - x_n.$$

Is this sequence periodical? If so, find its minimal period.

3. Find the general terms of the sequences $(x_n)_{n\geq 0}$ and $(y_n)_{n\geq 0}$ satisfying $x_0 = y_0 = 1$, $x_1 = 1$, $y_1 = 2$ and

$$x_{n+1} = \frac{2x_n + 3y_n}{5}, \quad y_{n+1} = \frac{2y_n + 3x_n}{5}.$$

4. A sequence $(x_n)_{n\geq 0}$ satisfies $x_0 = 2$, $x_1 = 3$ and for all $n \geq 1$

$$x_{n+1} = \sqrt{x_{n-1}x_n}.$$

Find the general term of this sequence (hint: take the logarithm of the recurrence relation).

5. Consider a map $f : (0, \infty) \to (0, \infty)$ such that

$$f(f(x)) = 6x - f(x)$$

for all $x > 0$. Let $x > 0$ and define a sequence $(z_n)_{n\geq 0}$ by $z_0 = x$ and $z_{n+1} = f(z_n)$ for $n \geq 0$.

(a) Prove that

$$z_{n+2} + z_{n+1} - 6z_n = 0$$

for $n \geq 0$.

(b) Deduce the existence of real numbers a, b such that

$$z_n = a \cdot 2^n + b \cdot (-3)^n$$

for all $n \geq 0$.

(c) Using the fact that $z_n > 0$ for all n, prove that $b = 0$ and conclude that $f(x) = 2x$ for all $x > 0$.

2.5 Solving the Equation $X^n = A$

Consider a matrix $A \in M_2(\mathbf{C})$ and an integer $n > 1$. In this section we will explain how to solve the equation $X^n = A$, with $X \in M_2(\mathbf{C})$.

A first key observation is that for any solution X of the equation we have

$$AX = XA.$$

Indeed, this is simply a consequence of the fact that $X^n \cdot X = X \cdot X^n$. We will need the following very useful:

Proposition 2.32. *Let $A \in M_2(\mathbf{C})$ be a non-scalar matrix. If $X \in M_2(\mathbf{C})$ commutes with A, then $X = \alpha I_2 + \beta A$ for some complex numbers α, β.*

Proof. Write $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $X = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$. The equality $AX = XA$ is equivalent, after an elementary computation, to

$$bz = cy, \quad ay + bt = bx + dy, \quad cx + dz = az + ct,$$

or

$$bz = cy, \quad (a-d)y = b(x-t), \quad c(x-t) = z(a-d).$$

If $a \neq d$, set $\beta = \frac{x-t}{a-d}$. Then $z = c\beta$, $y = b\beta$ and $\beta a - x = \beta d - t$. We deduce that $X = \alpha I_2 + \beta A$, where $\alpha = -\beta a + x = -\beta d + t$.

Suppose that $a = d$. If $x \neq t$, the previous relations yield $b = c = 0$ and so A is scalar, a contradiction. Thus $x = t$ and $bz = cy$. Moreover, one of b, c is nonzero (as A is not scalar), say b (the argument when $c \neq 0$ is identical). Setting $\beta = \frac{y}{b}$ and $\alpha = x - \beta a$ yields $X = \alpha I_2 + \beta A$.

□

Let us come back to our original problem, solving the equation $X^n = A$. Let λ_1 and λ_2 be the eigenvalues of A. We will discuss several cases, each of them having a very different behavior.

Let us start with the case $\lambda_1 \neq \lambda_2$. By Problem 2.21, we can then write $A = P \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} P^{-1}$ for some $P \in \mathrm{GL}_2(\mathbf{C})$. Since $AX = XA$ and A is not scalar, by Proposition 2.32 there are complex numbers a, b such that $X = aI_2 + bA$. Thus

$$X = P \begin{bmatrix} a + b\lambda_1 & 0 \\ 0 & a + b\lambda_2 \end{bmatrix} P^{-1}.$$

The equation $X^n = A$ is then equivalent to

$$\begin{bmatrix} (a + b\lambda_1)^n & 0 \\ 0 & (a + b\lambda_2)^n \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

It follows that $a + b\lambda_1 = z_1$ and $a + b\lambda_2 = z_2$, where $z_1^n = \lambda_1$ and $z_2^n = \lambda_2$, and $X = P \begin{bmatrix} z_1 & 0 \\ 0 & z_2 \end{bmatrix} P^{-1}$. Hence

Proposition 2.33. *Let $A \in M_2(\mathbf{C})$ be a matrix with distinct eigenvalues λ_1, λ_2. Let $P \in \mathrm{GL}_2(\mathbf{C})$ be a matrix such that $A = P \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} P^{-1}$. Then the solutions of the*

equation $X^n = A$ *are given by* $X = P \begin{bmatrix} z_1 & 0 \\ 0 & z_2 \end{bmatrix} P^{-1}$, *where* z_1 *and* z_2 *are solutions of the equations* $t^n = \lambda_1$ *and* $t^n = \lambda_2$ *respectively.*

Let us deal now with the case in which A is not scalar, but has equal eigenvalues, say both eigenvalues equal λ. Then the matrix $B = A - \lambda I_2$ satisfies $B^2 = O_2$ (by the Cayley–Hamilton theorem) and we have $A = B + \lambda I_2$. Now, since $AX = XA$ and A is not scalar, we can write $X = cI_2 + dA$ for some complex numbers c, d (Proposition 2.32). Since $A = B + \lambda I_2$, it follows that we can also write $X = aI_2 + bB$ for some complex numbers a, b. Since $B^2 = O_2$, the binomial formula and the given equation yield

$$A = X^n = (aI_2 + bB)^n = a^n I_2 + na^{n-1}bB.$$

Since $A = B + \lambda I_2$, we obtain

$$B + \lambda I_2 = na^{n-1}bB + a^n I_2.$$

Since B is not scalar (as A itself is not scalar), the previous relation is equivalent to

$$1 = na^{n-1}b \quad \text{and} \quad \lambda = a^n.$$

This already shows that $\lambda \neq 0$ (as the first equation shows that $a \neq 0$), so if $\lambda = 0$ (which corresponds to $A^2 = O_2$) then the equation has no solution. On the other hand, if $\lambda \neq 0$, then the equation $a^n = \lambda$ has n complex solutions, and for each of them we obtain a unique value of b, namely $b = \frac{1}{na^{n-1}}$. We have just proved the following

Proposition 2.34. *Suppose that* $A \in M_2(\mathbf{C})$ *is not scalar, but both eigenvalues of* A *are equal to some complex number* λ. *Then*

(a) If $\lambda = 0$, *the equation* $X^n = A$ *has no solutions for* $n > 1$, *and the only solution* $X = A$ *for* $n = 1$.
(b) If $\lambda \neq 0$, *then the solutions of the equation* $X^n = A$ *are given by*

$$X = aI_2 + \frac{1}{na^{n-1}}(A - \lambda I_2),$$

where a *runs over the* n *solutions of the equation* $z^n = \lambda$.

Finally, let us deal with the case when A is scalar, say $A = cI_2$ for some complex number c. If $c = 0$, then $X^n = O_2$ has already been solved, so let us assume that $c \neq 0$. Consider a solution X of the equation $X^n = cI_2$ and let λ_1, λ_2 be the eigenvalues of X. Then $\lambda_1^n = \lambda_2^n = c$. We have two possibilities:

- Either $\lambda_1 \neq \lambda_2$, in which case X has distinct eigenvalues and so (Problem 2.21) we can write $X = P\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}P^{-1}$ for some invertible matrix P. Then $X^n = P\begin{bmatrix}\lambda_1^n & 0\\ 0 & \lambda_2^n\end{bmatrix}P^{-1}$ and this equals cI_2 since $\lambda_1^n = \lambda_2^n = c$. The conclusion is that for each pair (λ_1, λ_2) of **distinct** solutions of the equation $t^n = c$ we obtain a whole family of solutions, namely the matrices $X = P\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}P^{-1}$ for some invertible matrix P.
- Suppose that $\lambda_1 = \lambda_2$ and let $Y = X - \lambda_1 I_2$, then $Y^2 = O_2$ and the equation $X^n = cI_2$ is equivalent to $(Y + \lambda_1 I_2)^n = cI_2$. Using again the binomial formula and the equality $Y^2 = O_2$, we can rewrite this equation as

$$\lambda_1^n I_2 + n\lambda_1^{n-1} Y = cI_2.$$

Since $\lambda_1^n = c$ and $\lambda_1 \neq 0$ (as $c \neq 0$), we deduce that necessarily $Y = O_2$ and so $X = \lambda_1 I_2$, with λ_1 one of the n complex solutions of the equation $t^n = c$. Thus we obtain n more solutions this way.

We can unify the previous two possibilities and obtain

Proposition 2.35. *If $c \neq 0$ is a complex number, the solutions in $M_2(\mathbf{C})$ of the equation $X^n = cI_2$ are given by*

$$X = P\begin{bmatrix}x & 0\\ 0 & y\end{bmatrix}P^{-1} \tag{2.6}$$

where x, y are solutions (not necessary distinct) of the equation $z^n = c$, and $P \in \mathrm{GL}_2(\mathbf{C})$ is arbitrary.

Problem 2.36. Let $t \in (0, \pi)$ be a real number and let $n > 1$ be an integer. Find all matrices $X \in M_2(\mathbf{R})$ such that

$$X^n = \begin{bmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{bmatrix}.$$

Solution. With the notations of Problem 2.29, we need to solve the equation $X^n = A_t$. Let X be a solution, then $XA_t = A_t X = X^{n+1}$. Writing $X = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$, the relation $XA_t = A_t X$ yields $b\sin t = -c\sin t$ and $-a\sin t = -d\sin t$, thus $a = d$ and $c = -b$. Hence $X = \begin{bmatrix}a & -b\\ b & a\end{bmatrix}$. Next, since $X^n = A_t$, we have

$$(\det X)^n = \det X^n = \det A_t = 1,$$

and since $\det X = a^2 + b^2 \geq 0$, we deduce that $a^2 + b^2 = 1$. Thus we can write $a = \cos x$ and $b = \sin x$ for some real number x. Then $X = A_x$ and the equation $X^n = A_t$ is equivalent (thanks to Problem 2.29) to $A_{nx} = A_t$. This is further equivalent to $nx = t + 2k\pi$ for some integer k. It is enough to restrict to $k \in \{0, 1, \ldots, n-1\}$. We conclude that the solutions of the problem are the matrices

$$X_k = \begin{bmatrix} \cos t_k & -\sin t_k \\ \sin t_k & \cos t_k \end{bmatrix},$$

where $t_k = \dfrac{t + 2k\pi}{n}$, $k = 0, 1, \ldots, n-1$. □

Problem 2.37. Let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in M_2(\mathbf{R})$. Prove that the following statements are equivalent:

(1) $A^n = I_2$ for some positive integer n;
(2) $a = \cos r\pi$, $b = \sin r\pi$ for some rational number r.

Solution. If $a = \cos(\frac{k}{n}\pi)$ and $b = \sin(\frac{k}{n}\pi)$ for some $n \geq 1$ and $k \in \mathbf{Z}$, then Problem 2.29 yields $A^{2n} = I_2$, thus (2) implies (1).

Assume now that (1) holds. Then $(\det A)^n = \det A^n = 1$ and since $\det A = a^2 + b^2 \geq 0$, we must have $\det A = 1$, that is $a^2 + b^2 = 1$. Thus we can find $t \in \mathbf{R}$ such that $a = \cos t$ and $b = \sin t$. Then $A = A_t$ and by Problem 2.29 we have $I_2 = A^n = A_{nt}$. This forces $\cos(nt) = 1$ and so t is a rational multiple of π. The problem is solved. □

2.5.1 *Problems for Practice*

1. Let $n > 1$ be an integer. Prove that the equation

$$X^n = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

has no solutions in $M_2(\mathbf{C})$.

2. Solve in $M_2(\mathbf{C})$ the binomial equation

$$X^4 = \begin{bmatrix} -1 & -2 \\ 1 & 2 \end{bmatrix}.$$

3. Let $n > 1$ be an integer. Prove that the equation

$$X^n = \begin{bmatrix} 3 & -1 \\ 0 & 0 \end{bmatrix}$$

has no solutions in $M_2(\mathbf{Q})$.

4. Find all matrices $X \in M_2(\mathbf{R})$ such that

$$X^3 = \begin{bmatrix} 4 & 3 \\ -3 & -2 \end{bmatrix}.$$

5. Find all matrices $A, B \in M_2(\mathbf{C})$ such that

$$AB = O_2 \quad \text{and} \quad A^5 + B^5 = O_2.$$

6. Solve in $M_2(\mathbf{R})$ the equation

$$X^n = \begin{bmatrix} 7 & -5 \\ -15 & 12 \end{bmatrix}.$$

7. Solve in $M_2(\mathbf{R})$ the equation

$$X^n = \begin{bmatrix} -6 & -2 \\ 21 & 7 \end{bmatrix}.$$

2.6 Application to Pell's Equations

Let $D > 1$ be an integer which is not a perfect square. The diophantine equation, called **Pell's equation**

$$x^2 - Dy^2 = 1 \tag{2.7}$$

has an obvious solution $(1, 0)$ in nonnegative integers. A well-known but nontrivial result (which we take for granted) is that this equation also has nontrivial solutions (i.e., different from $(0, 1)$).

In this section we explain how the theory developed so far allows finding all solutions of the Pell equation once we know the smallest nontrivial solution. Let S_D be the set of all solutions in **positive integers** to the Eq. (2.7) and let (x_1, y_1) be the **fundamental solution**, i.e., the solution in S_D for which the first component x_1 is minimal among the first components of the elements of S_D.

If x, y are positive integers, consider the matrix

$$A_{(x,y)} = \begin{bmatrix} x & Dy \\ y & x \end{bmatrix},$$

so that $(x, y) \in S_D$ if and only if $\det A_{(x,y)} = 1$. Elementary computations yield the fundamental relation

$$A_{(x,y)} \cdot A_{(u,v)} = A_{(xu+Dyv, xv+yu)} \tag{2.8}$$

Passing to determinants in (2.8) we obtain the **multiplication principle**:

$$\text{if} \quad (x, y), (u, v) \in S_D, \quad \text{then } (xu + Dyv, xv + yu) \in S_D.$$

It follows from the multiplication principle that if we write

$$A^n_{(x_1,y_1)} = \begin{bmatrix} x_n & Dy_n \\ y_n & x_n \end{bmatrix}, \quad n \geq 1,$$

then $(x_n, y_n) \in S_D$ for all n. The sequences x_n and y_n are described by the recursive system

$$\begin{cases} x_{n+1} = x_1 x_n + D y_1 y_n \\ y_{n+1} = y_1 x_n + x_1 y_n, \quad n \geq 1 \end{cases} \tag{2.9}$$

consequence of the equality $A^{n+1}_{(x_1,y_1)} = A_{(x_1,y_1)} A^n_{(x_1,y_1)}$. Moreover, Theorem 2.25 gives explicit formulae for x_n and y_n in terms of x_1, y_1, n: the characteristic equation of matrix $A_{(x_1,y_1)}$ is

$$\lambda^2 - 2x_1\lambda + 1 = 0$$

with $\lambda_{1,2} = x_1 \pm \sqrt{x_1^2 - 1} = x_1 \pm y_1\sqrt{D}$, and Theorem 2.25 yields, after an elementary computation of the matrices B, C involved in that theorem

$$\begin{cases} x_n = \dfrac{1}{2}[(x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n] \\ \\ y_n = \dfrac{1}{2\sqrt{D}}[(x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n], \quad n \geq 1. \end{cases} \tag{2.10}$$

Note that relation (2.10) also makes sense for $n = 0$, in which case it gives the trivial solution $(x_0, y_0) = (1, 0)$.

Theorem 2.38. *All solutions in positive integers of the Pell equation $x^2 - Dy^2 = 1$ are described by the formula (2.10), where (x_1, y_1) is the fundamental solution of the equation.*

Proof. Suppose that there are elements in S_D which are not covered by formula (2.10), and among them choose one (x, y) for which x is minimal. Using the multiplication principle, we observe that the matrix $A_{(x,y)} A^{-1}_{(x_1,y_1)}$ generates a solution in integers (x', y'), where

$$\begin{cases} x' = x_1 x - D y_1 y \\ y' = -y_1 x + x_1 y \end{cases}$$

We claim that x', y' are positive integers. This is clear for x', as $x > \sqrt{D}\, y$ and $x_1 > \sqrt{D}\, y_1$, thus $x_1 x > D y_1 y$. Also, $x_1 y > y_1 x$ is equivalent to $x_1^2(x^2 - 1) > x^2(x_1^2 - 1)$

or $x > x_1$, which holds because (x_1, y_1) is a fundamental solution and (x, y) is not described by relation (2.10) (while (x_1, y_1) is described by this relation, with $n = 1$). Moreover, since $A_{(x',y')}A_{(x_1,y_1)} = A_{(x,y)}$, we have $x = x'x_1 + Dy'y_1 > x'$ and $y = x'y_1 + y'x_1 > y'$. By minimality, (x', y') must be of the form (2.10), i.e., $A_{(x,y)}A^{-1}_{(x_1,y_1)} = A^k_{(x_1,y_1)}$ for some positive integer k. Therefore $A_{(x,y)}=A^{k+1}_{(x_1,y_1)}$, i.e., (x, y) is of the form (2.10), a contradiction. □

Problem 2.39. Find all solutions in positive integers to Pell's equation

$$x^2 - 2y^2 = 1.$$

Solution. The fundamental solution is $(x_1, y_1) = (3, 2)$ and the associated matrix is

$$A_{(3,2)} = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$$

The solutions $(x_n, y_n)_{n\geq 1}$ are given by $A^n_{(3,2)}$, i.e.

$$\begin{cases} x_n = \dfrac{1}{2}[(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n] \\ \\ y_n = \dfrac{1}{2\sqrt{2}}[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n]. \end{cases}$$

□

We can extend slightly the study of the Pell equation by considering the more general equation

$$ax^2 - by^2 = 1 \tag{2.11}$$

where we assume that ab is not a perfect square (it is not difficult to see that if ab is a square, then the equation has only trivial solutions). Contrary to the Pell equation, this Eq. (2.11) does not always have solutions (the reader can check that the equation $3x^2 - y^2 = 1$ has no solutions in integers by working modulo 3).

Define the **Pell resolvent** of (2.11) by

$$u^2 - abv^2 = 1 \tag{2.12}$$

and let $S_{a,b}$ be the set of solutions in positive integers of Eq. (2.11). Thus $S_{1,ab}$ is the set denoted S_{ab} when considering the Pell equation (it is the set of solutions of the Pell resolvent). If x, y, u, v are positive integers consider the matrices

$$B_{(x,y)} = \begin{bmatrix} x & by \\ y & ax \end{bmatrix}, \quad A_{u,v} = \begin{bmatrix} u & abv \\ v & u \end{bmatrix},$$

the second matrix being the matrix associated with the Pell resolvent equation.

An elementary computation shows that

$$B_{(x,y)}A_{(u,v)} = B_{(xu+byv,axv+yu)},$$

Passing to determinants in the above relation and noting that $(x, y) \in S_{a,b}$ if and only if $\det B_{(x,y)} = 1$, we obtain the multiplication principle:

$$\text{if} \quad (x, y) \in S_{a,b} \quad \text{and} \quad (u, v) \in S_{ab}, \quad \text{then} \quad (xu + byv, axv + yu) \in S_{a,b},$$

i.e., the product $B_{(x,y)}A_{(u,v)}$ generates the solution $(xu + byv, axv + yu)$ of (2.11). Using the previous theorem and the multiplication principle, one easily obtains the following result, whose formal proof is left to the reader.

Theorem 2.40. *Assume that Eq. (2.11) is solvable in positive integers, and let (x_0, y_0) be its minimal solution (i.e., x_0 is minimal). Let (u_1, v_1) be the fundamental solution of the resolvent Pell equation (2.14). Then all solutions (x_n, y_n) in positive integers of Eq. (2.11) are generated by*

$$B_{(x_n,y_n)} = B_{(x_0,y_0)}A^n_{(u_1,v_1)}, \quad n \geq 0 \tag{2.13}$$

It follows easily from (2.13) that

$$\begin{cases} x_n = x_0u_n + by_0v_n \\ y_n = y_0u_n + ax_0v_n, \quad n \geq 0 \end{cases} \tag{2.14}$$

where $(u_n, v_n)_{n\geq 1}$ is the general solution to the Pell resolvent equation.

Problem 2.41. Solve in positive integers the equation

$$6x^2 - 5y^2 = 1.$$

Solution. This equation is solvable and its minimal solution is $(x_0, y_0) = (1, 1)$. The Pell resolvent equation is $u^2 - 30v^2 = 1$, with fundamental solution $(u_1, v_1) = (11, 2)$. Using formulae (2.14) and then (2.10), we deduce that the solutions in positive integers are $(x_n, y_n)_{n\geq 1}$, where

$$\begin{cases} x_n = \dfrac{6+\sqrt{30}}{12}(11 + 2\sqrt{30})^n + \dfrac{6-\sqrt{30}}{12}(11 - 2\sqrt{30})^n \\ y_n = \dfrac{5+\sqrt{30}}{12}(11 + 2\sqrt{30})^n + \dfrac{5-\sqrt{30}}{12}(11 - 2\sqrt{30})^n. \end{cases}$$

□

2.6.1 Problems for Practice

1. A triangular number is a number of the form $1 + 2 + \ldots + n$ for some positive integer n. Find all triangular numbers which are perfect squares.
2. Find all positive integers n such that $n + 1$ and $3n + 1$ are simultaneously perfect squares.
3. Find all integers a, b such that $a^2 + b^2 = 1 + 4ab$.
4. The difference of two consecutive cubes equals n^2 for some positive integer n. Prove that $2n - 1$ is a perfect square.
5. Find all triangles whose sidelengths are consecutive integers and whose area is an integer.

Chapter 3
Matrices and Linear Equations

Abstract This chapter introduces and studies the reduced row-echelon form of a matrix, and applies it to the resolution of linear systems of equations and the computation of the inverse of a matrix. The approach is algorithmic.

Keywords Linear systems • Homogeneous Systems • Row-echelon form • Gaussian reduction

The resolution of linear systems of equations is definitely one of the key motivations of linear algebra. In this chapter we explain an algorithmic procedure which allows the resolution of linear systems of equations, by performing some simple operations on matrices. We consider this problem as a motivation for the introduction of basic operations on the rows (or columns) of matrices. A much deeper study of these objects will be done in later chapters, using a more abstract (and much more powerful) setup. We will fix a field F in the following discussion, which the reader might take $\mathbf{R}$ or $\mathbf{C}$.

3.1 Linear Systems: The Basic Vocabulary

A **linear equation in the variables** $x_1, \ldots, x_n$ is an equation of the form

$$a_1x_1 + \ldots + a_nx_n = b,$$

where $a_1, \ldots, a_n, b \in F$ are given scalars and n is a given positive integer. The unknowns $x_1, \ldots, x_n$ are supposed to be elements of F.

A **linear system in the variables** $x_1, \ldots, x_n$ is a family of linear equations, usually written as

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \qquad\qquad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{3.1}$$

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_3

Here $a_{11}, a_{12}, \ldots, a_{mn}$ and $b_1, \ldots, b_m$ are given scalars. There is a much shorter notation for the previous system, using matrices and vectors: denoting X the (column) vector with coordinates $x_1, \ldots, x_n$, A the matrix $[a_{ij}]_{1 \leq i \leq m, 1 \leq j \leq n}$, and b the (column) vector whose coordinates are $b_1, \ldots, b_m$, the system can be rewritten as

$$AX = b. \tag{3.2}$$

Finally, we can rewrite the system in terms of vectors: if $C_1, \ldots, C_n$ are the columns of the matrix A, seen as vectors in F^m (written in column form), the system is equivalent to

$$x_1 C_1 + x_2 C_2 + \ldots + x_n C_n = b. \tag{3.3}$$

Definition 3.1. (a) The linear system (3.1) is called **homogeneous** if $b_1 = \ldots = b_m = 0$.

(b) The homogeneous linear system associated with the system (3.2) is the system $AX = 0$.

Thus a homogeneous system is one of the form $AX = 0$ for some matrix A. For the resolution of linear systems, homogeneous systems play a crucial role, thanks to the following proposition, which shows that solving a general linear system reduces to finding **one** solution and then solving a homogeneous linear system.

Proposition 3.2 (Superposition Principle). *Let $A \in M_{m,n}(F)$ and $b \in F^m$. Let $\mathcal{S} \subset F^n$ be the set of solutions of the homogeneous linear system $AX = 0$. If the system $AX = b$ has a solution X_0, then the set of solutions of this system is $X_0 + \mathcal{S}$.*

Proof. By assumption $AX_0 = b$. Now the relation $AX = b$ is equivalent to $AX = AX_0$, or $A(X - X_0) = 0$. Thus a vector X is a solution of the system $AX = b$ if and only if $X - X_0$ is a solution of the homogeneous system $AY = 0$, i.e., $X - X_0 \in \mathcal{S}$. This is equivalent to $X \in X_0 + \mathcal{S}$. □

Definition 3.3. A linear system is called **consistent** if it has at least one solution. It is called **inconsistent** if it is not consistent, i.e., it has no solution.

Let us introduce a final definition for this section:

Definition 3.4. (a) Two linear systems are **equivalent** if they have exactly the same set of solutions.

(b) Let A, B be matrices of the same size. If the systems $AX = 0$ and $BX = 0$ are equivalent, we write $A \sim B$.

Remark 3.5. (a) Typical examples of inconsistent linear systems are

$$\begin{cases} x_1 = 0 \\ x_1 = 1 \end{cases}$$

or

$$\begin{cases} x_1 - 2x_2 = 1 \\ 2x_2 - x_1 = 0 \end{cases}$$

(b) Note that **homogeneous systems are always consistent**: any homogeneous system has an obvious solution, namely the vector whose coordinates are all equal to 0. We will call this the **trivial solution**. It follows from Proposition 3.2 that if the system $AX = b$ is consistent, then it has a unique solution if and only if the associated homogeneous system $AX = 0$ has only the trivial solution.

3.1.1 Problems for Practice

1. For which real numbers a is the system

$$\begin{cases} x_1 + 2x_2 = 1 \\ 3x_1 + 6x_2 = a \end{cases}$$

consistent? Solve the system in this case.
2. Find all real numbers a and b for which the systems

$$\begin{cases} x_1 + 2x_2 = 3 \\ -x_1 + 3x_2 = 1 \end{cases}$$

and

$$\begin{cases} x_1 + ax_2 = 2 \\ -x_1 + 2x_2 = b \end{cases}$$

are equivalent.
3. Let a, b be real numbers, not both equal to 0.

(a) Prove that the system

$$\begin{cases} ax_1 + bx_2 = 0 \\ -bx_1 + ax_2 = 0 \end{cases}$$

has only the trivial solution.

(b) Prove that for all real numbers c, d the system

$$\begin{cases} ax_1 + bx_2 = c \\ -bx_1 + ax_2 = d \end{cases}$$

has a unique solution and find this solution in terms of a, b, c, d.

4. Let $A \in M_2(\mathbf{C})$ be a matrix and consider the homogeneous system $AX = 0$. Prove that the following statements are equivalent:
   (a) This system has only the trivial solution.
   (b) A is invertible.
5. Let A and B be $n \times n$ matrices such that the system $ABX = 0$ has only the trivial solution. Show that the system $BX = 0$ also has only the trivial solution.
6. Let C and D be $n \times n$ matrices such that the system $CDX = b$ is consistent for every choice of a vector b in $\mathbf{R}^n$. Show that the system $CY = b$ is consistent for every choice of a vector b in $\mathbf{R}^n$.
7. Let $A \in M_n(F)$ be an invertible matrix with entries in a field F. Prove that for all $b \in F^n$ the system $AX = b$ is consistent (the converse holds but the proof is much harder, see Theorem 3.25).

3.2 The Reduced Row-Echelon form and Its Relevance to Linear Systems

Consider a matrix A with entries in a field F. If R is a row of A, say R is zero if all entries in row R are equal to 0. If R is nonzero, the **leading entry** of R or the **pivot** of R is the first nonzero entry in that row. We say that A is in **reduced row-echelon form** if A has the following properties:

(1) All zero rows of A are at the bottom of A (so no nonzero row can lie below a zero row).
(2) The pivot in a nonzero row is strictly to the right of the pivot in the row above.
(3) In any nonzero row, the pivot equals 1 and it is the only nonzero element in its column.

For instance, the matrix I_n is in reduced row-echelon form, and so is the matrix O_n. The matrix

$$A = \begin{bmatrix} 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{3.4}$$

is in reduced row-echelon form, but the slightly different matrix

$$B = \begin{bmatrix} 1 & -2 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

is not in reduced row-echelon form, as the pivot for the second row is not the only nonzero entry in its column.

What is the relevance of this very special form of matrices with respect to the original problem, consisting in solving linear systems of equations? We will see in the next sections that any matrix can be put (in an algorithmic way) in reduced row-echelon form and that this form is unique. Also, we will see that if A_{ref} is the reduced row-echelon form of A, then the systems $AX = 0$ and $A_{ref}X = 0$ are equivalent. Moreover, it is very easy to solve the system $A_{ref}X = 0$ since A_{ref} is in reduced row-echelon form.

Example 3.6. Let us solve the system $AX = 0$, where A is the reduced row-echelon matrix given in relation (3.4). The system is

$$\begin{cases} x_1 - 2x_2 - x_4 = 0 \\ x_3 + x_4 = 0 \end{cases}$$

We can simply express $x_3 = -x_4$ and $x_1 = 2x_2 + x_4$, thus the general solution of the system is

$$(2a + b, a, -b, b)$$

with $a, b \in F$.

In general, consider a matrix A which is in reduced row-echelon form and let us see how to solve the system $AX = 0$. The only meaningful equations are those given by the nonzero rows of A (recall that all zero rows of A are at the bottom). Suppose that the ith row of A is nonzero for some i and let the pivot of that row be in column j, so that the pivot is $a_{ij} = 1$. The ith equation of the linear system is then of the form

$$x_j + \sum_{k=j+1}^{n} a_{ik}x_k = 0.$$

We call x_j the **pivot variable** of the row L_i. So to each nonzero row we associate a unique pivot variable. All the other variables of the system are called **free variables**. One solves the system starting from the bottom, by successively expressing the pivot

variables in terms of free variables. This yields the general solution of the system, in terms of free variables, which can take any value in F. If $y_1, \ldots, y_s$ are the free variables, then the solutions of the system will be of the form

$$X = \begin{bmatrix} b_{11}y_1 + b_{12}y_2 + \ldots + b_{1s}y_s \\ b_{21}y_1 + b_{22}y_2 + \ldots + b_{2s}y_s \\ \ldots \\ b_{n1}y_1 + b_{n2}y_2 + \ldots + b_{ns}y_s \end{bmatrix}$$

for some scalars b_{ij}. This can also be written as

$$X = y_1 \begin{bmatrix} b_{11} \\ b_{21} \\ \ldots \\ b_{n1} \end{bmatrix} + \ldots + y_s \begin{bmatrix} b_{1s} \\ b_{2s} \\ \ldots \\ b_{ns} \end{bmatrix}.$$

We call

$$Y_1 = \begin{bmatrix} b_{11} \\ b_{21} \\ \ldots \\ b_{n1} \end{bmatrix}, \ldots, \quad Y_s = \begin{bmatrix} b_{1s} \\ b_{2s} \\ \ldots \\ b_{ns} \end{bmatrix}$$

the **fundamental solutions** of the system $AX = 0$. The motivation for their name is easy to understand: $Y_1, \ldots, Y_s$ are solutions of the system $AX = 0$ which "generate" all other solutions, in the sense that all solutions of the system $AX = 0$ are obtained by all possible linear combinations of $Y_1, \ldots, Y_s$ (corresponding to all possible values that the free variables $y_1, \ldots, y_s$ can take).

Example 3.7. Let us consider the matrix in reduced row-echelon form

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & -1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and the associated homogeneous linear system $AX = 0$. This can be written as

$$\begin{cases} x_1 + x_2 - x_5 + 2x_7 = 0 \\ x_3 + 3x_5 + x_7 = 0 \\ x_4 - x_7 = 0 \\ x_6 = 0 \end{cases}$$

The pivot variables are x_1, x_3, x_4, x_6, as the pivots appear in columns $1, 3, 4, 6$. So the free variables are x_2, x_5, x_7. Next, we solve the system starting with the last equation and going up, at each step expressing the pivot variables in terms of free variables. The last equation gives $x_6 = 0$. Next, we obtain $x_4 = x_7$, then $x_3 = -3x_5 - x_7$ and $x_1 = -x_2 + x_5 - 2x_7$. Thus

$$X = \begin{bmatrix} -x_2 + x_5 - 2x_7 \\ x_2 \\ -3x_5 - x_7 \\ x_7 \\ x_5 \\ 0 \\ x_7 \end{bmatrix} = x_2 \cdot \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_5 \cdot \begin{bmatrix} 1 \\ 0 \\ -3 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + x_7 \cdot \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

The three column vectors appearing in the right-hand side are the fundamental solutions of the system $AX = 0$. All solutions of the system are given by all possible linear combinations of the three fundamental solutions.

The number of fundamental solutions of the system $AX = 0$ is the total number of variables minus the number of pivot variables. We deduce that the system $AX = 0$ has the unique solution $X = 0$ if and only if there are no free variables, or equivalently every variable is a pivot variable. This is the same as saying that the number of pivot variables equals the number of columns of A. Combining these observations with the superposition principle (Proposition 3.2) we obtain the very important:

Theorem 3.8. *(a) A homogeneous linear system having more variables than equations has nontrivial solutions. If the field containing the coefficients of the equations is infinite (for instance* $\mathbf{R}$ *or* $\mathbf{C}$*), then the system has infinitely many solutions.*

(b) A ***consistent*** *linear system $AX = b$ having more variables than equations has at least 2 solutions and, if the field F is infinite (for instance $F = \mathbf{R}$ or $F = \mathbf{C}$), then it has infinitely many solutions.*

We turn now to the fundamental problem of transforming a matrix into a reduced row-echelon form matrix. In order to solve this problem we introduce three types of simple operations that can be applied to the rows of a matrix. We will see that one can use these operations to transform any matrix into a reduced row-echelon form matrix. These operations have a very simple motivation from the point of view of linear systems: the most natural operations that one would do in order to solve a linear system are:

- multiplying an equation by a nonzero scalar;
- adding a multiple of an equation to a second (and different) equation;
- interchanging two equations.

Note that these operations are reversible: for example, the inverse operation of multiplication of an equation by a nonzero scalar a is multiplication of that equation by the inverse of a. It is therefore clear that by performing any finite sequence of such operations on a linear system we obtain a new linear system which has precisely the same set of solutions as the original one (i.e., a new linear system which is equivalent to the original one). These operations on equations of the system can be seen as operations on the matrix associated with the system. More precisely:

Definition 3.9. An **elementary operation** on the rows of a matrix A (or **elementary row operation**) is an operation of one of the following types:

(1) row swaps: interchanging two rows of the matrix A.
(2) row scaling: multiplying a row of A by a nonzero scalar.
(3) transvection: replacing a row L by $L + cL'$ for some scalar c and some row L' of A, **different from** L.

The previous discussion shows that if A is a matrix and B is obtained from A by a sequence of elementary row operations, then $A \sim B$, where we recall (Definition 3.4) that this simply means that the systems $AX = 0$ and $BX = 0$ are equivalent.

Corresponding to these operations, we define elementary matrices:

Definition 3.10. A matrix $A \in M_n(F)$ is called an **elementary matrix** if it is obtained from I_n by performing **exactly one** elementary row operation.

Note that elementary matrices have the same number of rows and columns. There are three types of elementary matrices:

(1) Transposition matrices: those obtained from I_n by interchanging two of its rows.
(2) Dilation matrices: those obtained from I_n by multiplying one of its rows by a nonzero scalar.
(3) Transvection matrices: those obtained from I_n by adding to a row a multiple of a second (and different) row.

A simple, but absolutely crucial observation is the following:

Proposition 3.11. *Let $A \in M_{m,n}(F)$ be a matrix. Performing an elementary row operation on A is equivalent to multiplying A **on the left** by the elementary matrix corresponding to that operation.*

Proof. If E is any $m \times m$ matrix and $A \in M_{m,n}(F)$, then the ith row of EA is $e_{i1}L_1 + e_{i2}L_2 + \ldots + e_{im}L_m$, where $L_1, \ldots, L_m$ are the rows of A and e_{ij} are the entries of E. The result follows readily from the definitions. □

We now reach **the most important theorem of this chapter**: it is one of the most important theorems in linear algebra, since using it we will obtain algorithmic ways of solving many practical problems, concerning linear systems, invertibility of matrices, linear independence of vectors, etc.

Theorem 3.12. *Any matrix $A \in M_{m,n}(F)$ can be put into a reduced row-echelon form by performing elementary row operations on its rows.*

Proof. The proof is algorithmic. Start with any matrix A and consider its first column. If it is zero, then pass directly to the next column. Suppose that the first column C_1 is nonzero and consider the first nonzero entry, say it is a_{i1}. Then interchange rows L_1 and L_i (if $i = 1$ we skip this operation), so in the new matrix we have a nonzero entry x in position $(1, 1)$. Multiply the first row by $1/x$ to obtain a new matrix, in which the entry in position $(1, 1)$ is 1. Using transvections, we can make all entries in the first column below the $(1, 1)$ entry equal to 0: for $i \geq 2$ subtract b_{i1} times the first row, where b_{i1} is the entry in position $(i, 1)$. Thus after some elementary row operations we end up with a matrix B whose first column is either 0 or has a pivot in position $(1, 1)$ and zeros elsewhere.

Next, we move to the second column C_2 of this new matrix B. If every entry **below** b_{12} is zero, go directly to the third column of B. Suppose that some entry below b_{12} is nonzero. By possibly swapping the second row and a suitable other row (corresponding to the first nonzero entry below b_{12}), we may assume that $b_{22} \neq 0$. Multiply the second row by $1/b_{22}$ so that the entry in position $(2, 2)$ becomes 1. Now make the other entries in the second column zero by transvections. We now have pivots equal to 1 in the first and second columns. Needless to say, we continue this process with each subsequent column and we end up with a matrix in reduced row-echelon form. □

Remark 3.13. The algorithm used in the proof of the previous theorem is called **Gaussian reduction** or **row-reduction**.

By combining the Gaussian reduction theorem (Theorem 3.12) and Proposition 3.11 we obtain the following result, which will be constantly used in the next section:

Proposition 3.14. *For any matrix $A \in M_{m,n}(F)$ we can find a matrix $B \in M_m(F)$ which is a product of elementary matrices, such that $A_{ref} = BA$.*

Remark 3.15. In order to find the matrix B in practice, the best way is to row-reduce the matrix $[A|I_m]$ if A is $m \times n$. The row-reduction will yield the matrix $[A_{ref}|B]$, as the reader can check.

Example 3.16. Let us perform the Gaussian reduction on the matrix

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ -1 & 0 & 1 & 2 & 3 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 1 & -1 & 0 & 2 \end{bmatrix} \in M_{4,5}(\mathbf{R}).$$

The first nonzero entry in column C_1 appears in position $(2, 1)$ and equals -1, so we swap the first and second rows, then we multiply the new first row by -1 to get a pivot equal to 1 in the first row. We end up with the matrix

$$A_1 = \begin{bmatrix} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 & 1 \\ 3 & 1 & -1 & 0 & 2 \end{bmatrix}.$$

We make zeros elsewhere in the first column, by subtracting three times the first row from the last row. The new matrix is

$$A_2 = \begin{bmatrix} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 6 & 11 \end{bmatrix}.$$

Since we are done with the first column, we go on to the second one. The entry in position $(2, 2)$ is already equal to 1, so we don't need to swap rows or to scale them. Thus we make directly zeros elsewhere in the second column, so that the only nonzero entry is the 1 in position $(2, 2)$. For this, we subtract the second row from the third and the fourth. The new matrix is

$$A_3 = \begin{bmatrix} 1 & 0 & -1 & -2 & -3 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & -1 & -2 & -3 \\ 0 & 0 & 0 & 3 & 7 \end{bmatrix}.$$

We next consider the third column. The first nonzero entry **below** the entry in position $(2, 3)$ is -1, so we multiply the third row by -1 and then make the 1 in position $(3, 3)$ the only nonzero entry in that column by transvections. We end up with

$$A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -2 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 3 & 7 \end{bmatrix}.$$

We repeat the procedure with the fourth column: we multiply the last row by $1/3$ (so that the first nonzero entry below the one in position $(3, 4)$ becomes 1 our pivot) and then make the entry in position $(4, 4)$ the only nonzero entry in its column by transvections. The final matrix is the reduced row-echelon form of A, namely

$$A_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1/3 \\ 0 & 0 & 1 & 0 & -5/3 \\ 0 & 0 & 0 & 1 & 7/3 \end{bmatrix}.$$

Problem 3.17. Solve the homogeneous linear system $AX = 0$, where A is the matrix from the previous example.

Solution. The systems $AX = 0$ and $A_{ref}X = 0$ being equivalent, it suffices to solve the latter system. The pivot variables are x_1, x_2, x_3, x_4 and the free variable is x_5. The system $A_{ref}X = 0$ is given by

$$\begin{cases} x_1 = 0 \\ x_2 + \frac{x_5}{3} = 0 \\ x_3 - \frac{5}{3}x_5 = 0 \\ x_4 + \frac{7}{3}x_5 = 0 \end{cases}$$

The resolution is then immediate and gives the solutions

$$(0, -\frac{1}{3}t, \frac{5}{3}t, -\frac{7}{3}t, t), \quad t \in \mathbf{R}. \qquad \square$$

3.2.1 Problems for Practice

1. Find the reduced row-echelon form of the matrix with real entries

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 7 \end{bmatrix}.$$

2. Implement the Gaussian reduction algorithm on the matrix

$$A = \begin{bmatrix} 0 & 2 & 1 & 1 & 2 \\ 1 & 1 & 0 & 2 & 1 \\ -3 & 1 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

3. Determine the fundamental solutions of the homogeneous linear system of equations $AX = 0$, where A is the matrix

$$A = \begin{bmatrix} 1 & -2 & 1 & 0 \\ -2 & 4 & 0 & 2 \\ -1 & 2 & 1 & 2 \end{bmatrix}.$$

4. (a) Write the solutions of the homogeneous system of equations $AX = 0$ in parametric vector form, where

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & -1 \\ -1 & 1 & -4 \end{bmatrix}.$$

   (b) Find a solution to the system for which the sum of the first two coordinatesis 1.
5. Solve the homogeneous system

$$\begin{cases} x + 2y - 3z = 0 \\ 2x + 5y + 2z = 0 \\ 3x - y - 4z = 0 \end{cases}$$

6. Show that the homogeneous system of equations $AX = 0$ has nontrivial solutions, where

$$A = \begin{bmatrix} 2 & -1 & 3 & 1 \\ 1 & 0 & 2 & 2 \\ 3 & 1 & 7 & 0 \\ 1 & 2 & 4 & -1 \end{bmatrix}.$$

   Then determine a matrix B of size 4×3 obtained from A by erasing one of its columns such that the system $BY = 0$ has only the trivial solution.
7. Let $n > 2$ be an integer. Solve in real numbers the linear system

$$x_2 = \frac{x_1 + x_3}{2}, \quad x_3 = \frac{x_2 + x_4}{2}, \quad \ldots, \quad x_{n-1} = \frac{x_{n-2} + x_n}{2}.$$

3.3 Solving the System $AX = b$

Consider a linear system $AX = b$ with $A \in M_{m,n}(F)$ and $b \in F^m$, in the variables $x_1, \ldots, x_n$, which are the coordinates of the vector $X \in F^n$. In order to solve this system, we consider the **augmented matrix** $(A|b)$ obtained by adding to the matrix A a new column (at the right), given by the coordinates of the vector b. Elementary row operations on the equations of the system come down to elementary row operations on the augmented matrix, thus in order to solve the system we can first transform $(A|b)$ into its reduced row-echelon form by the Gaussian reduction algorithm, then solve the new (much easier) linear system. The key point is the following easy but important observation:

Proposition 3.18. *Consider the linear system $AX = b$. Suppose that the matrix $(A'|b')$ is obtained from the augmented matrix $(A|b)$ by a sequence of elementary row operations. Then the systems $AX = b$ and $A'X = b'$ are equivalent, i.e., they have exactly the same set of solutions.*

Proof. As we have already noticed, performing elementary row operations on $(A|b)$ comes down to performing elementary operations on the equations of the system $AX = b$, and these do not change the set of solutions, as they are reversible. □

We now reach the second fundamental theorem of this chapter, the **existence and uniqueness theorem**.

Theorem 3.19. *Assume that $(A|b)$ has been brought to a reduced row-echelon form $(A'|b')$ by elementary row operations.*

(a) The system $AX = b$ is consistent if and only if $(A'|b')$ does not have a pivot in the last column.
(b) If the system is consistent, then it has a unique solution if and only if A' has pivots in every column.

Proof. (a) Assume that $(A'|b')$ has a pivot in the last column. If the pivot appears in row i, then the ith row of $(A'|b')$ is of the form $(0, \ldots, 0, 1)$. Thus among the equations of the system $A'X' = b'$ we have the equation $0x'_1 + \ldots + 0x'_n = 1$, which has no solution. Thus the system $A'X' = b'$ has no solution and so the system $AX = b$ is not consistent.

Conversely, suppose that $(A'|b')$ does not have a pivot in the last column. Say A' has pivots in columns $j_1 < \ldots < j_k \leq n$ and call $x_{j_1}, \ldots, x_{j_k}$ the pivot variables, and all other variables the free variables. Give the value 0 to all free variables, getting in this way a system in the variables $x_{j_1}, \ldots, x_{j_k}$. This system is triangular and can be solved successively from the bottom, by first finding x_{j_k}, then $x_{j_{k-1}}, \ldots$, then x_{j_1}. In particular, the system has a solution and so the system $AX = b$ is consistent.

(b) Since we can give any value to the free variables, the argument in the second paragraph of the proof of (a) shows that the solution is unique if and only if there are no free variables, or equivalently if and only if A' has a pivot in every column. □

For simplicity, assume that $F = \mathbf{R}$, i.e., the coefficients of the equations of the linear system $AX = b$ are real numbers. **In order to find the number of solutions of the system, we proceed as follows.** First, we consider the augmented matrix $[A|b]$ and perform the Gaussian reduction on it to reach a matrix $[A'|b']$. If this new matrix has a row of the form $(0, 0, \ldots, 0, |c)$ for some nonzero real number c, then the system is inconsistent. If this is not the case, then we check whether every column of A' has a pivot. If this is the case, then the system has a unique solution. If not, then the system has infinitely many solutions.

Problem 3.20. Let us consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 2 & 4 & 4 \end{bmatrix}.$$

Given a vector $b \in \mathbf{R}^3$, find a necessary and sufficient condition in terms of the coordinates of b such that the system $AX = b$ is consistent.

Solution. The augmented matrix of the system is

$$[A|b] = \begin{bmatrix} 1 & 2 & 2 & b_1 \\ 0 & 1 & 1 & b_2 \\ 2 & 4 & 4 & b_3 \end{bmatrix}.$$

In order to obtain its row-reduction, we subtract twice the first row from the third one, and in the new matrix we subtract twice the second row from the first one. We end up with

$$[A|b] \sim \begin{bmatrix} 1 & 0 & 0 & b_1 - 2b_2 \\ 0 & 1 & 1 & b_2 \\ 0 & 0 & 0 & b_3 - 2b_1 \end{bmatrix}.$$

By the previous theorem, the system $AX = b$ is consistent if and only if this last matrix has no pivot in the last column, which is equivalent to $b_3 = 2b_1$. □

Using the fact that for two matrices A, B differing by a sequence of elementary row operations the systems $AX = 0$ and $BX = 0$ are equivalent, we can give a proof of the uniqueness of the reduced row-echelon form of a matrix. The following simple and elegant proof of this nontrivial theorem is due to Thomas Yuster.[1]

Theorem 3.21. *The reduced row-echelon form of a matrix is unique.*

Proof. The proof goes by induction on the number n of columns of the matrix $A \in M_{m,n}(F)$. The result being clear for $n = 1$, assume that $n > 1$ and that the result holds for $n - 1$. Let $A \in M_{m,n}(F)$ and let A' be the matrix obtained from A by deleting the nth column. Suppose that B and C are two distinct reduced row-echelon forms of A. Since any sequence of elementary row operations bringing A to a reduced row-echelon form also bring A' to a reduced row-echelon form, by applying the induction hypothesis we know that B and C differ in the nth column only.

Let j be such that $b_{jn} \neq c_{jn}$ (such j exists by the previous paragraph and the assumption that $B \neq C$). If X is a vector such that $BX = 0$, then $CX = 0$ (as

[1] See the article "The reduced row-echelon form of a matrix is unique: a simple proof", Math. Magazine, Vol. 57, No 2, Mar 1984, pp. 93–94.

the systems $BX = 0$ and $CX = 0$ are equivalent to the system $AX = 0$), so that $(B-C)X = 0$. Since B and C differ in the nth column only, the jth equation of the system $(B - C)X = 0$ reads $(b_{jn} - c_{jn})x_n = 0$ and so $x_n = 0$ whenever $BX = 0$ or $CX = 0$. It follows that x_n is not a free variable for B and C and thus B and C must have a pivot in the nth column. Again, since B and C only differ in the last column and since they are in reduced row-echelon form, the row in which the pivot in the last column appears is the same for B and C. Since all other entries in the last column of B and C are equal to 0 (as B and C are in reduced echelon form), we conclude that B and C have the same nth column, contradicting the fact that $b_{jn} \neq c_{jn}$. Thus $B = C$ and the inductive step is completed, proving the desired result.

□

3.3.1 Problems for Practice

1. Write down the solution set of the linear system

$$\begin{cases} x_1 & -3x_2 & -2x_3 & = -5 \\ & x_2 & -x_3 & = 4 \\ -2x_1 & +3x_2 & +7x_3 & = -2 \end{cases}$$

   in parametric vector form.
2. Let A be a matrix of size $m \times n$ and let b and c be two vectors in $\mathbf{R}^m$ such that the system $AX = b$ has a unique solution and the system $AX = c$ has no solution. Explain why $m > n$ must hold.
3. Find a necessary and sufficient condition on the coordinates of the vector $b \in \mathbf{R}^4$ for the system $AX = b$ to be consistent, where

$$A = \begin{bmatrix} 3 & -6 & 2 & -1 \\ -2 & 4 & 1 & 3 \\ 0 & 0 & 1 & 1 \\ 1 & -2 & 1 & 0 \end{bmatrix}.$$

4. Find x, y, z and w so that

$$\begin{bmatrix} x & 3 \\ y & 4 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ z & w \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

   Find one solution with x positive and one with x negative.
5. Explain why a linear system of 10 equations in 11 variables cannot have a unique solution.

6. Find all possible values for h and k such that the system with augmented matrix

$$\left[\begin{array}{cc|c} 1 & 2 & h \\ 2 & k & 12 \end{array}\right]$$

has

(a) a unique solution.
(b) infinitely many solutions.
(c) no solution.

7. For what value of s is the vector $v_1 = (s, -7, -6)$ a linear combination of the vectors $v_2 = (1, 0, -1)$ and $v_3 = (1, -7, -4)$?
8. Let a, b be real numbers. Solve in real numbers the system

$$\begin{cases} x + y = a \\ y + z = b \\ z + t = a \\ t + x = b \end{cases}$$

3.4 Computing the Inverse of a Matrix

Recall that a matrix $A \in M_n(F)$ is invertible if there is a matrix B such that $AB = BA = I_n$. Such a matrix is then unique and is called the inverse of A and denoted A^{-1}. A fundamental observation is that elementary matrices are invertible, which follows immediately from the fact that elementary row operations on matrices are reversible (this also shows that the inverse of an elementary matrix is still an elementary matrix). For instance, if a matrix E is obtained from I_n by exchanging rows i and j, then E^{-1} is obtained from I_n by doing the same operation that is $E^{-1} = E$. Also, if E is obtained by adding λ times row j to row i in I_n, then E^{-1} is obtained by adding $-\lambda$ times row j to row i in I_n. Due to its importance, let us state this as a proposition:

Proposition 3.22. *Elementary matrices are invertible and their inverses are also elementary matrices.*

Here is an important consequence of the previous proposition and Proposition 3.14.

Theorem 3.23. *For a matrix $A \in M_n(F)$ the following statements are equivalent:*

(a) A is invertible.
(b) $A_{ref} = I_n$.
(c) A is a product of elementary matrices.

Proof. First, let us note that any product of elementary matrices is invertible, since any elementary matrix is invertible and since invertible matrices are stable under product. This already proves that (c) implies (a). Assume that (a) holds. By Proposition 3.14 and our initial observation, we can find an invertible matrix B such that $A_{ref} = BA$. Since A is invertible, so is BA and so A_{ref} is invertible. In particular, all rows in A_{ref} are nonzero (it is easy to see that if A_{ref} has an entire row consisting of zeros, then $A_{ref}C$ is never equal to I_n) and so A_{ref} has n pivots, one in each column. Since moreover A_{ref} is in reduced row-echelon form, we must have $A_{ref} = I_n$. Thus (b) holds.

Finally, if (b) holds, then by Proposition 3.14 we can find a matrix B which is a product of elementary matrices such that $BA = I_n$. By the previous proposition B is invertible and B^{-1} is a product of elementary matrices. Since $BA = I_n$, we have $A = B^{-1}BA = B^{-1}$ and so A is a product of elementary matrices. Thus (b) implies (c) and the theorem is proved. □

The following proposition expresses the solutions of the system $AX = b$ when A is an invertible matrix. Of course, in order to make this effective, one should have an algorithm allowing one to compute A^{-1}. We will see such an algorithm (based again on row-reduction) later on (see the discussion following Corollary 3.26).

Proposition 3.24. *If $A \in M_n(F)$ is invertible, then for all $b \in F^n$ the system $AX = b$ has a unique solution, namely $X = A^{-1}b$.*

Proof. Let X be a solution of the system. Multiplying the equality $AX = b$ on the left by A^{-1} yields $A^{-1}(AX) = A^{-1}b$. Since

$$A^{-1}(AX) = (A^{-1}A)X = I_nX = X,$$

we conclude that $X = A^{-1}b$, thus the system has at most one solution. To see that this is indeed a solution, we compute

$$A(A^{-1}b) = (AA^{-1})b = I_nb = b.$$

□

It turns out that the converse is equally true, but much trickier. In fact, we have the fundamental:

Theorem 3.25. *Let $A \in M_n(F)$ be a matrix. The following statements are equivalent:*

(a) A is invertible
(b) For all $b \in F^n$ the system $AX = b$ has a unique solution $X \in F^n$.
(c) For all $b \in F^n$ the system $AX = b$ is consistent.

Proof. We have already proved that (a) implies (b). It is clear that (b) implies (c), so let us assume that (c) holds. Let A_{ref} be the reduced row-echelon form of A. By Proposition 3.14 we can find a matrix B which is a product of elementary matrices

(thus invertible) such that $A_{ref} = BA$. We deduce that the system $A_{ref}X = Bb$ has at least one solution for all $b \in F^n$ (indeed, if $AX = b$, then $A_{ref}X = BAX = Bb$). Now, for any $b' \in F^n$ we can find b such that $b' = Bb$, by taking $b = B^{-1}b'$. We conclude that the system $A_{ref}X = b$ is consistent for every $b \in F^n$. But then any row of A_{ref} must be nonzero (if row i is zero, then choosing any vector b with the ith coordinate equal to 1 yields an inconsistent system) and, as in the first paragraph of the proof of Theorem 3.23 we obtain $A_{ref} = I_n$. Using Theorem 3.23 we conclude that A is invertible and so (a) holds. The theorem is proved. □

Here is a nice and nontrivial consequence of the previous theorem:

Corollary 3.26. *Let $A, B \in M_n(F)$ be matrices.*

(a) If $AB = I_n$, then A is invertible and $B = A^{-1}$.
(b) If $BA = I_n$, then A is invertible and $B = A^{-1}$.

Proof. (a) For any $b \in F^n$ the vector $X = Bb$ satisfies $AX = A(Bb) = (AB)b = b$, thus the system $AX = b$ is consistent for every $b \in F^n$. By the previous theorem, A is invertible. Multiplying the equality $AB = I_n$ on the left by A^{-1} we obtain $B = A^{-1}AB = A^{-1}$, thus $B = A^{-1}$.

(b) By part (a), we know that B is invertible and $A = B^{-1}$. But then A itself is invertible and $A^{-1} = B$, since by definition $B \cdot B^{-1} = B^{-1} \cdot B = I_n$. □

The previous corollary gives us a **practical way of deciding whether a square matrix A is invertible and, if this is the case, computing its inverse**. Indeed, A is invertible if and only if we can find a matrix X such that $AX = I_n$, as then $X = A^{-1}$. The equation $AX = I_n$ is equivalent to n linear systems: $AX_1 = e_1$, $AX_2 = e_2, \ldots, AX_n = e_n$, where e_i is the ith column of I_n and X_i denotes the ith column of X. We already know how to solve linear systems, using the reduced row echelon form, so this gives us a practical way of computing X (if at least one of these systems is inconsistent, then A is not invertible).

In practice, one can avoid solving n linear systems by the following trick: instead of considering n augmented matrices $[A|e_i]$, consider only one augmented matrix $[A|I_n]$, in which we add the matrix I_n to the right of A (thus $[A|I_n]$ has $2n$ columns). Thus we solve simultaneously the n linear systems we are interested in by enlarging the augmented matrix! Now find the reduced row-echelon form $[A'|X]$ of this $n \times 2n$ matrix $[A|I_n]$. If A' is different from I_n, then A is not invertible. If $A' = I_n$, then the inverse of A is simply the matrix X.

Example 3.27. Consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 2 & 1 & 2 \\ 1 & 2 & 2 & 2 \end{bmatrix} \in M_4(\mathbf{R}).$$

We will try to see whether the matrix A is invertible and, if this is the case, compute its inverse. Consider the augmented matrix $B = [A|I_4]$ and let us find its reduced

row-echelon form using Gaussian reduction. Subtracting twice the first row from each of the second, third, and fourth row of B, we end up with

$$B_1 = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & -3 & -2 & -2 & -2 & 1 & 0 & 0 \\ 0 & -2 & -3 & -2 & -2 & 0 & 1 & 0 \\ 0 & -2 & -2 & -3 & -2 & 0 & 0 & 1 \end{bmatrix}.$$

Multiply the second row by $-1/3$. In the new matrix, add twice the second row to the third and fourth row. We end up with

$$B_2 = \begin{bmatrix} 1 & 2 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & \frac{2}{3} & \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} & 0 & 0 \\ 0 & 0 & -\frac{5}{3} & -\frac{2}{3} & -\frac{2}{3} & -\frac{2}{3} & 1 & 0 \\ 0 & 0 & -\frac{2}{3} & -\frac{5}{3} & -\frac{2}{3} & -\frac{2}{3} & 0 & 1 \end{bmatrix}.$$

Multiply the third row by $-\frac{3}{5}$. In the new matrix add $2/3$ times the third row to the fourth one, then multiply the fourth row by $-5/7$. Continuing the Gaussian reduction in the usual way, we end up (after quite a few steps which are left to the reader) with the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & -\frac{5}{7} & \frac{2}{7} & \frac{2}{7} & \frac{2}{7} \\ 0 & 1 & 0 & 0 & \frac{2}{7} & -\frac{5}{7} & \frac{2}{7} & \frac{2}{7} \\ 0 & 0 & 1 & 0 & \frac{2}{7} & \frac{2}{7} & -\frac{5}{7} & \frac{2}{7} \\ 0 & 0 & 0 & 1 & \frac{2}{7} & \frac{2}{7} & \frac{2}{7} & -\frac{5}{7} \end{bmatrix}.$$

This shows that A is invertible and

$$A^{-1} = \begin{bmatrix} -\frac{5}{7} & \frac{2}{7} & \frac{2}{7} & \frac{2}{7} \\ \frac{2}{7} & -\frac{5}{7} & \frac{2}{7} & \frac{2}{7} \\ \frac{2}{7} & \frac{2}{7} & -\frac{5}{7} & \frac{2}{7} \\ \frac{2}{7} & \frac{2}{7} & \frac{2}{7} & -\frac{5}{7} \end{bmatrix}.$$

Let us take a closer look at this example, with another proof (this proof works in general when the coefficients of the matrix have sufficient symmetry). Let us consider solving the system $AX = Y$. This can be written

$$\begin{cases} x_1 + 2x_2 + 2x_3 + 2x_4 = y_1 \\ 2x_1 + x_2 + 2x_3 + 2x_4 = y_2 \\ 2x_1 + 2x_2 + x_3 + 2x_4 = y_3 \\ 2x_1 + 2x_2 + 2x_3 + x_4 = y_4 \end{cases}$$

We can easily solve this system by introducing

$$S = x_1 + x_2 + x_3 + x_4.$$

Then the equations become

$$2S - x_i = y_i, \quad 1 \leq i \leq 4.$$

Thus $x_i = 2S - y_i$. Taking into account that

$$S = x_1 + x_2 + x_3 + x_4 =$$

$$(2S - y_1) + (2S - y_2) + (2S - y_3) + (2S - y_4) = 8S - (y_1 + y_2 + y_3 + y_4),$$

we deduce that

$$S = \frac{y_1 + y_2 + y_3 + y_4}{7}$$

and so

$$x_1 = -\frac{5}{7}y_1 + \frac{2}{7}y_2 + \frac{2}{7}y_3 + \frac{2}{7}y_4$$

and similarly for x_2, x_3, x_4. This shows that for any choice of $Y \in \mathbf{R}^4$ the system $AX = Y$ is consistent. Thus A is invertible and the solution of the system is given by $X = A^{-1}Y$. If the first row of A^{-1} is (a, b, c, d), then

$$x_1 = ay_1 + by_2 + cy_3 + dy_4.$$

But since we know that

$$x_1 = -\frac{5}{7}y_1 + \frac{2}{7}y_2 + \frac{2}{7}y_3 + \frac{2}{7}y_4$$

and since y_1, y_2, y_3, y_4 are arbitrary, we deduce that

$$a = -\frac{5}{7}, \quad b = c = d = \frac{2}{7}.$$

In this way we can find the matrix A^{-1} and, of course, we obtain the same result as before (but the reader will have noticed that we obtain this result with much less effort!).

3.4.1 Problems for Practice

1. Is the matrix

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

invertible? If so, compute its inverse.

2. For which real numbers x is the matrix

$$A = \begin{bmatrix} 1 & x & 1 \\ 0 & 1 & x \\ 1 & 0 & 1 \end{bmatrix}$$

invertible? For any such number x, compute the inverse of A.

3. Let x, y, z be real numbers. Compute the inverse of the matrix

$$A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}.$$

4. Determine the inverse of the matrix

$$A = \begin{bmatrix} n & 1 & 1 & \dots & 1 \\ 1 & n & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & n \end{bmatrix} \in M_n(\mathbf{R}).$$

5. Let a be a real number. Determine the inverse of the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ a & 1 & 0 & \dots & 0 & 0 \\ a^2 & a & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a^{n-2} & a^{n-3} & a^{n-4} & \dots & 1 & 0 \\ a^{n-1} & a^{n-2} & a^{n-3} & \dots & a & 1 \end{bmatrix} \in M_n(\mathbf{R}).$$

Chapter 4
Vector Spaces and Subspaces

Abstract In this chapter we formalize and generalize many of the ideas encountered in the previous chapters, by introducing the key notion of vector space. The central focus is a good theory of dimension for vector spaces spanned by finitely many vectors. This requires a detailed study of spanning and linear independent families of vectors in a vector space.

Keywords Vector space • Vector subspace • Span • Linearly independent set • Dimension • Direct sum • Basis

In this chapter we formalize and generalize many of the ideas encountered in the previous chapters, by introducing the key notion of vector space. It turns out that many familiar spaces of functions are vector spaces, and developing an abstract theory of vector spaces has the advantage of being applicable to all these familiar spaces simultaneously. A good deal of work is required in order to define a good notion of dimension for vector spaces, but once the theory is developed, a whole family of nontrivial tools are at our disposal and can be used for a deeper study of vector spaces.

In all this chapter we fix a field $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{F}_2\}$, which the reader might want to take **R** or **C**, for simplicity. The elements of F are called **scalars**.

4.1 Vector Spaces-Definition, Basic Properties and Examples

We refer the reader to the appendix on algebraic preliminaries for the notion of group and commutative group (we will recall below everything we need, anyway). Let us simply recall that a commutative group $(V, +)$ is a set V endowed with an addition rule $+ : V \times V \to V$, denoted $(v, w) \to v + w$, and satisfying natural identities (which are supposed to mimic the properties of addition on integers, rational numbers, real numbers, etc.). We are now ready to introduce a fundamental definition, that of a vector space over a field F. The prototype example to keep in mind is F^n (n being any positive integer), which has already been introduced in the first chapter.

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_4

Definition 4.1. A **vector space over** F or an F**-vector space** is a commutative group $(V, +)$ endowed with a map $F \times V \to V$, called **scalar multiplication** and denoted $(a, v) \to a \cdot v$ such that for all $a, b \in F$ and $u, v \in V$ we have

a) $a \cdot (v + w) = a \cdot v + a \cdot w$ and $(a + b) \cdot v = a \cdot v + b \cdot v$.
b) $1 \cdot v = v$.
c) $(ab) \cdot v = a \cdot (b \cdot v)$.

The elements of V are called **vectors**.

Remark 4.2. 1) We usually write av instead of $a \cdot v$.
2) By definition, a vector space over F is nonempty!

Before giving quite a few examples of vector spaces we will make the definition more explicit and then try to explain different ways of understanding a vector space.

Thus a vector space over F is a set V, whose elements are called vectors, in which two operations can be performed

- addition, taking two vectors v, w and returning a vector $v + w$
- scalar multiplication, taking a scalar $c \in F$ and a vector $v \in V$, and returning the vector cv.

Moreover, the following properties/rules should hold:

1) addition is commutative: $v + w = w + v$ for all vectors $v, w \in V$.
2) addition is associative: $(u + v) + w = u + (v + w)$ for all vectors $u, v, w \in V$.
3) addition has an identity: there is a vector $0 \in V$ such that $0 + v = v + 0 = v$ for all $v \in V$.
4) there are additive inverses: for all $v \in V$ there is a vector $w \in V$ such that $v + w = 0$.
5) We have $1v = v$ for all $v \in V$.
6) For all scalars $a, b \in F$ and all $v \in V$ we have $(ab)v = a(bv)$.
7) Scalar multiplication is additive: for all scalars $a \in F$ and all $v, w \in V$ we have $a(v + w) = av + aw$.
8) scalar multiplication distributes over addition: for all scalars $a, b \in F$ and all $v \in V$ we have $(a + b)v = av + bv$.

One can hardly come up with a longer definition of a mathematical object, but one has to understand that most of the imposed conditions are natural and fairly easy to check. Actually, most of the time we will not even bother checking these conditions since they will be apparent on the description of the space V and its operations. The key point is that we simply want to add vectors and multiply them by scalars without having too many difficulties.

Remark 4.3. An important observation is that the addition $+ : V \to V$ is an **internal** operation, while the scalar multiplication $\cdot : F \times V \to V$ is an **external** operation.

Let us make a few simple, but important remarks concerning the previous rules. First of all, one should be careful to distinguish the scalar $0 \in F$ and the vector

$0 \in V$ which is the identity for the addition rule. Of course, they are denoted in exactly the same way, but they live in quite different worlds, so that there should not be any risk of confusion. Next, since addition is associative, we will not bother writing $((u+v)+w)+z$, but simply $u+v+w+z$.

Now let us focus a little bit on property 4. So let us start with any vector $v \in V$. Property 4 ensures the existence of a vector $w \in V$ for which $v+w=0$. A natural question is whether such a vector is unique. The answer is positive (and this holds in any group): suppose that w' is another such vector. Then using properties 2 (associativity) and 3 we obtain

$$w = w+0 = w+(v+w') = (w+v)+w' = 0+w' = w'.$$

Thus w is uniquely determined by v, and we will denote it as $-v$.

Another natural question is whether this vector $-v$ coincides with the vector $(-1)v$ obtained by multiplying v by the scalar -1. Since mathematical definitions are (usually) coherent, one expects that the answer is again positive, which is the case. Indeed, on the one hand properties 5 and 8 yield

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

and on the other hand property 8 gives

$$0v+0v = (0+0)v = 0v.$$

Adding $-0v$ to the previous relation we obtain $0v=0$, thus

$$0v = 0, \quad (-1)v = -v$$

for all $v \in V$. There are a lot of such formulae which can be obtained by simple algebraic manipulations straight from the definitions. Again, we will simplify notations and write $v-w$ for $v+(-w)$.

In the proof that $0v=0$ we used a trick which deserves to be glorified since it is very useful:

Proposition 4.4 (Cancellation law). *Let V be a vector space over F.*

a) If $v+u=w+u$ for some $u,v,w \in V$, then $v=w$.
b) If $au=av$ for some $v,w \in V$ and some ***nonzero*** *$a \in F$, then $u=v$.*

Proof. a) We have

$$v = v+0 = v+(u-u) = (v+u)-u = (w+u)-u = w+(u-u) = w+0 = w,$$

hence $v=w$, as desired.

b) Similarly, we have

$$u = 1\cdot u = (a^{-1}a)u = a^{-1}(au) = a^{-1}(av) = (a^{-1}a)v = 1\cdot v = v. \qquad \square$$

It is now time to see some **concrete vector spaces**. We have already encountered quite a few in previous chapters. Let us explain why. Let us fix a field F.

First, the field F itself is a vector space over F. Indeed, addition and multiplication on F satisfy all properties 1–8 by definition of a field! Note here that scalar multiplication coincides with the multiplication in F. The zero vector 0 in F coincides with the natural unit for addition in F.

Another very important class of vector spaces over F occurs as follows: let K be a field containing F. Then K is a vector space over F, for essentially the same reasons as in the previous paragraph. Important examples of this situation are $\mathbf{Q} \subset \mathbf{R}$, $\mathbf{R} \subset \mathbf{C}$, $\mathbf{Q} \subset \mathbf{C}$. Thus $\mathbf{R}$ is a vector space over $\mathbf{Q}$, $\mathbf{C}$ is a vector space over $\mathbf{R}$, $\mathbf{C}$ is a vector space over $\mathbf{Q}$.

Next, consider a positive integer n and recall that F^n is the set of n-tuples of elements of F, written in column form, $X = \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix}$. We add two such vectors component-wise and we re-scale them by scalars in F component-wise

$$\begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \cdots \\ x_n + y_n \end{bmatrix} \quad \text{and} \quad c \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix} = \begin{bmatrix} cx_1 \\ cx_2 \\ \cdots \\ cx_n \end{bmatrix}.$$

It is not difficult to check that properties 1–8 are all satisfied: they all follow from the corresponding properties of addition and multiplication in F, since all operations are defined component-wise. Thus F^n is a vector space for these two operations. Its zero vector 0 is the vector $\begin{bmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{bmatrix}$ having all coordinates equal to 0.

Consider next the set $V = M_{m,n}(F)$ of $m \times n$ matrices with entries in F, where m, n are given positive integers. Recall that addition and scalar multiplication on V are defined component-wise by

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}] \quad \text{and} \quad c[a_{ij}] = [ca_{ij}]$$

for matrices $[a_{ij}], [b_{ij}] \in V$ and scalars $c \in F$. Again, all properties $1 - -8$ follow from the corresponding properties of the operations in F. The zero vector in V is the matrix $O_{m,n}$ all of whose entries are equal to 0.

We consider now **function spaces**. In complete generality, let X be any nonempty set and consider the set $V = F^X$ of functions $f : X \to F$. We can define addition and scalar multiplication on V by the rules

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (cf)(x) = cf(x)$$

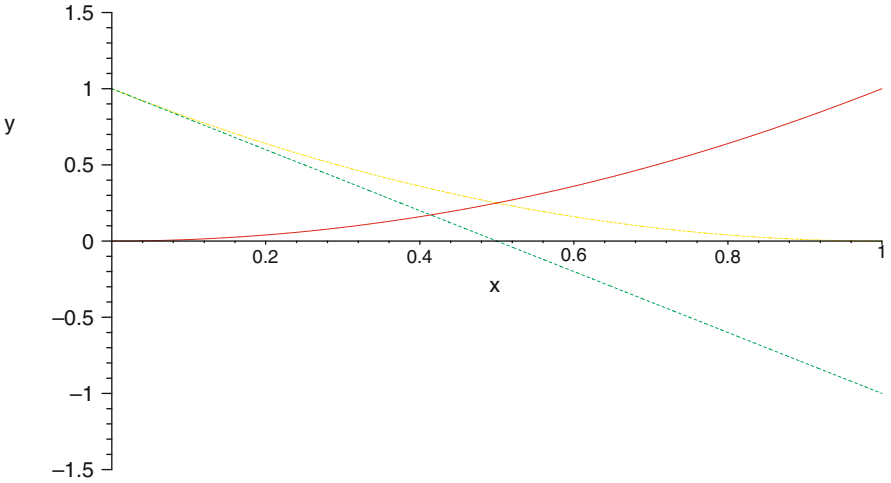

Fig. 4.1 The functions $f(x) = x^2$, $g(x) = 1 - 2x$ and their sum $(f + g)(x) = x - 2x + 1$

for $c \in F$ and $x \in X$. Then V is a vector space over F, again thanks to the fact that all operations are induced directly from the corresponding operations in F. The zero vector 0 of V is the map $0 : X \to F$ sending every $x \in X$ to $0 \in F$. Note that for $X = \{1, 2, \ldots, n\}$ we recover the space F^n: giving a map $f : \{1, 2, \ldots, n\} \to F$ is the same as giving a n-tuple of elements of F (namely the images of $1, 2, \ldots, n$), that is an element of F^n.

One can impose further natural properties on the maps $f : X \to F$ and still get vector spaces, contained in F^X. For instance, consider the set $\mathsf{C}[0, 1]$ of real-valued continuous functions on the interval $[0, 1]$. Thus an element of $\mathsf{C}[0, 1]$ is a continuous map $f : [0, 1] \to \mathbf{R}$. The addition and scalar multiplication are inherited from those on the vector space $\mathbf{R}^{[0,1]}$ of all real-valued maps on $[0, 1]$. For example, if $f(x) = x^2$ and $g(x) = 1 - 2x$, then $(f + g)(x) = x^2 - 2x + 1$, for all x in the interval $[0, 1]$ (see Fig. 4.1).

As another example, the function f given by $f(x) = \sin 5\pi x$ and its re-scaling $-\frac{3}{2}f$ are depicted in Fig. 4.2.

The key point is that the sum of two continuous maps is still a continuous map, and if f is continuous and c is a real number, then cf is also continuous. This ensures that the addition and scalar multiplication laws are well defined on $\mathsf{C}[0, 1]$. They satisfy all properties 1–8, since these properties are already satisfied on the larger space $\mathbf{R}^{[0,1]}$. Then $\mathsf{C}[0, 1]$ is itself a vector space over $\mathbf{R}$, contained in $\mathbf{R}^{[0,1]}$. This is an example of **vector subspace** of a vector space, a crucial notion which will be introduced and studied at length in the sequel.

There is nothing special about the interval $[0, 1]$: for each interval I we obtain a vector space of continuous real-valued maps on I. If the real numbers are replaced with complex numbers, we obtain a corresponding vector space of complex-valued continuous maps on I.

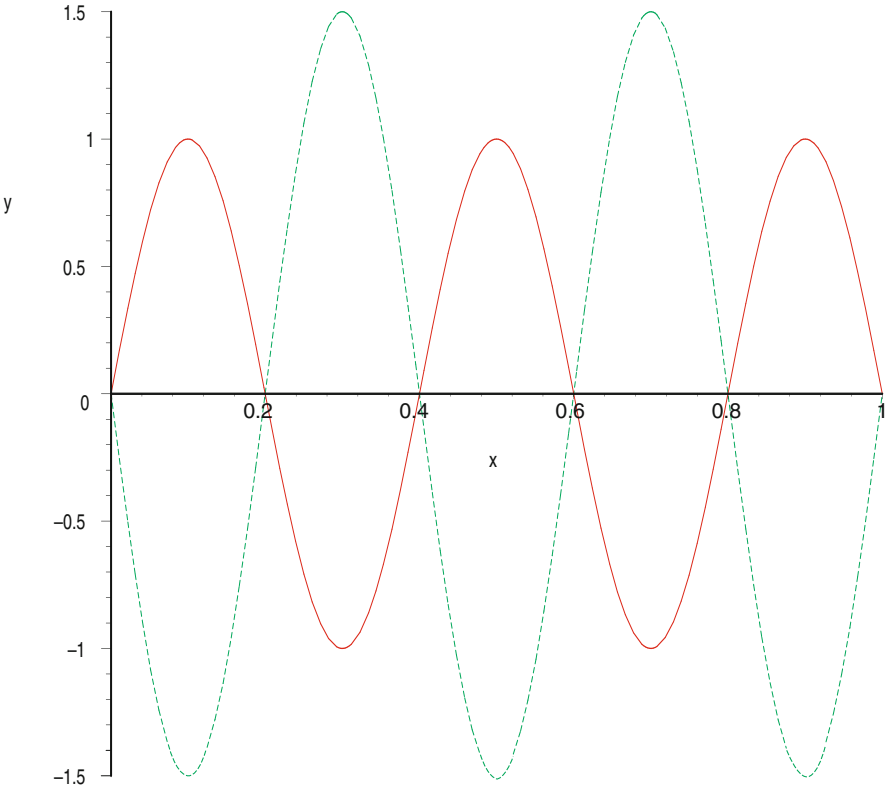

Fig. 4.2 The function $f(x) = \sin 5\pi x$ and its re-scaling by a factor of $-\frac{3}{2}$

In fact, there are many other function spaces: we could consider the vector space of piecewise continuous functions, differentiable functions, bounded functions, integrable functions, etc, as long as any two functions in such a space add up to another function in the same space and re-scaling of a function in the space is another function in the space. The possibilities are endless.

Let us consider now another very important class of vector spaces, namely **spaces of polynomials**. Consider the set $\mathbf{R}[X]$ of polynomials in one variable and having real coefficients. This set is a vector space over $\mathbf{R}$. Recall that the addition and re-scaling of polynomials are done coefficient-wise, so the fact that $\mathbf{R}[X]$ is a vector space over $\mathbf{R}$ follows directly from the fact that $\mathbf{R}$ itself is a field. The zero vector in $\mathbf{R}[X]$ is the zero polynomial (i.e., the polynomial all of whose coefficients are 0).

The vector space $\mathbf{R}[X]$ contains a whole bunch of other vector spaces over $\mathbf{R}$: for each nonnegative integer n consider the set $\mathbf{R}_n[X]$ of polynomials in $\mathbf{R}[X]$ whose degree does not exceed n. For example the polynomials

$$1 + X^2, \qquad \frac{3}{4}X + \pi X^2, \qquad 1 - X - X^3$$

are all in $\mathbf{R}_3[X]$, only the first two are in $\mathbf{R}_2[X]$ and none of them is in $\mathbf{R}_1[X]$. Since the sum of two polynomials of degree at most n is a polynomial of degree at most n, and since $\deg(cP) \leq n$ for any real number c and any $P \in \mathbf{R}_n[X]$, we deduce that $\mathbf{R}_n[X]$ is stable under the addition and scalar multiplication defined on $\mathbf{R}[X]$, thus it forms itself a vector space over $\mathbf{R}$. To be completely explicit, any polynomial in $\mathbf{R}_n[X]$ can be written in the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

where a_i, $0 \leq i \leq n$, are real numbers, and then

$$(a_0 + a_1X + \cdots + a_nX^n) + (b_0 + b_1X + \cdots + b_nX^n)$$

$$= (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n$$

and for $c \in F$

$$c(a_0 + a_1X + \cdots + a_nX^n) = (ca_0) + (ca_1)X + \cdots + (ca_n)X^n.$$

4.1.1 Problems for Practice

1. Consider the set $V = \mathbf{R}^2$ endowed with an addition rule defined by

   $$(x, y) + (x', y') = (x + x', y + y')$$

   and with a multiplication rule by elements λ of $\mathbf{R}$ as follows

   $$\lambda \cdot (x, y) = (2x, 0).$$

   Is V endowed with these operations a vector space over $\mathbf{R}$?
2. Define an operation $+_*$ on $(0, \infty)$ by

   $$a +_* b = ab$$

   for $a, b \in (0, \infty)$, and an external multiplication by real numbers as follows

   $$a \cdot_* b = b^a$$

   for $a \in \mathbf{R}, b \in (0, \infty)$. Does $(0, \infty)$ endowed with this new addition and scalar multiplication become a vector space over $\mathbf{R}$?

3. (Complexification of a real vector space) Let V be a vector space over $\mathbf{R}$. Let $V_{\mathbf{C}}$ be the product $V \times V$ (this is the set of ordered pairs (x, y) of elements of V) endowed with the following addition rule

$$(x, y) + (x', y') = (x + x', y + y').$$

Also, for each complex number $z = a + ib$, consider the "multiplication by z rule"

$$z \cdot (x, y) := (ax - by, ay + bx)$$

on $V_{\mathbf{C}}$. Prove that $V_{\mathbf{C}}$ endowed with these operations becomes a $\mathbf{C}$-vector space (this space is called the **complexification of the vector space** V).

4.2 Subspaces

We have already seen in the previous subsection a lot of subspaces of concrete vector spaces. In this section we formalize the concept of vector subspace of a given vector space and then study some of its basic properties.

Definition 4.5. Let V be an F-vector space. A **subspace** of V is a nonempty subset W of V which is stable under the operations of addition and scalar multiplication: $v + w \in W$ and $cv \in W$ for all $v, w \in W$ and $c \in F$.

Example 4.6. Let V be the vector space over $\mathbf{R}$ of all maps $f : \mathbf{R} \to \mathbf{R}$. Then the following sets V_1, V_2, V_3, V_4 are subspaces over $\mathbf{R}$.

I) $V_1 = \{f \in V \mid f \text{ is a continuous function on } \mathbf{R}\}$.
II) $V_2 = \{f \in V \mid f \text{ is a differentiable function on } \mathbf{R}\}$.
III) $V_3 = \{f \in V \mid f \text{ is an integrable function on the interval } [a, b],$ where $a, b \in \mathbf{R}\}$.
IV) $V_4 = \{f \in V \mid \text{ there exists } \theta \in \mathbf{R} \text{ such that } |f(x)| \leq \theta, \ \forall\, x \in \mathbf{R}\}$.

The previous definition invites a whole series of easy observations, which are however very useful in practice.

Remark 4.7. 1. First, note that a vector subspace of a vector space **must contain the zero vector**. Indeed, say W is a vector subspace of V. Since W is nonempty, there is $v \in W$, but then $0 = 0v \in W$. Thus if a subset W of a vector space V does not contain the zero vector, then this subset W has no chance of being a vector subspace of V.

2. Next, a key observation is that **if W is a subspace of V, then W becomes itself an F-vector space, by restricting the operations in V to W**. Indeed, since properties 1–8 in the definition of a vector space are satisfied in V, they are automatically satisfied in the subset W of V. This was essentially implicitly used

(or briefly explained) in the previous section, where many examples of vector spaces were constructed as vector subspaces of some standard vector spaces.

3. In practice, one can avoid checking two conditions (stability under addition and under scalar multiplication) by checking only one: $v + cw \in W$ whenever $v, w \in W$ and $c \in F$. More generally, a nonempty subset W of V is a vector subspace if and only if

$$av + bw \in W$$

for all $a, b \in F$ and $v, w \in W$. We deduce by induction on n that if W is a vector subspace of V and $w_1, \ldots, w_n \in W$ and $c_1, \ldots, c_n \in F$, then $c_1 w_1 + \ldots + c_n w_n \in W$.

4. Another very important observation is the **stability under arbitrary intersections** of vector subspaces. More precisely, if $(W_i)_{i \in I}$ is a family of subspaces of V, then

$$W := \cap_{i \in I} W_i$$

is again a subspace of V. Indeed, W is nonempty because it contains 0 (as any subspace of V contains 0) and clearly W is stable under addition and scalar multiplication, since each W_i has this property.

Problem 4.8. Consider the vector space $V = \mathbf{R}^3$ over $\mathbf{R}$ and the subsets V_1, V_2 defined by

$$V_1 = \{(x, y, z) \in \mathbf{R}^3 \mid x + y + z = 1\}$$

$$V_2 = \{(x, y, z) \in \mathbf{R}^3 \mid x + 2y + z > \sqrt{2}\}.$$

Which (if either) of these is a subspace of V?

Solution. Neither V_1 nor V_2 contain $(0, 0, 0)$, thus they are not subspaces of V. □

Problem 4.9. Let $V = \mathbf{R}^3$ and

$$U = \{(x, y, z) \in \mathbf{R}^3 \mid x^2 + y^2 + z^2 \leq 1\}.$$

Is U a subspace of V?

Solution. U is not a subspace of V, since the vector $u = (1, 0, 0)$ belongs to U, but the vector $2u = (2, 0, 0)$ does not belong to U. □

Problem 4.10. Determine if W is a subspace of V where

(a) $V = \mathsf{C}[0, 1]$ and W consists in those functions f in V for which $f(0) = 0$.
(b) $V = \mathsf{C}[0, 1]$ and W consists in those functions f in V for which $f(1) = 1$.

(c) $V = \mathsf{C}[0,1]$ and W consists in those functions f in V for which

$$\int_0^1 f(x)\,dx = 0.$$

(d) $V = \mathsf{C}[0,1]$ and W consists in those functions f in V for which

$$\int_0^1 f(x)\,dx = 1.$$

(e) V is the space of three times differentiable functions on $[0,1]$ and W consists in those functions in V whose third derivative is 0.

Solution. a) If $f(0) = 0$ and $g(0) = 0$, then $(f + cg)(0) = 0$ for all $c \in \mathbf{R}$, and $f + cg$ is a continuous map. Thus W is a subspace of V.
b) W does not contain the zero element of V (which is the constant map equal to 0), thus W is not a subspace of V.
c) If $f, g \in W$, then for all $c \in \mathbf{R}$ the map $f + cg$ is continuous and

$$\int_0^1 (f + cg)(x)dx = \int_0^1 f(x)dx + c\int_0^1 g(x)dx = 0,$$

thus $f + cg \in W$. It follows that W is a subspace of V.
d) W does not contain the zero map in V, thus it is not a subspace of V.
e) If f, g are three times differentiable and the third derivative is 0, then $f + cg$ has the same property for all real numbers c, since $(f + cg)^{(3)} = f^{(3)} + cg^{(3)}$. Thus W is a subspace of V (consisting actually of polynomial functions of degree at most 2). □

Problem 4.11. Let U and V be the sets of vectors

$$U = \{\, (x_1, x_2) \mid x_1, x_2 \geq 0 \,\} \quad \text{and} \quad V = \{\, (x_1, x_2) \mid x_1 x_2 \geq 0 \,\}$$

in $\mathbf{R}^2$.

(a) Show that U is closed under addition.
(b) Show that V is closed under re-scaling.
(c) Show that neither U nor V is a subspace of $\mathbf{R}^2$.

Solution. It is clear that U is stable under addition, since nonnegative real numbers are closed under addition. To see that V is closed under re-scaling, consider a scalar c and $v = (x_1, x_2)$ in V. Then $cv = (cx_1, cx_2)$ and $(cx_1)(cx_2) = c^2 x_1 x_2 \geq 0$ because $c^2 \geq 0$ and $x_1 x_2 \geq 0$.

U is not a subspace of $\mathbf{R}^2$ as $v = (1,1) \in U$ but $-v = (-1)v \notin U$. V is not a subspace of $\mathbf{R}^2$ since $v_1 = (2,2) \in V$, $v_2 = (-1,-3) \in V$, but $v_1 + v_2 = (1,-1) \notin V$. □

The **union** of two subspaces W_1, W_2 of V is **almost never** a subspace of V, as the following problem shows.

Problem 4.12. Let V be a vector space over a field F and let V_1, V_2 be subspaces of V. Prove that the union of V_1, V_2 is a subspace of V if and only if

$$V_1 \subseteq V_2 \quad \text{or} \quad V_2 \subseteq V_1.$$

Solution. If $V_1 \subseteq V_2$ (resp. $V_2 \subseteq V_1$), then $V_1 \cup V_2 = V_2$ (resp. $V_1 \cup V_2 = V_1$). Therefore in both cases $V_1 \cup V_2$ is a subspace of V.

Conversely, suppose that $V_1 \cup V_2$ is a subspace of V. If $V_1 \subset V_2$, then we are done, so suppose that this is not the case. Thus we can find $v \in V_1$ which does not belong to V_2. We will prove that $V_2 \subset V_1$.

Take any vector $x \in V_2$. Since $V_1 \cup V_2$ is a subspace of V containing x and v, it contains their sum $x + v$. Thus $x + v \in V_1$ or $x + v \in V_2$. If $x + v \in V_2$, then $v = (x + v) - x \in V_2$, since V_2 is a subspace of V. This contradicts the choice of v, thus we must have $x + v \in V_1$. Since $v \in V_1$, we also have $-v \in V_1$ and so $x = (x + v) - v \in V_1$. Thus any element of V_2 belongs to V_1 and we have $V_2 \subset V_1$, as desired. □

We now define a very important operation on subspaces of an F-vector space:

Definition 4.13. Let $W_1, W_2, \ldots, W_n$ be subspaces of a vector space V. Their sum $W_1 + W_2 + \ldots + W_n$ is the subset of V consisting of all vectors $w_1 + w_2 + \ldots + w_n$ with $w_1 \in W_1, \ldots, w_n \in W_n$.

One could extend the previous definition to an arbitrary family $(W_i)_{i \in I}$ of subspaces of V. In this case $\sum_{i \in I} W_i$ consists of all sums $\sum_{i \in I} w_i$ with $w_i \in W_i$ for all $i \in I$ **and all but finitely many of the vectors** w_i **are zero**, so that the sum $\sum_{i \in I} w_i$ has only finitely many nonzero terms and thus makes sense, even if I if infinite. In practice we will however deal with finite collections of subspaces. The following result also holds for infinite families of vector subspaces, but in the sequel we prefer to focus on finite families, for simplicity.

Proposition 4.14. *If $W_1, W_2, \ldots, W_n$ are subspaces of a vector space V, then $W_1 + W_2 + \ldots + W_n$ is a subspace of V.*

Proof. Let us denote for simplicity $S = W_1 + W_2 + \ldots + W_n$. Let $s, s' \in S$ and let c be a scalar. It remains to prove that $s + cs' \in S$. By definition, we can find $w_1, \ldots, w_n$ and $w_1', \ldots, w_n'$ such that $w_i, w_i' \in W_i$ for $1 \leq i \leq n$ and

$$s = w_1 + w_2 + \ldots + w_n, \quad s' = w_1' + w_2' + \ldots + w_n'.$$

Then

$$s + cs' = w_1 + w_2 + \ldots + w_n + c(w_1' + w_2' + \ldots + w_n') =$$

$$w_1 + w_2 + \ldots + w_n + cw_1' + cw_2' + \ldots + cw_n' = (w_1 + cw_1') + \ldots + (w_n + cw_n').$$

Since W_i is a subspace of V and since $w_i, w_i' \in W_i$, it follows that $w_i + cw_i' \in W_i$ for all $1 \leq i \leq n$. The previous displayed formula expresses therefore $s + cs'$ as a sum of vectors in $W_1, \ldots, W_n$ and shows that $s + cs' \in S$. This finishes the proof that S is a subspace of V. □

Problem 4.15. Prove that $W_1 + W_2 + \ldots + W_n$ is the smallest subspace of V containing all subspaces $W_1, \ldots, W_n$.

Solution. It is clear that $W_1 + \ldots + W_n$ contains $W_1, W_2, \ldots, W_n$, since each vector w_i of W_i can be written as $0+0+\ldots+0+w_i+0+\ldots+0$ and $0 \in W_1 \cap \ldots \cap W_n$. We need to prove that if W is any subspace of V which contains each of the subspaces $W_1, \ldots, W_n$, then W contains $W_1+W_2+\ldots+W_n$. Take any vector v of $W_1+\ldots+W_n$. By definition, we can write $v = w_1 + w_2 + \ldots + w_n$ for some vectors $w_i \in W_i$. Since W contains $W_1, \ldots, W_n$, it contains each of the vectors $w_1, \ldots, w_n$. And since W is a subspace of V, it must contain their sum, which is v. We proved that any element of $W_1 + \ldots + W_n$ belongs to W, thus $W_1 + \ldots + W_n \subset W$ and the result follows. □

We now introduce a second crucial notion, that of **direct sum of subspaces**:

Definition 4.16. Let $W_1, W_2, \ldots, W_n$ be subspaces of a vector space V. We say that $W_1, W_2, \ldots, W_n$ are **in direct sum position** if the equality

$$w_1 + w_2 + \ldots + w_n = 0$$

with $w_1 \in W_1, \ldots, w_n \in W_n$ forces $w_1 = w_2 = \ldots = w_n = 0$.

There are quite a few different ways of expressing this condition. Here is one of them:

Proposition 4.17. *Subspaces $W_1, \ldots, W_n$ of a vector space V are in direct sum position if and only if every element of $W_1 + W_2 + \ldots + W_n$ can be uniquely written as a sum $w_1 + \ldots + w_n$ with $w_1 \in W_1, \ldots, w_n \in W_n$.*

Proof. Suppose that $W_1, \ldots, W_n$ are in direct sum position and take an element v of $W_1 + \ldots + W_n$. By definition we can express $v = w_1 + \ldots + w_n$ with $w_i \in W_i$ for all $1 \leq i \leq n$. Suppose that we can also write $v = w_1' + \ldots + w_n'$ with $w_i' \in W_i$. We need to prove that $w_i = w_i'$ for all $1 \leq i \leq n$. Subtracting the two relations yields

$$0 = v - v = (w_1 - w_1') + (w_2 - w_2') + \ldots + (w_n - w_n').$$

Let $u_i = w_i - w_i'$. Since W_i is a subspace of V, we have $u_i \in W_i$. Moreover, $u_1 + \ldots + u_n = 0$. Since $W_1, \ldots, W_n$ are in direct sum position, it follows that $u_1 = \ldots = u_n = 0$, and so $w_i = w_i'$ for all $1 \leq i \leq n$, which is what we needed.

Conversely, suppose every element of $W_1+W_2+\cdots+W_n$ can be written uniquely as a sum of elements of $W_1, \ldots, W_n$. Then $0 = 0 + 0 + \cdots 0$ must be the unique

decomposition of 0. Thus whenever $w_1 \in W_1$, $w_2 \in W_2, \ldots, w_n \in W_n$ satisfy $w_1 + w_2 + \cdots + w_n = 0$, we have $w_1 = w_2 = \cdots = w_n = 0$. Thus $W_1, \ldots, W_n$ are in direct sum position. □

Finally, we make another key definition:

Definition 4.18. a) We say that a vector space V is the **direct sum** of its subspaces $W_1, W_2, \ldots, W_n$ and write

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$$

if $W_1, W_2, \ldots, W_n$ are in direct sum position and $V = W_1 + W_2 + \ldots + W_n$.

b) If V_1, V_2 are subspaces of a vector space V, we say that V_2 is a **complement** (or **complementary subspace**) of V_1 if $V_1 \oplus V_2 = V$.

By the previous results, $V = W_1 \oplus \ldots \oplus W_n$ if and only if every vector $v \in V$ can be **uniquely** written as a sum $w_1 + w_2 + \ldots + w_n$, with $w_i \in W_i$ for all i. Hence, if V_1, V_2 are subspaces of V, then V_2 is a complement of V_1 if and only if every vector $v \in V$ can be uniquely expressed as $v = v_1 + v_2$ with $v_1 \in V_1$ and $v_2 \in V_2$.

The result of the following problem is extremely useful in practice.

Problem 4.19. Prove that V_2 is a complement of V_1 if and only if $V_1 + V_2 = V$ and $V_1 \cap V_2 = \{0\}$.

Solution. Assume that V_2 is a complement of V_1, thus $V = V_1 \oplus V_2$ and each $v \in V$ can be uniquely written as the sum of an element of V_1 and an element of V_2. This clearly implies that $V_1 + V_2 = V$. If $v \in V_1 \cap V_2$, then we can write $v = v + 0 = 0 + v$ and by uniqueness $v = 0$, thus $V_1 \cap V_2 = \{0\}$.

Conversely, assume that $V_1 \cap V_2 = \{0\}$ and $V_1 + V_2 = V$. The second relation implies that each vector of V is the sum of a vector in V_1 and one in V_2. Assume that $v \in V$ can be written both $v_1 + v_2$ and $v_1' + v_2'$ with $v_1, v_1' \in V_1$ and $v_2, v_2' \in V_2$. Then $v_1 - v_1' = v_2' - v_2$. Now the left-hand side belongs to V_1 while the right-hand side belongs to V_2, thus they both belong to $V_1 \cap V_2 = \{0\}$ and so $v_1 = v_1'$ and $v_2 = v_2'$, giving the desired uniqueness result. □

Example 4.20. 1. The vector space $V = \mathbf{R}^2$ is the direct sum of its subspaces $V_1 = \{(x, 0) \mid x \in \mathbf{R}\}$ and $V_2 = \{(0, y) \mid y \in \mathbf{R}\}$. Indeed, any $(x, y) \in \mathbf{R}^2$ can be uniquely in the form $(a, 0) + (0, b)$, via $a = x$ and $b = y$.

2. Let $V = M_n(\mathbf{R})$ be the vector space of $n \times n$ matrices with real entries. If V_1 and V_2 are the subspaces of symmetric, respectively skew-symmetric matrices, then $V = V_1 \oplus V_2$. Indeed, any matrix $A \in V$ can be uniquely written as the sum of a symmetric matrix and a skew-matrix matrix: the only way to have $A = B + C$ with B symmetric and C skew-symmetric is via $B = \frac{1}{2}(A + {}^tA)$ and $C = \frac{1}{2}(A - {}^tA)$.

3. Let V be the vector space of all real-valued maps on $\mathbf{R}$. Let V_1 (respectively V_2) be the subspace of V consisting in even (respectively odd) functions. Recall that a map $f : \mathbf{R} \to \mathbf{R}$ is even (respectively odd) if $f(x) = f(-x)$ for all

x (respectively $f(-x) = -f(x)$ for all x). Then $V = V_1 \oplus V_2$. Indeed, for any map f, the only way to write $f = g + h$ with g even and h odd is via $g(x) = \frac{f(x)+f(-x)}{2}$ and $h(x) = \frac{f(x)-f(-x)}{2}$.

Problem 4.21. Let V be the space of continuous real-valued maps on $[-1, 1]$ and let

$$V_1 = \{f \in V | \int_{-1}^{1} f(t)dt = 0\}$$

and V_2 be the subset of V consisting of constant functions.

a) Prove that V_1, V_2 are subspaces of V.
b) Prove that $V = V_1 \oplus V_2$.

Solution. a) If f_1, f_2 are in V_1 and $c \in \mathbf{R}$, then $cf_1 + f_2$ is continuous and

$$\int_{-1}^{1} (cf_1 + f_2)(t)dt = c \int_{-1}^{1} f_1(t)dt + \int_{-1}^{1} f_2(t)dt = 0,$$

thus $cf_1 + f_2 \in V_1$ and V_1 is a subspace of V. It is clear that V_2 is a subspace of V.

b) By the previous problem, we need to check that $V_1 \cap V_2 = \{0\}$ and $V = V_1 + V_2$. Assume that $f \in V_1 \cap V_2$, thus f is constant and $\int_{-1}^{1} f(t)dt = 0$. Say $f(t) = c$ for all $t \in [-1, 1]$, then

$$0 = \int_{-1}^{1} f(t)dt = 2c,$$

thus $c = 0$ and $f = 0$. This shows that $V_1 \cap V_2 = \{0\}$.

In order to prove that $V = V_1 + V_2$, let $f \in V$ and let us try to write $f = c + g$ with c a constant and $g \in V_1$. We need to ensure that

$$\int_{-1}^{1} g(t)dt = 0,$$

that is

$$\int_{-1}^{1} (f(t) - c)dt = 0.$$

It suffices therefore to take

$$c = \frac{1}{2} \int_{-1}^{1} f(t)dt$$

and $g = f - c$. □

4.2.1 Problems for Practice

1. Show that none of the following sets of vectors is a subspace of $\mathbf{R}^3$:
   (a) The set U of vectors $x = (x_1, x_2, x_3)$ such that $x_1^2 + x_2^2 + x_3^2 = 1$.
   (b) The set V of vectors in $\mathbf{R}^3$ all of whose coordinates are integers.
   (c) The set W of vectors in $\mathbf{R}^3$ that have at least one coordinate equal to 0.
2. Determine if U is a subspace of $M_2(\mathbf{R})$, where
   (a) U is the set of 2×2 matrices such that the sum of the entries in the first column is 0.
   (b) U is the set of 2×2 matrices such that the product of the entries in the first column is 0.
3. Is $\mathbf{R}$ a subspace of the $\mathbf{C}$-vector space $\mathbf{C}$?
4. Let V be the set of all periodic sequences of real numbers. Is V a subspace of the space of all sequences of real numbers?
5. Let V be the set of vectors $(x, y, z) \in \mathbf{R}^3$ such that $x(y^2 + z^2) = 0$. Is V a subspace of $\mathbf{R}^3$?
6. Let V be the set of twice differentiable functions $f : \mathbf{R} \to \mathbf{R}$ such that for all x we have
$$f''(x) + x^2 f'(x) - 3f(x) = 0.$$
   Is V a subspace of the space of all maps $f : \mathbf{R} \to \mathbf{R}$?
7. Let V be the set of differentiable functions $f : \mathbf{R} \to \mathbf{R}$ such that for all x we have
$$f'(x) - f(x)^2 = x.$$
   Is V a subspace of the space of all maps $f : \mathbf{R} \to \mathbf{R}$?
8. a) Is the set of bounded sequences of real numbers a vector subspace of the space of all sequences of real numbers?
   b) Answer the same question if instead of bounded sequences we consider monotonic sequences.
9. Let V be the set of all sequences $(x_n)_{n \geq 0}$ of real numbers such that
$$x_{n+2} + n x_{n+1} - (n-1)x_n = 0$$
   for all $n \geq 0$. Prove that V is a subspace of the space of all sequences of real numbers.
10. Let V be the space of all real-valued maps on $\mathbf{R}$ and let W be the subset of V consisting of maps f such that $f(0) + f(1) = 0$.
    a) Check that W is a subspace of V.
    b) Find a subspace S of V such that $V = W \oplus S$.

11. Let V be the space of continuously differentiable maps $f : \mathbf{R} \to \mathbf{R}$ and let W be the subspace of those maps f for which $f(0) = f'(0) = 0$. Let Z be the subspace of V consisting of maps $x \mapsto ax + b$, with $a, b \in \mathbf{R}$. Prove that $V = W \oplus Z$.
12. Let V be the space of convergent sequences of real numbers. Let W be the subset of V consisting of sequences converging to 0 and let Z be the subset of V consisting of constant sequences. Prove or disprove that W, Z are subspaces of V and $W \oplus Z = V$.
13. (**Quotient space**) Let V be a vector space over F and let $W \subset V$ be a subspace. For a vector $v \in V$, let $[v] = \{v + w : w \in W\}$. Note that $[v_1] = [v_2]$ if $v_1 - v_2 \in W$. Define the quotient space V/W to be $\{[v] : v \in V\}$. Define an addition and scalar multiplication on V/W by $[u] + [v] = [u + v]$ and $a[v] = [av]$. Prove that the addition and multiplication above are well defined and V/W equipped with these operations is a vector space.
14. Let $F \in \{\mathbf{R}, \mathbf{C}\}$ and let V be a nonzero vector space over F. Suppose that V is the union of finitely many subspaces of V. Prove that one of these subspaces is V.

4.3 Linear Combinations and Span

Let V be a vector space over a field F and let $v_1, v_2, \ldots, v_n$ be vectors in V. By definition, V contains all vectors $c_1v_1 + \ldots + c_nv_n$, with $c_1, \ldots, c_n \in F$. The collection of all these vectors plays a very important role in the sequel and so deserves a formal definition:

Definition 4.22. Let $v_1, v_2, \ldots, v_n$ be vectors in a vector space V over F.

a) A vector $v \in V$ is a **linear combination of** $v_1, v_2, \ldots, v_n$ if there are scalars $c_1, c_2, \ldots, c_n \in F$ such that

$$v = c_1v_1 + c_2v_2 + \ldots + c_nv_n \tag{4.1}$$

b) The **span** of $v_1, \ldots, v_n$ is the subset of V consisting in all linear combinations of $v_1, v_2, \ldots, v_n$. It is denoted $\mathrm{Span}(v_1, v_2, \ldots, v_n)$.

Example 4.23. 1) The span $\mathrm{Span}(v)$ of a single vector v in $\mathbf{R}^m$ consists in all re-scaled copies of v (we also say all scalar multiples of v). Using the geometric interpretation of vectors in $\mathbf{R}^2$ (or $\mathbf{R}^3$), if $v \neq 0$ then $\mathrm{Span}(v)$ is represented by the line through the origin in the direction of the vector v.
2) Let $e_1 = (1, 0, 0)$ and $e_2 = (0, 1, 0)$. Then

$$x_1e_1 + x_2e_2 = (x_1, x_2, 0).$$

Since x_1 and x_2 are arbitrary we see that $\text{Span}(e_1, e_2)$ consists in all vectors in $\mathbf{R}^3$ whose third coordinate is 0. This is the x_1x_2-plane in $\mathbf{R}^3$. In general, if two vectors v_1 and v_2 in $\mathbf{R}^3$ are not collinear, then their span is the unique plane through the origin that contains them.

Problem 4.24. Show that the vector $(1, 1, 1)$ cannot be expressed as a linear combination of the vectors

$$v_1 = (1, 0, 0), \qquad v_2 = (0, 1, 0) \qquad \text{and} \qquad v_3 = (1, 1, 0).$$

Solution. An arbitrary linear combination

$$x_1v_1 + x_2v_2 + x_3v_3 = (x_1 + x_3, x_2 + x_3, 0)$$

of v_1, v_2 and v_3 has 0 as the third coordinate, and so cannot be equal to $(1, 1, 1)$. □

More generally, let us consider the following practical problem: given a family of vectors $v_1, v_2, \ldots, v_k$ in F^n and a vector $v \in F^n$, decide whether this vector is a linear combination of $v_1, \ldots, v_k$, that is $v \in \text{Span}(v_1, \ldots, v_k)$. Consider the $n \times k$ matrix A whose columns are $v_1, \ldots, v_k$. Saying that $v \in \text{Span}(v_1, \ldots, v_k)$ is the same as saying that we can find $x_1, \ldots, x_k \in F$ such that $v = x_1v_1 + \ldots + x_kv_k$, or equivalently the system $AX = v$ is consistent (and then $x_1, \ldots, x_k$ are given by the coordinates of X). Since we have a practical way of deciding whether this system is consistent (via row-reduction of the augmented matrix $[A|v]$), we see that we have an algorithmic solution to the previous problem. Of course, we can solve the previous problem via this method, too.

Problem 4.25. Consider the vectors $v_1 = (1, 0, 1, 2)$, $v_2 = (3, 4, 2, 1)$ and $v_3 = (5, 8, 3, 0)$. Is the vector $v = (1, 0, 0, 0)$ in the span of $\{v_1, v_2, v_3\}$? What about the vector $w = (4, 4, 3, 3)$?

Solution. In order to solve this problem, we use the method described above. Namely, we consider the matrix

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

We want to know if the system $AX = v$ is consistent. The row-reduction of the augmented matrix $[A|v]$ is

$$[A|v] \sim \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Looking at the third row in the matrix appearing in the right-hand side, we see that the system is not consistent, thus v is not in the span of $\{v_1, v_2, v_3\}$.

For the vector w, we use the same method. The row-reduction of the augmented matrix $[A|w]$ is now

$$[A|w] \sim \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

which shows that the system is consistent and so w is in the span of $\{v_1, v_2, v_3\}$. If we want to explicitly find the linear combination of v_1, v_2, v_3 giving w, all we need is to solve the system

$$\begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

This yields without any problem $x_1 = x_3 + 1$ and $x_2 = 1 - 2x_3$. Thus we can write

$$w = (1 + x_3)v_1 + x_2v_2 + (1 - 2x_3)v_3$$

and this for any choice of x_3. We can take for instance $x_3 = 0$ and obtain $w = v_1 + v_2$. □

The following result is easily proved, but explains the importance of the notion of span:

Proposition 4.26. *Let V be a vector space over F and let $v_1, v_2, \ldots, v_n \in V$. Then*

a) $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ *is the intersection of all subspaces of V which contain $v_1, v_2, \ldots, v_n$.*

b) $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ *is the smallest vector subspace of V which contains $v_1, v_2, \ldots, v_n$.*

Proof. Since an arbitrary intersection of vector subspaces is a vector subspace, part a) implies part b), so we will focus on the proof of part a).

First, let us prove that $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ is contained in every vector subspace W of V that contains $v_1, v_2, \ldots, v_n$. This will imply that $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ is contained in the intersection of all such subspaces W. Or, since W is a subspace of V and since $v_1, v_2, \ldots, v_n \in W$, we also have $c_1v_1 + c_2v_2 + \ldots + c_nv_n \in W$ for all scalars $c_1, c_2, \ldots, c_n \in F$. Thus W contains all linear combinations of $v_1, v_2, \ldots, v_n$, i.e., it contains $\mathrm{Span}(v_1, v_2, \ldots, v_n)$.

It remains to see that $\text{Span}(v_1, v_2, \ldots, v_n)$ is a vector subspace of V (as it contains $v_1, v_2, \ldots, v_n$, this will imply that it contains the intersection of vector subspaces containing $v_1, v_2, \ldots, v_n$). So let $x, y \in \text{Span}(v_1, v_2, \ldots, v_n)$ and $c \in F$ a scalar. Since x, y are linear combinations of $v_1, v_2, \ldots, v_n$, we can write $x = a_1v_1 + a_2v_2 + \ldots + a_nv_n$ and $y = b_1v_1 + b_2v_2 + \ldots + b_nv_n$ for some scalars $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$. Then

$$x + cy = (a_1 + cb_1)v_1 + (a_2 + cb_2)v_2 + \ldots + (a_n + cb_n)v_n$$

is also a linear combination of $v_1, v_2, \ldots, v_n$, thus it belongs to $\text{Span}(v_1, v_2, \ldots, v_n)$. The result follows. □

Remark 4.27. It follows from the previous proposition and Problem 4.15 that

$$\text{Span}(v_1, v_2, \ldots, v_n) = \sum_{i=1}^{n} Fv_i,$$

where Fv_i is the subspace of V consisting in all multiples cv_i of v_i (equivalently, $Fv_i = \text{Span}(v_i)$).

We can extend slightly the previous definition and results by considering arbitrary subsets of V:

Definition 4.28. Let S be a subset of V.

a) $\text{Span}(S)$ is the subset of V consisting in all linear combinations $c_1v_1 + c_2v_2 + \ldots + c_nv_n$, where $v_1, v_2, \ldots, v_n$ is a **finite** subset of S and $c_1, c_2, \ldots, c_n$ are scalars.
b) We say that S is a **spanning set** or **generating set** for V if $\text{Span}(S) = V$.

Example 4.29. 1) Consider the space $V = F^n$ and the canonical basis

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \ldots \\ 0 \end{bmatrix}, \ldots, \quad e_n = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \ldots \\ 1 \end{bmatrix}.$$

Then $e_1, \ldots, e_n$ is a spanning set for F^n, since any vector $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \ldots \\ x_n \end{bmatrix}$ can be written $X = x_1e_1 + x_2e_2 + \ldots + x_ne_n$.

2) Similarly, consider the space $V = M_{m,n}(F)$ of $m \times n$ matrices with entries in F. If E_{ij} is the matrix in V having the (i, j)-entry equal to 1 and all other entries 0,

then the family $(E_{ij})_{1\leq i\leq m, 1\leq j\leq n}$ is a spanning family for V, since any matrix $A = [a_{ij}]$ can be written

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}.$$

3) In the space $\mathbf{R}_n[X]$ of polynomials with real coefficients and degree bounded by n, the family $1, X, \ldots, X^n$ is spanning.

Similarly, one can prove (or deduce from the previous proposition) that for an arbitrary subset S of V, the set $\mathrm{Span}(S)$ is the smallest vector subspace of V which contains S. Note the very useful

$$\text{if} \quad S_1 \subset S_2 \quad \text{then} \quad \mathrm{Span}(S_1) \subset \mathrm{Span}(S_2). \tag{4.2}$$

Indeed, $\mathrm{Span}(S_2)$ is a vector subspace containing S_2, thus also S_1, hence it contains $\mathrm{Span}(S_1)$. Alternatively, this follows from the fact that any linear combination of finitely many elements of S_1 is also a linear combination of finitely many elements of S_2. It follows from relation (4.2) that **any subset of V containing a spanning set for V is a spanning set for V**.

Row-reduction is also very useful in understanding $\mathrm{Span}(v_1, \ldots, v_k)$, when $v_1, \ldots, v_k \in F^n$. Indeed, consider the $k \times n$ matrix A whose **rows** are the coordinates of the vectors $v_1, \ldots, v_k$ in the canonical basis of F^n. Performing elementary operations on the rows of A does not affect the span of the set of its rows, hence $\mathrm{Span}(v_1, \ldots, v_k)$ is precisely the span of the rows of A_{ref}, where we recall that A_{ref} is the reduced row-echelon form of A (of course, it suffices to consider only the nonzero rows of A_{ref}). **This gives in practice a quite manageable form of $\mathrm{Span}(v_1, \ldots, v_k)$.**

Example 4.30. Consider the vectors $v_1 = (1, 2, 3, 4)$, $v_2 = (3, 1, 2, 1)$ and $v_3 = (1, 2, 1, 2)$ in $\mathbf{R}^4$. We would like to obtain a simple description of $V = \mathrm{Span}(v_1, v_2, v_3)$.

Consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 \end{bmatrix}$$

whose first row is given by the coordinates $1, 2, 3, 4$ of v_1 with respect to the canonical basis of $\mathbf{R}^4$, and similarly for the second and third row (replacing v_1 with v_2 and v_3 respectively). Row-reduction yields

$$A_{ref} = \begin{bmatrix} 1 & 0 & 0 & -\frac{3}{5} \\ 0 & 1 & 0 & \frac{4}{5} \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Thus

$$V = \text{Span}((1, 0, 0, -\frac{3}{5}), (0, 1, 0, \frac{4}{5}), (0, 0, 1, 1))$$

and this is the same as the set of vectors

$$w = (a, b, c, -\frac{3}{5}a + \frac{4}{5}b + c)$$

with $a, b, c \in \mathbf{R}$.

4.3.1 Problems for Practice

1. Find at least three different ways to express the matrix

$$B = \begin{bmatrix} 2 & -1 \\ -2 & 1 \end{bmatrix}$$

as a linear combination of the matrices

$$A_1 = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \qquad \text{and} \qquad A_3 = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}.$$

2. Show that the vector $(1, 1, 1)$ cannot be expressed as a linear combination of

$$a_1 = (1, -1, 0), \qquad a_2 = (1, 0, -1) \qquad \text{and} \qquad a_3 = (0, 1, -1).$$

3. Let W be the subset of $\mathbf{R}^n$ consisting of those vectors whose sum of coordinates equals 0. Let Z be the span of $(1, 1, \ldots, 1)$ in $\mathbf{R}^n$. Prove or disprove that $W \oplus Z = \mathbf{R}^n$.
4. Let P be the span of $(1, 1, 1)$ and $(1, 1, -1)$ in $\mathbf{R}^3$, and let D be the span of $(0, 1, -1)$. Is it true that $P \oplus D = \mathbf{R}^3$?
5. One of the vectors $b_1 = (3, -7, -6)$ and $b_2 = (0, 2, 4)$ is in the plane spanned by the vectors $v_1 = (1, 0, -1)$ and $v_2 = (1, -7, -4)$. Determine which one and write it as linear combination of the vectors v_1 and v_2. Also, prove that the other vector is not in the plane spanned by v_1 and v_2.
6. Let V be the vector space of real-valued maps on $\mathbf{R}$ and let f_n (respectively g_n) be the map sending x to $\cos nx$ (respectively $\cos^n(x)$). Prove or disprove that

$$\text{Span}(\{f_n | n \geq 0\}) = \text{Span}(\{g_n | n \geq 0\}).$$

4.4 Linear Independence

Consider some vectors $v_1, v_2, \ldots, v_n$ in a vector space V over F, and a vector v in $\text{Span}(v_1, v_2, \ldots, v_n)$. By definition, there are scalars $c_1, c_2, \ldots, c_n$ such that

$$v = c_1v_1 + c_2v_2 + \ldots + c_nv_n.$$

There is nothing in the definition of the span that requires $c_1, c_2, \ldots, c_n$ in relation (4.2) to be unique.

Problem 4.31. Let v_1, v_2, v_3 be three vectors in $\mathbf{R}^n$ such that $3v_1 + v_2 + v_3 = 0$ and let $v = v_1 + v_2 - 2v_3$. Find infinitely many different ways to write v as a linear combination of v_1, v_2, v_3.

Solution. Let α be an arbitrary real number. Re-scaling both sides of the equality $3v_1 + v_2 + v_3 = 0$ by α and adding the corresponding relation to the equality $v = v_1 + v_2 - 2v_3$ yields

$$v = (3\alpha + 1)v_1 + (\alpha + 1)v_2 + (\alpha - 2)v_3.$$

Thus each value of α provides a different way to write v as a linear combination of v_1, v_2, v_3. □

Suppose now that a vector v can be written as $v = a_1v_1 + a_2v_2 + \ldots + a_nv_n$. If $b_1, b_2, \ldots, b_n$ are scalars such that we also have $v = b_1v_1 + b_2v_2 + \ldots + b_nv_n$, then subtracting the two relations we obtain

$$0 = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \ldots + (a_n - b_n)v_n.$$

Thus we would be able to conclude that $a_1, a_2, \ldots, a_n$ are unique if the equation (with $z_1, \ldots, z_n \in F$)

$$z_1v_1 + z_2v_2 + \ldots + z_nv_n = 0$$

would force $z_1 = \ldots = z_n = 0$. As we said above, this is not always the case: take for instance $n = 1$, $v_1 = 0$, then $a_1v_1 = 0$ for any choice of the scalar a_1. On the other hand, vectors $v_1, \ldots, v_n$ having the uniqueness property play a fundamental role in linear algebra and they also deserve a formal definition:

Definition 4.32. a) Vectors $v_1, v_2, \ldots, v_n$ in some vector space V are **linearly dependent** if there is a relation

$$c_1v_1 + c_2v_2 + \ldots + c_nv_n = 0$$

for which at least one of the scalars $c_1, c_2, \ldots, c_n$ is nonzero.

b) Vectors $v_1, v_2, \ldots, v_n$ in the vector space V are **linearly independent** if whenever we have scalars $a_1, a_2, \ldots, a_n$ with $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$, then $a_1 = a_2 = \cdots = a_n = 0$.

Example 4.33. In all situations considered in example 4.29, the corresponding generating family is also linearly independent.

Before going on to more abstract things, let us consider the following very **concrete problem**: given some vectors $v_1, \ldots, v_k$ in F^n (take for simplicity $F = \mathbf{R}$), decide whether they are linearly independent. We claim that this problem can be solved algorithmically in a fairly simple way. Indeed, we need to know if we can find $x_1, \ldots, x_k \in F$, not all equal to 0 and such that

$$x_1 v_1 + \ldots + x_k v_k = 0.$$

Let A be the $n \times k$ matrix whose columns are given by the coordinates of $v_1, \ldots, v_k$ with respect to the canonical basis of F^n. Then the previous relation is equivalent to $AX = 0$, where X is the column vector with coordinates $x_1, \ldots, x_k$. Thus $v_1, \ldots, v_k$ are linearly independent if and only if the homogeneous linear system $AX = 0$ has a nontrivial solution. We know that this problem can be solved algorithmically, via the row-reduction algorithm: **let A_{ref} be the reduced row-echelon form of A. If there is a pivot in every column of A_{ref}, then $v_1, \ldots, v_k$ are linearly independent, otherwise they are not.** Thus the original problem can also be solved algorithmically. Also, note that since every homogeneous linear system with more variables than equations has a nontrivial solution, we deduce that **if we have more than n vectors in F^n, then they are never linearly independent!** Thus sometimes we can solve the original problem with absolutely no effort, simply by counting the number of vectors we are given!

Problem 4.34. Consider the vectors $v_1 = (1, 2, 3, 4, 5)$, $v_2 = (2, 3, 4, 5, 1)$, $v_3 = (1, 3, 5, 7, 9)$, $v_4 = (3, 5, 7, 9, 1)$ in $\mathbf{R}^5$. Are these vectors linearly independent? If the answer is negative, give a nontrivial linear dependency relation between these vectors.

Solution. We consider the matrix

$$A = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 3 & 3 & 5 \\ 3 & 4 & 5 & 7 \\ 4 & 5 & 7 & 9 \\ 5 & 1 & 9 & 1 \end{bmatrix}.$$

Row-reduction yields

$$A_{ref} = \begin{bmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since there is no pivot in the last column, the vectors v_1, v_2, v_3, v_4 are linearly dependent.

To find a nontrivial linear dependency relation, we solve the system $AX = 0$, which is equivalent to the system $A_{ref}X = 0$. This system is further equivalent to

$$x_1 = 2x_4, \quad x_2 = -2x_4, \quad x_3 = -x_4.$$

Taking $x_4 = 1$ (we can take any nonzero value we like), we obtain the dependency relation

$$2v_1 - 2v_2 - v_3 + v_4 = 0. \qquad \square$$

Problem 4.35. Show that the 4 vectors

$$v_1 = (2, 1, 3, 1),\ v_2 = (-1, 0, 1, 2),\ v_3 = (3, 2, 7, 4),\ v_4 = (1, 2, 0, -1)$$

are linearly dependent, and find three of them that are linearly independent.

Solution. Row reduction yields

$$\begin{bmatrix} 2 & -1 & 3 & 1 \\ 1 & 0 & 2 & 2 \\ 3 & 1 & 7 & 0 \\ 1 & 2 & 4 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus the 4 vectors are dependent. Eliminating the vector v_3 (the one that does not have a pivot in its column) yields the linearly independent set of vectors $\{v_1, v_2, v_4\}$. $\square$

One may argue that the above definition is a little bit restrictive in the sense that it only deals with finite families of vectors. If we had an infinite family $(v_i)_{i\in I}$ of vectors of V, we would not be able to give a meaning to the infinite sum $\sum_{i\in I} c_i v_i$ for any choice of the scalars c_i. However, if all but finitely many of the scalars c_i were 0, then the previous sum would be a finite sum and would thus make sense. So one can extend the previous definition by saying that the family $(v_i)_{i\in I}$ is linearly dependent if one can find scalars $(c_i)_{i\in I}$ such that all but finitely many are 0, not all of them are 0 and $\sum_{i\in I} c_i v_i = 0$. Equivalently, and perhaps easier to understand, **an arbitrary family is linearly dependent if there is a finite subfamily which is linearly dependent. A family of vectors is linearly independent if any finite subfamily is linearly independent.** Thus, a (possibly infinite) set L is linearly independent if whenever we have distinct elements $l_1, \ldots, l_n \in L$ and scalars $a_1, a_2, \ldots, a_n$ with $a_1 l_1 + a_2 l_2 + \cdots + a_n l_n = 0$, then $a_1 = a_2 = \cdots = a_n = 0$.

Remark 4.36. We note the following simple but extremely useful facts:

a) **A subfamily of a linearly independent family is linearly independent**. Indeed, let $(v_i)_{i\in I}$ be a linearly independent family and let J be a subset of I. Assume that $(v_i)_{i\in J}$ is linearly dependent, thus (by definition) we can find a finite linearly dependent subfamily $v_{i_1}, \ldots, v_{i_n}$ with $i_1, \ldots, i_n \in J$. But $i_1, \ldots, i_n \in I$, thus $v_{i_1}, \ldots, v_{i_n}$ is a finite linearly dependent subfamily of the linearly independent family $(v_i)_{i\in I}$, contradiction.

b) **If two vectors in a family of vectors are equal, then this family is automatically linearly dependent.** Indeed, say vector v appears at least twice in the linearly independent family $(v_i)_{i\in I}$. Then by part a), the subfamily v, v should be linearly independent. But this is absurd, since an obvious nontrivial linear-dependency relation is $1 \cdot v + (-1)v = 0$.

Problem 4.37. Let V be the vector space of all real-valued maps on $\mathbf{R}$. Prove that the maps $x \to |x-1|$, $x \to |x-2|$,..., $x \to |x-10|$ are linearly independent.

Solution. Let $f_i(x) = |x-i|$ for $1 \leq i \leq 10$ and suppose that

$$a_1 f_1 + a_2 f_2 + \ldots + a_{10} f_{10} = 0$$

for some real numbers $a_1, \ldots, a_{10}$. Suppose that some a_i is nonzero. Dividing by a_i, we obtain that f_i is a linear combination of $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_{10}$. But $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_{10}$ are all differentiable at i, hence f_i is also differentiable at i. This is obviously wrong, hence $a_i = 0$ for all $1 \leq i \leq 10$, and the result follows. □

One can relate the notions of span and that of being linearly dependent, as the following proposition shows. It essentially says that **a set $v_1, v_2, \ldots, v_n$ is linearly dependent if and only if one of the vectors $v_1, \ldots, v_n$ is a linear combination of the other vectors**. Note that we used the word set and not family, that is in the above statement we assume that $v_1, \ldots, v_n$ are pairwise distinct (as we observed at the end of the previous paragraph, if two vectors are equal among $v_1, \ldots, v_n$, then the family $v_1, \ldots, v_n$ is automatically linearly dependent).

Proposition 4.38. *Let S be a **set** of vectors in some vector space V. Then S is linearly dependent if and only if there is $v \in S$ such that $v \in \mathrm{Span}(S \setminus \{v\})$.*

Proof. We deal separately with each implication. First, suppose that S is linearly dependent. By definition, this means that we can find finitely many vectors $v_1, v_2, \ldots, v_n \in S$ and some scalars $a_1, a_2, \ldots, a_n$, not all 0, such that

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0.$$

Note that $v_1, \ldots, v_n$ are pairwise distinct, since the elements of S are assumed to be pairwise distinct.

Since not all scalars are 0, there is $i \in \{1, 2, \ldots, n\}$ such that $a_i \neq 0$. Dividing the previous equality by a_i, we obtain

$$\frac{a_1}{a_i}v_1 + \ldots + \frac{a_{i-1}}{a_i}v_{i-1} + v_i + \frac{a_{i+1}}{a_i}v_{i+1} + \ldots + \frac{a_n}{a_i}v_n = 0,$$

hence

$$v_i = -\frac{a_1}{a_i}v_1 - \ldots - \frac{a_{i-1}}{a_i}v_{i-1} - \frac{a_{i+1}}{a_i}v_{i+1} - \ldots - \frac{a_n}{a_i}v_n.$$

We deduce that v_i belongs to the span of $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$, which is contained in the span of $S \setminus \{v_i\}$, as $\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n\} \subset S \setminus \{v_i\}$. This proves one implication.

Next, suppose that there is $v \in S$ such that $v \in \text{Span}(S \setminus \{v\})$. That means that we can find $v_1, v_2, \ldots, v_n \in S \setminus \{v\}$ and scalars $a_1, a_2, \ldots, a_n$ such that

$$v = a_1v_1 + a_2v_2 + \ldots + a_nv_n$$

But then

$$1 \cdot v + (-a_1)v_1 + \ldots + (-a_n)v_n = 0$$

and the vectors $v, v_1, \ldots, v_n$ are linearly dependent. Since $v \notin \{v_1, \ldots, v_n\}$, it follows that S has a finite subset which is linearly dependent and so S is linearly dependent. The result follows. □

The following rather technical and subtle result (the **Steinitz exchange lemma**) is the **fundamental theorem** in the basic theory of vector spaces. We will deduce from it a lot of very nontrivial results, which will help building the theory of finite dimensional vector spaces.

Theorem 4.39 (Exchange lemma). *Let $L = \{v_1, v_2, \ldots, v_n\}$ and $S = \{w_1, w_2, \ldots, w_m\}$ be two finite subsets of a vector space V, with L linearly independent and S a spanning set. Then $n \leq m$ and we can find vectors $s_1, \ldots, s_{m-n}$ in S such that $L \cup \{s_1, s_2, \ldots, s_{m-n}\}$ is a spanning set.*

Proof. The result will be proved by induction on n. There is nothing to be proved when $n = 0$, so assume that the result holds for n and let us prove it for $n + 1$. Since $v_1, v_2, \ldots, v_{n+1}$ are linearly independent, so are $v_1, v_2, \ldots, v_n$ by Remark 4.36. Thus by the inductive hypothesis we already have $n \leq m$ and the existence of vectors $s_1, \ldots, s_{m-n}$ such that $\{v_1, \ldots, v_n, s_1, \ldots, s_{m-n}\}$ is a spanning set. In particular, we can express v_{n+1} as a linear combination

$$v_{n+1} = a_1v_1 + \ldots + a_nv_n + b_1s_1 + \ldots + b_{m-n}s_{m-n}.$$

If $m = n$, then the previous relation can be written

$$v_{n+1} = a_1 v_1 + \ldots + a_n v_n$$

and contradicts the hypothesis that $v_1, v_2, \ldots, v_n$ are linearly independent. Thus $m \neq n$ and since $n \leq m$, we must have $n + 1 \leq m$. The same argument also proves that at least one of $b_1, b_2, \ldots, b_{m-n}$ is nonzero. Permuting the vectors $s_1, \ldots, s_{m-n}$, we may assume that $b_1 \neq 0$. Dividing the relation

$$v_{n+1} = a_1 v_1 + \ldots + a_n v_n + b_1 s_1 + \ldots + b_{m-n} s_{m-n}$$

by b_1 and rearranging terms yields

$$s_1 = -\frac{a_1}{b_1} v_1 - \ldots - \frac{a_n}{b_n} v_n + \frac{1}{b_1} v_{n+1} - \ldots - \frac{b_{m-n}}{b_1} s_{m-n}$$

which shows that $s_1 \in \text{Span}(v_1, \ldots, v_n, v_{n+1}, s_2, \ldots, s_{m-n})$. Thus

$$V = \text{Span}(v_1, \ldots, v_n, s_1, \ldots, s_{m-n}) \subset \text{Span}(v_1, \ldots, v_n, v_{n+1}, s_2, \ldots, s_{m-n})$$

and $L \cup \{s_2, \ldots, s_{m-n}\}$ is a spanning set, which is exactly what we needed. □

Remark 4.40. One can slightly refine the previous theorem by no longer assuming that L is finite (but still assuming that S is finite). Indeed, any subset of L is still linearly independent. Hence Theorem 4.39 shows that any finite subset of L has size at most m and hence L is finite and has size $n \leq m$.

4.4.1 Problems for Practice

1. Are the vectors

$$v_1 = (1, 2, 1), \quad v_2 = (-3, 4, 5), v_3 = (0, 2, -3)$$

linearly independent in $\mathbf{R}^3$?

2. Consider the vectors

$$v_1 = (1, 2, 1, 3), \quad v_2 = (1, -1, 1, -1), \quad v_3 = (3, 0, 3, 1)$$

in $\mathbf{R}^4$.

a) Prove that v_1, v_2, v_3 are not linearly independent.
b) Express one of these vectors as a linear combination of two other vectors.

3. Let V be the vector space of polynomials with real coefficients whose degree does not exceed 3. Are the following vectors

$$1 + 3X + X^2, \quad X^3 - 3X + 1, \quad 3X^3 - X^2 - X - 1$$

linearly independent in V?

4. Let V be the space of all real-valued maps on $\mathbf{R}$.

   a) If $a_1 < \ldots < a_n$ are real numbers, compute

$$\lim_{x \to \infty} \sum_{i=1}^{n} e^{(a_i - a_n)x}.$$

   b) Prove that the family of maps $(x \mapsto e^{ax})_{a \in \mathbf{R}}$ is linearly independent in V.

5. Let V be the space of all maps $\varphi : [0, \infty) \to \mathbf{R}$. For each $a \in (0, \infty)$ consider the map $f_a \in V$ defined by

$$f_a(x) = \frac{1}{x + a}.$$

   a) Let $a_1 < \ldots < a_n$ be positive real numbers and suppose that $\alpha_1, \ldots, \alpha_n$ are real numbers such that

$$\sum_{i=1}^{n} \alpha_i f_{a_i}(x) = 0$$

   for all $x \geq 0$. Prove that for all real numbers x we have

$$\sum_{i=1}^{n} \alpha_i \cdot \prod_{j \neq i} (x + a_j) = 0.$$

   By making suitable choices of x, deduce that $\alpha_1 = \ldots = \alpha_n = 0$.

   b) Prove that the family $(f_a)_{a>0}$ is linearly independent in V.

6. Consider $V = \mathbf{R}$, seen as vector space over $F = \mathbf{Q}$.

   a) Prove that $1, \sqrt{2}, \sqrt{3}$ is a linearly independent set in V. Hint: if a, b, c are rational numbers such that $a + b\sqrt{2} + c\sqrt{3} = 0$, check that $a^2 + 2ab\sqrt{2} + 2b^2 = 3c^2$.

   b) Prove that the set of numbers $\ln p$, where p runs over the prime numbers, is linearly independent in V.

7. a) If m, n are nonnegative integers, compute

$$\int_0^{2\pi} \cos(mx)\cos(nx)dx.$$

   b) Deduce that the maps $x \mapsto \cos nx$, with n nonnegative integer, form a linearly independent set in the space of all real-valued maps on $\mathbf{R}$.
8. Let $v_1, v_2, \ldots, v_n$ be linearly independent vectors in $\mathbf{R}^n$. Is it always the case that $v_1, v_1 + v_2, \ldots, v_1 + v_2 + \ldots + v_n$ are linearly independent?

4.5 Dimension Theory

We are now ready to develop the dimension theory of vector spaces. For general vector spaces, this is rather subtle, but we will stick to finite dimensional vector spaces, for which the arguments are rather elementary consequences of the subtle exchange lemma proved in the last section. We fix a field F and all vector spaces in this section will be over F.

Definition 4.41. A vector space V is called **finite dimensional** if it has a finite spanning set.

Thus V is finite dimensional if we can find a finite family of vectors $v_1, v_2, \ldots, v_n \in V$ such that all vectors in V are linear combinations of $v_1, v_2, \ldots, v_n$. For instance, the spaces F^n, $M_{m,n}(F)$ and $\mathbf{R}_n[X]$ are finite dimensional, by example 4.29. However, not all vector spaces are finite dimensional (actually most of them are not).

Problem 4.42. Prove that the vector space V of all polynomials with real coefficients is not a finite dimensional $\mathbf{R}$-vector space.

Proof. Suppose that V has a finite spanning set, so there are polynomials $P_1, \ldots, P_n \in V$ such that $V = \text{Span}(P_1, \ldots, P_n)$. Let d be the maximum of $\deg(P_1), \ldots, \deg(P_n)$. Since all P_i have degree at most d, so does any linear combination of $P_1, \ldots, P_n$. It follows that any vector in V has degree at most d, which is certainly absurd since X^{d+1} has degree greater than d. □

We would like to define the dimension of a finite dimensional vector space. This should be an invariant of the vector space and should correspond to the geometric picture (you might prefer to take $F = \mathbf{R}$ for a better geometric intuition): a line (namely F) should have dimension 1, a plane (i.e., F^2) should have dimension 2, in general F^n should have dimension n. Before stating and proving the main result, let us introduce a crucial definition and practice some problems to get a better feeling about it.

Definition 4.43. A **basis** of a vector space V is a subset of V which is linearly independent and spanning.

For instance, the generating families appearing in example 4.29 are all bases of the corresponding vector spaces (this explains why we called them canonical bases in previous chapters!).

Problem 4.44. Given the matrix

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \in M_2(\mathbf{R}),$$

find a basis of the subspace U of $M_2(\mathbf{R})$ defined by

$$U = \{X \in M_2(\mathbf{R}) \mid XA = AX\}.$$

Solution. Consider a square matrix $X = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$. Then $X \in U$ if and only if $XA = AX$, which can be rewritten as

$$\begin{bmatrix} 2a_1 & 3a_2 \\ 2a_3 & 3a_4 \end{bmatrix} = \begin{bmatrix} 2a_1 & 2a_2 \\ 3a_3 & 3a_4 \end{bmatrix}.$$

This equality is equivalent to $a_2 = a_3 = 0$. Thus

$$U = \{\begin{bmatrix} a_1 & 0 \\ 0 & a_4 \end{bmatrix} | a_1, a_4 \in \mathbf{R}\},$$

and so a basis of U is given by the matrices $X_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $X_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ (it is not difficult to check that X_1 and X_2 are linearly independent). □

Problem 4.45. Determine a basis of the subspace U of $\mathbf{R}^4$, where

$$U = \{(a, b, c, d) \in \mathbf{R}^4 \mid a + b = 0,\ c = 2d\}.$$

Solution. Since $b = -a$ and $c = 2d$, we can write

$$U = \{(a, -a, 2d, d) | a, d \in \mathbf{R}\} = \{av_1 + dv_2 | a, d \in \mathbf{R}\},$$

where $v_1 = (1, -1, 0, 0)$ and $v_2 = (0, 0, 2, 1)$. Thus v_1, v_2 form a generating family for U. Moreover, they are linearly independent, since the relation $av_1 + dv_2 = 0$ is equivalent to $(a, -a, 2d, d) = (0, 0, 0, 0)$ and forces $a = d = 0$. We conclude that a basis of U is given by v_1 and v_2. □

Problem 4.46. Consider the subspaces U, V of $\mathbf{R}^4$ defined by

$$U = \{(x, y, z, w) \in \mathbf{R}^4 \mid y + z + w = 0\}$$

and

$$V = \{(x, y, z, w) \in \mathbf{R}^4 \mid x = -y,\ z = 2w\}.$$

Find a basis for each of the subspaces of U, V and $U \cap V$ of $\mathbf{R}^4$.

Solution. Expressing w in terms of y and z, we obtain

$$U = \{(x, y, z, -y - z) | y, z \in \mathbf{R}\} = \{xu_1 + yu_2 + zu_3 | x, y, z \in \mathbf{R}\},$$

where $u_1 = (1, 0, 0, 0)$, $u_2 = (0, 1, 0, -1)$ and $u_3 = (0, 0, 1, -1)$. Let us see whether u_1, u_2, u_3 are linearly independent. The equality $xu_1 + yu_2 + zu_3 = 0$ is equivalent to $(x, y, z, -y - z) = (0, 0, 0, 0)$ and forces $x = y = z = 0$. Thus u_1, u_2, u_3 are linearly independent and therefore they form a basis of U.

Let us deal now with V. Clearly

$$V = \{(-y, y, 2w, w) | y, w \in \mathbf{R}\} = \{yv_1 + wv_2 | y, w \in \mathbf{R}\},$$

where $v_1 = (-1, 1, 0, 0)$ and $v_2 = (0, 0, 2, 1)$. As above, v_1 and v_2 are linearly independent, since the relation $yv_1 + wv_2 = 0$ is equivalent to $(-y, y, 2w, w) = (0, 0, 0, 0)$ and forces $y = w = 0$. Thus v_1, v_2 form a basis of V.

Finally, a vector $(x, y, z, w) \in \mathbf{R}^4$ belongs to $U \cap V$ if and only if

$$x = -y, \quad z = 2w, \quad y + z + w = 0.$$

This is equivalent to $x = 3w$, $z = 2w$ and $y = -3w$, or

$$(x, y, z, w) = (3w, -3w, 2w, w) = w(3, -3, 2, 1).$$

Thus $(3, -3, 2, 1)$ forms a basis of $U \cap V$. □

Problem 4.47. Consider the space V of functions $f : \mathbf{R} \to \mathbf{R}$ spanned by the functions in $B = \{1, x \mapsto \sin(2x), x \mapsto \cos(2x)\}$.

a) Prove that B forms a basis of V.
(b) Prove that $x \mapsto \sin^2(x)$ is a function in V and write it as a linear combination of elements of B.

Solution. a) We need to prove that the vectors in B are linearly independent. In other words, we need to prove that if a, b, c are real numbers such that

$$a + b \sin(2x) + c \cos(2x) = 0$$

for all real numbers x, then $a = b = c = 0$. Taking $x = 0$ we obtain $a + c = 0$, then taking $x = \pi/2$ yields $a - c = 0$. Thus $a = c = 0$. Finally, taking $x = \pi/4$ yields $b = 0$.

b) For all $x \in \mathbf{R}$ we have

$$\cos(2x) = 2\cos^2(x) - 1 = 2(1 - \sin^2(x)) - 1 = 1 - 2\sin^2(x),$$

thus

$$\sin^2(x) = \frac{1 - \cos(2x)}{2}.$$

We deduce that $x \mapsto \sin^2(x)$ is in V and the previous formula expresses it as a linear combination

$$\sin^2(x) = \frac{1}{2} \cdot 1 + 0 \cdot \sin(2x) - \frac{1}{2}\cos(2x).$$

□

Let us prove now the first fundamental result regarding dimension theory of vector spaces.

Theorem 4.48. *Let V be a finite dimensional vector space. Then*

a) V contains a basis with finitely many elements.
b) Any two bases of V have the same number of elements (in particular any basis has finitely many elements).

Proof. a) Among all finite spanning sets S of V (we know that there is at least one such set) consider a set B with the smallest possible number of elements. We will prove that B is a basis. By our choice, B is a spanning set, so all we need to prove is that B is linearly independent. If this is not the case, then Proposition 4.38 yields the existence of a vector $v \in B$ such that $v \in \mathrm{Span}(B \setminus \{v\})$. It follows that $B \setminus \{v\}$ is also a spanning set. This contradicts the minimality of B and shows that B is indeed linearly independent.

b) Let B be a basis with finitely many elements, say n. Let B' be another basis of V. Then B' is a linearly independent set and B is a spanning set with n elements, thus by Remark 4.40 B' is finite, with at most n elements. This shows that any basis has at most n elements. But now we can play the following game: say B' has d elements. We saw that $d \leq n$. We exchange B and B' in the previous argument, to get that any basis has at most d elements, thus $n \leq d$. It follows that $n = d$ and so all bases have the same number of elements. □

The previous theorem allows us to make the following:

Definition 4.49. Let V be a finite dimensional vector space. The **dimension** $\dim V$ of V is the number of elements of any basis of V.

Example 4.50. a) Consider the vector space F^n. Its canonical basis $e_1, \ldots, e_n$ is a basis of F^n with n elements, thus $\dim F^n = n$.

b) Consider the space $F[X]_n$ of polynomials with coefficients in F, whose degree does not exceed n. A basis of $F[X]_n$ is given by $1, X, \ldots, X^n$, thus

$$\dim F[X]_n = n + 1.$$

c) Consider the vector space $M_{m,n}(F)$ of $m \times n$ matrices with entries in F. A basis of this vector space is given by the elementary matrices E_{ij} with $1 \leq i \leq m$ and $1 \leq j \leq n$ (the canonical basis of $M_{m,n}(F)$). It follows that

$$\dim M_{m,n}(F) = mn.$$

Problem 4.51. Find a basis as well as the dimension of the subspace

$$V = \{(a, 2a) \mid a \in \mathbf{R}\} \subset \mathbf{R}^2.$$

Solution. By definition V is the linear span of the vector $(1, 2)$, since $(a, 2a) = a(1, 2)$. Since $(1, 2) \neq (0, 0)$, we deduce that a basis of V is given by $(1, 2)$ and $\dim V = 1$. □

The second fundamental theorem concerning dimension theory is the following:

Theorem 4.52. *Let V be a vector space of dimension $n < \infty$. Then*

a) Any linearly independent set in V has at most n elements.
b) Any spanning set in V has at least n elements.
c) If S is a subset of V with n elements, then the following assertions are equivalent:

i) S is linearly independent
ii) S is a spanning set
iii) S is a basis of V.

Proof. Fix a basis B of V. By definition, B has n elements.

a) Since B is a spanning set with n elements, the result follows directly from Remark 4.40.
b) Let S be a spanning set and suppose that S has $d < n$ elements. Since B is linearly independent, Theorem 4.39 yields $n \leq d$, a contradiction.
c) Clearly iii) implies i) and ii). It suffices therefore to prove that each of i) and ii) implies iii). Suppose that S is linearly independent. By Theorem 4.39 we can add $n - n = 0$ vectors to S so that the new set is a spanning set. Clearly the new set is nothing more than S, so S is a spanning set and thus a basis (since by assumption S is linearly independent).

Now suppose that S is a spanning set and that S is not linearly independent. By Proposition 4.38 we can find $v \in S$ such that $v \in \mathrm{Span}(S \setminus \{v\})$. Then $S \setminus \{v\}$ is a spanning set with $n - 1$ elements, contradicting part b). Thus S is linearly independent and a basis of V. □

The following problems are all applications of the previous theorem.

Problem 4.53. Prove that the set U, where

$$U = \{(1,1,1), (1,2,1), (2,1,1)\}$$

is a basis of $\mathbf{R}^3$.

Solution. Let $v_1 = (1,1,1)$, $v_2 = (1,2,1)$ and $v_3 = (2,1,1)$. Since $\dim \mathbf{R}^3 = 3$, it suffices to prove that v_1, v_2, v_3 are linearly independent. Suppose that $x, y, z \in \mathbf{R}$ satisfy

$$xv_1 + yv_2 + zv_3 = 0.$$

This can be written as

$$\begin{cases} x + y + 2z = 0 \\ x + 2y + z = 0 \\ x + y + z = 0 \end{cases}$$

Combining the first and the last equation yields $z = 0$, and similarly, combining the second and the last equation yields $y = 0$. Coming back to the first equation, we also find $x = 0$, and the result follows. □

Problem 4.54. Determine a basis of $\mathbf{R}^3$ that includes the vector $v = (2,1,1)$.

Solution. Let e_1, e_2, e_3 be the canonical basis of $\mathbf{R}^3$. Then $v = 2e_1 + e_2 + e_3$. It follows that e_3 belongs to the span of v, e_1, e_2, thus the span of v, e_1, e_2 is $\mathbf{R}^3$. Thus v, e_1, e_2 form a basis of $\mathbf{R}^3$, since $\dim \mathbf{R}^3 = 3$ (of course, one can also check directly that v, e_1, e_2 are linearly independent). □

Problem 4.55. Let $\mathbf{R}_n[X]$ be the vector space of polynomials with real coefficients whose degree does not exceed n. Prove that if $P_0, P_1, \ldots, P_n \in \mathbf{R}_n[X]$ satisfy $\deg P_k = k$ for $0 \leq k \leq n$, then $P_0, P_1, \ldots, P_n$ form a basis of $\mathbf{R}_n[X]$.

Solution. Since $\dim \mathbf{R}_n[X] = n + 1$, it suffices to prove that $P_0, P_1, \ldots, P_n$ are linearly independent. Suppose that $a_0, a_1, \ldots, a_n \in \mathbf{R}$ are not all zero and

$$a_0 P_0 + a_1 P_1 + \ldots + a_n P_n = 0.$$

Let j be the largest index for which $a_j \neq 0$. Then by hypothesis $a_0 P_0 + a_1 P_1 + \ldots + a_j P_j$ has degree exactly j, which contradicts the fact that this polynomial is the zero polynomial (since $a_{j+1} = \ldots = a_n = 0$ and $a_0 P_0 + \ldots + a_n P_n = 0$) and that the zero polynomial has degree $-\infty$. □

Problem 4.56. Let $P \in \mathbf{R}[X]$ be a polynomial. Prove that the following assertions are equivalent:

a) $P(n)$ is an integer for all integers n.

b) There are integers n and $a_0, \ldots, a_n$ such that

$$P(X) = \sum_{k=0}^{n} a_k \frac{X(X-1)\ldots(X-k+1)}{k!},$$

with the convention that the first term in the sum equals a_0.

Solution. Let $P_k = \frac{X(X-1)\ldots(X-k+1)}{k!}$, with $P_0 = 1$. It is not difficult to see that $P_k(\mathbf{Z}) \subset \mathbf{Z}$ (as the values of P_k at all integers are, up to a sign, binomial coefficients). This makes it clear that b) implies a).

Suppose that a) holds and let $d = \deg P$. Since $\deg P_k = k$ for $0 \leq k \leq d$, Problem 4.55 yields **real** numbers $a_0, a_1, \ldots, a_d$ such that $P = a_0 P_0 + a_1 P_1 + \ldots + a_d P_d$. We need to prove that $a_0, \ldots, a_d$ are actually integers. But by hypothesis

$$P(m) = a_0 + \binom{m}{1} a_1 + \binom{m}{2} a_2 + \ldots \binom{m}{m-1} a_{m-1} + a_m$$

are integers, for $m = 0, \ldots, d$. Using the relation

$$a_m = P(m) - \left(a_0 + \binom{m}{1} a_1 + \binom{m}{2} a_2 + \ldots \binom{m}{m-1} a_{m-1} \right)$$

it is easy to prove by induction on j that $a_0, \ldots, a_j$ are integers for $0 \leq j \leq d$. Thus $a_0, \ldots, a_n$ are all integers and the problem is solved. □

Before moving on to another fundamental theorem, let us stop and try to explain how to solve a few **practical problems**. First, consider some vectors $v_1, \ldots, v_k$ in $\mathbf{R}^n$ and consider the problem of deciding whether this is a basis of $\mathbf{R}^n$. By the previous results, this is the case if and only if $k = n$ and $v_1, \ldots, v_k$ are linearly independent. This is equivalent to saying that $k = n$ and $A_{ref} = I_n$. We see that we have an algorithmic solution for our problem.

Consider now the problem: given $v_1, \ldots, v_k$ in $\mathbf{R}^n$, decide whether they span $\mathbf{R}^n$. To solve this problem, we consider the matrix A whose rows are given by the coordinates of the vectors $v_1, \ldots, v_k$ with respect to the canonical basis of $\mathbf{R}^n$. We row-reduce A and obtain its reduced echelon-form A_{ref}. Then $v_1, \ldots, v_k$ span $\mathbf{R}^n$ if and only if the rows of A_{ref} span $\mathbf{R}^n$. This is the case if and only if A_{ref} has a pivot in every column.

Next, consider the following trickier problem: given some vectors $v_1, \ldots, v_k$ in $\mathbf{R}^n$, find a subset of $\{v_1, \ldots, v_k\}$ which forms a basis of $\mathbf{R}^n$. Of course, if $v_1, \ldots, v_k$ do not span $\mathbf{R}^n$, then the problem has no solution (and we can test this using the procedure described in the previous paragraph). Assume now that $v_1, \ldots, v_k$ span $\mathbf{R}^n$. Let A be the matrix whose **columns** are given by the coordinates of $v_1, \ldots, v_k$ in the canonical basis of $\mathbf{R}^n$. We leave it to the reader to convince himself that those vectors v_i corresponding to columns of A containing a pivot form a basis of $\mathbf{R}^n$.

Example 4.57. Consider the vectors $v_1 = (1, 0, -1, 0)$, $v_2 = (0, 1, -1, 1)$, $v_3 = (2, 3, -12, -1)$, $v_4 = (1, 1, 1, 1)$, $v_5 = (1, -1, 0, -1)$. We would like to find a subset of these vectors which gives a basis of $\mathbf{R}^4$. Let us check first whether they span $\mathbf{R}^4$. For that, we consider the matrix

$$A = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 1 \\ 2 & 3 & -12 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & -1 \end{bmatrix}.$$

The row-reduction is

$$A_{ref} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and it has pivots in every column, thus $v_1, \ldots, v_5$ span $\mathbf{R}^4$.

Now, to solve the original problem, we consider the matrix

$$A' = \begin{bmatrix} 1 & 0 & 2 & 1 & 1 \\ 0 & 1 & 3 & 1 & -1 \\ -1 & -1 & -12 & 1 & 0 \\ 0 & 1 & -1 & 1 & -1 \end{bmatrix}$$

whose columns are the coordinates of v_1, v_2, v_3, v_4, v_5. Its row-reduction is

$$A'_{ref} = \begin{bmatrix} 1 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 1 & 0 & 0 & -\frac{2}{3} \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\frac{1}{3} \end{bmatrix}.$$

The columns containing pivots are the first four, so v_1, v_2, v_3, v_4 form a basis of $\mathbf{R}^4$.

Note that we could have read whether $v_1, \ldots, v_5$ span $\mathbf{R}^4$ directly on A', without the need to introduce the matrix A. Indeed, it suffices to check that A' has a pivot in every row, which is the case.

Problem 4.58. Let S be the set

$$S = \left\{ \begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} -5 \\ 6 \\ -8 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \right\}.$$

a) Show that S spans the space $\mathbf{R}^3$ and find a basis for $\mathbf{R}^3$ contained in S.
b) What are the coordinates of the vector $c = (1, 1, 1)$ with respect to the basis found in a)?

Solution. a) Consider the matrix

$$A = \begin{bmatrix} 1 & 0 & -5 & 1 \\ -2 & 1 & 6 & -2 \\ 0 & 2 & -8 & 1 \end{bmatrix}.$$

Its row-reduction is

$$A_{ref} = \begin{bmatrix} 1 & 0 & -5 & 0 \\ 0 & 1 & -4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since A has a pivot in each row, the columns of A span $\mathbf{R}^3$, thus S spans $\mathbf{R}^3$. Considering the pivot columns of A, we also deduce that a subset of S that forms a basis of $\mathbf{R}^3$ consists of $\begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$.

b) Since

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ -2 & 1 & -2 & 1 \\ 0 & 2 & 1 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -5 \end{array}\right],$$

the coordinates of c with respect to this basis given by the last column of the matrix above, namely $6, 3, -5$. □

Theorem 4.59. *Let V be a finite dimensional vector space and let W be a subspace of V. Then*

a) W is finite dimensional and $\dim W \leq \dim V$. *Moreover, we have equality if and only if $W = V$.*
b) Any basis of W can be extended to a basis of V.

Proof. Let $n = \dim V$.

a) If S is any linearly independent set in W, then S is a linearly independent set in V and so S has at most n elements by part a) of Theorem 4.52. Note that if we manage to prove that W is finite dimensional, then the previous observation automatically implies that $\dim W \leq n$ (as any basis of W is a linearly independent set in W). Suppose that W is not finite dimensional. Since W is nonzero, we can choose $w_1 \in W$ nonzero. Since $\{w_1\}$ is not a spanning

set for W, we can choose $w_2 \in W$ not in the span of w_1. Assuming that we constructed $w_1, \ldots, w_k$, simply choose any vector w_{k+1} in W but not in the span of $w_1, \ldots, w_k$. Such a vector exists, since by assumption the finite set $\{w_1, \ldots, w_k\}$ is not a spanning set for W. By construction, $w_1, \ldots, w_k$ are linearly independent for all k. Thus $w_1, \ldots, w_{n+1}$ is a linearly independent set with more than n elements in W, which is absurd. Thus W is finite dimensional and $\dim W \leq n$.

We still have to prove that $\dim W = n$ implies $W = V$. Let B be a basis of W. Then B has n elements and is a linearly independent set in V. By part c) of Theorem 4.52 B is a spanning set for V, and since it is contained in W, we deduce that $W = V$.

b) Let $d = \dim W \leq n$ and let B be a basis of W. Let B' be a basis of V. By Theorem 4.39 applied to the linearly independent set B in V and to the spanning set B' in V, we can add $n-d$ elements to B to make it a spanning set. This set has n elements and is a spanning set, thus it is a basis of V (part c) of Theorem 4.52) and contains B. This is exactly what we needed. □

The following result is very handy when estimating the dimension of a sum of subspaces of a given vector space.

Theorem 4.60 (Grassmann's formula). *If W_1, W_2 are subspaces of a finite dimensional vector space V, then*

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

Proof. Let $m = \dim W_1$, $n = \dim W_2$ and $k = \dim(W_1 \cap W_2)$. Let $B = \{v_1, \ldots, v_k\}$ be a basis of $W_1 \cap W_2$. Since $W_1 \cap W_2$ is a subspace of both W_1 and W_2, Theorem 4.59 yields bases B_1, B_2 of W_1 and W_2 which contain B. Say $B_1 = \{v_1, \ldots, v_k, u_1, \ldots, u_{m-k}\}$ and $B_2 = \{v_1, \ldots, v_k, w_1, \ldots, w_{n-k}\}$. We will prove that the family

$$S = \{v_1, \ldots, v_k, u_1, \ldots, u_{m-k}, w_1, \ldots, w_{n-k}\}$$

is a basis of $W_1 + W_2$, and so

$$\dim(W_1 + W_2) = k + m - k + n - k = m + n - k,$$

as desired.

We start by proving that S is a spanning set for $W_1 + W_2$. Let x be any vector in $W_1 + W_2$. By definition we can write $x = x_1 + x_2$ with $x_1 \in W_1$ and $x_2 \in W_2$. Since B_1 and B_2 are spanning sets for W_1 and W_2, we can write

$$x_1 = a_1 v_1 + \ldots + a_k v_k + b_1 u_1 + \ldots + b_{m-k} u_{m-k}$$

and

$$x_2 = c_1v_1 + \ldots + c_kv_k + d_1w_1 + \ldots + d_{n-k}w_{n-k}$$

for some scalars a_i, b_j, c_l, d_r. Then

$$x = (a_1+c_1)v_1+\ldots+(a_k+c_k)v_k+b_1u_1+\ldots+b_{m-k}u_{m-k}+d_1w_1+\ldots+d_{n-k}w_{n-k}$$

is in the span of S. Since x was arbitrary in W_1+W_2, it follows that S spans W_1+W_2.

Finally, let us prove that S is a linearly independent set in $W_1 + W_2$. Suppose that

$$a_1v_1 + \ldots + a_kv_k + b_1u_1 + \ldots + b_{m-k}u_{m-k} + c_1w_1 + \ldots + c_{n-k}w_{n-k} = 0$$

for some scalars a_i, b_j, c_l. Then

$$a_1v_1 + .. + a_kv_k + b_1u_1 + \ldots + b_{m-k}u_{m-k} = -(c_1w_1 + \ldots + c_{n-k}w_{n-k}).$$

The left-hand side belongs to W_1 and the right-hand side belongs to W_2, hence both sides belong to $W_1 \cap W_2$, and so they are linear combinations of $v_1, \ldots, v_k$. Thus we can write

$$a_1v_1 + \ldots + a_kv_k + b_1u_1 + \ldots + b_{m-k}u_{m-k} = d_1v_1 + \ldots + d_kv_k$$

for some scalars $d_1, \ldots, d_k$. Writing the previous relation as

$$(a_1 - d_1)v_1 + \ldots + (a_k - d_k)v_k + b_1u_1 + \ldots + b_{m-k}u_{m-k} = 0$$

and using the fact that $v_1, \ldots, v_k, u_1, \ldots, u_{m-k}$ are linearly independent, it follows that $a_1 = d_1, \ldots, a_k = d_k$ and $b_1 = \ldots = b_{m-k} = 0$. By symmetry we also obtain $c_1 = \ldots = c_{n-k} = 0$. Then $a_1v_1 + \ldots + a_kv_k = 0$ and since $v_1, \ldots, v_k$ are linearly independent, we conclude that $a_1 = \ldots = a_k = 0$. Thus all scalars a_i, b_j, c_l are 0 and S is a linearly independent set. This finishes the proof of the theorem. □

Remark 4.61. Suppose that W_1, W_2 are subspaces of a finite dimensional vector space V, such that $V = W_1 \oplus W_2$. If B_1 and B_2 are bases for W_1 and W_2, then $B_1 \cup B_2$ is a basis for V. This follows from the proof of the previous theorem, or it can simply be checked by unwinding definitions. More generally, if a vector space V is the direct sum of subspaces $W_1, \ldots, W_n$ and B_i is a basis for W_i $(1 \leq i \leq n)$, then $B_1 \cup \ldots \cup B_n$ is a basis for V. We leave this as an easy exercise for the reader.

Problem 4.62. Let $V_1, V_2, \ldots, V_k$ be subspaces of a finite dimensional vector space V. Prove that

$$\dim(V_1 + V_2 + \ldots + V_k) \leq \dim V_1 + \dim V_2 + \ldots + \dim V_k.$$

Solution. It suffices to prove the result for $k = 2$, as then an immediate induction on k yields the result in general (noting that $V_1 + V_2 + \ldots + V_k = (V_1 + V_2) + V_3 + \ldots + V_k$ for $k \geq 3$). But for $k = 2$ this follows from

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2) \leq \dim V_1 + \dim V_2. \qquad \square$$

Problem 4.63. Let V be a finite dimensional vector space over a field F. Let U, W be subspaces of V. Prove that $V = U \oplus W$ if and only if $V = U + W$ and

$$\dim V = \dim U + \dim W.$$

Solution. If $V = U \oplus W$, then clearly $V = U + W$ and we can obtain a basis of V by patching a basis of U and one of W, so $\dim V = \dim U + \dim W$. Suppose now that $V = U + W$ and $\dim V = \dim U + \dim W$. We need to prove that $U \cap W = \{0\}$. But

$$\dim(U \cap W) = \dim U + \dim W - \dim(U + W) = \dim V - \dim V = 0,$$

thus $U \cap W = 0$. $\square$

4.5.1 Problems for Practice

1. Do the following two sets of vectors span the same subspace of $\mathbf{R}^3$?

$$X = \{ (1,1,0),\ (3,2,2) \} \quad \text{and} \quad Y = \{ (7,3,8),\ (1,0,2),\ (8,3,10) \}$$

2. The set S consists in the following 5 matrices:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

   (a) Determine a basis B of $M_2(\mathbf{R})$ included in S.
   (b) Write $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ as a linear combination of elements of B.

3. Let e_1, e_2, e_3, e_4 be the canonical basis of $\mathbf{R}^4$ and consider the vectors

$$v_1 = e_1 + e_4, \quad v_2 = e_3, \quad v_3 = e_2, \quad v_4 = e_2 + e_4.$$

   a) Are the subspaces $\text{Span}(v_1, v_2)$ and $\text{Span}(v_3, v_4)$ in direct sum position?
   b) Are the subspaces $\text{Span}(v_1, v_2, v_3)$ and $\text{Span}(v_4)$ in direct sum position?

4. Let V be the set of polynomials f with real coefficients of degree not exceeding 4 and such that $f(1) = f(-1) = 0$.

   a) Prove that V is a subspace of the space of all polynomials with real coefficients.
   b) Find a basis of V and its dimension.

5. Let V be the set of vectors $(x, y, z, t) \in \mathbf{R}^4$ such that $x = z$ and $y = t$.

   a) Prove that V is a subspace of $\mathbf{R}^4$.
   b) Give a basis and the dimension of V.
   c) Complete the basis found in b) to a basis of $\mathbf{R}^4$.

6. Consider the set V of vectors $(x_1, x_2, x_3, x_4) \in \mathbf{R}^4$ such that

$$x_1 + x_3 = 0 \quad \text{and} \quad x_2 + x_4 = 0.$$

   a) Prove that V is a subspace of $\mathbf{R}^4$.
   b) Give a basis and the dimension of V.
   c) Let W be the span of the vectors $(1, 1, 1, 1)$, $(1, -1, 1, -1)$ and $(1, 0, 1, 0)$. Give a basis of W and find $V + W$ and $V \cap W$ (you are asked to give a basis for each of these spaces).

7. A set of three linearly independent vectors can be chosen among

$$u = (1, 0, -1), \quad v = (2, 1, 1) \quad w = (4, 1, -1), \quad \text{and} \quad x = (1, 1, 1).$$

   (a) Determine such a set and show that it is indeed linearly independent.
   (b) Determine a nontrivial dependence relation among the four given vectors.

8. Exactly one of the vectors $b_1 = (7, 2, 5)$ and $b_2 = (7, 2, -5)$ can be written as a linear combination of the column vectors of the matrix

$$A = \begin{bmatrix} 1 & 0 & 3 \\ 1 & 1 & 4 \\ 0 & 1 & 1 \end{bmatrix}.$$

   Determine which one and express it as a linear combination of the column vectors of A.

9. Let V be the set of matrices $A \in M_n(\mathbf{C})$ for which $a_{ij} = 0$ whenever $i - j$ is odd.

   a) Prove that V is a subspace of $M_n(\mathbf{C})$ and that the product of two matrices in V belongs to V.
   b) Find the dimension of V as $\mathbf{C}$-vector space.

10. Let V be the set of matrices $A \in M_n(\mathbf{R})$ such that

$$a_{n+1-i,n+1-j} = a_{ij}$$

for $i, j \in [1, n]$.

a) Prove that V is a subspace of $M_n(\mathbf{R})$.
b) Find the dimension of V as $\mathbf{R}$-vector space.

11. Find all real numbers x for which the vectors

$$v_1 = (1, 0, x), \quad v_2 = (1, 1, x), \quad v_3 = (x, 0, 1)$$

form a basis of $\mathbf{R}^3$.

12. Let $P_k = X^k(1 - X)^{n-k}$. Prove that $P_0, \ldots, P_n$ is a basis of the space of polynomials with real coefficients, whose degree does not exceed n.

13. Let V be a vector space of dimension n over $\mathbf{F}_2$. Prove that for all $d \in [1, n]$ the following assertions hold:

a) There are $(2^n - 1)(2^n - 2) \ldots (2^n - 2^{d-1})$ d-tuples $(v_1, \ldots, v_d)$ in V^d such that the family $v_1, \ldots, v_d$ is linearly independent.
b) There are $(2^n - 1)(2^n - 2) \ldots (2^n - 2^{n-1})$ invertible matrices in $M_n(\mathbf{F}_2)$.
c) There are

$$\frac{(2^n - 1)(2^{n-1} - 1) \ldots (2^{n-d+1} - 1)}{(2^d - 1)(2^{d-1} - 1) \ldots (2 - 1)}$$

subspaces of dimension d in V.

Chapter 5
Linear Transformations

Abstract While the previous chapter dealt with individual vector spaces, in this chapter we focus on the interaction between two vector spaces by studying linear maps between them. Using the representation of linear maps in terms of matrices, we obtain some rather surprising results concerning matrices, which would be difficult to prove otherwise.

Keywords Linear maps • Kernel • image • Projection • Symmetry • Stable subspace • Change of basis • Matrix • Rank

The goal of this chapter is to develop the theory of linear maps between vector spaces. In other words, while the previous chapter dealt with basic properties of individual vector spaces, in this chapter we are interested in the interactions between two vector spaces. We will see that one can understand linear maps between finite dimensional vector spaces in terms of matrices and, more importantly and perhaps surprisingly at first sight, that we can study properties of matrices using linear maps and properties of vector spaces that were established in the previous chapter.

5.1 Definitions and Objects Canonically Attached to a Linear Map

Unless stated otherwise, all vector spaces will be over a field F, which the reader can take **R** or **C**. In the previous chapter we defined and studied the basic properties of vector spaces. In this chapter we will deal with maps between vector spaces. We will not consider all maps, but only those which are compatible with the algebraic structures on vector spaces, namely addition and scalar multiplication. More precisely:

Definition 5.1. Let V, W be vector spaces over F. A **linear map** (or **linear transformation** or **homomorphism**) between V and W is a map $T : V \to W$ satisfying the following two properties:

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_5

1) $T(v_1 + v_2) = T(v_1) + T(v_2)$ for all vectors $v_1, v_2 \in V$, and
2) $T(cv) = cT(v)$ for all $v \in V$ and all scalars $c \in F$.

The reader will notice the difference between this definition and the definition of linear maps in other parts of mathematics: very often in elementary algebra or in real analysis when we refer to a linear map we mean a map $f : \mathbf{R} \to \mathbf{R}$ of the form $f(x) = ax + b$ for some real numbers a, b. Such a map is a linear map from the point of view of linear algebra if and only if $b = 0$ (we refer to the more general maps $x \to ax + b$ as **affine maps** in linear algebra).

In practice, instead of checking separately that T respects addition and scalar multiplication, it may be advantageous to prove directly that

$$T(v_1 + cv_2) = T(v_1) + cT(v_2)$$

for all vectors $v_1, v_2 \in V$ and all scalars $c \in F$.

Problem 5.2. If $T : V \to W$ is a linear transformation, then $T(0) = 0$ and $T(-v) = -T(v)$ for all $v \in V$.

Solution. Since T is linear, we have

$$T(0) = T(0 + 0) = T(0) + T(0)$$

thus $T(0) = 0$. Similarly,

$$T(-v) = T((-1)v) = (-1)T(v) = -T(v).$$ □

Example 5.3. a) If V is a vector space over F and $c \in F$ is a scalar, then the map $T : V \to V$ sending v to cv is linear (this follows from the definition of a vector space). For $c = 0$ we obtain the **zero map**, which we simply denote 0, while for $c = 1$ we obtain the **identity map**, denoted id. In general, linear maps of the form $v \to cv$ for some scalar $c \in F$ are called **scalar** linear maps.

b) Consider the vector space $V = \mathbf{R}[X]$ of polynomials with real coefficients (we could allow coefficients in any field). The map $T : V \to V$ sending P to its derivative P' is linear, as follows immediately from its definition. Note that if $\deg P \leq n$, then $\deg P' \leq n$, thus the map T restricts to a linear map $T : \mathbf{R}_n[X] \to \mathbf{R}_n[X]$ for all n (recall that $\mathbf{R}_n[X]$ is the vector subspace of V consisting of polynomials whose degree does not exceed n).

c) The map $T : \mathbf{R}^2 \to \mathbf{R}$ defined by $T(x, y) = xy + 1$ is not linear, since $T(0, 0) = 1 \neq 0$ (by Problem 5.2). Similarly, the map $T : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $T(x, y) = (x, y + 1)$ is not linear.

d) Consider the vector space V of continuous real-valued maps on $[0, 1]$. Then the map $T : V \to \mathbf{R}$ sending $f \in V$ to $\int_0^1 f(x)dx$ is linear. This follows from properties of integration.

e) Consider the **trace map** $\mathrm{Tr} : M_n(F) \to F$ defined by

$$\mathrm{Tr}(A) = a_{11} + a_{22} + \ldots + a_{nn} \quad \text{if} \quad A = [a_{ij}].$$

By definition of the operations in $M_n(F)$, this map is linear. It has the extremely important property that

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

for all matrices A, B. Indeed, one checks using the product rule that both terms are equal to $\sum_{i,j=1}^{n} a_{ij} b_{ji}$.

f) In the chapter devoted to basic properties of matrices, we saw that any matrix $A \in M_{m,n}(F)$ defines a linear map $F^n \to F^m$ via $X \to AX$. We also proved in that chapter that any linear map $T : F^n \to F^m$ comes from a unique matrix $A \in M_{m,n}(F)$. For example, the map $T : \mathbf{R}^3 \to \mathbf{R}^2$ defined by $T(x_1, x_2, x_3) = (x_1, x_2)$ for all $x_1, x_2, x_3 \in \mathbf{R}$ is linear and associated with the matrix $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. The linear maps $T : F^n \to F^m$ are exactly the maps

$$T(x_1, \ldots, x_n) = (a_{11}x_1 + \ldots + a_{1n}x_n, \ldots, a_{m1}x_1 + \ldots + a_{mn}x_n)$$

with $a_{ij} \in F$.

g) We introduce now a fundamental class of linear transformations: **projections onto subspaces**. Suppose that V is a vector space over a field F and that W_1, W_2 are subspaces of V such that $V = W_1 \oplus W_2$. The **projection onto** W_1 **along** W_2 is the map $p : V \to W_1$ defined as follows: for each $v \in V$, $p(v)$ is the unique vector in W_1 for which $v - p(v) \in W_2$. This makes sense, since by assumption v can be uniquely written as $v_1 + v_2$ with $v_1 \in W_1$ and $v_2 \in W_2$, and so necessarily $p(v) = v_1$. It may not be apparently clear that the map p is linear, but this is actually not difficult: assume that $v, v' \in V$ and let $w = p(v)$ and $w' = p(v')$. Then $w, w' \in W_1$ so $w + w' \in W_1$, and

$$(v + v') - (w + w') = (v - w) + (v' - w') \in W_2,$$

so by definition

$$p(v + v') = w + w' = p(v) + p(v').$$

We leave it to the reader to check that $p(av) = ap(v)$ for $v \in V$ and $a \in F$, using a similar argument. Note that $p(v) = v$ **for all** $v \in W_1$**, but** $p(v) = 0$ **for all** $v \in W_2$**.** In general, we call a linear map $T : V \to V$ a **projection** if there is a decomposition $V = W_1 \oplus W_2$ such that T is the projection onto W_1 along W_2.

h) Assume that we are in the situation described in g). We will define a second fundamental class of linear maps namely **symmetries with respect to subspaces**. More precisely, for any decomposition $V = W_1 \oplus W_2$ of V into the direct sum of two subspaces W_1, W_2 we define the **symmetry** $s : V \to V$ **with respect to** W_1 **along** W_2 as follows: take a vector $v \in V$, write it $v = w_1 + w_2$ with $w_1 \in W_1$ and $w_2 \in W_2$, and set

$$s(v) = w_1 - w_2.$$

Again, it is not difficult to check that s is a linear map. Note that $s(v) = v$ **whenever** $v \in W_1$ **and** $s(v) = -v$ **whenever** $v \in W_2$. Note that if $F = \mathbf{F}_2$, then s is the identity map, since $-v = v$ for all $v \in V$ if V is a vector space over $\mathbf{F}_2$. In general a linear map $T : V \to V$ is called a **symmetry** if there is a decomposition $V = W_1 \oplus W_2$ such that T is the symmetry with respect to W_1 along W_2.

Suppose that $T : V \to V$ is a linear transformation. If W is a subspace of V, there is no reason to have $T(W) \subset W$. However, the subspaces W with this property play an absolutely crucial role in the study of linear maps and deserve a special name and a definition. They will be extensively used in subsequent chapters dealing with deeper properties of linear maps.

Definition 5.4. Let $T : V \to V$ be a linear map on a vector space V. A subspace W of V is called **stable under** T or T**-stable** if $T(W) \subset W$.

Problem 5.5. Consider the map $T : \mathbf{R}^2 \to \mathbf{R}^2$ sending (x_1, x_2) to $(x_2, -x_1)$. Find all subspaces of $\mathbf{R}^2$ which are stable under T.

Solution. Let W be a subspace of $\mathbf{R}^2$ which is stable under T. Since $\mathbf{R}^2$ and $\{0\}$ are obviously stable under T, let us assume that $W \neq \{0\}, \mathbf{R}^2$. Then necessarily $\dim W = 1$, that is $W = \mathbf{R}v$ for some nonzero vector $v = (x_1, x_2)$. Since W is stable under T, there is a scalar $c \in \mathbf{R}$ such that $T(v) = cv$, that is $(x_2, -x_1) = (cx_1, cx_2)$. We deduce that $x_2 = cx_1$ and $-x_1 = cx_2 = c^2x_1$. Thus $(c^2 + 1)x_1 = 0$ and since $c \in \mathbf{R}$, we must have $x_1 = 0$ and then $x_2 = 0$, thus $v = 0$, a contradiction. This shows that the only subspaces stable under T are $\mathbf{R}^2$ and $\{0\}$. □

Remark 5.6. The result of the previous problem is no longer the same if we replace $\mathbf{R}$ by $\mathbf{C}$. In this new situation the line spanned by $(1, i) \in \mathbf{C}^2$ is stable under T.

If W is a stable subspace, then T restricts to a linear map $T : W \to W$. For instance, one-dimensional stable subspaces (i.e., lines in V stable under T) will be fundamental objects associated with linear transformations on finite dimensional vector spaces. The following exercise studies those linear maps T for which every line is a stable subspace.

Problem 5.7. Let V be a vector space over some field F and let $T : V \to V$ be a linear transformation. Suppose that all lines in V are stable subspaces under T. Prove that there is a scalar $c \in F$ such that $T(x) = cx$ for all $x \in V$.

Solution. Let $x \in V$ be nonzero and consider the line $L = Fx$ spanned by x. By hypothesis $T(L) \subset L$, thus we can find a scalar c_x such that $T(x) = c_x \cdot x$. We want to prove that we can choose c_x independently of x.

Suppose that x and y are linearly independent (in particular nonzero). Then $x + y \neq 0$ and the equality $T(x + y) = T(x) + T(y)$ can be written

$$c_{x+y} \cdot (x + y) = c_x \cdot x + c_y \cdot y$$

or equivalently

$$(c_{x+y} - c_x) \cdot x + (c_{x+y} - c_y) \cdot y = 0.$$

This forces $c_{x+y} = c_x = c_y$. Next, suppose that x and y are nonzero and linearly dependent. Thus $y = ax$ for some nonzero scalar a. Then $T(y) = aT(x)$ can be written $c_y \cdot y = ac_x \cdot x$ or equivalently $c_y \cdot y = c_x \cdot y$ and forces $c_x = c_y$. Thus as long as x, y are nonzero vectors of V, we have $c_x = c_y$. Letting c be the common value of c_x (when x varies over the nonzero vectors in V) yields the desired result. □

Let V and W be vector spaces over F and let us denote $\mathrm{Hom}(V, W)$ the set of linear transformations between V and W. It is a subset of the vector space $M(V, W)$ of all maps $f : V \to W$. Recall that the addition and scalar multiplication in $M(V, W)$ are defined by

$$(f + g)(v) = f(v) + g(v), \quad (cf)(v) = cf(v)$$

for $f, g \in M(V, W)$, $c \in F$ and $v \in V$.

Proposition 5.8. *Let V, W be vector spaces. The set* $\mathrm{Hom}(V, W)$ *of linear transformations between V and W is a subspace of $M(V, W)$.*

Proof. We need to prove that the sum of two linear transformations is a linear transformation and that cT is a linear transformation whenever c is a scalar and T is a linear transformation. Both assertions follow straight from the definition of a linear transformation. □

We introduce now a fundamental definition:

Definition 5.9. The **kernel** (or **null space**) of a linear transformation $T : V \to W$ is

$$\ker T = \{v \in V, T(v) = 0\}.$$

The **image** (or **range**) $\mathrm{Im}(T)$ of T is the set

$$\mathrm{Im}(F) = \{T(v) | v \in V\} \subset W.$$

The following criterion for injectivity is **extremely useful** and constantly used when dealing with linear maps.

Proposition 5.10. *If $T : V \to W$ is a linear transformation, then T is injective if and only if* $\ker T = \{0\}$.

Proof. Since $T(0) = 0$, it is clear that $\ker T = \{0\}$ if T is injective. Conversely, assume that $\ker T = \{0\}$. If $T(v_1) = T(v_2)$, then

$$T(v_1 - v_2) = T(v_1) - T(v_2) = 0,$$

thus $v_1 - v_2 \in \ker T$ and so $v_1 = v_2$. Thus T is injective. □

Problem 5.11. Find the dimension of the kernel of the linear map determined by the matrix

$$A = \begin{bmatrix} 1 & -2 & 1 & 0 \\ -1 & 2 & 1 & 2 \\ -2 & 4 & 0 & 2 \end{bmatrix} \in M_{3,4}(\mathbf{R}).$$

Solution. Let T be the corresponding linear map, so that

$$T(x_1, x_2, x_3, x_4) = (x_1 - 2x_2 + x_3, -x_1 + 2x_2 + x_3 + 2x_4, -2x_1 + 4x_2 + 2x_4).$$

A vector $x = (x_1, \ldots, x_4)$ belongs to $\ker(T)$ if and only

$$\begin{cases} x_1 - 2x_2 + x_3 = 0 \\ -x_1 + 2x_2 + x_3 + 2x_4 = 0 \\ -2x_1 + 4x_2 + 2x_4 = 0 \end{cases}$$

The matrix associated with this system is A and row-reduction yields

$$A_{ref} = \begin{bmatrix} 1 & -2 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus the previous system is equivalent to

$$\begin{cases} x_1 - 2x_2 - x_4 = 0 \\ x_3 + x_4 = 0 \end{cases}$$

We conclude that

$$\ker(T) = \{(x_1, x_2, 2x_2 - x_1, x_1 - 2x_2) | x_1, x_2 \in \mathbf{R}\}.$$

The last space is the span of the vectors $v_1 = (1, 0, -1, 1)$ and $v_2 = (0, 1, 2, -2)$ and since they are linearly independent (as $x_1 v_1 + x_2 v_2 = 0$ is equivalent to $(x_1, x_2, 2x_2 - x_1, x_1 - 2x_2) = (0, 0, 0, 0)$ and so to $x_1 = x_2 = 0$), it follows that $\dim \ker T = 2$. □

Problem 5.12. Give a basis for the kernel of the linear map $T : \mathbf{R}^3 \to \mathbf{R}^3$ given by

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

Solution. We need to find those (x, y, z) for which $T(x, y, z) = 0$, in other words we need to solve the system

$$\begin{cases} x - 2y + z = 0 \\ 2x - 3y + z = 0 \\ x + y - 2z = 0 \\ 3x - y - 2z = 0 \end{cases}$$

The matrix of this homogeneous system is

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

and row-reduction yields

$$A_{ref} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus the system is equivalent to

$$\begin{cases} x - z = 0 \\ y - z = 0 \end{cases}$$

and its solutions are given by (x, x, x) with $x \in \mathbf{R}$. In other words,

$$\mathrm{Ker}(T) = \{(x, x, x) | x \in \mathbf{R}\}$$

and a basis is given by the vector $(1, 1, 1)$. □

Problem 5.13. Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and let $T : M_2(\mathbf{R}) \to M_2(\mathbf{R})$ be the map defined by

$$F(X) = AX.$$

(a) Prove that F is a linear transformation.
(b) Find the dimension of $\ker(F)$ and a basis for $\ker(F)$.

Solution. (a) For any two matrices X and Y in $M_2(\mathbf{R})$ and any scalar c we have

$$F(X + cY) = A(X + cY) = AX + cAY = F(X) + cF(Y),$$

thus F is a linear transformation.

(b) We need to find the dimension and a basis of the space of matrices that are solutions of the matrix equation $AX = 0$. This equation is equivalent to

$$\begin{bmatrix} x_{11} + x_{21} & x_{12} + x_{22} \\ x_{11} + x_{21} & x_{12} + x_{22} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

or $x_{21} = -x_{11}$ and $x_{22} = -x_{12}$. Thus

$$\ker(F) = \{\begin{bmatrix} x_{11} & x_{12} \\ -x_{11} & -x_{12} \end{bmatrix} | x_{11}, x_{12} \in \mathbf{R}\}.$$

This last space is clearly two-dimensional, with a basis given by

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}.$$

□

Proposition 5.14. *If $T : V \to W$ is a linear transformation, then* $\ker T$ *and* $\mathrm{Im}(T)$ *are subspaces of V, respectively W. Moreover,* $\ker T$ *is stable under T, and if $V = W$ then* $\mathrm{Im}(T)$ *is stable under T.*

Proof. Let v_1, v_2 in $\ker T$ and let $c \in F$. We need to prove that $v_1 + cv_2 \in \ker T$. Indeed,

$$T(v_1 + cv_2) = T(v_1) + cT(v_2) = 0 + c \cdot 0 = 0.$$

Similarly, if $w_1, w_2 \in \mathrm{Im}(T)$, then we can write $w_1 = T(v_1)$ and $w_2 = T(v_2)$ for some $v_1, v_2 \in V$. Then

$$w_1 + cw_2 = T(v_1) + cT(v_2) = T(v_1 + cv_2) \in \mathrm{Im}(T)$$

for all scalars $c \in F$, thus $\mathrm{Im}(T)$ is a subspace of W.

It is clear that $\mathrm{Im}(T)$ is stable under T if $V = W$. To see that $\ker T$ is stable under T, take $v \in \ker T$, so that $T(v) = 0$. Then $T(T(v)) = T(0) = 0$, thus $T(v) \in \ker T$ and so $\ker T$ is stable. □

The following problem gives a characterization of projections as those linear maps T for which $T \circ T = T$.

Problem 5.15. Let V be a vector space over a field F and let $T : V \to V$ be a linear map on V. Prove that the following statements are equivalent:

a) T is a projection
b) We have $T \circ T = T$.
Moreover, if this is the case, then $\ker T \oplus \mathrm{Im}(T) = V$.

Solution. Assume that a) holds and let us prove b). Assume that T is the projection onto W_1 along W_2 for some decomposition $V = W_1 \oplus W_2$. Take $v \in V$ and write $v = w_1 + w_2$ with $w_1 \in W_1$ and $w_2 \in W_2$. Then $T(v) = w_1$ and $T(T(v)) = T(w_1) = w_1$, hence $T(T(v)) = T(v)$ for all $v \in V$ and so $T \circ T = T$ and b) holds.

Assume now that $T \circ T = T$ and let us prove b). We start by proving that $\ker T \oplus \mathrm{Im}(T) = V$. Suppose that $v \in \ker T \cap \mathrm{Im}(T)$, so that $v = T(w)$ for some $w \in V$, and $T(v) = 0$. We deduce that

$$0 = T(v) = T(T(w)) = T(w)$$

hence $v = T(w) = 0$ and $\ker T \cap \mathrm{Im}(T) = \{0\}$. Next, let $v \in V$ and put $v_1 = v - T(v)$ and $v_2 = T(v)$. Clearly $v = v_1 + v_2$ and $v_2 \in \mathrm{Im}(T)$. Moreover,

$$T(v_1) = T(v - T(v)) = T(v) - T(T(v)) = 0$$

and so $v_1 \in \ker T$. Hence $v \in \ker T + \mathrm{Im}(T)$ and $\ker T \oplus \mathrm{Im}(T) = V$ holds.

Set $W_1 = \mathrm{Im}(T)$ and $W_2 = \ker T$. By assumption $V = W_1 \oplus W_2$ and $T(v) \in W_1$ for all $v \in W$. It suffices therefore to prove that $v - T(v) \in W_2$ for all $v \in V$, as this implies that T is the projection onto W_1 along W_2. But $v - T(v) \in W_2$ if and only if $T(v - T(v)) = 0$, that is $T(v) = T^2(v)$, which follows from our assumption that b) holds. Note that the last statement of the problem has already been proved. □

Remark 5.16. We have a similar statement for symmetries assuming that $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$ (so we exclude $F = \mathbf{F}_2$). Namely, if V is a vector space over F and $T : V \to V$ is a linear map, then the following statements are equivalent:

a) T is a symmetry.
b) $T \circ T = \mathrm{id}$, the identity map of V (sending every vector of V to itself).

Moreover, if this is the case then $V = \mathrm{Ker}(T - \mathrm{id}) \oplus \mathrm{Ker}(T + \mathrm{id})$.

5.1.1 Problems for practice

In the next problems F is a field.

1. Let $f : \mathbf{C} \to \mathbf{C}$ be a $\mathbf{R}$-linear map. Prove the existence of complex numbers a, b such that $f(z) = az + b\bar{z}$ for all $z \in \mathbf{C}$.
2. Consider the map $f : \mathbf{R}^4 \to \mathbf{R}^3$ defined by

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2 + x_3 + x_4, 2x_1 + x_2 - x_3 + x_4, x_1 - x_2 + x_3 - x_4).$$

   a) Prove that f is a linear map.
   b) Give a basis for the kernel of f.

3. Let V be the space of polynomials with real coefficients whose degree does not exceed 3, and let the map $f : V \to \mathbf{R}^4$ be defined by

$$f(P) = (P(0), P(1), P(-1), P(2)).$$

   a) Prove that f is a linear map.
   b) Is f injective?

4. Let n be a positive integer and let V be the space of real polynomials whose degree does not exceed n. Consider the map

$$f : V \to V, \quad f(P(X)) = P(X) + (1 - X)P'(X),$$

   where $P'(X)$ is the derivative of P.

   a) Explain why f is a well-defined linear map.
   b) Give a basis for the kernel of f.

5. Find all subspaces of $\mathbf{R}^2$ which are stable under the linear transformation

$$T : \mathbf{R}^2 \to \mathbf{R}^2, \quad T(x, y) = (x + y, -x + 2y).$$

6. Let V be the space of polynomials with real coefficients whose degree does not exceed n. Let T be the linear transformation on V sending P to its derivative. Find all subspaces of V which are stable under T.
7. Let $T : \mathbf{R}[X] \to \mathbf{R}[X]$ be the map defined by

$$T(P(X)) = P(X) - 2(X^2 - 1)P''(X).$$

   a) Prove that T is a linear map.
   b) Prove that for all $n \geq 0$, the space of polynomials with real coefficients whose degree does not exceed n is stable under T.

8. Let V be a vector space over a field F and let $T_1, \ldots, T_n : V \to V$ be linear transformations. Prove that

$$\bigcap_{i=1}^{n} \ker T_i \subseteq \ker \left(\sum_{i=1}^{n} T_i \right).$$

9. Let V be a vector space over a field F and let $T_1, T_2 : V \to V$ be linear transformations such that $T_1 \circ T_2 = T_1$ and $T_2 \circ T_1 = T_2$. Prove that $\ker T_1 = \ker T_2$.
10. Let V be a vector space over F and let $T : V \to V$ be a linear transformation such that

$$\ker T = \ker T^2 \quad \text{and} \quad \mathrm{Im} T = \mathrm{Im} T^2.$$

Prove that

$$V = \ker T \oplus \mathrm{Im} T.$$

11. For each of the following maps $T : \mathbf{R}^3 \to \mathbf{R}^3$, check that T is linear and then check whether $\ker(T)$ and $\mathrm{Im}(T)$ are in direct sum position.

    a) $T(x, y, z) = (x - 2y + z, x - z, x - 2y + z)$.
    b) $T(x, y, z) = (3(x + y + z), 0, x + y + z)$.

12. Let $f : \mathbf{R} \to \mathbf{R}$ be a map such that $f(x + y) = f(x) + f(y)$ for all real numbers x, y. Prove that f is a linear map of $\mathbf{Q}$-vector spaces between $\mathbf{R}$ and itself.
13. (Quotient space) Let V be a finite dimensional vector space over F and let $W \subset V$ be a subspace. For a vector $v \in V$, let

$$[v] = \{v + w : w \in W\}.$$

    Note that $[v_1] = [v_2]$ if $v_1 - v_2 \in W$. Define the quotient space V/W to be $\{[v] : v \in V\}$. Define an addition and scalar multiplication on V/W by $[u] + [v] = [u + v]$ and $a[v] = [av]$. We recall that the addition and multiplication above are well defined and V/W equipped with these operations is a vector space.

    a) Show that the map $\pi : V \to V/W$ defined by $\pi(v) = [v]$ is linear with kernel W.
    b) Show that $\dim(W) + \dim(V/W) = \dim(V)$.
    c) Suppose $U \subset V$ is any subspace with $W \oplus U = V$. Show that $\pi|_U : U \to V/W$ is an isomorphism, i.e., a bijective linear map.
    d) Let $T : V \to U$ be a linear map, let $W \subset \ker T$ be a subspace of V, and $\pi : V \to V/W$ be the projection onto the quotient space. Show that there is a unique linear map $S : V/W \to U$ such that $T = S \circ \pi$.

5.2 Linear Maps and Linearly Independent Sets

The following result relates linear maps and notions introduced in the previous chapter: spanning sets, linearly independent sets. In general, if $T : V \to W$ is linear, it is not true that the image of a linearly independent set in V is linearly independent in W (think about the zero linear map). However, if T is injective, then this is the case, as the following proposition shows (dealing also with the analogous result for spanning sets).

Proposition 5.17. *Let $T : V \to W$ be a linear transformation.*

a) If T is injective and if L is a linearly independent set in V, then $T(L) := \{T(l), l \in L\}$ is a linearly independent set in W.

b) If T is surjective and if S is a spanning set in V, then $T(S)$ is a spanning set in W.
c) If T is bijective and if B is a basis in V, then $T(V)$ is a basis in W.

Proof. Part c) is simply a combination of a) and b), which we prove separately.

a) Suppose we have

$$c_1 T(l_1) + \cdots + c_n T(l_n) = 0$$

for some scalars $c_1, \ldots, c_n$. The previous relation can be written as $T(c_1 l_1 + \cdots + c_n l_n) = 0$, thus $c_1 l_1 + \cdots + c_n l_n \in \ker T$. Since T is injective, we deduce that $c_1 l_1 + \cdots + c_n l_n = 0$. Hence $c_1 = c_2 = \cdots = c_n = 0$. Thus $T(L)$ is linearly independent.

b) Let $w \in W$. Since T is surjective, there is $v \in V$ such that $T(v) = w$. Since S is a spanning set in V, we can write v as a linear combination of some elements $s_1, \ldots, s_n$ of S, say $v = c_1 s_1 + \ldots + c_n s_n$ for some scalars $c_1, \ldots, c_n$. Then

$$w = T(v) = T(c_1 s_1 + \ldots + c_n s_n) = c_1 T(s_1) + \ldots + c_n T(s_n).$$

Thus w is in the span of $T(s_1), \ldots, T(s_n)$, thus in the span of $T(S)$. Since $w \in W$ was arbitrary, the result follows. □

The following corollary is absolutely fundamental (especially part c)). It follows easily from the previous proposition and the rather subtle properties of finite dimensional vector spaces discussed in the previous chapter.

Corollary 5.18. *Let V and W be finite dimensional vector spaces and let $T : V \to W$ be a linear transformation.*

a) If T is injective, then $\dim V \leq \dim W$.
b) If T is surjective, then $\dim V \geq \dim W$.
c) If T is bijective, then $\dim V = \dim W$.

Proof. Again, part c) is a consequence of a) and b). For a), let B be a basis of V and let $v_1, \ldots, v_n$ be its elements. By Proposition 5.17 $T(v_1), \ldots, T(v_n)$ are linearly independent vectors in W. Thus $\dim W \geq n = \dim V$.

The argument for b) is similar, since Proposition 5.17 implies that the vectors $T(v_1), \ldots, T(v_n)$ form a spanning set for W, thus $n \geq \dim W$. □

We can sometimes prove the existence of a linear map T without having to explicitly write down the value of $T(x)$ for each vector x in its domain: if the domain is finite dimensional (this hypothesis is actually unnecessary), it suffices to give the images of the elements in a basis of the domain. More precisely:

Proposition 5.19. *Let V, U be vector spaces over a field F. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis of V and let $\{u_1, u_2, \ldots, u_n\}$ be any set of vectors in U. Then there is a unique linear transformation $T : V \to U$ such that*

$$T(v_1) = u_1,\ T(v_2) = u_2, \ldots, T(v_n) = u_n.$$

Proof. We start by proving the uniqueness. Suppose that we have two linear transformations $T, T' : V \to U$ such that $T(v_i) = T'(v_i) = u_i$ for $1 \leq i \leq n$. Then $T - T'$ is a linear transformation which vanishes at $v_1, \ldots, v_n$. Thus $\ker(T - T')$, which is a subspace of V, contains the span of $v_1, \ldots, v_n$, which is V. It follows that $T = T'$.

Let us prove existence now. Take any vector $v \in V$. Since $v_1, \ldots, v_n$ form a basis of V, we can uniquely express v as a linear combination $v = a_1 v_1 + \ldots + a_n v_n$ for some scalars $a_1, \ldots, a_n \in F$. Define $T(v) = a_1 u_1 + \ldots + a_n u_n$. By definition $T(v_i) = u_i$ for all i, and it remains to check that T is a linear transformation. Let $v, v' \in V$ and let c be a scalar. Write $v = a_1 v_1 + \ldots + a_n v_n$ and $v' = b_1 v_1 + \ldots + b_n v_n$ for some scalars $a_i, b_j \in F$. Then

$$v + cv' = (a_1 + cb_1)v_1 + \ldots + (a_n + cb_n)v_n,$$

thus

$$T(v + cv') = (a_1 + cb_1)u_1 + \ldots + (a_n + cb_n)u_n =$$

$$(a_1 u_1 + \ldots + a_n u_n) + c(b_1 u_1 + \ldots + b_n u_n) = T(v) + cT(v'),$$

which proves the linearity of T and finishes the proof. □

Problem 5.20. Find a linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^4$, whose image is the linear span of the set of vectors

$$\{(1, 2, 1, 1), (3, 1, 5, 2)\}.$$

Solution. Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$ be the standard basis of $\mathbf{R}^3$. Let $v_1 = (1, 2, 1, 1)$ and $v_2 = (3, 1, 5, 2)$. By Proposition 5.19 there is a linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^4$ such that

$$T(e_1) = v_1, \quad T(e_2) = v_2, \quad T(e_3) = 0.$$

The image of T is precisely the set of linear combinations of $T(e_1)$, $T(e_2)$ and $T(e_3)$, and this is clearly the span of v_1, v_2.

We note that T is very far from being unique: we could have taken $T(e_3) = v_2$ for instance (there are actually lots of linear maps with the desired property). □

Problem 5.21. Let

$$v_1 = (1, 0, 0), \quad v_2 = (1, 1, 0), \quad v_3 = (1, 1, 1)$$

and let $T : \mathbf{R}^3 \to \mathbf{R}^2$ be a linear transformation such that

$$T(v_1) = (3, 2), \quad T(v_2) = (-1, 2), \quad T(v_3) = (0, 1).$$

Compute the value of $T(5, 3, 1)$.

Solution. We look for scalars a, b, c such that

$$(5, 3, 1) = av_1 + bv_2 + cv_3,$$

as then, by linearity,

$$T(5, 3, 1) = aT(v_1) + bT(v_2) + cT(v_3).$$

The equality

$$(5, 3, 1) = av_1 + bv_2 + cv_3,$$

is equivalent to

$$(5, 3, 1) = (a, 0, 0) + (b, b, 0) + (c, c, c) = (a + b + c, b + c, c).$$

Thus $c = 1$, $b + c = 3$ and $a + b + c = 5$, which gives

$$c = 1, \quad b = 2, \quad a = 2.$$

It follows that

$$T(5, 3, 1) = 2T(v_1) + 2T(v_2) + T(v_3) = (6, 4) + (-2, 4) + (0, 1) = (4, 9). \square$$

Remark 5.22. One can easily check that v_1, v_2, v_3 form a basis of $\mathbf{R}^3$, thus such a map exists by Proposition 5.19.

Problem 5.23. Determine the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ such that

$$T(1, 0, 1) = (1, 0, 0), \quad T(0, 1, 1) = (0, 1, 0), \quad T(0, 0, 1) = (1, 1, 1).$$

Solution. We start with an arbitrary vector $v = (x_1, x_2, x_3)$ and look for scalars k_1, k_2, k_3 such that

$$v = k_1(1, 0, 1) + k_2(0, 1, 1) + k_3(0, 0, 1).$$

If we find such scalars, then

$$T(v) = k_1T(1, 0, 0) + k_2T(0, 1, 1) + k_3T(0, 0, 1) =$$

$$(k_1, 0, 0) + (0, k_2, 0) + (k_3, k_3, k_3) = (k_1 + k_3, k_2 + k_3, k_3).$$

The equality

$$v = k_1(1, 0, 1) + k_2(0, 1, 1) + k_3(0, 0, 1)$$

is equivalent to

$$(x_1, x_2, x_3) = (k_1, k_2, k_1 + k_2 + k_3)$$

or

$$k_1 = x_1, \quad k_2 = x_2, \quad k_3 = x_3 - x_1 - x_2.$$

Thus for all $(x_1, x_2, x_3) \in \mathbf{R}^3$

$$T(x_1, x_2, x_3) = (k_1 + k_3, k_2 + k_3, k_3) = (x_3 - x_2, x_3 - x_1, x_3 - x_1 - x_2). \quad \square$$

5.2.1 *Problems for practice*

1. Describe the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ such that

$$T(0, 1, 1) = (1, 2, 3), \quad T(1, 0, 1) = (1, -1, 2)$$

and

$$T(1, 1, 0) = (-1, -1, -1).$$

2. Is there a linear map $T : \mathbf{R}^2 \to \mathbf{R}^2$ such that

$$T(1, 1) = (1, 2), \quad T(1, -1) = (-1, 2), \quad T(2, 3) = (1, 2)?$$

3. Find all real numbers x for which there is a linear map $T : \mathbf{R}^3 \to \mathbf{R}^3$ such that

$$T(1, 1, 1) = (1, x, 1), \quad T(1, 0, -1) = (1, 0, 1)$$

and

$$T(-1, -1, 0) = (1, 2, 3), \quad T(1, -1, -1) = (1, x, -2).$$

4. Find a linear map $T : \mathbf{R}^4 \to \mathbf{R}^3$ whose image is the span of the vectors $(-1, -1, -1)$ and $(1, 2, 3)$.
5. a) Let V be the space of polynomials with real coefficients whose degree does not exceed 3. Find all positive integers n for which there is a bijective linear map between V and $M_n(\mathbf{R})$.
   b) Answer the same question if the word bijective is replaced with injective.
   c) Answer the same question if the word bijective is replaced with surjective.

5.3 Matrix Representation of Linear Transformations

We have already seen in the chapter devoted to matrices that all linear maps $T : F^n \to F^m$ are described by matrices $A \in M_{m,n}(F)$. We will try to extend this result and describe linear maps $F : V \to W$ between finite dimensional vector spaces V, W in terms of matrices. The description will not be canonical, we will need to fix bases in V and W. **All vector spaces in this section are finite dimensional over F.**

It will be convenient to introduce the following definition:

Definition 5.24. A linear transformation $T : V \to W$ is called an **isomorphism of vector spaces** or **invertible** if it is bijective. In this case we write $V \simeq W$ (the map T being understood).

Problem 5.25. Let $T : V \to W$ be an isomorphism of vector spaces. Prove that its inverse $T^{-1} : W \to V$ is an isomorphism of vector spaces.

Solution. The map T^{-1} is clearly bijective, with inverse T. We only need to check that T^{-1} is linear, i.e.

$$T^{-1}(w_1 + cw_2) = T^{-1}(w_1) + cT^{-1}(w_2)$$

for all vectors $w_1, w_2 \in W$ and all scalars $c \in F$. Let $v_1 = T^{-1}(w_1)$ and $v_2 = T^{-1}(w_2)$. Then $T(v_1) = w_1$ and $T(v_2) = w_2$, thus

$$T^{-1}(w_1 + cw_2) = T^{-1}(T(v_1) + cT(v_2)) = T^{-1}(T(v_1 + cv_2)) = v_1 + cv_2,$$

as needed. □

It turns out that we can completely classify finite dimensional nonzero vector spaces up to isomorphism: **for each positive integer n, all vector spaces of dimension n are isomorphic to F^n**. More precisely:

Theorem 5.26. *Let n be a positive integer and let V be a vector space of dimension n over F. If $B = (e_1, \ldots, e_n)$ is a basis, then the map $i_B : F^n \to V$ sending $(x_1, \ldots, x_n)$ to $x_1e_1 + x_2e_2 + \ldots + x_ne_n$ is an isomorphism of vector spaces.*

Proof. It is clear that i_B is linear and by definition of a basis it is bijective. The result follows. □

Remark 5.27. Conversely, if $T : V \to W$ is an isomorphism of vector spaces, then necessarily $\dim V = \dim W$. This is Corollary 5.18 (recall that we only work with finite dimensional vector spaces).

Thus the choice of a basis in a vector space of dimension n allows us to identify it with F^n. Consider now a linear map $T : V \to W$ and suppose that $\dim V = n$ and $\dim W = m$. **Choose** bases $B_V = (v_1, \ldots, v_n)$ and $B_W = (w_1, \ldots, w_m)$ in V and W, respectively. By the previous theorem we have isomorphisms

$$i_{B_V} : F^n \to V, \quad i_{B_W} : F^m \to W.$$

We produce a linear map φ by composing the maps $i_{B_V} : F^n \to V$, $T : V \to W$ and $i_{B_W}^{-1} : W \to F^m$:

$$\varphi_T : F^n \to F^m, \quad \varphi_T = i_{B_W}^{-1} \circ T \circ i_{B_V}.$$

Since φ_T is a linear map between F^n and F^m it is uniquely described by a matrix $A \in M_{m,n}(F)$. This is the **matrix of T with respect to the bases B_V and B_W**. It highly depends on the two bases, so we prefer to denote it $\mathrm{Mat}_{B_W,B_V}(T)$. We put B_W (i.e., the basis on the target of T) before B_V (the basis at the source of T) in the notation of the matrix for reasons which will be clear later on. When $V = W$ and we fix a basis B of V, we write $\mathrm{Mat}_B(T)$ instead of $\mathrm{Mat}_{B,B}(T)$, the matrix of T with respect to the basis B both at the source and target of T.

The previous construction looks rather complicated, but it is very natural: we have a parametrization of linear maps between F^n and F^m by matrices, and we can extend it to a description of linear maps between V and W by identifying V with F^n and W with F^m, via the choice of bases in V and W. Note the fundamental relation

$$i_{B_W}(AX) = T(i_{B_V}(X)) \quad \text{if} \quad X \in F^n \quad \text{and} \quad A = \mathrm{Mat}_{B_W,B_V}(T). \tag{5.1}$$

Taking for X a vector in the canonical basis of F^n, we can make everything completely explicit: let $e_1, \ldots, e_n$ be the canonical basis of F^n and $f_1, \ldots, f_m$ the canonical basis of F^m. If $A = [a_{ij}]$, then by definition $Ae_i = a_{1i} f_1 + \ldots + a_{mi} f_m$, thus for $X = e_i$ we have

$$\begin{aligned} i_{B_W}(AX) &= i_{B_W}(a_{1i} f_1 + a_{2i} f_2 + \ldots + a_{mi} f_m) \\ &= a_{1i} w_1 + a_{2i} w_2 + \ldots + a_{mi} w_m \end{aligned}$$

On the other hand, $i_{B_V}(e_i) = v_i$, thus relation (5.1) is equivalent to the fundamental and more concrete relation

$$T(v_i) = a_{1i} w_1 + a_{2i} w_2 + \ldots + a_{mi} w_m. \tag{5.2}$$

In other words:

Proposition 5.28. *Let $T : V \to W$ be a linear transformation and let $B_V = (v_1, \ldots, v_n)$, $B_W = (w_1, \ldots, w_m)$ be bases in V and W. Then column j of $\mathrm{Mat}_{B_W,B_V}(T) \in M_{m,n}(F)$ consists in the coordinates of $T(v_i)$ with respect to the basis B_W. In other words, if $\mathrm{Mat}_{B_W,B_V}(T) = [a_{ij}]$ then for all $1 \leq i \leq n$ we have*

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

Problem 5.29. Find the matrix representation of the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ defined by

$$T(x, y, z) = (x + 2y - z, y + z, x + y - 2z)$$

with respect to the standard basis of $\mathbf{R}^3$.

Solution. Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ be the standard basis of $\mathbf{R}^3$. Then

$$T(e_1) = T(1, 0, 0) = (1, 0, 1) = 1e_1 + 0e_2 + 1e_3$$

$$T(e_2) = T(0, 1, 0) = (2, 1, 1) = 2e_1 + 1e_2 + 1e_3$$

$$T(e_3) = T(0, 0, 1) = (-1, 1, -2) = -1e_1 + 1e_2 - 2e_3.$$

Thus the matrix representation of T with respect to the standard basis is

$$\begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 1 \\ 1 & 1 & -2 \end{bmatrix}.$$

□

Problem 5.30. Let P_n be the vector space of polynomials with real coefficients, of degree less than n. A linear transformation $T : P_3 \to P_5$ is given by

$$T(P(X)) = P(X) + X^2 P(X)$$

a) Find the matrix of this transformation with respect to the basis $B = \{1, X + 1, X^2 + 1\}$ of P_3 and the standard basis $C = \{1, X, X^2, X^3, X^4\}$ of P_5.
b) Show that T is not onto and it is injective.

Solution. a) We need to find the coordinates of $T(1)$, $T(X + 1)$ and $T(X^2 + 1)$ with respect to the basis C. We have

$$T(1) = 1 + X^2 = 1 \cdot 1 + 0 \cdot X + 1 \cdot X^2 + 0 \cdot X^3 + 0 \cdot X^4,$$

$$T(X+1) = X+1+X^2(X+1) = 1+X+X^2+X^3 = 1\cdot 1+1\cdot X+1\cdot X^2+1\cdot X^3+0\cdot X^4,$$

$$T(X^2+1) = X^2+1+X^2(X^2+1) = 1+2X^2+X^4 = 1\cdot 1+0\cdot X+2\cdot X^2+0\cdot X^3+X^4.$$

It follows that the required matrix is

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

b) Since $\dim P_5 = 5 > \dim P_3 = 3$, T cannot be onto. To prove that T is injective, it suffices to check that $\ker(T) = 0$. But if $P \in \ker(T)$, then $P(X) + X^2P(X) = 0$, thus $(1 + X^2)P(X) = 0$. Since $1 + X^2 \neq 0$, it follows that $P(X) = 0$ and so $\ker(T) = 0$. □

Problem 5.31. Let V be the space of polynomials with real coefficients whose degree does not exceed n, a fixed positive integer. Consider the map

$$T : V \to V, \quad T(P(X)) = P(X + 1).$$

(a) Prove that T is an invertible linear transformation.
(b) What are the matrices of T and T^{-1} with respect to the basis $1, X, \ldots, X^n$ of V?

Solution. a) It is not difficult to see that T is a linear transformation, for if P_1, P_2 are vectors in V and c is a scalar, we have

$$T((P_1 + cP_2)(X)) = (P_1 + cP_2)(X + 1) = P_1(X + 1) + cP_2(X + 1)$$

$$= T(P_1(X)) + cT(P_2(X)).$$

Next, to see that T is invertible it suffices to prove that T is bijective. We can easily find the inverse of T by solving the equation $P(X + 1) = Q(X)$. This is equivalent to $P(X) = Q(X-1)$, thus the inverse of T is given by $T^{-1}(P(X)) = P(X - 1)$.

b) For $0 \leq j \leq n$ the binomial formula yields

$$T(X^j) = (X + 1)^j = \sum_{i=0}^{j} \binom{j}{i} X^i$$

and

$$T^{-1}(X^j) = (X - 1)^j = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} X^i.$$

Thus if $A = [a_{ij}]$ and $B = [b_{ij}]$ are the matrices of T, respectively T^{-1} with respect to the basis $1, X, \ldots, X^n$, we have (with the standard convention that $\binom{n}{k} = 0$ for $n < k$)

$$a_{ij} = \binom{j}{i}, \quad b_{ij} = (-1)^{j-i} \binom{j}{i}.$$

□

Remark 5.32. Since T and T^{-1} are inverse to each other, the product of the matrices A and B is the identity matrix I_n. We invite the reader to use this in order to prove the following combinatorial identity:

$$\sum_{j=0}^{n}(-1)^{k-j}\binom{j}{i}\binom{k}{j} = \delta_{i,k},$$

where the right-hand side equals 1 if $i = k$ and 0 otherwise.

The next result follows formally from the fundamental bijection between linear maps $F^n \to F^m$ and matrices in $M_{m,n}(F)$. Recall that $\mathrm{Hom}(V, W)$ is the vector space of linear maps $T : V \to W$.

Theorem 5.33. *Let B_V, B_W be bases in two (finite-dimensional) vector spaces V, W. The map $T \to \mathrm{Mat}_{B_W,B_V}(T)$ sending a linear transformation $T : V \to W$ to its matrix with respect to B_V and B_W is an isomorphism of vector spaces*

$$\mathrm{Hom}(V, W) \simeq M_{m,n}(F).$$

Proof. Let $\varphi(T) = \mathrm{Mat}_{B_W,B_V}(T)$. It is clear from Proposition 5.28 that φ is a linear map from $\mathrm{Hom}(V, W)$ to $M_{m,n}(F)$. It is moreover injective, since if $\varphi(T) = 0$, Proposition 5.28 yields $T(v_i) = 0$ for all i, thus $\ker T$ contains $\mathrm{Span}(v_1, \ldots, v_n) = V$ and $T = 0$. To see that φ is surjective, start with any matrix $A = [a_{ij}] \in M_{m,n}(F)$. It induces a linear transformation $\varphi_A : F^n \to F^m$ defined by $X \to AX$. By construction, the linear transformation $T = i_{B_W} \circ \varphi_A \circ i_{B_V}^{-1}$ satisfies $\varphi(T) = A$. More concretely, since $v_1, \ldots, v_n$ is a basis of V, there is a unique linear map $T : V \to W$ such that

$$T(v_i) = \sum_{j=1}^{m} a_{ji} w_j$$

for all $1 \leq i \leq n$ (Proposition 5.19). By Proposition 5.28 we have $\mathrm{Mat}_{B_W,B_V} = A$ and we are done. □

Recall that $\dim M_{m,n}(F) = mn$, a basis being given by the canonical basis $(E_{ij})_{1\leq i\leq m, 1\leq j\leq n}$. The theorem and Remark 5.27 yield

$$\dim \mathrm{Hom}(V, W) = \dim V \cdot \dim W.$$

We conclude this section with some rather technical issues, but which are absolutely fundamental in the theory of linear transformations. First, we want to understand the link between the matrix of a composition $T \circ S$ of linear maps and the matrices of T and S. More precisely, fix two linear maps $T : V \to W$ and $S : W \to U$ and set $m = \dim V$, $n = \dim W$, $p = \dim U$. Also, fix three bases B_U, B_V and B_W in U, V, W respectively. Let us write for simplicity

$$\mathcal{A} = \mathrm{Mat}_{B_U,B_W}(S) \quad \text{and} \quad \mathcal{B} = \mathrm{Mat}_{B_W,B_V}(T).$$

Corresponding to B_U, B_V, B_W we have isomorphisms

$$i_{B_V} : F^m \to V, \quad i_{B_W} : F^n \to W, \quad i_{B_U} : F^p \to U$$

and by definition of $\mathcal{A}, \mathcal{B}$ we have (relation (5.1))

$$i_{B_W}(\mathcal{B}X) = T(i_{B_V}(X)), X \in F^m, \quad i_{B_U}(\mathcal{A}Y) = S(i_{B_W}(Y)), Y \in F^p.$$

Applying S to the first relation and then using the second one, we obtain for $X \in F^m$

$$S \circ T(i_{B_V}(X)) = S(i_{B_W}(\mathcal{B}X)) = i_{B_U}(\mathcal{A}\mathcal{B}X).$$

This last relation and the definition of $\mathrm{Mat}_{B_U,B_V}(S \circ T)$ show that

$$\mathrm{Mat}_{B_U,B_V}(S \circ T) = \mathcal{A} \cdot \mathcal{B}.$$

In other words, **composition of linear transformations comes down to multiplication of matrices** or formally

Theorem 5.34. *Let $T : V \to W$ and $S : W \to U$ be linear transformations between finite-dimensional vector spaces and let B_U, B_V, B_W be bases of U, V and W, respectively. Then*

$$\mathrm{Mat}_{B_U,B_V}(S \circ T) = \mathrm{Mat}_{B_U,B_W}(S) \cdot \mathrm{Mat}_{B_W,B_V}(T).$$

A less technical corollary which will be constantly used is the following:

Corollary 5.35. *Let $T_1, T_2 : V \to V$ be linear transformations on a finite dimensional vector space V and let B be a basis of V. Then*

$$\mathrm{Mat}_B(T_1 \circ T_2) = \mathrm{Mat}_B(T_1) \cdot \mathrm{Mat}_B(T_2).$$

Problem 5.36. Let V be the space of polynomials with real coefficients whose degree does not exceed 2. Consider the maps

$$T : \mathbf{R}^3 \to V, \quad T(a, b, c) = a + 2bX + 3cX^2$$

and

$$S : V \to M_2(\mathbf{R}), \quad S(a + bX + cX^2) = \begin{bmatrix} a & a+b \\ a-c & b \end{bmatrix}.$$

We consider the basis $B_1 = (1, X, X^2)$ of V, the canonical basis B_2 of $\mathbf{R}^3$ and the canonical basis $B_3 = (E_{11}, E_{12}, E_{21}, E_{22})$ of $M_2(\mathbf{R})$.

a) Check that T and S are linear maps.
b) Write down the matrices of T and S with respect to the previous bases.

c) Find the matrix of the composition $S \circ T$ with respect to the previous bases.
d) Compute explicitly $S \circ T$, then find directly its matrix with respect to the previous bases and check that you obtain the same result as in c).

Solution. a) Let u be a real number and let (a, b, c) and (a', b', c') be vectors in $\mathbf{R}^3$. Then

$$T(u(a,b,c) + (a',b',c')) = T(au + a', bu + b', cu + c')$$

$$= (au + a') + 2(bu + b')X + 3(cu + c')X^2 =$$

$$u(a + 2bX + 3cX^2) + (a' + 2b'X + 3c'X^2) = uT(a,b,c) + T(a',b',c'),$$

thus T is linear. One checks similarly that S is linear.

b) We start by computing the matrix $\mathrm{Mat}_{B_1,B_2}(T)$ of T with respect to B_1 and B_2. Let $B_2 = (e_1, e_2, e_3)$ be the canonical basis of $\mathbf{R}^3$, then

$$T(e_1) = T(1,0,0) = 1 = 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2,$$

$$T(e_2) = T(0,1,0) = 2X = 0 \cdot 1 + 2 \cdot X + 0 \cdot X^2,$$

$$T(e_3) = T(0,0,1) = 3X^2 = 0 \cdot 1 + 0 \cdot X + 3 \cdot X^2,$$

hence

$$\mathrm{Mat}_{B_1,B_2}(T) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Similarly, we compute

$$S(1) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = 1 \cdot E_{11} + 1 \cdot E_{12} + 1 \cdot E_{21} + 0 \cdot E_{22},$$

$$S(X) = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = 0 \cdot E_{11} + 1 \cdot E_{12} + 0 \cdot E_{21} + 1 \cdot E_{22},$$

$$S(X^2) = \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} = 0 \cdot E_{11} + 0 \cdot E_{12} + (-1) \cdot E_{21} + 0 \cdot E_{22},$$

hence

$$\mathrm{Mat}_{B_3,B_1}(S) = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}.$$

c) Using the theorem, we obtain

$$\mathrm{Mat}_{B_3,B_2}(S \circ T) = \mathrm{Mat}_{B_3,B_1}(S) \cdot \mathrm{Mat}_{B_1,B_2}(T)$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & -3 \\ 0 & 2 & 0 \end{bmatrix}.$$

d) We compute

$$(S \circ T)(a,b,c) = S(T(a,b,c) = S(a + 2bX + 3cX^2) = \begin{bmatrix} a & a+2b \\ a-3c & 2b \end{bmatrix}.$$

Next,

$$(S \circ T)(e_1) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = 1 \cdot E_{11} + 1 \cdot E_{12} + 1 \cdot E_{21} + 0 \cdot E_{22},$$

$$(S \circ T)(e_2) = \begin{bmatrix} 0 & 2 \\ 0 & 2 \end{bmatrix} = 0 \cdot E_{11} + 2 \cdot E_{12} + 0 \cdot E_{21} + 2 \cdot E_{22}$$

and

$$(S \circ T)(e_3) = \begin{bmatrix} 0 & 0 \\ -3 & 0 \end{bmatrix} = 0 \cdot E_{11} + 0 \cdot E_{12} + (-3) \cdot E_{21} + 0 \cdot E_{22}$$

and so the matrix of $S \circ T$ is

$$\mathrm{Mat}_{B_3,B_2}(S \circ T) = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & -3 \\ 0 & 2 & 0 \end{bmatrix},$$

which coincides of course with the one obtained in part c). □

Problem 5.37. Let $A \in M_n(F)$ and let $T : F^n \to F^n$ be the linear map sending X to AX. Prove that A is invertible if and only if T is bijective.

Solution. If A is invertible, let $B \in M_n(F)$ be such that $AB = BA = I_n$. Let $S : F^n \to F^n$ be the map $X \to BX$. Then $S \circ T$ has associated matrix (with respect to the canonical basis in F^n) $BA = I_n$, thus $S \circ T = \mathrm{Id}$. Similarly, $T \circ S = \mathrm{id}$, thus T is bijective.

Next, suppose that T is bijective and let B be the matrix of T^{-1} with respect to the canonical basis. Then AB is the matrix of $T \circ T^{-1} = \mathrm{id}$ with respect to the canonical basis, thus $AB = I_n$. Similarly $BA = I_n$ and A is invertible with inverse B. □

Next, suppose that we have a linear map $T : V \to W$, with a given matrix A with respect to two bases $\mathcal{B}_1, \mathcal{C}_1$ of V, W respectively. Let us choose two new bases $\mathcal{B}_2, \mathcal{C}_2$ of V, W respectively. We would like to understand the matrix of T with respect to the new bases. To answer this, we need to introduce an important object:

Definition 5.38. Let V be a vector space and let $B = (v_1, \ldots, v_n)$ and $B' = (v'_1, \ldots, v'_n)$ be two bases of V. The **change of basis matrix from B to B'** is the matrix $P = [p_{ij}]$ whose columns are the coordinates of the vectors $v'_1, \ldots, v'_n$ when expressed in the basis B. Thus

$$v'_j = p_{1j} v_1 + \ldots + p_{nj} v_n$$

for $1 \leq j \leq n$.

Problem 5.39. Consider the vectors

$$v_1 = (1, 2), \quad v_2 = (1, 3).$$

a) Prove that $\mathcal{B}' = (v_1, v_2)$ is a basis of $\mathbf{R}^2$.
b) Find the change of basis matrix from $\mathcal{B}'$ to the canonical basis of $\mathbf{R}^2$.

Solution. a) It suffices to check that v_1 and v_2 are linearly independent. If $av_1 + bv_2 = 0$ for some real numbers a, b, then

$$(a, 2a) + (b, 3b) = (0, 0)$$

thus

$$a + b = 0, \quad 2a + 3b = 0.$$

Replacing $b = -a$ in the second equation yields $a = b = 0$.

b) Let $\mathcal{B} = (e_1, e_2)$ be the canonical basis. We need to express e_1, e_2 in terms of v_1, v_2. Let us look for a, b such that

$$e_1 = av_1 + bv_2.$$

Equivalently, we want

$$a + b = 1, \quad 2a + 3b = 0.$$

This has the unique solution $a = 3, b = -2$, thus

$$e_1 = 3v_1 - 2v_2.$$

Similarly, we obtain

$$e_2 = -v_1 + v_2.$$

The coordinates $3, -2$ of e_1 when written in base $\mathcal{B}'$ yield the first column of the change of basis matrix, and the coordinates $-1, 1$ of e_2 when written in base $\mathcal{B}'$ yield the second column, thus the change of basis matrix is

$$P = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix}.$$

□

Problem 5.40. Let V, B, B', P be as above. Consider a vector $v \in V$ and let X and X' be the column vectors representing the coordinates of v with respect to the bases B and B'. Prove that $X = PX'$.

Solution. Indeed, by definition we have

$$v = x_1 v_1 + \ldots + x_n v_n = x'_1 v'_1 + \ldots + x'_n v'_n,$$

thus

$$\sum_{k=1}^{n} x_k v_k = \sum_{j=1}^{n} x'_j v'_j = \sum_{j=1}^{n} x'_j \sum_{k=1}^{n} p_{kj} v_k$$

$$= \sum_{k=1}^{n} (\sum_{j=1}^{n} p_{kj} x'_j) v_k = \sum_{k=1}^{n} (PX')_k v_k$$

and since $v_1, \ldots, v_n$ are linearly independent, it follows that $X = PX'$. □

Remark 5.41. The previous definition and problem are always a source of confusion and trouble, so let us insist on the following issue: the change of basis matrix from B to B' expresses B' in terms of B, **however** (and this is very important in practice) as the problem shows, the change of basis matrix takes coordinates with respect to B' to coordinates with respect to B. Thus we have a change of direction.

We also write $\mathrm{Mat}_B(B')$ for the change of basis matrix from B to B'. A simple but very important observation is that

$$\mathrm{Mat}_B(B') = \mathrm{Mat}_{B,B'}(\mathrm{id}_V),$$

as follows directly from Proposition 5.28. Using this observation and Theorem 5.34, we deduce that for any bases B, B', B'' of V we have

$$\mathrm{Mat}_B(B') \cdot \mathrm{Mat}_{B'}(B'') = \mathrm{Mat}_B(B'').$$

Since $\mathrm{Mat}_B(B) = I_n$ for any basis B, we deduce that

$$\mathrm{Mat}_B(B') \cdot \mathrm{Mat}_{B'}(B) = I_n.$$

Thus **the change of basis matrix is invertible** and its inverse is simply the change of basis matrix for the bases B', B.

Problem 5.42. Consider the families of vectors $\mathcal{B} = (v_1, v_2, v_3)$, $\mathcal{B}' = (w_1, w_2, w_3)$, where

$$v_1 = (0, 1, 1), \quad v_2 = (1, 0, 1), \quad v_3 = (1, 1, 0)$$

and

$$w_1 = (1, 1, -1), \quad w_2 = (1, 0, -1), \quad w_3 = (-1, -1, 0).$$

a) Prove that $\mathcal{B}$ and $\mathcal{B}'$ are bases of $\mathbf{R}^3$.
b) Find the change of basis matrix P from $\mathcal{B}$ to $\mathcal{B}'$ going back to the definition of P.
c) Find the change of basis matrix P using the canonical basis of $\mathbf{R}^3$ and the previous theorem.

Solution. a) To prove that $\mathcal{B}$ is a basis, we find the reduced row-echelon form of the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

using row-reduction. This yields

$$A_{ref} = I_3$$

and so v_1, v_2, v_3 are linearly independent, hence a basis of $\mathbf{R}^3$. We proceed similarly with w_1, w_2, w_3.

b) First, we use the definition of P: the columns of P are the coordinates of w_1, w_2, w_3 when expressed in the basis $\mathcal{B}$. First, we try to express

$$w_1 = av_1 + bv_2 + cv_3 = (b + c, a + c, a + b)$$

which gives

$$b + c = 1, \quad a + c = 1, \quad a + b = -1,$$

with the solution

$$a = -\frac{1}{2} = b, \quad c = \frac{3}{2}.$$

Thus

$$w_1 = -\frac{1}{2}v_1 - \frac{1}{2}v_2 + \frac{3}{2}v_3$$

and the first column of P is $\begin{bmatrix} -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{3}{2} \end{bmatrix}$. Similar arguments yield

$$w_2 = -v_1 + v_3,$$

hence the second column of P is $\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}$ and finally $w_3 = -v_3$, thus the third column of P is $\begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$. We conclude that

$$P = \begin{bmatrix} -\frac{1}{2} & -1 & 0 \\ -\frac{1}{2} & 0 & 0 \\ \frac{3}{2} & 1 & -1 \end{bmatrix}.$$

c) Let $\mathcal{B}'' = (e_1, e_2, e_3)$ be the canonical basis of $\mathbf{R}^3$. We want to find $\mathrm{Mat}_B(B')$ and we write it as

$$\mathrm{Mat}_{\mathcal{B}}(\mathcal{B}') = \mathrm{Mat}_{\mathcal{B}}(\mathcal{B}'') \cdot \mathrm{Mat}_{\mathcal{B}''}(\mathcal{B}') = (\mathrm{Mat}_{\mathcal{B}''}(\mathcal{B}))^{-1} \cdot \mathrm{Mat}_{\mathcal{B}''}(\mathcal{B}').$$

Next, by definition

$$\mathrm{Mat}_{\mathcal{B}''}(\mathcal{B}) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad \mathrm{Mat}_{\mathcal{B}''}(\mathcal{B}') = \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & -1 \\ -1 & -1 & 0 \end{bmatrix}.$$

Next, using either the row-reduction algorithm or by solving the system $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} X = b$, one computes

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

and finally

$$P = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & -1 \\ -1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} & -1 & 0 \\ -\frac{1}{2} & 0 & 0 \\ \frac{3}{2} & 1 & -1 \end{bmatrix}.$$

Without any miracle, we obtain the same result as in part b)! □

Similar arguments give the following fundamental:

Theorem 5.43. *Let $T : V \to W$ be a linear map and let B_1, B_2 be two bases of V, C_1, C_2 two bases of W. If $P = \mathrm{Mat}_{C_1}(C_2)$ and $Q = \mathrm{Mat}_{B_1}(B_2)$ are the change of basis matrices, then*

$$\mathrm{Mat}_{C_2,B_2}(T) = P^{-1}\mathrm{Mat}_{C_1,B_1}(T)Q.$$

Proof. By Theorem 5.34 we have

$$P\mathrm{Mat}_{C_2,B_2}(T) = \mathrm{Mat}_{C_1,C_2}(\mathrm{id}_W) \cdot \mathrm{Mat}_{C_2,B_2}(T) = \mathrm{Mat}_{C_1,B_2}(T)$$

and similarly

$$\mathrm{Mat}_{C_1,B_1}(T)Q = \mathrm{Mat}_{C_1,B_1}(T)\mathrm{Mat}_{B_1,B_2}(\mathrm{id}_V) = \mathrm{Mat}_{C_1,B_2}(T).$$

Thus

$$P\mathrm{Mat}_{C_2,B_2}(T) = \mathrm{Mat}_{C_1,B_1}(T)Q$$

and the result follows by multiplying on the left by the invertible matrix P. □

Here is a different proof which has the advantage that it also shows us how to recover the rather complicated formula in the previous theorem (experience shows that it is almost impossible to learn this formula by heart). It assumes familiarity with the result of Problem 5.40 (which is however much easier to remember!).

Write A_1 for the matrix of T with respect to B_1, C_1 and A_2 for the matrix of T with respect to B_2, C_2. Start with a vector v in V and write X_1, X_2 for its coordinates with respect to B_1 and B_2 respectively. By Problem 5.40 we have $X_1 = QX_2$. Let Y_1, Y_2 be the coordinates of $T(v)$ with respect to C_1 and C_2 respectively. Again by Problem 5.40 we have $Y_1 = PY_2$. On the other hand, by definition of A_1 and A_2 we have $A_1X_1 = Y_1$ and $A_2X_2 = Y_2$. Since P and Q are invertible, we obtain $X_2 = Q^{-1}X_1$ and so

$$A_1X_1 = Y_1 = PY_2 = PA_2X_2 = PA_2Q^{-1}X_1.$$

Since this holds for every $v \in V$ (equivalently, for any X_1), we deduce that $A_1 = PA_2Q^{-1}$ and so $A_2 = P^{-1}AQ$.

While the previous results are quite a pain in the neck to state and remember, the following special case is absolutely fundamental and rather easy to remember (or reprove)

Corollary 5.44. *Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V and let B, B' be bases of V. If P is the change of basis matrix from B to B', then*

$$\mathrm{Mat}_{B'}(T) = P^{-1}\mathrm{Mat}_B(T)P.$$

Here is how one should recover this result in case of doubt: write X_v, X'_v for the column vectors representing the coordinates of $v \in V$ with respect to B, B'. Then

$$X_{T(v)} = \mathrm{Mat}_B(T)X, \quad X'_{T(v)} = \mathrm{Mat}_{B'}(T)X'$$

and by Problem 5.40 we have $X_v = PX'_v$ and $X_{T(v)} = PX'_{T(v)}$. Thus Combining these relations yields

$$P\mathrm{Mat}_{B'}(T) = \mathrm{Mat}_B(T)P,$$

both being equal to $PX'_{T(v)}$. Multiplying by P^{-1} yields the desired result.

Problem 5.45. Consider the matrix

$$A = \begin{bmatrix} 2 & -1 & 0 \\ -2 & 1 & -2 \\ 1 & 1 & 3 \end{bmatrix}$$

and let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the associated linear transformation, thus $T(X) = AX$ for all $X \in \mathbf{R}^3$. Consider the vectors

$$v_1 = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}.$$

a) Prove that v_1, v_2, v_3 form a basis of $\mathbf{R}^3$ and compute the matrix of T with respect to this basis.
b) Find the change of basis matrix from the canonical basis to the basis (v_1, v_2, v_3).
c) Compute A^n for all positive integers n.

Solution. a) It suffices to check that v_1, v_2, v_3 are linearly independent. If a, b, c are real numbers such that $av_1 + bv_2 + cv_3 = 0$, we obtain

$$a + b + c = 0, \quad a - c = 0, \quad -a - b = 0.$$

The first and third equations yield $c = 0$, then the second one gives $a = 0$ and finally $b = 0$. Thus v_1, v_2, v_3 are linearly independent and hence they form a basis. Another method for proving this is as follows: consider the matrix whose columns are the vectors v_1, v_2, v_3 are use row-reduction to bring this matrix to its reduced row-echelon form. We end up with I_3 and this shows that v_1, v_2, v_3 is a basis of $\mathbf{R}^3$.

To compute the matrix of T with respect to the new basis, we simply express each of the vectors $T(v_1), T(v_2), T(v_3)$ in terms of v_1, v_2, v_3. We have

$$T(v_1) = Av_1 = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} = v_1,$$

then

$$T(v_2) = Av_2 = \begin{bmatrix} 2 \\ 0 \\ -2 \end{bmatrix} = 2v_2$$

and

$$T(v_3) = Av_3 = \begin{bmatrix} 3 \\ -3 \\ 0 \end{bmatrix} = 3v_3.$$

We conclude that the matrix of T with respect to the basis (v_1, v_2, v_3) is

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

b) Call the change of basis matrix P. By definition, the columns of P consist of the coordinates of v_1, v_2, v_3 with respect to the canonical basis of $\mathbf{R}^3$. Thus

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ -1 & -1 & 0 \end{bmatrix}.$$

c) The matrix of T with respect to (v_1, v_2, v_3) is, thanks to the change of matrix formula, equal to $P^{-1}AP$. Combining this observation with part a), we deduce that

$$P^{-1}AP = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Raising this equality to the nth power and taking into account that $(P^{-1}AP)^n = P^{-1}A^nP$ (this follows easily by induction on n) yields

$$P^{-1}A^nP = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{bmatrix}.$$

It follows that

$$A^n = P \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{bmatrix} P^{-1}.$$

We can easily compute P^{-1} either by expressing the vectors of the canonical basis in terms of v_1, v_2, v_3, or by solving the system $PX = b$. We end up with

$$P^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -2 \\ 1 & 0 & 1 \end{bmatrix}.$$

Finally,

$$A^n = P \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ 0 & 0 & 3^n \end{bmatrix} P^{-1} = \begin{bmatrix} 1 - 2^n + 3^n & 1 - 2^n & 1 - 2^{n+1} + 3^n \\ 1 - 3^n & 1 & 1 - 3^n \\ 2^n - 1 & 2^n - 1 & 2^{n+1} - 1 \end{bmatrix}.$$

□

Problem 5.46. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear map defined by

$$T(x, y, z) = (2x + y - z, y, x + y).$$

Let e_1, e_2, e_3 be the canonical basis of $\mathbf{R}^3$ and let

$$v_1 = e_1 + e_3, \quad v_2 = -e_1 + e_2, \quad v_3 = e_1 + e_2 + e_3.$$

a) Prove that (v_1, v_2, v_3) is a basis of $\mathbf{R}^3$.
b) Find the matrix of T with respect to this basis.

Solution. a) In order to prove that (v_1, v_2, v_3) is a basis of $\mathbf{R}^3$, it suffices to check that they are linearly independent. If

$$av_1 + bv_2 + cv_3 = 0,$$

for some real numbers a, b, c, then

$$(a - b + c)e_1 + (b + c)e_2 + (a + c)e_3 = 0.$$

Since e_1, e_2, e_3 are linearly independent, this forces

$$a - b + c = 0, \quad b + c = 0, \quad a + c = 0.$$

The first and third equations yield $b = 0$, then $c = 0$ and $a = 0$. Thus (v_1, v_2, v_3) is a basis of $\mathbf{R}^3$. Another method for proving this is as follows: consider the matrix A whose columns are the coordinates of v_1, v_2, v_3 when expressed in terms of the canonical basis, that is

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

Row-reduction yields $A_{ref} = I_3$ and the result follows.

b) We compute

$$T(v_1) = T(1,0,1) = (1,0,1) = v_1,$$

then

$$T(v_2) = T(-1,1,0) = (-1,1,0) = v_2$$

and finally

$$T(v_3) = T(1,1,1) = (2,1,2).$$

To conclude, we need to express the vector $(2,1,2)$ in terms of v_1, v_2, v_3. We look therefore for a, b, c such that

$$(2,1,2) = av_1 + bv_2 + cv_3$$

or equivalently

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

Solving the corresponding linear system yields

$$a = 1, \quad b = 0, \quad c = 1.$$

Thus $T(v_3) = v_1 + v_3$ and so the matrix of T with respect to (v_1, v_2, v_3) is

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

□

Motivated by the previous corollary, we introduce the following fundamental definition:

Definition 5.47. Two matrices $A, B \in M_n(F)$ are called **similar** or **conjugate** if there exists $P \in \mathrm{GL}_n(F)$ such that $B = P^{-1}AP$. Equivalently, they are similar if they represent the same linear transformation of $V = F^n$ in possibly two different bases.

It is an easy exercise for the reader to prove that similarity is an **equivalence relation** on $M_n(F)$, that is

- any matrix A is similar to itself.
- If A is similar to B, then B is similar to A.
- If A is similar to B and B is similar to C, then A is similar to C.

One of the most fundamental problems in linear algebra is the classification of matrices up to similarity. In fact, the main goal of the next chapters is to prove that suitable matrices are similar to rather simple matrices: we dedicate a whole chapter to matrices similar to diagonal and upper-triangular ones, and we will see in the last chapter that any symmetric matrix with real entries is similar to a diagonal matrix.

5.3.1 Problems for practice

1. Let $\mathcal{B} = (e_1, e_2)$ be the canonical basis of $\mathbf{R}^2$ and let $\mathcal{B}' = (f_1, f_2)$, where

$$f_1 = e_1 + e_2, \quad f_2 = e_1 + 2e_2.$$

   a) Prove that $\mathcal{B}'$ is a basis of $\mathbf{R}^2$.
   b) Find the change of basis matrix P from $\mathcal{B}$ to $\mathcal{B}'$, as well as its inverse.
   c) Let T be the linear transformation on $\mathbf{R}^2$ whose matrix with respect to the basis $\mathcal{B}$ (both on the source and target of $\mathbf{R}^2$) is $A = \begin{bmatrix} 1 & -1 \\ 2 & -3 \end{bmatrix}$. Find the matrix of T with respect to the bases $\mathcal{B}'$ on the target and $\mathcal{B}$ on the source.

2. Consider the matrix

$$A = \begin{bmatrix} 17 & -28 & 4 \\ 12 & -20 & 3 \\ 16 & -28 & 5 \end{bmatrix}$$

   and the associated linear map $T : \mathbf{R}^3 \to \mathbf{R}^3$ defined by $T(X) = AX$.

   a) Find a basis $\mathcal{B}_1$ of the kernel of T.
   b) Let V be the kernel of $T - \mathrm{id}$, where id is the identity map on $\mathbf{R}^3$. Give a basis $\mathcal{B}_2$ of V.
   c) Prove that $V \oplus \ker(T) = \mathbf{R}^3$.
   d) Find the matrix of T with respect to the basis $\mathcal{B}_1 \cup \mathcal{B}_2$ of $\mathbf{R}^3$.

3. Let $\mathcal{B} = (v_1, v_2, v_3)$, where

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

   and let $\mathcal{B}' = (w_1, w_2, w_3)$, where

$$w_1 = \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix}, \quad w_2 = \begin{bmatrix} -3 \\ -2 \\ -4 \end{bmatrix}, \quad w_3 = \begin{bmatrix} -2 \\ -3 \\ -4 \end{bmatrix}.$$

a) Prove that $\mathcal{B}$ and $\mathcal{B}'$ are both bases of $\mathbf{R}^3$.
b) Find the change of basis matrix P from $\mathcal{B}$ to $\mathcal{B}'$ as well as its inverse P^{-1}.
c) Consider the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ whose matrix with respect to the basis $\mathcal{B}$ (both on the source and target of T) is $\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$. Find the matrix of T with respect to $\mathcal{B}'$ (both on the source and target of T).

4. Let V be a vector space over a field F, of dimension n. Let $T : V \to V$ be a projection (recall that this is a linear map such that $T \circ T = T$).

a) Prove that $V = \mathrm{Ker}(T) \oplus \mathrm{Im}(T)$.
b) Prove that there is a basis of V in which the matrix of T is $\begin{bmatrix} I_i & 0 \\ 0 & O_{n-i} \end{bmatrix}$ for some $i \in \{0, 1, \ldots, n\}$.

5. Let V be a vector space over $\mathbf{C}$ or $\mathbf{R}$, of dimension n. Let $T : V \to V$ be a symmetry (that is a linear transformation such that $T \circ T = \mathrm{id}$ is the identity map of V).

a) Prove that $V = \ker(T - \mathrm{id}) \oplus \ker(T + \mathrm{id})$.
b) Deduce that there is $i \in [0, n]$ and a basis of V such that the matrix of T with respect to this basis is $\begin{bmatrix} I_i & 0 \\ 0 & -I_{n-i} \end{bmatrix}$.

6. Let T be the linear transformation on $\mathbf{R}^3$ whose matrix with respect to the canonical basis is

$$A = \begin{bmatrix} -1 & 1 & 1 \\ -6 & 4 & 2 \\ 3 & -1 & 1 \end{bmatrix}.$$

a) Check that $A^2 = 2A$.
b) Deduce that $T(v) = 2v$ for all $v \in \mathrm{Im}(T)$.
c) Prove that $\ker(T)$ and $\mathrm{Im}(T)$ are in direct sum position in $\mathbf{R}^3$.
d) Give bases for $\ker(T)$ and $\mathrm{Im}(T)$, and write the matrix of T with respect to the basis of $\mathbf{R}^3$ deduced by patching the two bases of $\ker(T)$ and $\mathrm{Im}(T)$ respectively.

7. Let $A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ and consider the map $T : M_2(\mathbf{C}) \to M_2(\mathbf{C})$ defined by

$$T(B) = AB - BA.$$

a) Prove that T is linear.
b) Find the matrix of T with respect to the canonical basis of $M_2(\mathbf{C})$.

8. Let V be the vector space of polynomials with complex coefficients whose degree does not exceed 3. Let $T : V \to V$ be the map defined by $T(P) = P + P'$. Prove that T is linear and find the matrix of T with respect to the basis $1, X, X^2, X^3$ of V.
9. a) Find the matrix with respect to the canonical basis of the map which projects a vector $v \in \mathbf{R}^3$ to the xy-plane.
   b) Find the matrix with respect to the canonical basis of the map which sends a vector $v \in \mathbf{R}^3$ to its reflection with respect to the xy-plane.
   c) Let $\theta \in \mathbf{R}$. Find the matrix with respect to the canonical basis of the map which sends a vector $v \in \mathbf{R}^2$ to its rotation through an angle θ, counterclockwise.
10. Let V be a vector space of dimension n over F. A **flag** in V is a family of subspaces $V_0 \subset V_1 \subset \ldots \subset V_n$ such that $\dim V_i = i$ for all $i \in [0, n]$. Let $T : V \to V$ be a linear transformation. Prove that the following statements are equivalent:

    a) There is a flag $V_0 \subset \ldots \subset V_n$ in V such that $T(V_i) \subset V_i$ for all $i \in [0, n]$.
    b) There is a basis of V with respect to which the matrix of T is upper-triangular.

11. Prove that the matrices

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

    are similar.

5.4 Rank of a Linear Map and Rank of a Matrix

In this section we discuss a very important numerical invariant associated with a linear transformation and to a matrix: its **rank**. All vector spaces over the field F will be assumed to be finite dimensional in this section.

Definition 5.48. Let V, W be finite dimensional vector spaces over F. The **rank** of a linear map $T : V \to W$ is the integer

$$\operatorname{rank}(T) = \dim \operatorname{Im}(T).$$

Let us try to understand more concretely the previous definition. Let $T : V \to W$ be a linear transformation and let $v_1, \ldots, v_n$ be a basis of V. Then the elements of $\operatorname{Im}(T)$ are of the form $T(v)$ with $v \in V$. Since $v_1, \ldots, v_n$ span V, each $v \in V$ can be written $v = x_1 v_1 + \ldots + x_n v_n$ with $x_i \in F$, and

$$T(v) = T(x_1 v_1 + \ldots + x_n v_n) = x_1 T(v_1) + \ldots + x_n T(v_n).$$

Thus $T(v_1), \ldots, T(v_n)$ is a spanning set for $\mathrm{Im}(T)$ and

$$\mathrm{rank}(T) = \dim \mathrm{Span}(T(v_1), \ldots, T(v_n)).$$

Since we have already seen an algorithmic way of computing the span of a finite family of vectors (using row-reduction, see the discussion preceding Example 4.30), this gives an algorithmic way of computing the rank of a linear transformation. More precisely, pick a basis $w_1, \ldots, w_m$ of W and express each of the vectors $T(v_1), \ldots, T(v_n)$ as linear combinations of $w_1, \ldots, w_m$. Consider the matrix A whose rows are the coordinates of $T(v_1), \ldots, T(v_n)$ when expressed in the basis $w_1, \ldots, w_m$ of W. Performing elementary operations on the rows of A does not change the span of $T(v_1), \ldots, T(v_n)$, so that $\mathrm{rank}(T)$ is the dimension of the span of the rows of A_{ref}, then reduced row-echelon form of A. On the other hand, it is very easy to compute the last dimension: by definition of the reduced row-echelon form, the dimension of the span of the rows of A_{ref} is precisely the number of nonzero rows in A_{ref} or, equivalently, the number of pivots in A_{ref}. Thus

$$\mathrm{rank}(T) = \text{number of nonzero rows of } A_{ref} = \text{number of pivots in } A_{ref}.$$

Let us see two concrete examples:

Problem 5.49. Compute the rank of the linear map $T : \mathbf{R}^3 \to \mathbf{R}^4$ defined by

$$T(x, y, z) = (x + y + z, x - y, y - z, z - x).$$

Solution. We let v_1, v_2, v_3 be the canonical basis of $\mathbf{R}^3$ and compute

$$T(v_1) = T(1, 0, 0) = (1, 1, 0, -1),$$

thus the first row of the matrix A in the previous discussion is $(1, 1, 0, -1)$. We do the same with v_2, v_3 and we obtain

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

Using row-reduction we compute

$$A_{ref} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

and we deduce that

$$\mathrm{rank}(T) = 3.$$

□

Problem 5.50. Let V be the space of polynomials with real coefficients of degree not exceeding 3, and let $T : V \to V$ be the linear map defined by

$$T(P(X)) = P(X + 1) - P(X).$$

Find rank(T).

Solution. We start by choosing the canonical basis $1, X, X^2, X^3$ of V and computing

$$T(1) = 0, \quad T(X) = X + 1 - X = 1, \quad T(X^2) = (X + 1)^2 - X^2 = 1 + 2X$$

and

$$T(X^3) = (X + 1)^3 - X^3 = 1 + 3X + 3X^2.$$

The matrix A in the previous discussion is

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

and row-reduction yields

$$A_{ref} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

There are three pivots, thus

$$\text{rank}(T) = 3.$$

□

We turn now to a series of more theoretical exercises, which establish some other important properties of the rank of a linear map. In all problems below we assume that the vector spaces appearing in the statements are finite dimensional.

Problem 5.51. Let $T : V \to W$ be a linear map. Prove that

$$\text{rank}(T) \leq \min(\dim V, \dim W).$$

Solution. Since $\text{Im}(T) \subset W$, we have $\text{rank}(T) \leq \dim W$. As we have already seen, if $v_1, \ldots, v_n$ is a basis of V, then $\text{Im}(T)$ is spanned by $T(v_1), \ldots, T(v_n)$, thus

$$\text{rank}(T) \leq n = \dim V.$$

The result follows by combining the two inequalities. □

Problem 5.52. Let $T_1 : U \to V$ and $T_2 : V \to W$ be linear maps. Prove that

$$\operatorname{rank}(T_2 \circ T_1) \leq \min(\operatorname{rank}(T_1), \operatorname{rank}(T_2)).$$

Solution. The image of $T_2 \circ T_1$ is included in that of T_2, thus $\operatorname{rank}(T_2 \circ T_1) \leq \operatorname{rank}(T_2)$. Next, we consider the restriction T_2' of T_2 to $\operatorname{Im}(T_1)$, obtaining a linear map $T_2' : \operatorname{Im}(T_1) \to W$ whose image clearly equals that of $T_2 \circ T_1$. Applying Problem 5.51 to T_2' we obtain

$$\operatorname{rank}(T_2 \circ T_1) = \operatorname{rank}(T_2') \leq \dim(\operatorname{Im}(T_1)) = \operatorname{rank}(T_1),$$

and the result follows. □

Problem 5.53. Let $T_1, T_2 : V \to W$ be linear transformations. Prove that

$$|\operatorname{rank}(T_1) - \operatorname{rank}(T_2)| \leq \operatorname{rank}(T_1 + T_2) \leq \operatorname{rank}(T_1) + \operatorname{rank}(T_2).$$

Solution. We have $\operatorname{Im}(T_1 + T_2) \subset \operatorname{Im}(T_1) + \operatorname{Im}(T_2)$ and so

$$\operatorname{rank}(T_1 + T_2) \leq \dim(\operatorname{Im}(T_1) + \operatorname{Im}(T_2)) \leq$$

$$\dim \operatorname{Im}(T_1) + \dim \operatorname{Im}(T_2) = \operatorname{rank}(T_1) + \operatorname{rank}(T_2),$$

establishing the inequality on the right. On the other hand, we clearly have $\operatorname{Im}(T_2) = \operatorname{Im}(-T_2)$, thus $\operatorname{rank}(T_2) = \operatorname{rank}(-T_2)$. Applying what we have already proved, we obtain

$$\operatorname{rank}(T_1 + T_2) + \operatorname{rank}(T_2) = \operatorname{rank}(T_1 + T_2) + \operatorname{rank}(-T_2) \geq \operatorname{rank}(T_1),$$

thus $\operatorname{rank}(T_1 + T_2) \geq \operatorname{rank}(T_1) - \operatorname{rank}(T_2)$. We conclude using the symmetry in T_1 and T_2. □

Problem 5.54. Prove that if $S_1 : U \to V$, $T : V \to W$ and $S_2 : W \to Z$ are linear maps such that S_1, S_2 are bijective, then

$$\operatorname{rank}(S_2 T S_1) = \operatorname{rank}(T).$$

Solution. Since S_1 is bijective, we have

$$(TS_1)(U) = T(S_1(U)) = T(V) = \operatorname{Im}(T).$$

Since S_2 is bijective, it realizes an isomorphism between $(TS_1)(U)$ and $S_2((TS_1)(U))$, thus these two spaces have the same dimension. We conclude that

$$\operatorname{rank}(T) = \dim \operatorname{Im}(T) = \dim(TS_1)(U) =$$

$$= \dim S_2((TS_1)(U)) = \dim(S_2 T S_1)(U) = \operatorname{rank}(S_2 T S_1).$$

Note that we only used the injectivity of S_1 and the surjectivity of S_2. □

We will now prove the **first fundamental theorem** concerning the rank of a linear map:

Theorem 5.55 (The Rank-Nullity Theorem). *Let V, W be vector spaces over a field F and let $T : V \to W$ be a linear transformation. If V is finite-dimensional, then*

$$\dim \ker T + \operatorname{rank}(T) = \dim V. \tag{5.3}$$

Proof. Let $n = \dim V$ and let $r = \dim \ker T$. Since $\ker T$ is a subspace of V, we have $r \leq n$, in particular $r < \infty$. We need to prove that $\dim \operatorname{Im} T = n - r$.

Let $v_1, \ldots, v_r$ be a basis of $\ker T$ and extend it to a basis $v_1, \ldots, v_n$ of V. We will prove that $T(v_{r+1}), \ldots, T(v_n)$ form a basis of $\operatorname{Im}(T)$, which will yield the desired result.

Let us start by proving that $T(v_{r+1}), \ldots, T(v_n)$ are linearly independent. Suppose that $a_{r+1}, \ldots, a_n$ are scalars in F such that

$$a_{r+1}T(v_{r+1}) + \ldots + a_n T(v_n) = 0.$$

This equality can be written as $T(a_{r+1}v_{r+1} + \ldots + a_n v_n) = 0$, or equivalently $a_{r+1}v_{r+1} + \ldots + a_n v_n \in \ker T$. We can therefore write

$$a_{r+1}v_{r+1} + \ldots + a_n v_n = b_1 v_1 + \ldots + b_r v_r$$

for some scalars $b_1, \ldots, b_r \in F$. But since $v_1, \ldots, v_n$ form a basis of V, the last relation forces $a_{r+1} = \ldots = a_n = 0$ and $b_1 = \ldots = b_r = 0$, proving that $T(v_{r+1}), \ldots, T(v_n)$ are linearly independent.

Next, we prove that $T(v_{r+1}), \ldots, T(v_n)$ span $\operatorname{Im}(T)$. Let $x \in \operatorname{Im}(T)$. By definition, there is $v \in V$ such that $x = T(v)$. Since $v_1, \ldots, v_n$ span V, we can find scalars $a_1, \ldots, a_n \in F$ such that $v = a_1 v_1 + \ldots + a_n v_n$. Since $v_1, \ldots, v_r \in \ker T$, we obtain

$$x = T(v) = \sum_{i=1}^{n} a_i T(v_i) = \sum_{i=r+1}^{n} a_i T(v_i) \in \operatorname{Span}(T(v_{r+1}), \ldots, T(v_n)).$$

This finishes the proof of the theorem. □

Corollary 5.56. *Let V be a finite-dimensional vector space over a field F and let $T : V \to V$ be a linear transformation. Then the following assertions are equivalent:*

a) T is injective.
b) T is surjective.
c) T is bijective.

Proof. Suppose that a) holds. Then the rank-nullity theorem and the fact that $\ker T = 0$ yield $\dim \operatorname{Im}(T) = \dim V$. Since $\operatorname{Im}(T)$ is a subspace of the finite-dimensional vector space V and $\dim \operatorname{Im}(T) = \dim V$, we deduce that $\operatorname{Im}(T) = V$ and so T is surjective, thus b) holds.

Suppose now that b) holds, thus $\dim \operatorname{Im}(T) = \dim V$. The rank-nullity theorem yields $\dim \ker T = 0$, thus $\ker T = 0$ and then T is injective. Since it is also surjective by assumption, it follows that c) holds. Since c) clearly implies a), the result follows. □

Remark 5.57. Without the assumption that V is finite dimensional, the previous result no longer holds: one can find linear transformations $T : V \to V$ which are injective and not surjective, and linear transformations which is surjective and not injective. Indeed, let V be the space of all sequences $(x_n)_{n\geq 0}$ of real numbers and define two maps $T_1, T_2 : V \to V$ by

$$T_1(x_0, x_1, \ldots) = (x_1, x_2, \ldots), \quad T_2(x_0, x_1, \ldots) = (0, x_0, x_1, \ldots).$$

Then T_1 is surjective but not injective, and T_2 is injective but not surjective.

Problem 5.58. Let A and B be $n \times n$ matrices such that AB is invertible. Show that both A and B are invertible.

Solution. Let $T_1 : F^n \to F^n$ and $T_2 : F^n \to F^n$ be the linear maps associated with A and B respectively (so $T_1(X) = AX$ and $T_2(X) = BX$). Then AB is the matrix of the linear map $T_1 \circ T_2$ with respect to the canonical basis of F^n (both on the source and on the target). Since AB is invertible, we deduce that $T_1 \circ T_2$ is bijective, hence T_2 is injective and T_1 is surjective. But an injective or surjective linear transformation on a finite dimensional vector space is automatically bijective. Thus T_1 and T_2 are both bijective and the result follows from Problem 5.37. □

Problem 5.59. Let $A, B \in M_n(\mathbf{C})$ satisfy $AB = I_n$. Prove that $BA = I_n$.

Solution. By the previous problem, A and B are invertible. Multiplying the relation $AB = I_n$ on the right by A^{-1} yields $B = A^{-1}$. Thus $BA = A^{-1}A = I_n$. □

Problem 5.60. Show that if A and B are square matrices in $M_n(\mathbf{C})$ with $AB = A + B$, then $AB = BA$.

Solution. The condition $AB = A + B$ implies $(A - I_n)(B - I_n) = I_n$. Therefore $A - I_n$ and $B - I_n$ are mutually inverse and $(B - I_n)(A - I_n) = I_n$, which implies $BA = A + B = AB$. □

Problem 5.61. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation defined by

$$T(x, y, z) = (x - y, 2x - y - z, x - 2y + z).$$

Find the kernel of T and the rank of T.

Solution. In order to find the kernel of T, we need to find those $x, y, z \in \mathbf{R}^3$ such that

$$x - y = 0, \quad 2x - y - z = 0, \quad x - 2y + z = 0.$$

The first equation gives $x = y$, the second one $z = x$ and so $x = y = z$, which satisfies all equations. It follows that the kernel of T is the subspace $\{(x, x, x) | x \in \mathbf{R}^3\}$, which is precisely the line spanned by the vector $(1, 1, 1)$.

Next, then rank of T can be determined from the rank-nullity theorem:

$$3 = \dim \mathbf{R}^3 = \dim \ker T + \operatorname{rank}(T) = 1 + \operatorname{rank}(T),$$

thus $\operatorname{rank}(T) = 2$. □

We turn now to the analogous concept for matrices

Definition 5.62. Let $A \in M_{m,n}(F)$. The **rank** of A is the integer $\operatorname{rank}(A)$ defined as the rank of the linear map $F^n \to F^m$ sending X to AX (i.e., the canonical linear map attached to A).

Remark 5.63. We can restate the results established in Problems 5.51, 5.52, 5.53, and 5.54 in terms of matrices as follows:

a) $\operatorname{rank}(A) \leq \min(m, n)$ if $A \in M_{m,n}(F)$.
b) $|\operatorname{rank}(A) - \operatorname{rank}(B)| \leq \operatorname{rank}(A + B) \leq \operatorname{rank}(A) + \operatorname{rank}(B)$ for all $A, B \in M_{m,n}(F)$.
c) $\operatorname{rank}(PAQ) = \operatorname{rank}(A)$ for all $P \in \mathrm{GL}_m(F)$, $A \in M_{m,n}(F)$ and $Q \in \mathrm{GL}_n(F)$. That is, **the rank of a matrix does not change if we multiply it (on the left or on the right) by invertible matrices**.
d) $\operatorname{rank}(AB) \leq \min(\operatorname{rank}(A), \operatorname{rank}(B))$ for $A \in M_{m,n}(F)$ and $B \in M_{n,p}(F)$.

Of course, we can also make the definition very concrete: let $A \in M_{m,n}(F)$ and let $e_1, e_2, \ldots, e_n$ be the canonical basis of F^n. Write $\varphi : F^n \to F^m$ for the linear map $X \to AX$ canonically attached to A. By the previous discussion $\operatorname{Im}(\varphi)$ is the span of $\varphi(e_1), \ldots, \varphi(e_n)$. Now, if $C_1, \ldots, C_n$ are the columns of A, seen as column vectors in F^m, then by definition $\varphi(e_i) = C_i$ for all i. We conclude that the image of φ is the span of $C_1, \ldots, C_n$.

Let us summarize the previous discussion in an important

Theorem 5.64. *Let $A \in M_{m,n}(F)$ and let $C_1, C_2, \ldots, C_n \in F^m$ be its columns. Then*

$$\operatorname{rank}(A) = \dim \operatorname{Span}(C_1, C_2, \ldots, C_n).$$

So, following the previous discussion, we obtain the following algorithm for computing the rank of A: consider **the transpose** ${}^tA$ of A (thus the columns of A become rows in the new matrix) and bring it to its reduced row-echelon form. Then count the number of nonzero rows or equivalently the number of pivots. This is the rank of A. We will see later on (see Problem 5.70) that the trick of considering the transpose of A is actually not necessary: A and ${}^tA$ have the same rank. Of course, we can also avoid considering the transpose matrix and instead using column operations on A.

Problem 5.65. Compute the rank of the matrix

$$A = \begin{bmatrix} -1 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \\ 0 & 2 & -1 & -1 \\ 1 & 1 & 1 & -2 \\ 1 & 3 & -1 & 1 \end{bmatrix}.$$

Solution. Following the previous discussion we bring the matrix

$${}^tA = \begin{bmatrix} -1 & 2 & 0 & 1 & 1 \\ 1 & 2 & 2 & 1 & 3 \\ 0 & 1 & -1 & 1 & -1 \\ 1 & 0 & -1 & -2 & 1 \end{bmatrix}$$

to its reduced row-echelon form by row-reduction

$$({}^tA)_{ref} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}.$$

Since there are 4 nonzero rows, we deduce that

$$\operatorname{rank}(A) = 4.$$

□

Problem 5.66 (Sylvester's Inequality). Prove that for all $A, B \in M_n(F)$ we have

$$\operatorname{rank}(AB) \geq \operatorname{rank}(A) + \operatorname{rank}(B) - n.$$

Solution. Consider $V = F^n$ and the linear transformations $T_1, T_2 : V \to V$ sending X to AX, respectively BX. We need to prove that

$$\operatorname{rank}(T_1 \circ T_2) \geq \operatorname{rank}(T_1) + \operatorname{rank}(T_2) - \dim V.$$

By the rank-nullity theorem we know that

$$\operatorname{rank}(T_1) - \dim V = -\dim \ker T_1,$$

thus it suffices to prove that

$$\operatorname{rank}(T_2) - \operatorname{rank}(T_1 \circ T_2) \leq \dim \ker T_1.$$

Let $W = T_2(V) = \mathrm{Im}(T_2)$ and let $T_1' : W \to V$ be the restriction of T_1 to W. Then using again the rank-nullity theorem, we obtain

$$\mathrm{rank}(T_1 \circ T_2) = \dim T_1(W) = \mathrm{rank}(T_1')$$

$$= \dim W - \dim \ker T_1'.$$

Now $\dim W = \mathrm{rank}(T_2)$, so we are reduced to proving that

$$\dim \ker T_1' \leq \dim \ker T_1.$$

This is clear, as $\ker T_1' = \ker T_1 \cap W \subset \ker T_1$. □

Problem 5.67. Let $A \in M_{3,2}(\mathbf{R})$ and $B \in M_{2,3}(\mathbf{R})$ be matrices such that

$$AB = \begin{bmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{bmatrix}.$$

a) Check that $(AB)^2 = AB$ and that AB has rank 2.
b) Prove that BA is invertible.
c) Prove that $(BA)^3 = (BA)^2$ and deduce that $BA = I_2$.

Solution. a) One checks using the product rule that the matrix

$$X = \begin{bmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 2 \end{bmatrix}$$

satisfies $X^2 = X$. Next, one computes the rank of X by computing the reduced row-echelon form of ${}^tX$:

$$({}^tX)_{ref} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since there are two pivots, $AB = X$ has rank 2.

b) Using Remark 5.63, we obtain

$$\mathrm{rank}(BA) \geq \mathrm{rank}(A(BA)B) = \mathrm{rank}((AB)^2) = \mathrm{rank}(AB) = 2.$$

On the other hand, BA is a 2×2 matrix, thus necessarily $\mathrm{rank}(BA) = 2$ and so BA is invertible.

c) Since $(AB)^2 = AB$, we have

$$B(AB)^2A = B(AB)A = (BA)^2.$$

The left-hand side equals $(BA)^3$ and so $(BA)^3 = (BA)^2$. Since BA is invertible, it follows that $BA = I_2$ and the problem is solved. □

The **second fundamental theorem** concerning rank is the following:

Theorem 5.68. *Let $A \in M_{m,n}(F)$ and let $0 \leq r \leq \min(m,n)$. Then $\operatorname{rank}(A) = r$ if and only if there are matrices $P \in \mathrm{GL}_m(F)$ and $Q \in \mathrm{GL}_n(F)$ such that $A = PJ_rQ$, where*

$$J_r = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \in M_{m,n}(F).$$

Proof. If $A = PJ_rQ$, then by part c) of Remark 5.63 we have $\operatorname{rank}(A) = \operatorname{rank}(J_r)$. The linear map associated with J_r is $(x_1, \ldots, x_n) \to (x_1, \ldots, x_r)$, and its image is F^r, which has dimension r, thus $\operatorname{rank}(J_r) = r$. This proves one implication.

Assume now that $\operatorname{rank}(A) = r$ and let $T : F^n \to F^m$ be the linear map sending X to AX, so that A is the matrix of T with respect to the canonical bases of F^n and F^m. Thanks to Theorem 5.43, it suffices to prove that we can find two bases B_1, B_2 of F^n, F^m respectively such that the matrix of T with respect to B_1, B_2 is J_r. In order to construct B_1 and B_2, we start with a basis $e_1, \ldots, e_{n-r}$ of $\ker T$ (note that $\dim \ker T = n - r$ by the rank-nullity theorem) and we complete it to a basis $e_1, \ldots, e_n$ of F^n. Let $f_i = T(e_{n-r+i})$ for $1 \leq i \leq r$. We claim that $f_1, \ldots, f_r$ is a basis of $\operatorname{Im}(T)$. Since $\dim \operatorname{Im}(T) = r$, it suffices to see that $f_1, \ldots, f_r$ span $\operatorname{Im}(T)$. But any $x \in \operatorname{Im}(T)$ can be written $x = T(a_1e_1 + \ldots + a_ne_n)$ and since $T(e_j) = 0$ for $1 \leq j \leq n - r$, we have

$$x = a_{n-r+1}f_1 + \ldots + a_nf_r \in \operatorname{Span}(f_1, \ldots, f_r),$$

proving the claim (this argument has already been used in the last paragraph of the proof of the rank-nullity theorem).

Complete now $f_1, \ldots, f_r$ to a basis $f_1, \ldots, f_m$ of F^m. Call $B_1 = (e_{n-r+1}, \ldots, e_n, e_1, \ldots, e_r)$ and $B_2 = (f_1, \ldots, f_m)$. Then by construction the matrix of T with respect to B_1, B_2 is J_r and the theorem is proved. □

Corollary 5.69. *Let $A, B \in M_{m,n}(F)$. Then $\operatorname{rank}(A) = \operatorname{rank}(B)$ if and only if there are matrices $P \in \mathrm{GL}_m(F)$ and $Q \in \mathrm{GL}_n(F)$ such that $B = PAQ$.*

Proof. If $B = PAQ$ with P, Q invertible, then the result follows from part c) of Remark 5.63. Assume that $\operatorname{rank}(A) = \operatorname{rank}(B) = r$, then by the previous theorem we can write $A = P_1J_rQ_1$ and $B = P_2J_rQ_2$ for invertible matrices P_1, P_2, Q_1, Q_2. Setting $P = P_2P_1^{-1}$ and $Q = Q_1^{-1}Q_2$ we obtain $B = PAQ$. □

Problem 5.70. Prove that for all $A \in M_{m,n}(F)$ we have

$$\operatorname{rank}(A) = \operatorname{rank}({}^tA).$$

Solution. Say A has rank r and write $A = PJ_rQ$ with $P \in \mathrm{GL}_m(F)$ and $Q \in \mathrm{GL}_n(F)$. Then ${}^tA = {}^tQ\,{}^tJ_r\,{}^tP$ and since ${}^tP, {}^tQ$ are invertible, we have $\operatorname{rank}({}^tA) = \operatorname{rank}({}^tJ_r)$. Since ${}^tJ_r = J_r$, we conclude that $\operatorname{rank}({}^tA) = \operatorname{rank}(A) = r$. □

Problem 5.71. Let $A \in M_n(\mathbf{C})$. Find, as a function of A, the smallest integer r such that A can be written as a sum of r matrices of rank 1.

Solution. For all matrices $X, Y \in M_n(\mathbf{C})$ we have

$$\operatorname{rank}(X+Y) \le \operatorname{rank}(X) + \operatorname{rank}(Y)$$

thus if $A = A_1 + \cdots + A_s$ with $\operatorname{rank}(A_i) = 1$, then

$$\operatorname{rank}(A) = \operatorname{rank}\left(\sum_{i=1}^{s} A_i\right) \le \sum_{i=1}^{s} \operatorname{rank}(A_i) = s.$$

We will prove that we can write A as a sum of $\operatorname{rank}(A)$ matrices of rank 1, which will imply that the answer of the problem is $\operatorname{rank}(A)$. Indeed, if A has rank k, write $A = PJ_kR$ for some $P, R \in GL_n(\mathbf{C})$. Thus $A = A_1 + A_2 + \cdots + A_k$, where $A_i = PE_{ii}Q$ and E_{ii} is the matrix having all entries 0 except for entry (i,i), which is 1. Clearly A_i has rank 1 (since P, Q are invertible and E_{ii} has rank 1). □

Problem 5.72. Let $A \in M_n(F)$ have rank $r \in [1, n-1]$. Prove that there exist $B \in M_{n,r}(F)$, $C \in M_{r,n}(F)$ with

$$\operatorname{rank}(B) = \operatorname{rank}(C) = r,$$

such that $A = BC$.

Solution. Write $A = PJ_rQ$, where P, Q are invertible $n \times n$ matrices. Note that choosing $B_1 = \begin{bmatrix} I_r \\ 0 \end{bmatrix} \in M_{n,r}(F)$ and $C_1 = \begin{bmatrix} I_r & 0 \end{bmatrix} \in M_{r,n}(F)$ we have $J_r = B_1C_1$ and B_1, C_1 both have rank r. But then

$$xA = PJ_rQ = (PB_1)(C_1Q)$$

and $B = PB_1 \in M_{n,r}(F)$, $C = C_1Q \in M_{r,n}(F)$ both have rank r, since P, Q are invertible (Remark 5.63). The problem is solved. □

Problem 5.73. Let $A = [a_{ij}] \in M_n(\mathbf{C})$ be a matrix of rank 1. Prove that there exist complex numbers $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ such that $a_{ij} = x_i y_j$ for all integers $1 \le i, j \le n$.

Solution. According to the previous problem there exist two matrices

$$B \in M_{n,1}(\mathbf{C}) \quad , \quad C \in M_{1,n}(\mathbf{C})$$

so that $A = BC$. If

$$B = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \quad , \quad C = (y_1 \ \ y_2 \ \dots \ y_n)\,,$$

then

$$A = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \cdot (y_1 \ \ y_2 \ \dots \ y_n) = \begin{pmatrix} x_1y_1 & x_1y_2 & \dots & x_1y_n \\ x_2y_1 & x_2y_2 & \dots & x_2y_n \\ \dots & \dots & \dots & \dots \\ x_ny_1 & x_ny_2 & \dots & x_ny_n \end{pmatrix}.$$

□

5.4.1 Problems for practice

1. a) Find the rank of the linear transformation

$$T : \mathbf{R}^3 \to \mathbf{R}^3, \quad T(x, y, z) = (x - y, y - z, z - x).$$

   b) Answer the same question with $\mathbf{R}$ replaced with $\mathbf{F}_2$.
2. Let T be the linear transformation on $\mathbf{R}^3$ whose matrix with respect to the canonical basis is

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{bmatrix}.$$

   Find a basis of $\mathrm{Im}(T)$ and $\ker(T)$, and compute the rank of T.
3. Compute the rank of the matrices

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

4. Let $A, B \in M_3(F)$ be two matrices such that $AB = O_3$. Prove that

$$\min(\text{rank}(A), \text{rank}(B)) \leq 1.$$

5. Let $A \in M_3(\mathbf{C})$ be a matrix such that $A^2 = O_3$.

   a) Prove that A has rank 0 or 1.
   b) Deduce the general form of all matrices $A \in M_3(\mathbf{C})$ such that $A^2 = O_3$.

6. Find the rank of the matrix $A = [\cos(i - j)]_{1 \leq i,j \leq n}$.
7. a) Let V be an n-dimensional vector space over F and let $T : V \to V$ be a linear transformation. Let T^j be the j-fold iterate of T (so $T^2 = T \circ T$, $T^3 = T \circ T \circ T$, etc). Prove that

$$\text{Im}(T^n) = \text{Im}(T^{n+1}).$$

   Hint: check that if $\text{Im}(T^j) = \text{Im}(T^{j+1})$ for some j, then $\text{Im}(T^k) = \text{Im}(T^{k+1})$ for $k \geq j$.

   b) Let $A \in M_n(\mathbf{C})$ be a matrix. Prove that A^n and A^{n+1} have the same rank.
8. Let $A \in M_n(F)$ be a matrix of rank 1. Prove that

$$A^2 = \text{Tr}(A)A.$$

9. Let $A \in M_m(F)$ and $B \in M_n(F)$. Prove that

$$\text{rank} \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} = \text{rank}(A) + \text{rank}(B).$$

10. Prove that for any matrices $A \in M_{n,m}(F)$ and $B \in M_m(F)$ we have

$$\text{rank} \begin{bmatrix} I_n & A \\ 0 & B \end{bmatrix} = n + \text{rank}(B).$$

11. Let $n > 2$ and let $A = [a_{ij}] \in M_n(\mathbf{C})$ be a matrix of rank 2. Prove the existence of real numbers x_i, y_i, z_i, t_i for $1 \leq i \leq n$ such that for all $i, j \in \{1, 2, \ldots, n\}$ we have

$$a_{ij} = x_i y_j + z_i t_j.$$

12. Let $A = \left(a_{ij}\right)_{1 \leq i,j \leq n}$, $B = \left(b_{ij}\right)_{1 \leq i,j \leq n}$ be complex matrices such that

$$a_{ij} = 2^{i-j} \cdot b_{ij}$$

for all integers $1 \leq i, j \leq n$. Prove that rank A = rank B.

13. Let $A \in M_n(\mathbf{C})$ be a matrix such that $A^2 = A$, i.e., A is the matrix of a projection. Prove that

$$\operatorname{rank}(A) + \operatorname{rank}(I_n - A) = n.$$

14. Let $n > k$ and let $A_1, \ldots, A_k \in M_n(\mathbf{R})$ be matrices of rank $n - 1$. Prove that $A_1 A_2 \ldots A_k$ is nonzero. Hint: using Sylvester's inequality prove that $\operatorname{rank}(A_1 \ldots A_j) \geq n - j$ for $1 \leq j \leq k$.
15. Let $A \in M_n(\mathbf{C})$ be a matrix of rank at least $n - 1$. Prove that $\operatorname{rank}(A^k) \geq n - k$ for $1 \leq k \leq n$. Hint: use Sylvester's inequality.
16. a) Prove that for any matrix $A \in M_n(\mathbf{R})$ we have

$$\operatorname{rank}(A) = \operatorname{rank}({}^t AA).$$

Hint: if $X \in \mathbf{R}^n$ is a column vector such that ${}^t AAX = 0$, write ${}^t X\, {}^t AAX = 0$ and express the left-hand side as a sum of squares.

b) Let $A = \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}$. Find the rank of A and ${}^t AA$ and conclude that part a) of the problem is no longer true if $\mathbf{R}$ is replaced with $\mathbf{C}$.

17. Let A be an $m \times n$ matrix with rank r. Prove that there is an $m \times m$ matrix B with rank $m - r$ such that $BA = O_{m,n}$.
18. (Generalized inverses) Let $A \in M_{m,n}(F)$. A generalized inverse of A is a matrix $X \in M_{n,m}(F)$ such that $AXA = A$.

a) If $m = n$ and A is invertible, show that the only generalized inverse of A is A^{-1}.
b) Show that a generalized inverse of A always exists.
c) Give an example to show that the generalized inverse need not be unique.

Chapter 6
Duality

Abstract After an in-depth study of duality for finite dimensional vector spaces, we prove Jordan's classification result of nilpotent transformations on a finite dimensional vector space. We also explain how to describe vector subspaces by equations using hyperplanes.

Keywords Duality • Dual basis • Linear form • Hyperplane • Orthogonal

This chapter focuses on a restricted class of linear maps between vector spaces, namely linear maps between a vector space and the field of scalars (seen as a vector space of dimension 1 over itself). Such linear maps are called linear forms on the vector space. Even though the whole chapter might look rather formal at first sight, the study of linear forms (known as duality) on finite dimensional vector spaces is very important and yields a lot of surprising properties. For instance, we will use duality to prove a famous result due to Jordan which completely classifies the nilpotent linear transformations on a finite dimensional vector space. This is one of the most important results in linear algebra! We will also use duality in the last chapter, in a more geometric context.

6.1 The Dual Basis

We fix a field F in the sequel. The reader may take $F \in \{\mathbf{R}, \mathbf{C}\}$ if he/she prefers.

Definition 6.1. The **dual** V^* of a vector space V over F is the set of linear maps $l : V \to F$, endowed with the structure of a vector space over F by defining

$$(l_1 + l_2)(v) = l_1(v) + l_2(v) \quad \text{and} \quad (cl)(v) = cl(v)$$

for $l_1, l_2, l \in V^*$, $v_1, v_2, v \in V$ and $c \in F$.

We leave to the reader the immediate verification of axioms of a vector space, which show that V^* is indeed a vector space over F when endowed with the previous operations. An element l of V^* is called a **linear form** on V. These objects

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_6

are not very mysterious: assume for instance that $V = F^n$ and let $e_1, \ldots, e_n$ be the canonical basis. Then for all $(x_1, \ldots, x_n) \in V$ we have

$$l(x_1, \ldots, x_n) = l(x_1 e_1 + \ldots + x_n e_n) = x_1 l(e_1) + \ldots + x_n l(e_n) = a_1 x_1 + \ldots + a_n x_n,$$

where $a_i = l(e_i) \in F$. Conversely, any map of the form $(x_1, \ldots, x_n) \mapsto a_1 x_1 + \ldots + a_n x_n$ is a linear form on $\mathbf{R}^n$. In general, if V is a finite dimensional vector space and $e_1, \ldots, e_n$ is a basis of V, then the linear forms on V are precisely those maps $l : V \to F$ of the form

$$l(x_1 e_1 + \ldots + x_n e_n) = a_1 x_1 + \ldots + a_n x_n$$

with $a_1, \ldots, a_n \in F$.

By definition we have a canonical map

$$V^* \times V \to F, \quad (l, v) \mapsto l(v).$$

We also denote this map as $(l, v) \mapsto \langle l, v \rangle$ and call it the **canonical pairing** between V and its dual. Unwinding definitions, we obtain the useful formulae

$$\langle c l_1 + l_2, v \rangle = c \langle l_1, v \rangle + \langle l_2, v \rangle, \quad \text{and} \quad \langle l, c v_1 + v_2 \rangle = c \langle l, v_1 \rangle + \langle l, v_2 \rangle.$$

The canonical pairing is a key example of a bilinear form, a topic which will be studied in much greater depth in subsequent chapters.

Each vector $v \in V$ gives rise to a natural linear form

$$\mathrm{ev}_v : V^* \to F, \quad l \mapsto l(v)$$

on V^*, obtained by evaluating linear forms at v. We obtain therefore a map

$$\iota : V \to V^{**}, \quad \iota(v) = \mathrm{ev}_v,$$

called the **canonical biduality map**. Note that by definition

$$\langle \iota(v), l \rangle = \langle l, v \rangle$$

for all linear forms l on V and all vectors $v \in V$. A fundamental property of the biduality map is that it is always injective. **In other words, if v is a nonzero vector in V, then we can always find a linear form l on V such that $l(v) \neq 0$.** The proof of this rather innocent-looking statement uses the existence of bases for general vector spaces, so we prefer to take the following theorem for granted: we will see in short time that the biduality map is an isomorphism when V is finite dimensional, with an easy proof, and this is all we will need in this book.

Theorem 6.2. *For any vector space V over F, the canonical biduality map $\iota : V \to V^{**}$ is injective.*

Before moving on, let us introduce a useful and classical notation, called the **Kronecker symbol**:

Definition 6.3. If i, j are integers, we let $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$.

Let us assume now that V is **finite dimensional**, of dimension $n \geq 1$ and let us consider a basis $e_1, e_2, \ldots, e_n$ of V. If v is a vector in V, then we can write $v = x_1 e_1 + \ldots + x_n e_n$ for some scalars $x_1, \ldots, x_n$ which are uniquely determined. Define the i**th coordinate form** by

$$e_i^* : V \to F, \quad e_i^*(v) = x_i \quad \text{if} \quad v = x_1 e_1 + \ldots + x_n e_n.$$

Thus by definition for all $v \in V$ we have

$$v = \sum_{i=1}^{n} e_i^*(v) e_i,$$

or equivalently

$$v = \sum_{i=1}^{n} \langle e_i^*, v \rangle e_i.$$

Note that for all $1 \leq i, j \leq n$ we have

$$e_i^*(e_j) = \delta_{ij}.$$

We are now ready to state and prove the first fundamental result of this chapter:

Theorem 6.4. *Let V be a vector space of dimension $n \geq 1$ and let $e_1, \ldots, e_n$ be a basis of V. Then the coordinate forms $e_1^*, \ldots, e_n^*$ form a basis of V^* as vector space over F.*

Proof. Let us check first that e_i^* is an element of V^*, i.e., that e_i^* is linear. But if $x = x_1 e_1 + \ldots + x_n e_n$ and $y = y_1 e_1 + \ldots + y_n e_n$, and if $c \in F$ is a scalar, then

$$x + cy = (x_1 + cy_1)e_1 + \ldots + (x_n + cy_n)e_n,$$

thus

$$e_i^*(x + cy) = x_i + cy_i = e_i^*(x) + ce_i^*(y),$$

so e_i^* is linear.

Next, let us prove that $e_1^*, \ldots, e_n^*$ are linearly independent. Suppose that $c_1, \ldots, c_n \in F$ are scalars such that

$$c_1 e_1^* + \ldots + c_n e_n^* = 0.$$

Evaluating at e_i yields

$$c_1 \langle e_1^*, e_i \rangle + \ldots + c_n \langle e_n^*, e_i \rangle = 0.$$

The left-hand side equals

$$\sum_{j=1}^{n} c_j \langle e_j^*, e_i \rangle = \sum_{j=1}^{n} c_j \delta_{ij} = c_i.$$

Thus $c_i = 0$ for all i and so $e_1^*, \ldots, e_n^*$ are linearly independent.

Finally, let us prove that $e_1^*, \ldots, e_n^*$ are a generating family for V^*. Let $l \in V^*$ be an arbitrary linear form. If $v = x_1 e_1 + \ldots + x_n e_n$ is a vector in V, then linearity of l gives

$$\langle l, v \rangle = x_1 \langle l, e_1 \rangle + \ldots + x_n \langle l, e_n \rangle = \langle l, e_1 \rangle \langle e_1^*, v \rangle + \ldots + \langle l, e_n \rangle \langle e_n^*, v \rangle$$

$$= \langle \langle l, e_1 \rangle e_1^* + \langle l, e_2 \rangle e_2^* + \ldots + \langle l, e_n \rangle e_n^*, v \rangle,$$

showing that

$$l = \langle l, e_1 \rangle e_1^* + \langle l, e_2 \rangle e_2^* + \ldots + \langle l, e_n \rangle e_n^*.$$

Thus l belongs to the span of $e_1^*, \ldots, e_n^*$, which finishes the proof of the theorem. □

Remark 6.5. The proof shows that for any $l \in V^*$ we have the useful relation

$$l = \langle l, e_1 \rangle e_1^* + \langle l, e_2 \rangle e_2^* + \ldots + \langle l, e_n \rangle e_n^*.$$

This is the "dual" relation of the tautological relation

$$v = \sum_{i=1}^{n} \langle e_i^*, v \rangle e_i,$$

valid for all $v \in V$.

The previous theorem explains the following:

Definition 6.6. If $e_1, \ldots, e_n$ is a basis of a vector space V over F, we call $e_1^*, \ldots, e_n^*$ the **dual basis** of $e_1, \ldots, e_n$. It is uniquely characterized by the property that

$$e_i^*(e_j) = \delta_{ij} \quad \text{for all} \quad 1 \leq i, j \leq n.$$

A crucial consequence of the previous theorem is the following:

Corollary 6.7. *For all finite dimensional vector spaces V over F we have*

$$\dim V = \dim V^*.$$

Moreover, the canonical biduality map $\iota : V \to V^{**}$ is an isomorphism of vector spaces over F.

Proof. The first part is clear from the previous theorem and the fact that all bases in a finite dimensional vector space have the same number of elements, namely the dimension of the space. To prove that ι is an isomorphism, it suffices to prove that ι is injective, since

$$\dim V = \dim V^* = \dim V^{**},$$

as follows from what we have already proved.

So suppose that $\iota(v) = 0$, which means that $\langle l, v\rangle = 0$ for all $l \in V^*$. Let $e_1, \ldots, e_n$ be a basis of V. Then $\langle e_i^*, v\rangle = 0$ for all $1 \leq i \leq n$, and since

$$v = \sum_{i=1}^{n} \langle e_i^*, v\rangle e_i,$$

we obtain $v = 0$, establishing therefore the injectivity of ι. □

Remark 6.8. Conversely, one can prove that if the biduality map is an isomorphism, then V is finite dimensional. In other words, the biduality map is never an isomorphism for an infinite dimensional vector space!

Recall that $\mathbf{R}_n[X]$ is the vector space of polynomials with real coefficients whose degree does not exceed n.

Problem 6.9. Let $V = \mathbf{R}_n[X]$. It is easy to see that the maps $P \mapsto P^{(k)}(0)$ (where $P^{(i)}$ is the ith derivative of P) are elements of V^*. Express the dual basis of $1, X, \ldots, X^n$ in terms of these maps.

Solution. Let $e_i = X^i \in V$ and let $e_0^*, \ldots, e_n^*$ be the dual basis. By definition $e_i^*(e_j) = \delta_{ij}$. Thus for all $P = a_0 + a_1 X + \ldots + a_n X^n \in V$ we have

$$e_i^*(P) = a_i = \frac{1}{i!} P^{(i)}(0).$$

Thus e_i^* is the linear form given by $P \mapsto \frac{1}{i!} P^{(i)}(0)$. □

The following problem gives a beautiful and classical application of the ideas developed so far:

Problem 6.10 (Lagrange Interpolation). Let $V = \mathbf{R}_n[X]$ and let $x_0, \ldots, x_n$ be pairwise distinct real numbers. For $0 \leq i \leq n$ define

$$L_i(X) = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - x_j}{x_i - x_j}.$$

a) Show that

$$L_i(x_j) = \delta_{ij} \quad \text{for all} \quad 1 \leq i, j \leq n.$$

b) Prove that $L_0, \ldots, L_n$ form a basis of V.
c) Describe the dual basis of $L_0, \ldots, L_n$.
d) Prove **Lagrange's interpolation formula**: for all $P \in V$ we have

$$P = \sum_{i=0}^{n} P(x_i) L_i.$$

e) Prove that for any $b_0, \ldots, b_n \in \mathbf{R}$ we can find a unique polynomial $P \in V$ with $P(x_i) = b_i$ for $0 \leq i \leq n$. This polynomial P is called the **Lagrange interpolation polynomial associated with** $b_0, \ldots, b_n$.

Solution. a) By construction we have $L_i(x_j) = 0$ for $j \neq i$. On the other hand,

$$L_i(x_i) = \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x_i - x_j}{x_i - x_j} = 1,$$

thus

$$L_i(x_j) = \delta_{ij}.$$

b) Since $\dim V = n + 1$ (a basis being given by $1, X, \ldots, X^n$), it suffices to check that $L_0, \ldots, L_n$ are linearly independent. Suppose that $a_0 L_0 + \ldots + a_n L_n = 0$ for some scalars $a_0, \ldots, a_n$. Evaluating this equality at x_i and using part a) yields

$$0 = \sum_{j=0}^{n} a_j L_j(x_i) = \sum_{j=0}^{n} a_j \delta_{ij} = a_i$$

for all $0 \leq i \leq n$, thus $L_0, \ldots, L_n$ are linearly independent.
c) By definition of the dual basis and by part a), we have

$$L_i^*(L_j) = \delta_{ij} = \delta_{ji} = L_j(x_i)$$

for all i, j. Fix $i \in \{0, \ldots, n\}$. Since $L_i^*(L_j) = L_j(x_i)$ for all $0 \leq j \leq n$ and since $L_0, \ldots, L_n$ span V, we deduce that

$$L_i^*(P) = P(x_i) \quad \text{for all} \quad P \in V.$$

d) By definition of the dual basis

$$P = \sum_{i=0}^{n} \langle L_i^*, P \rangle L_i.$$

By part c) we have $\langle L_i^*, P \rangle = P(x_i)$, which yields the desired result.

e) It suffices to take $P = \sum_{i=0}^{n} b_i L_i$ in order to prove the existence part. For uniqueness, if $Q \in V$ also satisfies $Q(x_i) = b_i$ for $0 \leq i \leq n$, it follows that $P - Q$ is a polynomial whose degree does not exceed n and which has at least $n + 1$ distinct roots, thus $P - Q = 0$ and $P = Q$.

□

Problem 6.11. Let $x_0, \ldots, x_n \in [0, 1]$ be pairwise distinct and let $V = \mathbf{R}_n[X]$.

a) Prove that the map$l : V \to \mathbf{R}$ defined by

$$l(P) = \int_0^1 P(x)dx$$

is a linear form on V.

b) Using the previous problem, prove that there is a unique $n + 1$-tuple $(a_0, \ldots, a_n)$ of real numbers such that

$$\int_0^1 P(x)dx = \sum_{i=0}^{n} a_i P(x_i)$$

for all $P \in V$.

Solution. a) This is a direct consequence of basic properties of integral calculus.

b) We use the result and notations of the previous problem, which establishes that $L_0^*, \ldots, L_n^*$ is a basis of V^*, and $L_i^*(P) = P(x_i)$ for all $P \in V$. Thus saying that

$$\int_0^1 P(x)dx = \sum_{i=0}^{n} a_i P(x_i)$$

for all $P \in V$ is equivalent to saying that

$$I(P) = \sum_{i=0}^{n} a_i L_i^*(P)$$

for all $P \in V$, in other words

$$I = \sum_{i=0}^{n} a_i L_i^*$$

as elements of V^*. Since $L_0^*, \ldots, L_n^*$ is a basis of V^*, the existence and uniqueness of $a_0, \ldots, a_n$ is clear. □

Let us consider now the following **practical problem**: given a basis $v_1, \ldots, v_n$ of $\mathbf{R}^n$, express the dual basis $v_1^*, \ldots, v_n^*$ in terms of the dual basis $e_1^*, \ldots, e_n^*$ of the canonical basis of $\mathbf{R}^n$. To do so, write

$$v_i = \sum_{j=1}^{n} a_{ji} e_j \quad \text{and} \quad v_i^* = \sum_{j=1}^{n} b_{ji} e_j^*.$$

Note that in practice we have an easy access to the matrix $A = [a_{ij}]$: its columns are precisely the coordinates of $v_1, \ldots, v_n$ with respect to the canonical basis $e_1, \ldots, e_n$ of $\mathbf{R}^n$. We are interested in finding $B = [b_{ij}]$. Using the identity $v_i^*(v_j) = \delta_{ij}$, we obtain

$$\delta_{ij} = v_i^*(v_j) = \sum_{k=1}^{n} b_{ki} e_k^*(v_j) = \sum_{k=1}^{n} b_{ki} \cdot \sum_{l=1}^{n} a_{lj} e_k^*(e_l)$$

$$= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{lj} b_{ki} \delta_{kl} = \sum_{k=1}^{n} a_{kj} b_{ki} = ({}^t B \cdot A)_{ij}.$$

Since this holds for all i, j, we deduce that

$${}^t B \cdot A = I_n, \quad i.e., \quad B = {}^t A^{-1}.$$

Thus in practice we need to compute A^{-1} (via row-reduction on the matrix $(A|I_n)$) and take the transpose!

Problem 6.12. Let e_1^*, e_2^*, e_3^* be the dual basis of the canonical basis of $\mathbf{R}^3$. Express in terms of e_1^*, e_2^*, e_3^* the dual basis of the basis of $\mathbf{R}^3$ consisting in

$$v_1 = \begin{bmatrix} -3 \\ 2 \\ 1 \end{bmatrix}, \quad v_2 = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}, \quad v_3 = \begin{bmatrix} 0 \\ -2 \\ 3 \end{bmatrix}.$$

Solution. We leave to the reader to check that v_1, v_2, v_3 form a basis of $\mathbf{R}^3$, using row-reduction on the matrix A whose columns are v_1, v_2, v_3. Using row-reduction on $(A|I_3)$, one obtains

$$A^{-1} = \frac{1}{7} \begin{bmatrix} -5 & -3 & -2 \\ 8 & 9 & 6 \\ -1 & -2 & 1 \end{bmatrix}.$$

With the above notations

$$B = \frac{1}{7} \begin{bmatrix} -5 & 8 & -1 \\ -3 & 9 & -2 \\ -2 & 6 & 1 \end{bmatrix}$$

and then

$$v_1^* = -\frac{5}{7} e_1^* - \frac{3}{7} e_2^* - \frac{2}{7} e_3^*,$$

$$v_2^* = \frac{8}{7} e_1^* + \frac{9}{7} e_2^* + \frac{6}{7} e_3^*,$$

$$v_3^* = -\frac{1}{7} e_1^* - \frac{2}{7} e_2^* + \frac{1}{7} e_3^*.$$

□

Consider now the following **inverse problem: given a basis $f_1, \ldots, f_n$ of V^*, is there always a basis $e_1, \ldots, e_n$ of V whose dual basis is $f_1, \ldots, f_n$? If so, how to find such a basis?**

Let us start with any basis $v_1, \ldots, v_n$ of V (we know that $\dim V = n$ since we know that $\dim V^* = n$). Of course, in practice the choice of $v_1, \ldots, v_n$ will be the natural one (for instance if $V = \mathbf{R}^n$ then we will take for $v_1, \ldots, v_n$ the canonical basis, if $V = \mathbf{R}_{n-1}[X]$, we will take for $v_1, \ldots, v_n$ the basis $1, X, \ldots, X^{n-1}$, etc). Define a matrix

$$A = [a_{ij}], \quad a_{ij} = f_i(v_j).$$

This will be known in practice. On the other hand, we are looking for a basis $e_1, \ldots, e_n$ of V such that $e_i^* = f_i$, that is

$$f_i(e_j) = \delta_{ij}$$

for $1 \leq i, j \leq n$. We are therefore looking for an invertible matrix B such that setting

$$e_i = \sum_{j=1}^{n} b_{ji} v_j,$$

these vectors satisfy the previous relations. Well, these relations are equivalent to

$$\delta_{ij} = f_i(e_j) = \sum_{k=1}^{n} b_{kj} f_i(v_k) = \sum_{k=1}^{n} b_{kj} a_{ik} = (AB)_{ij},$$

that is

$$AB = I_n.$$

In other words, $e_1, \ldots, e_n$ exist if and only if the matrix A is invertible, and then $e_1, \ldots, e_n$ are uniquely determined by

$$B = A^{-1}.$$

It is however not clear that the matrix A is invertible. This is however the case, as the following theorem shows:

Theorem 6.13. *Let $v_1, \ldots, v_n$ be a basis of V and let $f_1, \ldots, f_n$ be a basis of V^*. The matrix $A = [a_{ij}]$ with $a_{ij} = f_i(v_j)$ is invertible. Consequently (thanks to the above discussion) for any basis $f_1, \ldots, f_n$ of V^* there is a unique basis $e_1, \ldots, e_n$ of V whose dual basis is $f_1, \ldots, f_n$.*

Proof. Assume that A is not invertible. We can thus find a nonzero vector $X \in F^n$ with coordinates $x_1, \ldots, x_n$ such that $AX = 0$. Thus for all $j \in \{1, 2, \ldots, n\}$ we have

$$0 = \sum_{i=1}^{n} a_{ji} x_i = \sum_{i=1}^{n} f_j(v_i) x_i = f_j(\sum_{i=1}^{n} x_i v_i).$$

The vector $v = x_1 v_1 + \ldots + x_n v_n$ is therefore nonzero (since $v_1, \ldots, v_n$ are linearly independent and $X \neq 0$) and we have

$$f_1(v) = \ldots = f_n(v) = 0.$$

Since $f_1, \ldots, f_n$ is a spanning set for V^*, we deduce that $l(v) = 0$ for all $l \in V^*$. Thus v is a nonzero vector in the kernel of the biduality map $V \to V^{**}$, which was however shown to be an isomorphism. This contradiction shows that A is invertible and finishes the proof. □

In practice, it is helpful to know that a converse of the theorem holds:

Theorem 6.14. *Let V be a vector space of dimension n over a field F. If the matrix $A = [a_{ij}]$ with $a_{ij} = f_i(v_j)$ is invertible for some $v_1, \ldots, v_n \in V$ and some $f_1, \ldots, f_n \in V^*$, then $v_1, \ldots, v_n$ form a basis of V and $f_1, \ldots, f_n$ form a basis of V^*.*

Proof. Suppose that $v_1, \ldots, v_n$ are linearly independent, say $x_1 v_1 + \ldots + x_n v_n = 0$ for some $x_1, \ldots, x_n \in F$, not all equal to 0. Applying f_j to this relation, we obtain

$$0 = f_j(x_1 v_1 + \ldots + x_n v_n) = a_{j1} x_1 + \ldots + a_{jn} x_n$$

for all $j \in \{1, 2, \ldots, n\}$, thus $AX = 0$, where $X \in F^n$ has coordinates $x_1, \ldots, x_n$, contradicting that A is invertible. Thus $v_1, \ldots, v_n$ are linearly independent and since $\dim V = n$, they form a basis of V.

Similarly, if $f_1, \ldots, f_n$ were linearly dependent, we could find a nontrivial dependency relation $x_1 f_1 + \ldots + x_n f_n = 0$, which evaluated at each v_i would yield

$$\sum_{i=1}^{n} a_{ij} x_i = 0,$$

that is ${}^t AX = 0$ and ${}^t A$ would not be invertible, a contradiction. □

Problem 6.15. Consider the following linear forms on $\mathbf{R}^3$:

$$l_1(x, y, z) = x + 2y + 3z, \quad l_2(x, y, z) = 2x + 3y + z, \quad l_3(x, y, z) = 3x + y + 2z.$$

a) Prove that l_1, l_2, l_3 form a basis of the dual of $\mathbf{R}^3$.
b) Find the basis of $\mathbf{R}^3$ whose dual basis is l_1, l_2, l_3.

Solution. a) Consider the canonical basis e_1, e_2, e_3 of $\mathbf{R}^3$ and the matrix

$$A = [l_i(e_j)] = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

This matrix is invertible, as one easily shows using row-reduction. It follows from the previous theorem that l_1, l_2, l_3 form a basis of the dual of $\mathbf{R}^3$.

b) We compute the inverse of A using row-reduction. We obtain

$$A^{-1} = \frac{1}{18} \begin{bmatrix} -5 & 1 & 7 \\ 1 & 7 & -5 \\ 7 & -5 & 1 \end{bmatrix}.$$

Using the previous discussion, we read the desired basis v_1, v_2, v_3 of $\mathbf{R}^3$ on the columns of A^{-1}:

$$v_1 = \frac{1}{18} \begin{bmatrix} -5 \\ 1 \\ 7 \end{bmatrix}, \quad v_2 = \frac{1}{18} \begin{bmatrix} 1 \\ 7 \\ -5 \end{bmatrix}, \quad v_3 = \frac{1}{18} \begin{bmatrix} 7 \\ -5 \\ 1 \end{bmatrix}.$$

□

Problem 6.16. Let $V = \mathbf{R}_2[X]$ and, for $P \in V$, set

$$l_1(P) = P(1), \quad l_2(P) = P'(1), \quad l_3(P) = \int_0^1 P(x)dx.$$

a) Prove that l_1, l_2, l_3 is a basis of V^*.

b) Find a basis e_1, e_2, e_3 of V whose dual basis is l_1, l_2, l_3.

Solution. a) It is not difficult to check that l_1, l_2, l_3 are linear forms on V. In order to prove that they form a basis of V^*, we will use the previous theorem. Namely, we consider the canonical basis $v_1 = 1$, $v_2 = X$ and $v_3 = X^2$ of V and the matrix

$$A = [l_i(v_j)].$$

Noting that if $P = aX^2 + bX + c$ then

$$l_1(P) = a + b + c, \quad l_2(P) = 2a + b, \quad l_3(P) = \frac{a}{3} + \frac{b}{2} + c,$$

we deduce that

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & \frac{1}{2} & \frac{1}{3} \end{bmatrix}.$$

One easily checks using row-reduction that A is invertible and by the previous theorem l_1, l_2, l_3 form a basis of V^*.

b) Using the method discussed before Theorem 6.13, we see that we have to compute the matrix $B = A^{-1}$. Row-reduction yields

$$B = A^{-1} = \begin{bmatrix} -2 & \frac{1}{2} & 3 \\ 6 & -2 & -6 \\ -3 & \frac{3}{2} & 3 \end{bmatrix}.$$

Moreover, using that method we deduce that

$$e_1 = -2v_1 + 6v_2 - 3v_3 = -2 + 6X - 3X^2,$$

$$e_2 = \frac{1}{2}v_1 - 2v_2 + \frac{3}{2}v_3 = \frac{1}{2} - 2X + \frac{3}{2}X^2,$$

$$e_3 = 3v_1 - 6v_2 + 3v_3 = 3 - 6X + 3X^2.$$

□

6.1.1 Problems for Practice

In the following problems we let $\mathbf{R}_n[X]$ be the space of polynomials with real coefficients whose degree does not exceed n.

1. Find the dual basis of the basis of $\mathbf{R}^3$ consisting of

$$v_1 = (1, -1, 0), \quad v_2 = (0, 0, 1), \quad v_3 = (1, 1, 1).$$

2. Consider the linear forms on $\mathbf{R}^3$

$$l_1(x, y, z) = 2x + 4y + z, \quad l_2(x, y, z) = 4x + 2y + 3z, \quad l_3(x, y, z) = x + y.$$

   a) Prove that l_1, l_2, l_3 form a basis of the dual of $\mathbf{R}^3$.
   b) Find the basis of $\mathbf{R}^3$ whose dual basis is l_1, l_2, l_3.

3. Let V be a finite dimensional vector space over a field F. Prove that for all $x \neq y \in V$ we can find a linear form l on V such that $l(x) \neq l(y)$.
4. Define $P_0 = 1$ and, for $k \geq 1$,

$$P_k(X) = X(X - 1) \dots (X - k + 1).$$

Also, let $f_k : \mathbf{R}_n[X] \to \mathbf{R}$ be the map defined by $f_k(P) = P(k)$.

a) Prove that $P_0, \ldots, P_n$ is a basis of $\mathbf{R}_n[X]$.
b) Prove that $f_0, \ldots, f_n$ is a basis of $\mathbf{R}_n[X]^*$.
c) Let $(P_0^*, \ldots, P_n^*)$ be the dual basis of $(P_0, \ldots, P_n)$. Express P_k^* in terms of $f_0, \ldots, f_n$.

5. Let $a \neq b$ be real numbers and for $k \in \{0, 1, 2\}$ set

$$P_k(X) = (X - a)^k (X - b)^{2-k}.$$

a) Prove that P_0, P_1, P_2 form a basis of $\mathbf{R}_2[X]$.
b) Let $c = \frac{a+b}{2}$ and, for $\alpha \in \{a, b, c\}$, let $f_\alpha : \mathbf{R}_2[X] \to \mathbf{R}$ be the map defined by $f_\alpha(P) = P(\alpha)$. Prove that f_a, f_b, f_c form a basis of $\mathbf{R}_2[X]^*$.
c) Express the dual basis P_0^*, P_1^*, P_2^* in terms of the basis f_a, f_b, f_c.

6. For $i \geq 0$ let $f_i : \mathbf{R}_2[X] \to \mathbf{R}$ be the map defined by

$$f_i(P) = \int_0^1 x^i P(x) dx.$$

a) Prove that f_0, f_1, f_2 form a basis of $\mathbf{R}_2[X]^*$.
b) Find a basis of $\mathbf{R}_2[X]$ whose dual basis is f_0, f_1, f_2.

7. Let V be the vector space of all sequences $(x_n)_{n\geq 0}$ of real numbers such that

$$x_{n+2} = x_{n+1} + x_n$$

for all $n \geq 0$.

a) Prove that V has dimension 2.
b) Let $l_0, l_1 : V \to \mathbf{R}$ be the linear forms sending a sequence $(x_n)_{n\geq 0}$ to x_0, respectively x_1. Find the basis e_0, e_1 of V whose dual basis is l_0, l_1.

8. Let X be a finite set and let V be the space of all maps $\varphi : X \to F$. For each $x \in X$, consider the map $l_x : V \to F$ sending f to $f(x)$. Prove that the family $(l_x)_{x\in X}$ is a basis of V^*.
9. Let l be a linear form on $\mathbf{R}_n[X]$ and let $k \in [0, n]$ be an integer. Prove that the following statements are equivalent:

a) We have $l(X^k P) = 0$ for all polynomials $P \in \mathbf{R}_{n-k}[X]$.
b) There are real numbers $\alpha_0, \ldots, \alpha_{k-1}$ such that for all $P \in \mathbf{R}_n[X]$

$$l(P) = \sum_{i=0}^{k-1} \alpha_i P^{(i)}(0).$$

10. a) Let $a_0, \ldots, a_n$ be pairwise distinct real numbers. Prove that there is a unique $n+1$-tuple of real numbers $(b_0, \ldots, b_n)$ such that for any $P \in \mathbf{R}_n[X]$ we have
$$P(0) + P'(0) = \sum_{k=0}^{n} b_k P(a_k).$$
b) Find such numbers $b_0, \ldots, b_n$ for $n = 2$, $a_0 = 1$, $a_1 = 2$ and $a_2 = 3$.
11. Prove **Simpson's formula**: for all $P \in \mathbf{R}_2[X]$
$$\int_a^b P(x)dx = \frac{b-a}{6}\left(P(a) + 4P\left(\frac{a+b}{2}\right) + f(b)\right).$$
12. a) Let l_1, l_2 be nonzero linear forms on some nonzero vector space V over $\mathbf{R}$. Prove that we can find $v \in V$ such that $l_1(v)l_2(v)$ is nonzero.
b) Generalize this to any finite number of nonzero linear forms.
13. Let V, W be vector spaces. Prove that $(V \times W)^*$ is isomorphic to $V^* \times W^*$.

6.2 Orthogonality and Equations for Subspaces

Let V be a vector space over a field F, let l be a linear form on V and $v \in V$. We say that l and v are **orthogonal** if
$$\langle l, v\rangle = 0, \quad \text{i.e.} \quad l(v) = 0, \quad \text{or equivalently} \quad v \in \ker l.$$

If S is any subset of V, we let
$$S^\perp = \{l \in V^* | \quad \langle l, v\rangle = 0 \quad \forall v \in S\}$$
be the **orthogonal of** S. **These are the linear forms on** V **which vanish on** S, or equivalently on the span of S (by linearity). Thus
$$S^\perp = \mathrm{Span}(S)^\perp.$$
Note that $S^\perp$ **is a subspace of** V^*, since if l_1 and l_2 vanish on S, then so does $l_1 + cl_2$ for all scalars $c \in F$.

Similarly, if S is a subset of V^*, we let
$$S^\perp = \{v \in V | \quad \langle l, v\rangle = 0 \quad \forall l \in S\}$$
be the orthogonal of S. **The elements of** $S^\perp$ **are the vectors killed by all linear forms in** S, thus
$$S^\perp = \bigcap_{l \in S} \ker l.$$

This makes it clear that $S^\perp$ **is a subspace of** V, as intersection of the subspaces $(\ker l)_{l\in S}$ of V. Again, by linearity we have

$$S^\perp = (\mathrm{Span}(S))^\perp$$

for all $S \subset V^*$.

In practice, finding the orthogonal of a subset of a finite dimensional vector space or of its dual comes down to solving linear systems, problem which can be easily solved using row-reduction for instance. Indeed, let V be a finite dimensional vector space over F and let S be a set of vectors in V. Finding $S^\perp$ comes down to finding those linear forms l on V vanishing on each element of S. Let $e_1, \ldots, e_n$ be a basis of V, then a linear form l on V is of the form

$$l(x_1e_1 + \ldots + x_ne_n) = a_1x_1 + \ldots + a_nx_n$$

for some $a_1, \ldots, a_n \in F$. Writing each element $s \in S$ with respect to the basis $e_1, \ldots, e_n$ yields

$$s = \alpha_{s1}e_1 + \ldots + \alpha_{sn}e_n$$

for some scalars α_{si}. Then $l \in S^\perp$ if and only if

$$a_1\alpha_{s1} + \ldots + a_n\alpha_{sn} = 0$$

for all $s \in S$. This is a linear system in $a_1, \ldots, a_n$, but the reader will probably be worried that it may have infinitely many equations (if S is infinite). This is not a problem, since as we have already seen $S^\perp = (\mathrm{Span}(S))^\perp$ and $\mathrm{Span}(S)$ is finite dimensional (since a subspace of V), thus by choosing a basis of $\mathrm{Span}(S)$ say $s_1, \ldots, s_k$, we reduce the problem to solving the system

$$a_1\alpha_{s_j1} + \ldots + a_n\alpha_{s_jn} = 0$$

for $1 \leq j \leq k$. The discussion is similar if we want to compute the orthogonal of a subset of V^*.

Let us see some concrete examples:

Problem 6.17. Consider the subspace W of $\mathbf{R}^3$ defined by

$$W = \{(x, y, z) \in \mathbf{R}^3 \,|\, x + y + z = 0\}.$$

Give a basis of the orthogonal $W^\perp$ of W.

Solution. By definition, a linear form l on $\mathbf{R}^3$ belongs to $W^\perp$ if and only if $l(x, y, z) = 0$ whenever $x + y + z = 0$. In other words,

$$l(x, y, -x - y) = 0 \quad \text{for all} \quad x, y \in \mathbf{R},$$

which can be written as

$$xl(1,0,-1) + yl(0,1,-1) = 0.$$

Thus $l \in W^{\perp}$ if and only if

$$l(1,0,-1) = l(0,1,-1) = 0.$$

Now, a linear form l on $\mathbf{R}^3$ is of the form

$$l(x,y,z) = ax + by + cz,$$

where a, b, c are real numbers. Thus $l \in W^{\perp}$ if and only if

$$a - c = 0, \quad b - c = 0,$$

or equivalently $a = b = c$. It follows that the linear form

$$l_0(x,y,z) = x + y + z$$

is a basis of $W^{\perp}$. □

Problem 6.18. Let $S = \{v_1, v_2, v_3\} \subset \mathbf{R}^4$, where

$$v_1 = (1,0,1,0), \quad v_2 = (0,1,1,0), \quad v_3 = (-1,1,0,1).$$

Describe $S^{\perp}$ by giving a basis of this space.

Solution. A linear form l on $\mathbf{R}^4$ is of the form

$$l(x,y,z,t) = ax + by + cz + dt,$$

where a, b, c, d are real numbers. The condition $l \in S^{\perp}$ is equivalent to

$$l(v_1) = l(v_2) = l(v_3) = 0.$$

Thus $l \in S^{\perp}$ if and only if a, b, c, d are solutions of the system

$$\begin{cases} a + c = 0 \\ b + c = 0 \\ -a + b + d = 0 \end{cases}$$

This system can be solved without difficulty: the first and second equations give $a = b = -c$ and the third equation yields $d = 0$, thus the solutions of the system are $\{(u,u,-u,0) | u \in \mathbf{R}\}$. The corresponding linear forms are

$$l_u(x,y,z,t) = u(x + y - z),$$

hence a basis of $S^\perp$ is given by

$$l_1(x, y, z, t) = x + y - z.$$

□

Problem 6.19. Consider the set $S = \{l_1, l_2\}$ where

$$l_1(x, y, z) = 2x + 3y - z, \quad l_2(x, y, z) = x - 2y + z.$$

Find a basis for $S^\perp$.

Solution. A vector (x, y, z) is in $S^\perp$ if and only if

$$l_1(x, y, z) = l_2(x, y, z) = 0,$$

that is

$$\begin{cases} 2x + 3y - z = 0 \\ x - 2y + z = 0 \end{cases}$$

Solving the system yields

$$y = -3x, \quad z = -7x.$$

Thus a basis of $S^\perp$ is given by $(1, -3, -7)$. □

Let us continue with an easy, but important theoretical exercise.

Problem 6.20. a) If $S_1 \subset S_2$ are subsets of V or of V^*, then $S_2^\perp \subset S_1^\perp$.
b) If S is a subset of V or V^*, then $S \subset (S^\perp)^\perp$.

Solution. a) Suppose that S_1, S_2 are subsets of V. If $l \in S_2^\perp$, then l vanishes on S_2. Since $S_1 \subset S_2$, it follows that l vanishes on S_1 and so $l \in S_1^\perp$. Thus $S_2^\perp \subset S_1^\perp$.

Suppose that S_1, S_2 are subsets of V^*. If $v \in S_2^\perp$, then all elements of S_2 vanish at v. Since $S_1 \subset S_2$, it follows that all elements of S_1 vanish at v and so $v \in S_1^\perp$. The result follows.

b) Suppose that $S \subset V$ and let $v \in S$. We need to prove that if $l \in S^\perp$, then $\langle l, v\rangle = 0$, which is clear by definition! Similarly, if $S \subset V^*$ and $l \in S$, we need to prove that $\langle l, v\rangle = 0$ for all $v \in S^\perp$, which is again clear. □

Remark 6.21. **While it is tempting to believe that the inclusion in part b) of the problem is actually an equality, this is completely false**: $(S^\perp)^\perp$ is a subspace of V or V^*, while S has no reason to be a subspace of V or V^* (it was an arbitrary subset). **Actually, we will see that the inclusion is an equality if S is a subspace of V or V^* when V is finite dimensional.**

The fundamental theorem concerning duality of vector spaces is the following:

Theorem 6.22. *Let V be a **finite dimensional** vector space over F. Then for all subspaces W of V or V^* we have*

$$\dim W + \dim W^\perp = \dim V.$$

Proof. Let $n = \dim V$. Let W be a subspace of V, of dimension $m \leq n$, and let $e_1, \ldots, e_m$ be a basis of W, completed to a basis $e_1, \ldots, e_n$ of V. We need to prove that $\dim W^\perp = n - m$. Let $e_1^*, \ldots, e_n^*$ be the dual basis of V^* associated with $e_1, \ldots, e_n$. We will prove that $e_{m+1}^*, \ldots, e_n^*$ is a basis of $W^\perp$, which will prove the equality $\dim W^\perp = n - m$. First, notice that $e_{m+1}^*, \ldots, e_n^*$ belong to $W^\perp$, since e_j^* vanishes at $e_1, \ldots, e_m$ for all $m < j \leq n$, thus it vanishes on $W = \mathrm{Span}(e_1, \ldots, e_m)$.

Since $e_{m+1}^*, \ldots, e_n^*$ form a subfamily of the linearly independent family $e_1^*, \ldots, e_n^*$, it suffices to prove that they span $W^\perp$. Let $l \in W^\perp$, so that l vanishes on W. Using Remark 6.5, we obtain

$$l = \sum_{i=m+1}^{n} \langle l, e_i \rangle e_i^* \in \mathrm{Span}(e_{m+1}^*, \ldots, e_n^*)$$

and the proof of the equality $\dim W^\perp = n - m$ is finished.

Suppose now that W is a subspace of V^*. By definition $W^\perp$ consists of vectors $v \in V$ such that $\langle l, v \rangle = 0$ for all $l \in W$. Let $\iota : V \to V^{**}$ be the canonical biduality map. The equality $\langle l, v \rangle = 0$ is equivalent to $\langle \iota(v), l \rangle = 0$. Thus $v \in W^\perp$ if and only if $\iota(v) \in (V^*)^*$ vanishes on W. Since ι is an isomorphism and since the space of $g \in (V^*)^*$ which vanish on W has dimension $\dim V^* - \dim W = \dim V - \dim W$ by the first paragraph, we conclude that $\dim W^\perp = \dim V - \dim W$, finishing the proof of the theorem. □

Let us also mention the following very important consequence of the previous theorem: we can recover a subspace in a finite dimensional vector space (or its dual) from its orthogonal:

Corollary 6.23. *Let V be a finite dimensional vector space over F and let W be a subspace of V or V^*. Then $(W^\perp)^\perp = W$.*

Proof. By Problem 6.20 we have an inclusion $W \subset (W^\perp)^\perp$. By the previous theorem

$$\dim(W^\perp)^\perp = \dim V - \dim W^\perp = \dim W.$$

Thus we must have $(W^\perp)^\perp = W$. □

The previous result allows us to give equations for a subspace W of a finite dimensional vector space V over F. Indeed, let $n = \dim V$ and $p = \dim W$, thus $\dim W^\perp = n - p$ by the previous theorem. Let $l_1, \ldots, l_{n-p}$ be a basis of $W^\perp$. Then by the previous corollary

$$W = (W^\perp)^\perp = \{v \in V \,|\, l_1(v) = \ldots = l_{n-p}(v) = 0\}.$$

If $e_1, \ldots, e_n$ is a fixed basis of V, the linear form l_i is of the form

$$l_i(x_1e_1 + \ldots + x_ne_n) = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n$$

for some $a_{ij} \in F$. We deduce that

$$W = \{x_1e_1 + \ldots + x_ne_n \in V \,|\, a_{i1}x_1 + \ldots + a_{in}x_n = 0 \quad \text{for all} \quad 1 \leq i \leq n-p\},$$

in other words W can be defined by $n - p$ equations, which are linearly independent (since $l_1, \ldots, l_{n-p}$ form a basis of W and thus are linearly independent). Moreover, one can actually write down explicitly these equations if we know the coefficients a_{ij}, in other words if we can find a basis of $W^\perp$. But if W is given, then we have already explained how to compute $W^\perp$, and we also know how to compute a basis of a given vector space, thus all the previous steps can actually be implemented in practice (we will see a concrete example in a few moments).

Conversely, if $l_1, \ldots, l_{n-p}$ are linearly independent linear forms on V, then

$$Z = \{v \in V \,|\, l_1(v) = \ldots = l_{n-p}(v) = 0\}$$

is a vector subspace of V of dimension p, since

$$Z = (\mathrm{Span}(l_1, \ldots, l_{n-p}))^\perp,$$

thus by Theorem 6.22

$$\dim Z = n - \dim \mathrm{Span}(l_1, \ldots, l_{n-p}) = n - (n-p) = p.$$

We can summarize the previous discussion in the following fundamental:

Theorem 6.24. *Let V be a vector space of dimension n over a field.*

a) If W is a subspace of V of dimension p, then we can find linearly independent linear forms $l_1, \ldots, l_{n-p}$ on V such that

$$W = \{v \in V \,|\, l_1(v) = \ldots = l_{n-p}(v) = 0\}.$$

*We say that $l_1(v) = \ldots = l_{n-p}(v) = 0$ are **equations of** W (of course, there are many possible equations for W!).*

b) Conversely, if $l_1, \ldots, l_{n-p}$ are linearly independent linear forms on V, then

$$W = \{v \in V \,|\, l_1(v) = \ldots = l_{n-p}(v) = 0\}$$

is a subspace of dimension p of V.

With the above notations, the case $p = n - 1$ is particularly important and deserves a

Definition 6.25. Let V be a finite dimensional vector space over F. A subspace W of V is called a **hyperplane** if

$$\dim W = \dim V - 1.$$

For instance, the hyperplanes in $\mathbf{R}^2$ are the subspaces of dimension 1, i.e., the lines. On the other hand, the hyperplanes in $\mathbf{R}^3$ are the subspaces of dimension 2, i.e., planes spanned by two linearly independent vectors (this really corresponds to the geometric intuition). There are several possible definitions of a hyperplane and actually the previous one, though motivated by the previous theorem, is not the most natural one since it does not say anything about the case of infinite dimensional vector spaces. The most general and useful definition of a hyperplane in a (not necessarily finite dimensional) vector space V over F is that of a subspace W of V of the form $\ker l$, where l is a nonzero linear form on V. **In other words, hyperplanes are precisely the kernels of nonzero linear forms**. Of course, this new definition is equivalent to the previous one in the case of finite dimensional vector spaces (for instance, by the rank-nullity theorem or by the previous theorem). It also shows that **the hyperplanes in F^n are precisely the subspaces of the form**

$$H = \{(x_1, \ldots, x_n) \in F^n \,|\, a_1 x_1 + \ldots + a_n x_n = 0\}$$

for some nonzero vector $(a_1, \ldots, a_n) \in F^n$. In general, if $e_1, \ldots, e_n$ is a basis of V, then the hyperplanes in V are precisely the subspaces of the form

$$H = \{v = x_1 e_1 + \ldots + x_n e_n \in V \,|\, a_1 x_1 + \ldots + a_n x_n = 0\}.$$

Notice that if H is a hyperplane in a finite dimensional vector space, then $H^\perp$ has dimension 1, thus it is a line in V.

We say that hyperplanes $H_1, \ldots, H_p$ are linearly independent if they are the kernels of a linearly independent family of linear forms. The previous theorem can be rewritten as:

Theorem 6.26. *a) Any subspace of dimension p in a vector space of dimension n is the intersection of $n - p$ linearly independent hyperplanes of V.*

b) Conversely, the intersection of $n-p$ linearly independent hyperplanes in a vector space of dimension n is a subspace of dimension p.

We end this section with two concrete problems:

Problem 6.27. Let W be the subspace of $\mathbf{R}^4$ spanned by the vectors

$$v_1 = (1, 1, -1, 0) \quad \text{and} \quad v_2 = (-1, 2, -1, 1).$$

Find equations for W.

Solution. Here $V = \mathbf{R}^4$ and e_1, e_2, e_3, e_4 is the canonical basis of V. As the discussion above shows, the problem comes down to finding a basis of $W^\perp$. Now $W^\perp$ consists in those linear forms

$$l(x, y, z, t) = ax + by + cz + dt$$

which vanish on v_1 and v_2, i.e., such that

$$a + b - c = 0, \quad -a + 2b - c + d = 0.$$

We obtain

$$c = a + b, \quad d = a + c - 2b = 2a - b$$

and so

$$l(x, y, z, t) = ax + by + (a + b)z + (2a - b)t$$

$$= a(x + z + 2t) + b(y + z - t).$$

We deduce that a basis of $W^\perp$ is given by

$$l_1(x, y, z, t) = x + z + 2t \quad \text{and} \quad l_2(x, y, z, t) = y + z - t.$$

As we have already seen above, we have

$$W = \{v \in V \,|\, l_1(v) = l_2(v) = 0\} =$$

$$\{(x, y, z, t) \in \mathbf{R}^4 \,|\, x + z + 2t = y + z - t = 0\}$$

and $l_1(v) = l_2(v) = 0$ are equations for W. □

Problem 6.28. Let $V = \mathbf{R}_3[X]$. Write the vector subspace of W spanned by $1 + X$ and $1 - X + X^3$ as the intersection of 2 linearly independent hyperplanes.

Solution. Consider the canonical basis

$$e_1 = 1, e_2 = X, e_3 = X^2, e_4 = X^3$$

of V and

$$v_1 = 1 + X = e_1 + e_2, \quad v_2 = 1 - X + X^3 = e_1 - e_2 + e_4.$$

Writing $W = \text{Span}(v_1, v_2)$ as the intersection of 2 linearly independent hyperplanes is equivalent to finding two equations defining W, say $l_1(v) = l_2(v) = 0$, as then

$$W = H_1 \cap H_2, \quad \text{where} \quad H_i = \ker l_i.$$

Thus we are reduced to finding a basis l_1, l_2 of $W^\perp$. A linear form l on V is of the form

$$l(x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4) = ax_1 + bx_2 + cx_3 + dx_4$$

for some real numbers a, b, c, d. This linear form belongs to $W^{\perp}$ if and only if $l(v_1) = l(v_2) = 0$, which is equivalent to

$$a + b = a - b + d = 0.$$

This gives $b = -a$ and $d = -2a$, that is

$$l(x_1e_1 + \ldots + x_4e_4) = a(x_1 - x_2 - 2x_4) + cx_3.$$

We deduce that a basis l_1, l_2 of $W^{\perp}$ is given by

$$l_1(x_1e_1 + \ldots + X_4e_4) = x_1 - x_2 - 2x_4, \quad l_2(x_1e_1 + \ldots + x_4e_4) = x_3$$

and so W is the intersection of two linearly independent hyperplanes

$$H_1 = \ker l_1 = \{a + bX + cX^2 + dX^3 \in V \,|\, a - b - 2d = 0\}$$

and

$$H_2 = \ker l_2 = \{a + bX + cX^2 + dX^3 \in V \,|\, c = 0\}.$$

□

6.2.1 Problems for Practice

1. Consider the linear forms

$$l_1(x, y) = x - 2y, \quad l_2(x, y) = 2x + 3y$$

on $\mathbf{R}^2$. Give a basis of $S^{\perp}$, where $S = \{l_1, l_2\}$.

2. Give a basis of $S^{\perp}$, where S consists of the linear forms

$$l_1(x, y, z) = x + y - z, \quad l_2(x, y, z) = 2x - 3y + z, \quad l_3(x, y, z) = 3x - 2y$$

on $\mathbf{R}^3$.

3. Find a basis of $W^{\perp}$, where

$$W = \{(x, y, z, t) \in \mathbf{R}^4 | x + 2y + z - t = 0\}.$$

4. Let $S = \{(v_1, v_2, v_3)\}$, where

$$v_1 = (0, 1, 1), \quad v_2 = (1, 1, 0), \quad v_3 = (3, 5, 2).$$

Describe $S^{\perp}$.

5. Give equations for the subspace of $\mathbf{R}^4$ spanned by

$$v_1 = (1, -2, 2, -1), \quad v_2 = (-1, 0, 4, -2).$$

6. a) Find the dimension p of the subspace W of $\mathbf{R}^4$ spanned by

$$v_1 = (1, 2, -2, 1), \quad v_2 = (-1, 2, 0, -3), \quad v_3 = (0, 4, -2, -2).$$

   b) Write W as an intersection of $4 - p$ linearly independent hyperplanes.
   c) Can we write W as the intersection of $3 - p$ hyperplanes?
7. Let $V = M_n(\mathbf{R})$ and for each $A \in V$ consider the map

$$l_A : V \to \mathbf{R}, \quad L_A(B) = AB.$$

   a) Prove that $l_A \in V^*$ for all $A \in V$.
   b) Prove that the map

$$V \to V^*, \quad A \mapsto l_A$$

   is a bijective linear map (thus an isomorphism of vector spaces).
   c) Let S_n and A_n be the subspaces of V consisting of symmetric, respectively skew-symmetric matrices. Prove that

$$S_n^{\perp} = \{l_A |\, A \in A_n\} \quad \text{and} \quad A_n^{\perp} = \{l_A |\, A \in S_n\}.$$

8. Let V be the space of polynomials with real coefficients and let W be the subspace of V^* spanned by the linear forms $(l_n)_{n \geq 0}$, where $l_n(P) = P^{(n)}(0)$. Prove that $W^{\perp} = \{0\}$, but $W \neq V^*$. Thus if W is a subspace of V^*, we do not always have $(W^{\perp})^{\perp} = W$ (this is the case if V is finite dimensional, or, more generally, if W is finite dimensional).
9. Let l be a linear form on $M_n(\mathbf{R})$ such that

$$l(AB) = l(BA)$$

   for all $A, B \in M_n(\mathbf{R})$. Let $(E_{ij})_{1 \leq i,j \leq n}$ be the canonical basis of $M_n(\mathbf{R})$.

   a) Prove that $l(E_{11}) = \ldots = l(E_{nn})$. Hint: for $i \neq j$ $E_{ij}E_{ji} = E_{ii}$ and $E_{ji}E_{ij} = E_{jj}$.
   b) Prove that $l(E_{ij}) = 0$ for $i \neq j$. Hint: $E_{ii}E_{ij} = E_{ij}$ and $E_{ij}E_{ii} = O_n$.
   c) Deduce that there is a real number c such that

$$l(A) = c \cdot \mathrm{Tr}(A) \quad \text{for all} \quad A \in M_n(\mathbf{R}).$$

10. Using the previous problem, determine the span of the set of matrices of the form $AB - BA$, with $A, B \in M_n(\mathbf{R})$ (hint: consider the orthogonal of the span).

11. Let V be a vector space and let W_1, W_2 be subspaces of V or V^*. Prove that

$$(W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp.$$

12. Let V be a finite dimensional vector space and let W_1 and W_2 be subspaces of V. Prove that

$$(W_1 \cap W_2)^\perp = W_1^\perp + W_2^\perp.$$

Hint: use the previous problem and Corollary 6.23.

13. Let W_1, W_2 be complementary subspaces in a finite dimensional vector space V over a field F. Prove that $W_1^\perp$ and $W_2^\perp$ are complementary subspaces in V^*.
14. Let H_1, H_2 be distinct hyperplanes in a vector space V of dimension $n \geq 2$ over $\mathbf{R}$. Find $\dim(H_1 \cap H_2)$.
15. Prove that a nonzero finite dimensional vector space over $\mathbf{R}$ is not the union of finitely many hyperplanes.
16. Prove that the hyperplanes in $M_n(\mathbf{R})$ are precisely the subspaces of the form

$$\{X \in M_n(\mathbf{R}) | \operatorname{Tr}(AX) = 0\}$$

for some nonzero matrix $A \in M_n(\mathbf{R})$.

17. Let W be a subspace of dimension p in a vector space V of dimension n. Prove that the minimal number of hyperplanes whose intersection is W is $n - p$.
18. Let V be a finite dimensional vector space and let $l, l_1, \ldots, l_n \in V^*$ be linear forms. Prove that $l \in \operatorname{Span}(l_1, \ldots, l_n)$ if and only if $\cap_{i=1}^n \ker l_i \subset \ker l$.

6.3 The Transpose of a Linear Transformation

Let V, W be vector spaces over a field F and let $T : V \to W$ be a linear transformation. For each $l \in W^*$ we can consider the composite $l \circ T : V \to F$, which is a linear form on V. We obtain therefore a map

$$^tT : W^* \to V^*, \quad {}^tT(l) = l \circ T.$$

In terms of the canonical pairing between V and V^*, and between W and W^*, we have

$$\langle {}^tT(l), v \rangle = \langle l, T(v) \rangle$$

for all $l \in W^*$ and $v \in V$. We call ${}^tT$ the **transpose** of the linear transformation T.

If V and W are finite dimensional, the following theorem completely elucidates the map ${}^tT$:

Theorem 6.29. *Let $T : V \to W$ be a linear transformation between finite dimensional vector spaces and let $\mathcal{B}$ and $\mathcal{B}'$ be two bases of V and W respectively. If A is the matrix of T with respect to $\mathcal{B}$ and $\mathcal{B}'$, then the matrix of ${}^tT : W^* \to V^*$ with respect to the dual bases of $\mathcal{B}'$ and $\mathcal{B}$ is ${}^tA$.*

Proof. Let $\mathcal{B} = (v_1, \ldots, v_n)$ and $\mathcal{B}' = (w_1, \ldots, w_m)$. Write $A = [a_{ij}]$ and let $B = [b_{ij}]$ be the matrix of ${}^tT$ with respect to the bases $w_1^*, \ldots, w_m^*$ and $v_1^*, \ldots, v_n^*$. By definition we have

$$T(v_i) = \sum_{j=1}^{m} a_{ji} w_j, \quad \forall 1 \leq i \leq n$$

and

$${}^tT(w_i^*) = \sum_{k=1}^{n} b_{ki} v_k^*, \quad \forall 1 \leq i \leq m.$$

Fix $1 \leq i \leq m$ and write the last equality as

$$\sum_{k=1}^{n} b_{ki} v_k^* = w_i^* \circ T.$$

Evaluating at v_j, with $j \in [1, n]$ arbitrary, we obtain

$$\sum_{k=1}^{n} b_{ki} v_k^*(v_j) = \sum_{k=1}^{n} b_{ki} \delta_{kj} = b_{ji}$$

and

$$w_i^*(T(v_j)) = w_i^*(\sum_{l=1}^{m} a_{lj} w_l) = \sum_{l=1}^{m} a_{lj} \delta_{il} = a_{ij}.$$

Comparing the two expressions yields

$$a_{ij} = b_{ji} \quad \text{for all} \quad i, j,$$

which is exactly saying that $B = {}^tA$. □

The following problems establish basic properties of the correspondence $T \to {}^tT$. For linear maps between finite dimensional vector spaces, they follow immediately from the previous theorem and properties of the transpose map on matrices that we have already established in the first chapter. If we want to deal with arbitrary vector spaces, we cannot use these results. Fortunately, the results are still rather easy to establish in full generality.

Problem 6.30. Prove that for all linear transformations $T_1, T_2 : V \to W$ and all scalars $c \in F$ we have

$$^t(T_1 + cT_2) = {}^tT_1 + c\,{}^tT_2.$$

Solution. We need to prove that if l is a linear form on W, then

$$l \circ (T_1 + cT_2) = l \circ T_1 + cl \circ T_2.$$

This follows from the fact that l is linear. □

Problem 6.31. a) Let $T_1 : V_1 \to V_2$ and $T_2 : V_2 \to V_3$ be linear transformations. Prove that

$$^t(T_2 \circ T_1) = {}^tT_1 \circ {}^tT_2.$$

b) Deduce that if $T : V \to V$ is an isomorphism, then so is ${}^tT : V^* \to V^*$, and $({}^tT)^{-1} = {}^t(T^{-1})$.

Solution. a) Let l be a linear form on V_3. Then

$$^t(T_2 \circ T_1)(l) = l \circ (T_2 \circ T_1) = (l \circ T_2) \circ T_1 =$$

$$^tT_1(l \circ T_2) = {}^tT_1({}^tT_2(l)) = {}^tT_1 \circ {}^tT_2(l).$$

The result follows.

b) Since T is an isomorphism, there is a linear transformation T^{-1} such that $T \circ T^{-1} = T^{-1} \circ T = \mathrm{id}$. Using part a) and the obvious equality ${}^t\mathrm{id} = \mathrm{id}$, we obtain

$$^tT \circ {}^t(T^{-1}) = \mathrm{id} = {}^t(T^{-1}) \circ {}^t T,$$

from where the result follows. □

Problem 6.32. Let $T : V \to W$ be a linear transformation and let $\iota_V : V \to V^{**}$, $\iota_W : W \to W^{**}$ be the canonical biduality maps. Prove that

$$\iota_W \circ T = {}^t({}^tT) \circ \iota_V.$$

Solution. Let $v \in W$, then

$$^t({}^tT) \circ \iota_V(v) = {}^t({}^tT)(\mathrm{ev}_v) = \mathrm{ev}_v \circ {}^tT.$$

The last map sends $l \in W^*$ to

$$\mathrm{ev}_v \circ {}^tT(l) = \mathrm{ev}_v(l \circ T) = (l \circ T)(v) = l(T(v))$$

$$= \mathrm{ev}_{T(v)}(l) = \iota_W(T(v))(l).$$

Thus

$$^t(^tT) \circ \iota_V(v) = \mathrm{ev}_v \circ {}^tT = \iota_W(T(v))$$

for all $v \in V$, which is exactly the desired equality. □

The following technical but very important result makes the link between the transpose operation and orthogonality. This allows us to use the powerful results established in the previous section.

Theorem 6.33. *Let $T : V \to W$ be a linear transformation between finite dimensional vector spaces. We have*

$$\ker(^tT) = (\mathrm{Im}(T))^\perp, \qquad \ker T = (\mathrm{Im}(^tT))^\perp$$

and

$$\mathrm{Im}(^tT) = (\ker T)^\perp, \quad \mathrm{Im}(T) = (\ker(^tT))^\perp.$$

Proof. By definition we have

$$\ker(^tT) = \{l \in W^* \,|\, l \circ T = 0\} = \{l \in W^* \,|\, l(T(v)) = 0 \,\forall\, v \in V\}$$

$$= \{l \in W^* \,|\, l(w) = 0 \,\forall\, w \in \mathrm{Im}(T)\} = (\mathrm{Im}(T))^\perp.$$

Similarly, we have

$$(\mathrm{Im}(^tT))^\perp = \{v \in V \,|\, {}^tT(l)(v) = 0 \,\forall\, l \in W^*\}$$

$$= \{v \in V \,|\, l(T(v)) = 0 \,\forall\, l \in W^*\} = \{v \in V \,|\, T(v) = 0\} = \ker T.$$

Note that we could have also deduced this second result by using the already established equality $\ker(^tT) = (\mathrm{Im}(T))^\perp$, applying it to ${}^tT$ and using the previous problem (and the fact that ι_V and ι_W are isomorphisms).

Using what we have already established and the fact that our spaces are finite dimensional (thus we can use Corollary 6.23), we obtain

$$(\ker T)^\perp = ((\mathrm{Im}(^tT))^\perp)^\perp = \mathrm{Im}(^tT).$$

We proceed similarly for the equality $\mathrm{Im}(T) = (\ker(^tT))^\perp$. □

The previous theorem allows us to give a new proof of the classical but nontrivial result that a matrix and its transpose have the same rank:

Problem 6.34. a) Let $T : V \to W$ be a linear transformation between finite dimensional vector spaces. Prove that T and ${}^tT$ have the same rank.

b) Prove that if $A \in M_{m,n}(F)$, then A and its transpose have the same rank.

Solution. Using Theorem 6.29, we see that b) is simply the matrix translation of a). In order to prove part a), we use Theorem 6.33, which yields

$$\operatorname{rank}({}^tT) = \dim(\operatorname{Im}({}^tT)) = \dim(\ker T)^{\perp}.$$

By Theorem 6.22 and the rank-nullity theorem, the last expression equals

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

The result follows.

□

6.3.1 Problems for Practice

In the next problems we fix a field F.

1. Consider the linear map

$$T : \mathbf{R}^3 \to \mathbf{R}^2, \quad T(x, y, z) = (x - 2y + 3z, x - y + z).$$

   Let e_1^*, e_2^* be the dual basis of $\mathbf{R}^2$. Find the coordinates of the vector ${}^tT(e_1^* - e_2^*, e_1^* + e_2^*)$ with respect to the dual basis of the canonical basis of $\mathbf{R}^3$.
2. Find the matrix of ${}^tT$ with respect to the dual base of the canonical base of $\mathbf{R}^3$, knowing that

$$T(x, y, z) = (x - 2y + 3z, 2y - z, x - 4y + 3z).$$

3. Let $T : V \to W$ be a linear transformation between finite dimensional vector spaces over F. Prove that

   a) T is injective if and only if ${}^tT$ is surjective.
   b) T is surjective if and only if ${}^tT$ is injective.

4. Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V over F, and let W be a subspace of V. Prove that W is stable under T if and only if $W^{\perp}$ is stable under ${}^tT$.
5. Find all planes of $\mathbf{R}^3$ which are invariant under the linear transformation

$$T : \mathbf{R}^3 \to \mathbf{R}^3, \quad T(x, y, z) = (x - 2y + z, 0, x + y + z).$$

6. Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation such that any hyperplane of V is stable under T. Prove that T is a scalar times the identity (hint: prove that any line in V^* is stable under ${}^tT$).

6.4 Application to the Classification of Nilpotent Matrices

In this section we will use the results established in the previous sections to give a simple proof of a beautiful and extremely important theorem of Jordan. This will be used later on to completely classify matrices in $M_n(\mathbf{C})$ up to similarity. Actually, the proof will be split into a series of (relatively) easy exercises, many of them having their own interest. We will work over an arbitrary field F in this section, but the reader may assume that $F = \mathbf{R}$ or $\mathbf{C}$ if he/she wants.

We have seen several important classes of matrices so far: diagonal, upper-triangular, symmetric, orthogonal, etc. It is time to introduce another fundamental class of matrices and linear transformations:

Definition 6.35. a) Let V be a vector space over F and let $T : V \to V$ be a linear transformation. We say that T is **nilpotent** if $T^k = 0$ for some $k \geq 1$, where $T^k = T \circ T \circ \ldots \circ T$ (k times). The smallest such positive integer k is called the **index of** T. Thus if k is the index of T, then $T^k = 0$ but $T^{k-1} \neq 0$.

b) A matrix $A \in M_n(F)$ is called **nilpotent** if $A^k = O_n$ for some $k \geq 1$. The smallest such positive integer k is called the **index of** A.

If V is a finite dimensional vector space over F, if $\mathcal{B}$ is a basis of V and if $T : V \to V$ is a linear transformation whose matrix with respect to $\mathcal{B}$ is $A \in M_n(F)$, then the matrix of T^k with respect to $\mathcal{B}$ is A^k. It follows that T **is nilpotent if and only if** A **is nilpotent, and in this case the index of** T **equals the index of** A. In particular, any matrix similar to a nilpotent matrix is nilpotent and has the same index. This can also be proved directly using matrix manipulations: if A is nilpotent, P is invertible, and $B = PAP^{-1}$, then an easy induction shows that

$$B^k = PA^kP^{-1}$$

for all $k \geq 1$, thus $B^k = O_n$ if and only if $A^k = O_n$, establishing the previous statement.

Problem 6.36. Let T_1, T_2 be two linear transformations on a vector space V and assume that $T_1 \circ T_2 = T_2 \circ T_1$. If T_1, T_2 are nilpotent, then so are $T_1 \circ T_2$ and $T_1 + T_2$.

Solution. Say $T_1^{k_1} = 0$ and $T_2^{k_2} = 0$ for some $k_1, k_2 \geq 1$. Then $T_1^k = T_2^k = 0$ where $k = k_1 + k_2$. Since T_1 and T_2 commute, we obtain

$$(T_1 \circ T_2)^k = T_1^k \circ T_2^k = 0$$

and

$$(T_1 + T_2)^{2k} = \sum_{i=0}^{2k} \binom{2k}{k} T_1^{2k-i} T_2^i.$$

For each $0 \leq i \leq k$ we have $T_1^{2k-i} = 0$ and for each $i \in [k+1, 2k]$ we have $T_2^i = 0$. Thus $T_1^{2k-i} T_2^i = 0$ for all $0 \leq i \leq 2k$ and so $(T_1 + T_2)^{2k} = 0$, establishing that $T_1 + T_2$ is nilpotent. □

Remark 6.37. 1) Similarly (and actually a consequence of the problem), the sum/product of two nilpotent **commuting** matrices is a nilpotent matrix.

2) **The result of the previous problem is no longer true if we don't assume that T_1 and T_2 commute**: the matrices $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are nilpotent, but their sum is not nilpotent, also the matrices $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}$ are nilpotent, but their product is not nilpotent.

3) It follows from 2) that the nilpotent matrices in $M_n(F)$ **do not** form a vector subspace of $M_n(F)$. A rather challenging exercise for the reader is to prove that the vector subspace of $M_n(F)$ spanned by the nilpotent matrices is precisely the set of matrices of trace 0.

The result established in the following problem is very important:

Problem 6.38. a) Let $T : V \to V$ be a nilpotent transformation of index k and let $v \in V$ be a vector such that $T^{k-1}(v) \neq 0$. Prove that the family $(v, T(v), \ldots, T^{k-1}(v))$ is linearly independent in V.

b) Deduce that if V is finite dimensional then the index of any nilpotent transformation on V does not exceed $\dim V$.

c) Prove that if $A \in M_n(F)$ is nilpotent, then its index does not exceed n.

Solution. a) Suppose that

$$a_0 v + a_1 T(v) + \ldots + a_{k-1} T^{k-1}(v) = 0 \tag{6.1}$$

for some scalars $a_0, \ldots, a_{k-1}$. Applying T^{k-1} to this relation and taking into account that $T^j = 0$ for $j \geq k$ yields

$$a_0 T^{k-1}(v) + 0 + \ldots + 0 = 0,$$

and since $T^{k-1}(v) \neq 0$, we obtain $a_0 = 0$. Applying now T^{k-2} to relation (6.1) gives $a_1 T^{k-1}(v) = 0$ and then $a_1 = 0$. Continuing by induction yields $a_0 = \ldots = a_{k-1} = 0$ and the result follows.

b) Suppose that T is nilpotent on V, of index k. Part a) shows that V contains a linearly independent family with k elements, thus $\dim V \geq k$ and we are done.

c) This follows from b) applied to $V = F^n$ and the linear map $T : V \to V$ sending X to AX (using the discussion preceding the problem, which shows that A and T have the same index). □

Using the previous problem, we are ready to introduce a fundamental kind of nilpotent matrix: **Jordan blocks**. This is the goal of the next problem:

Problem 6.39. Let $T : V \to V$ be a nilpotent linear transformation on index k on a vector space, let $v \in V$ and let

$$W = \text{Span}(v, T(v), \ldots, T^{k-1}(v)).$$

a) Prove that W is stable under T.
b) Prove that if $T^{k-1}(v) \neq 0$, then $T^{k-1}(v), T^{k-2}(v), \ldots, T(v), v$ form a basis of W (thus $\dim W = k$) and the matrix of the linear transformation $T : W \to W$ with respect to this basis is

$$J_k = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

This matrix is called a **Jordan block of size** k (note that $J_1 = O_1$, the 1×1 matrix with one entry equal to 0).

Solution. a) Any element of W is of the form

$$w = a_0 v + a_1 T(v) + \ldots + a_{k-1} T^{k-1}(v).$$

Since $T^k(v) = 0$, we have

$$T(w) = a_0 T(v) + \ldots + a_{k-2} T^{k-1}(v) \in W,$$

thus W is stable under T.
b) If $T^{k-1}(v) \neq 0$, part a) of the previous problem shows that $T^{k-1}(v), \ldots, T(v), v$ is a linearly independent family and since it also spans W, it is a basis of W. Moreover, since $T^k(v) = 0$ and

$$T(T^i(v)) = T^{i+1}(v)$$

for $k - 2 \geq i \geq 0$, it is clear that the matrix of $T : W \to W$ with respect to this basis is J_k. □

The **main theorem concerning nilpotent linear transformations on finite dimensional vector spaces** is the following beautiful:

Theorem 6.40 (Jordan). *Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a nilpotent linear transformation. Then there is a basis of V with respect to which the matrix of T is of the form*

$$A = \begin{bmatrix} J_{k_1} & 0 & \dots & 0 \\ 0 & J_{k_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{k_d} \end{bmatrix}$$

for some sequence of positive integers $k_1 \geq k_2 \geq \ldots \geq k_d$ *with*

$$k_1 + \ldots + k_d = n.$$

Moreover, the sequence $(k_1, \ldots, k_d)$ *is uniquely determined.*

We can restate the previous theorem in terms of matrices:

Theorem 6.41 (Jordan). *Any nilpotent matrix* $A \in M_n(F)$ *is similar to a block-diagonal matrix* $\begin{bmatrix} J_{k_1} & 0 & \dots & 0 \\ 0 & J_{k_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{k_d} \end{bmatrix}$ *for a unique sequence of positive integers* $(k_1, \ldots, k_d)$ *with* $k_1 \geq k_2 \geq \ldots \geq k_d$ *and*

$$k_1 + k_2 + \ldots + k_d = n.$$

The matrix $\begin{bmatrix} J_{k_1} & 0 & \dots & 0 \\ 0 & J_{k_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{k_d} \end{bmatrix}$ is called the **Jordan normal (or canonical) form of** A **or** T.

The next series of problems is devoted to the proof of this theorem. We will start with the uniqueness of the sequence $(k_1, \ldots, k_d)$. The proof, given in the next three problems, will also show how to compute explicitly these integers and therefore how to find in practice the Jordan normal form of a nilpotent matrix.

Problem 6.42. Let T be the linear transformation on F^n associated with the Jordan block J_n. Prove that for all $1 \leq k \leq n-1$ we have

$$\operatorname{rank}(T^k) = n - k$$

and deduce that

$$\operatorname{rank}(J_n^k) = n - k$$

for $1 \leq k \leq n-1$.

Solution. If $e_1, \ldots, e_n$ is the canonical basis of F^n, then

$$T(e_1) = 0, \quad T(e_2) = e_1, \quad T(e_3) = e_2, \ldots, \quad T(e_n) = e_{n-1}.$$

In other words, $T(e_i) = e_{i-1}$ for $1 \leq i \leq n$, with the convention that $e_0 = 0$. We deduce that $T^2(e_i) = T(e_{i-1}) = e_{i-2}$ for $1 \leq i \leq n$, with $e_{-1} = 0$. An immediate induction yields

$$T^j(e_i) = e_{i-j}$$

for $1 \leq j \leq n-1$ and $1 \leq i \leq n$, with $e_r = 0$ for $r \leq 0$. Thus

$$\mathrm{Im}(T^j) = \mathrm{Span}(e_1, e_2, \ldots, e_{n-j})$$

and this space has dimension $n - j$, which yields

$$\mathrm{rank}(T^k) = n - k$$

for $1 \leq k \leq n-1$. The second part is an immediate consequence of the first part. □

Problem 6.43. Suppose that $A \in M_n(F)$ is similar to

$$\begin{bmatrix} J_{k_1} & 0 & \ldots & 0 \\ 0 & J_{k_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d} \end{bmatrix}.$$

Let N_j be the number of terms equal to j in the sequence $(k_1, \ldots, k_d)$. Prove that for all $1 \leq j \leq n$

$$\mathrm{rank}(A^j) = N_{j+1} + 2N_{j+2} + \ldots + (n-j)N_n.$$

Solution. If $A_1, \ldots, A_d$ are square matrices, then

$$\mathrm{rank}\left(\begin{bmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A_d \end{bmatrix}\right) = \mathrm{rank}(A_1) + \ldots + \mathrm{rank}(A_d),$$

as the reader can easily check by using the fact that the rank of a matrix is the dimension of the span of its column set. Since similar matrices have the same rank, we deduce that for all $j \geq 1$ we have

$$\mathrm{rank}(A^j) = \mathrm{rank}\left(\begin{bmatrix} J_{k_1}^j & 0 & \ldots & 0 \\ 0 & J_{k_2}^j & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d}^j \end{bmatrix}\right) = \sum_{i=1}^{d} \mathrm{rank}(J_{k_i}^j).$$

By the previous problem, $\operatorname{rank}(J_{k_i}^j)$ equals $k_i - j$ if $j \leq k_i$ and 0 otherwise. Thus, since N_t is the number of indices i for which $k_i = t$, we have

$$\sum_{i=1}^{d} \operatorname{rank}(J_{k_i}^j) = \sum_{t \geq j} \sum_{k_i = t} \operatorname{rank}(J_t^j)$$

$$= \sum_{t \geq j} N_t \cdot (t - j) = N_{j+1} + 2N_{j+2} + \ldots + (n - j)N_n.$$

□

Problem 6.44. Prove that if $k_1 \geq \ldots \geq k_d$ and $k'_1 \geq \ldots \geq k'_{d'}$ are sequences of positive integers adding up to n and such that $A = \begin{bmatrix} J_{k_1} & 0 & \ldots & 0 \\ 0 & J_{k_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d} \end{bmatrix}$ is similar to $B = \begin{bmatrix} J_{k'_1} & 0 & \ldots & 0 \\ 0 & J_{k'_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k'_{d'}} \end{bmatrix}$, then these sequences are equal. This is the uniqueness part of Jordan's theorem.

Solution. Let N_j be the number of terms equal to j in the sequence $(k_1, \ldots, k_d)$, and define similarly N'_j for the sequence $(k'_1, \ldots, k'_{d'})$. We are asked to prove that $N_j = N'_j$ for $1 \leq j \leq n$.

Since A and B are similar, A^j and B^j are similar for all $j \geq 1$, thus they have the same rank. Using the previous problem, we deduce that

$$N_{j+1} + 2N_{j+2} + \ldots + (n - j)N_n = N'_{j+1} + 2N'_{j+2} + \ldots + (n - j)N'_n$$

for $j \geq 1$. Setting $j = n - 1$ gives $N_n = N'_n$, then setting $j = n - 2$ and using $N_n = N'_n$ gives $N_{n-1} = N'_{n-1}$. Continuing this way yields $N_j = N'_j$ for $2 \leq j \leq n$. We still need to prove that $N_1 = N'_1$, but this follows from

$$N_1 + 2N_2 + \ldots + nN_n = N'_1 + 2N'_2 + \ldots + nN'_n = n,$$

since

$$k_1 + \ldots + k_d = k'_1 + \ldots + k'_{d'} = n.$$

□

Remark 6.45. The previous two problems show how to compute the sequence $(k_1, \ldots, k_d)$ in practice. Namely, we are reduced to computing $N_1, \ldots, N_n$. For this, we use the relations

$$\operatorname{rank}(A^j) = N_{j+1} + 2N_{j+2} + \ldots + (n - j)N_n$$

for $1 \leq j \leq n$ (it suffices to take $j \leq k$ if A has index k, noting that the previous relation for $j = k$ already yields $N_{k+1} = \ldots = N_n = 0$). These determine completely $N_2, \ldots N_n$. To find N_1, we use the relation

$$N_1 + 2N_2 + \ldots + nN_n = n.$$

Example 6.46. As a concrete example, consider the matrix

$$A = \begin{bmatrix} 1 & -1 & 1 & 2 \\ 1 & -1 & 1 & 2 \\ 0 & 0 & -2 & 4 \\ 0 & 0 & -1 & 2 \end{bmatrix}.$$

One can easily check that this matrix is nilpotent: we compute using the product rule

$$A^2 = \begin{bmatrix} 0 & 0 & -4 & 8 \\ 0 & 0 & -4 & 8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and then $A^3 = O_3$, using again the product rule. Thus A is nilpotent of index $k = 3$. It follows that $N_4 = 0$ and

$$N_1 + 2N_2 + 3N_3 = 4.$$

Next, it is easy to see that the rank of A is 2, since the first and second rows are identical, the last row is half the third row, and the first and third row are linearly independent. Thus

$$2 = \text{rank}(A) = N_2 + 2N_3 + 3N_4 = N_2 + 2N_3$$

Next, it is clear that A^2 has rank 1, thus

$$1 = \text{rank}(A^2) = N_3 + 2N_4 = N_3.$$

It follows that

$$N_1 = 1, \quad N_2 = 0, \quad N_3 = 1, \quad N_4 = 0$$

and so the Jordan normal form of A is

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The uniqueness part of Jordan's theorem being proved, it remains to prove the existence part, which is much harder. The basic idea is however not very surprising: we work by strong induction on $\dim V$, the case $\dim V = 1$ being clear (as then $T = 0$). Assume that the result holds for $\dim V < n$ and let us consider the case $\dim V = n$. We may assume that $T \neq 0$, otherwise we are done. Let $k_1 = k$ be the index of T and let $v \in V$ such that $T^{k-1}(v) \neq 0$. By Problem 6.39, the subspace

$$W = \mathrm{Span}(v, T(v), \ldots, T^{k-1}(v))$$

is invariant under T, which acts on it as the matrix J_k on F^k. Moreover, $\dim W = k$. If $k = n$, then we are done. If not, we look for a complementary subspace W' of W **which is stable under** T. If we could find such a space W', then we could apply the inductive hypothesis to the map $T : W' \to W'$ (note that its index does not exceed k_1) and find a basis of W' in which the matrix of T has the desired form. Patching the basis $T^{k-1}(v), \ldots, T(v), v$ and this basis of W' would yield the desired basis of V and would finish the inductive proof. **The key difficulty is proving the existence of** W'. This will be done in the two problems below.

Problem 6.47. a) Prove that if $A \in M_n(F)$ is nilpotent, then ${}^tA$ is nilpotent and has the same index as A.

b) Suppose that V is a finite dimensional vector space over F. Prove that if $T : V \to V$ is nilpotent, then ${}^tT : V^* \to V^*$ is also nilpotent and has the same index as T.

Solution. a) For all $k \geq 1$ we have

$$({}^tA)^k = {}^t(A^k),$$

thus $({}^tA)^k = O_n$ if and only if $A^k = O_n$. The result follows.

b) Let $\mathcal{B}$ be a basis of V and let $\mathcal{B}^*$ be the dual basis of $\mathcal{B}$. If A is the matrix of T with respect to $\mathcal{B}$, then the matrix of ${}^tT$ with respect to $\mathcal{B}^*$ is ${}^tA$, by Theorem 6.29. The result follows now from part a).

We can also prove this directly as follows: if $k \geq 1$, then $({}^tT)^k = 0$ if and only if $({}^tT)^k(l) = 0$ for all $l \in V^*$, equivalently $l \circ T^k = 0$ for all $l \in V^*$. This can be written as: for all $v \in V$ and all $l \in V^*$ we have $l(T^k(v)) = 0$. Now, the assertion that $l(T^k(v)) = 0$ for all $l \in V^*$ is equivalent to $T^k(v) = 0$, by injectivity of the biduality map $V \to V^{**}$. Thus $({}^tT)^k = 0$ if and only if $T^k = 0$, and this even when V is infinite dimensional. In other words, part b) holds in all generality (but the proof requires the injectivity of the map $V \to V^{**}$, which is difficult and was not given for infinite dimensional vector spaces). □

Problem 6.48. Let $T : V \to V$ be a nilpotent transformation of index k on a finite dimensional vector space V and let $v \in V$ be such that $T^{k-1}(v) \neq 0$. We denote for simplicity $S = {}^tT : V^* \to V^*$ and we recall that S is nilpotent of index k by the previous problem.

a) Explain why we can find a linear form $l \in V^*$ such that

$$l(T^{k-1}(v)) \neq 0.$$

b) Prove that the orthogonal W' of

$$Z = \mathrm{Span}(l, S(l), \ldots, S^{k-1}(l)) \subset V^*$$

is stable under T.

c) Prove that $\dim W' + \dim W = \dim V$.

d) Deduce that $W' \oplus W = V$, thus W' is a complementary subspace of W, stable under T. This finishes the proof of Jordan's theorem!

Solution. a) This is a direct consequence of the injectivity (and actually bijectivity since our space is finite dimensional) of the biduality map $V \to V^{**}$.

b) Let us try to understand concretely the space $Z^\perp$. A vector x is in $Z^\perp$ if and only if $S^j(l)(x) = 0$ for $0 \leq j \leq k-1$. Since $S = T^*$, we have

$$S^j(l)(x) = (l \circ T^j)(x) = l(T^j(x)),$$

thus

$$Z^\perp = \{x \in V \,|\, l(T^j(x)) = 0 \quad \text{for all} \quad 0 \leq j \leq k-1\}.$$

Now let $x \in Z^\perp$ and let us prove that $T(x) \in Z^\perp$, i.e., that

$$l(T^j(T(x))) = 0$$

for $0 \leq j \leq k-1$, or equivalently $l(T^j(x)) = 0$ for $1 \leq j \leq k$. This is clear for $1 \leq j \leq k-1$, since $x \in Z^\perp$, and it is true for $j = k$ since by assumption $T^k = 0$.

c) By Theorem 6.22 we have

$$\dim(W') = \dim(Z^\perp) = \dim V^* - \dim Z = \dim V - \dim Z.$$

It suffices therefore to prove that $\dim Z = \dim W$. Now $\dim W = k$ by Problem 6.39, and $\dim Z = k$ by the same problem applied to V^*, S (which is nilpotent of index k) and l (note that $S^{k-1}(l) = l \circ T^{k-1} \neq 0$ since $l(T^{k-1}(v)) \neq 0$). Thus $\dim W' + \dim W = \dim V$.

d) By part c) it suffices to prove that $W' \cap W = \{0\}$. Let $w \in W$ and write

$$w = a_0 v + a_1 T(v) + \ldots + a_{k-1} T^{k-1}(v)$$

for some scalars $a_0, \ldots, a_{k-1}$. Suppose that $w \in W'$, thus $w \in Z^\perp$, that is $l(T^j(w)) = 0$ for $0 \leq j \leq k-1$. Taking $j = k-1$ and using the fact that $T^m = 0$ for $m \geq k$ yields

$$a_0 l(T^{k-1}(v)) = 0.$$

Since $l(T^{k-1}(v)) \neq 0$, we must have $a_0 = 0$. Taking $j = k-2$ gives similarly $a_1 l(T^{k-1}(v)) = 0$ and so $a_1 = 0$. Continuing like this we obtain $a_0 = \ldots = a_{k-1} = 0$ and so $w = 0$. This finishes the solution of the problem. □

6.4.1 Problems for Practice

In the problems below F is a field.

1. Let $T : V \to V$ be a linear transformation on a finite dimensional vector space such that for all $v \in V$ there is a positive integer k such that $T^k(v) = 0$. Prove that T is nilpotent.
2. Let V be the space of polynomials with real coefficients and let $T : V \to V$ be the map sending a polynomial to its derivative. Prove that for all $v \in V$ there is a positive integer k such that $T^k(v) = 0$, but T is not nilpotent.
3. Describe the possible Jordan normal forms for a nilpotent matrix $A \in M_4(F)$.
4. Find, up to similarity, all nilpotent 3×3 matrices with real entries.
5. A nilpotent matrix $A \in M_5(\mathbf{C})$ satisfies $\text{rank}(A) = 3$ and $\text{rank}(A^2) = 1$. Find its Jordan normal form.
6. a) Prove that the matrix

$$A = \begin{bmatrix} 3 & 1 & 3 \\ 2 & 0 & 2 \\ -3 & -1 & -3 \end{bmatrix}$$

   is nilpotent and find its index.
   b) Find the Jordan normal form of A.
7. Find the Jordan normal form of the matrix

$$A = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 1 & 2 \\ 1 & -1 & 0 \end{bmatrix}.$$

8. Consider the matrix

$$A = \begin{bmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{bmatrix}.$$

   a) Prove that A is nilpotent.
   b) Find its Jordan normal form.

9. Describe up to similarity all matrices $A \in M_n(F)$ such that $A^2 = O_n$.
10. Let $A \in M_n(F)$ be a nilpotent matrix. Prove that A has index n if and only if $\text{rank}(A) = n - 1$.
11. Let $A \in M_n(F)$ be a nilpotent matrix, say $A^k = O_n$ for some $k \geq 1$. Prove that $I_n + xA$ is invertible for all $x \in F$ and

$$(I_n + xA)^{-1} = I_n - xA + x^2A^2 - \ldots + (-1)^{k-1}x^{k-1}A^{k-1}.$$

12. (Fitting decomposition) Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear transformation. Write

$$N = \bigcup_{k \geq 1} \ker T^k, \quad I = \bigcap_{k \geq 1} \text{Im}(T^k).$$

    a) Prove that N and I are subspaces of V, stable under T.
    b) Prove that there exists n such that $N = \ker T^n$ and $I = \text{Im}(T^n)$.
    c) Deduce that $V = N \oplus I$.
    d) Prove that the restriction of T to N is nilpotent and the restriction of T to I is invertible. We call this decomposition $V = N \oplus I$ the **Fitting decomposition of** T.
    e) Prove that if $V = V_1 \oplus V_2$ is a decomposition of V into subspaces stable under T and such that $T|_{V_1}$ is nilpotent and $T|_{V_2}$ is invertible, then $V_1 = N$ and $V_2 = I$.

13. Find the Fitting decomposition of the matrix

$$A = \begin{bmatrix} -1 & 2 \\ -2 & 4 \end{bmatrix}.$$

    Do the same with the matrix

$$A = \begin{bmatrix} -2 & 1 \\ -4 & 2 \end{bmatrix}.$$

Chapter 7
Determinants

Abstract This rather technical chapter is devoted to the study of determinants of matrices and linear transformations. These are introduced and studied via multilinear maps. The present chapter is rich in examples, both numerical and theoretical.

Keywords Determinant • Multilinear map • Laplace expansion • Cofactor

This rather technical chapter is devoted to the study of determinants of matrices and linear transformations. We have already seen in the chapter devoted to square matrices of order 2 that determinants are absolutely fundamental in the study of matrices. The advantage in that case is that many key properties of the determinant can be checked by easy computations, while this is no longer the case for general matrices: it is actually not even clear what the analogue of the determinant should be for $n \times n$ matrices.

The definition of the determinant of a matrix is rather miraculous at first sight, so we spend a large part of this chapter explaining why this definition is natural and motivated by the study of multilinear forms (which will also play a key role in the last chapter of this book). Once the machinery is developed, the proofs of the main properties of the determinants are rather formal, while they would be very painful if one had to manipulate the brutal definition of a determinant as polynomial expression of the entries of the matrix.

Permutations play a key role in this chapter, so the reader not familiar with them should start by reading the corresponding section in the appendix dealing with algebraic preliminaries. The most important thing for us is that the set S_n of permutations of $\{1, 2, \ldots, n\}$ is a group of order $n!$ with respect to the composition of permutations, and there is a nontrivial homomorphism $\varepsilon : S_n \to \{-1, 1\}$, the signature.

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_7

7.1 Multilinear Maps

Let $V_1, V_2, \ldots, V_d$ and W be vector spaces over a field F (the reader might prefer to take $\mathbf{R}$ or $\mathbf{C}$ in the sequel).

Definition 7.1. A map $f : V_1 \times \ldots \times V_d \to W$ is called **multilinear** if for all $i \in \{1, 2, \ldots, d\}$ and all $v_1 \in V_1, \ldots, v_{i-1} \in V_{i-1}, v_{i+1} \in V_{i+1}, \ldots, v_d \in V_d$ the map

$$V_i \to W, \quad v_i \mapsto f(v_1, v_2, \ldots, v_d)$$

is linear.

Let us see what the condition really says in a few simple cases. First, if $d = 1$, then it simply says that the map $f : V_1 \to W$ is linear. Secondly, if $d = 2$, the condition is that $x \mapsto f(a, x)$ and $x \mapsto f(x, b)$ are linear for all $a \in V_1$ and $b \in V_2$. Such maps are also called **bilinear** and they will be studied rather extensively in the last chapter of the book. If $d = 3$, the condition is that $x \mapsto f(a, b, x)$, $x \mapsto f(a, x, c)$ and $x \mapsto f(x, b, c)$ should be linear for all $a \in V_1, b \in V_2$ and $c \in V_3$.

There is a catch with the previous definition: one might naively believe that a multilinear map is the same as a linear map $f : V_1 \times \ldots \times V_d \to W$. This is definitely **not** the case: consider the map $f : \mathbf{R}^2 \to \mathbf{R}$ sending (x, y) to xy. It is bilinear since for all a the map $x \mapsto ax$ is linear, but the map f is not linear, since

$$f((1, 0)) + f((0, 1)) = 0 \neq f((1, 0) + (0, 1)) = 1.$$

One can develop a whole theory (of tensor products) based on this observation, and the reader will find the basic results of this theory in a series of exercises at the end of this section (see the problems for practice section).

Though one can develop a whole theory in the general setting introduced before, we will specialize to the case $V_1 = V_2 = \ldots = V_d$ and we will simply call this space V. Multilinear maps $f : V^d \to W$ will also be called **d-linear maps**. The next problem gives an important recipe which yields d-linear forms from linear forms.

Problem 7.2. Let $f_1, f_2, \ldots, f_d : V \to K$ be linear forms and consider the map

$$f : V^d \to K, \quad (x_1, \ldots, x_d) \mapsto f_1(x_1) \ldots f_d(x_d).$$

Prove that f is d-linear.

Solution. If $i \in \{1, \ldots, d\}$ and $x_1 \in V_1, \ldots, x_{i-1} \in V_{i-1}, x_{i+1} \in V_{i+1}, \ldots, x_d \in V_d$, then the map $x_i \mapsto f(x_1, \ldots, x_d)$ is simply the map $x_i \mapsto af_i(x_i)$ where $a = \prod_{j \neq i} f_j(x_j)$ is a scalar. Since f_i is a linear form, so is af_i, thus $x_i \mapsto af_i(x_i)$ is a linear map and the result follows. □

Not all d-linear forms are just products of linear forms:

Problem 7.3. Prove that the map $f : (\mathbf{R}^2)^2 \to \mathbf{R}$ given by

$$f((x_1, x_2), (y_1, y_2)) = x_1y_1 + x_2y_2$$

is 2-linear, but is not a product of two linear maps, i.e., we cannot find linear maps $l_1, l_2 : \mathbf{R}^2 \to \mathbf{R}$ such that $f(x, y) = l_1(x)l_2(y)$ for all $x, y \in \mathbf{R}^2$.

Solution. If x_1 and x_2 are fixed, then it is not difficult to see that the map $(y_1, y_2) \mapsto x_1y_1 + x_2y_2$ is linear. Similarly, if y_1, y_2 are fixed, then the map $(x_1, x_2) \mapsto x_1y_1 + x_2y_2$ is linear. Thus f is 2-linear. Assume by contradiction that $f(x, y) = l_1(x)l_2(y)$ for two linear maps $l_1, l_2 : \mathbf{R}^2 \to \mathbf{R}$ and for all $x = (x_1, x_2)$ and $y = (y_1, y_2)$ in $\mathbf{R}^2$. It follows that we can find real numbers $a = l_1(1, 0)$, $b = l_1(0, 1)$, $c = l_2(1, 0)$ and $d = l_2(0, 1)$ such that

$$x_1y_1 + x_2y_2 = (ax_1 + bx_2)(cy_1 + dy_2)$$

for all $x_1, y_1, x_2, y_2 \in \mathbf{R}$. We cannot have $(a, b) = (0, 0)$, so assume without loss of generality that $b \neq 0$. Taking $x_2 = -\frac{ax_1}{b}$ we obtain

$$x_1y_1 = \frac{ax_1}{b}y_2$$

for all real numbers x_1, y_1, y_2. This is plainly absurd and the result follows. □

Let us consider now a d-linear form $f : V^d \to W$ and a permutation $\sigma \in S_d$. We define a new map $\sigma(f) : V^d \to W$ by

$$\sigma(f)(x_1, \ldots, x_d) = f(x_{\sigma(1)}, \ldots, x_{\sigma(d)}).$$

It follows easily from the definition of d-linear maps that $\sigma(f)$ is also a d-linear map. Moreover, for all $\sigma, \tau \in S_d$ and all d-linear maps f we have the crucial relation (we say that **the symmetric group S_d acts on the space of d-linear forms**)

$$(\sigma\tau)(f) = \sigma(\tau(f)) \tag{7.1}$$

Indeed, by definition we have

$$(\sigma\tau)(f)(x_1, \ldots, x_d) = f(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(d))})$$

while[1]

$$\sigma(\tau(f))(x_1, \ldots, x_d) = \tau(f)(x_{\sigma(1)}, \ldots, x_{\sigma(d)}) = f(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(d))}).$$

[1]Note that setting $y_i = x_{\sigma(i)}$, we have $y_{\tau(i)} = x_{\sigma(\tau(i))}$.

Recall (see the appendix on algebraic preliminaries for more details on permutations) that there is a special map $\varepsilon : S_d \to \{-1, 1\}$, the **signature**. The precise definition is

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

This map ε is multiplicative, that is

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$$

for all $\sigma, \tau \in S_d$. Recall that a **transposition** is a permutation σ for which there are integers $i \neq j \in \{1, 2, \ldots, d\}$ such that $\sigma(i) = j$, $\sigma(j) = i$ and $\sigma(k) = k$ for all $k \neq i, j$. In this case we write $\sigma = (i, j)$. We note that $\varepsilon(\sigma) = -1$ for any transposition σ. We also recall that any permutation is a product of transpositions.

We introduce now two fundamental classes of d-linear maps:

Definition 7.4. Let $f : V^d \to W$ be a d-linear map.

a) We say that f is **antisymmetric** if $\sigma(f) = \varepsilon(\sigma) f$ for all $\sigma \in S_d$.
b) We say that f is **alternating** if $f(x_1, x_2, \ldots, x_d) = 0$ whenever $x_1, x_2, \ldots, x_d \in V$ are not pairwise distinct.

The two definitions look quite different, but most of the time they are equivalent. There are however some subtleties related to the field F, as the following problems show. However, the reader should keep in mind that **over fields such as the real, rational, or complex numbers there is no difference between alternating and antisymmetric d-linear maps**.

Problem 7.5. Prove that an alternating d-linear map $f : V^d \to W$ is antisymmetric.

Solution. Since any permutation is a product of transpositions and since ε is multiplicative, relation (7.1) reduces the problem to proving that $\tau(f) = -f$ for any transposition $\tau = (i, j)$, with $i < j$. Consider arbitrary vectors $x_1, x_2, \ldots, x_d$ and note that

$$f(x_1, \ldots, x_{i-1}, x_i + x_j, x_{i+1}, \ldots, x_{j-1}, x_i + x_j, x_{j+1}, \ldots, x_d) = 0$$

since f is alternating. Using the d-linearity of f, the previous relation can be written

$$f(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_d) + f(x_1, \ldots, x_j, \ldots, x_j, \ldots x_d) +$$

$$f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_d) + f(x_1, \ldots, x_d) = 0.$$

Using again the fact that f is alternating, it follows that the first two terms in the above sum are zero and we obtain the desired result, noting that the third term is $\tau(f)(x_1, \ldots, x_d)$. □

Problem 7.6. Suppose that $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$. Prove that an antisymmetric d-linear map $f : V^d \to W$ (with V, W vector spaces over F) is alternating. Thus over such a field F there is no difference between antisymmetric and alternating d-linear maps.

Solution. Suppose that $x_1, \ldots, x_d$ are not pairwise distinct, say $x_i = x_j$ for some $i < j$. Consider the transposition $\tau = (i, j)$. Since f is antisymmetric and $\varepsilon(\tau) = -1$, we deduce that $\tau(f) = -f$. Evaluating this equality at $(x_1, \ldots, x_d)$ yields

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_d) = -f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_d).$$

But since $x_i = x_j$, the previous relation can be written

$$2f(x_1, \ldots, x_d) = 0.$$

Since $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$, the previous relation yields $f(x_1, \ldots, x_d) = 0$ (note that this would be completely wrong if we had $F = \mathbf{F}_2$, see also the example below). Thus f is alternating. □

Example 7.7. Bad things happen when $F = \mathbf{F}_2$. Let $f : F^2 \to F$ be the multiplication map, that is $f(x, y) = xy$. It is clearly bilinear and it is not alternating, since $f(1, 1) = 1 \neq 0$. On the other hand, f is antisymmetric. Indeed, we only need to check that $f(x, y) = -f(y, x)$, or equivalently $2xy = 0$. This holds since $2 = 1 + 1 = 0$.

A natural question is: how to construct antisymmetric or alternating d-linear maps? The following problem shows that starting with any d-linear map f we can obtain an antisymmetric one by taking a weighted average of the values $\sigma(f)$. This will play a crucial role in the next section, when defining the determinant of a family of vectors.

Problem 7.8. Let $f : V^d \to W$ be a d-linear map. Prove that

$$A(f) := \sum_{\sigma \in S_d} \varepsilon(\sigma)\sigma(f)$$

is an antisymmetric d-linear map.

Solution. It is clear that $A(f)$ is a d-linear map, since it is a linear combination of d-linear maps. Let $\tau \in S_d$ and let us prove that $\tau(A(f)) = \varepsilon(\tau)A(f)$. Note that by relation (7.1) we have

$$\tau(A(f)) = \sum_{\sigma \in S_d} \varepsilon(\sigma)\tau(\sigma(f)) = \sum_{\sigma \in S_d} \varepsilon(\sigma)(\tau\sigma)(f).$$

Thus, using the fact that $\varepsilon(\tau)\varepsilon(\sigma) = \varepsilon(\tau\sigma)$, we obtain

$$\varepsilon(\tau)\tau(A(f)) = \sum_{\sigma\in S_d} \varepsilon(\tau\sigma)(\tau\sigma)(f).$$

Note that the map $\sigma \mapsto \tau\sigma$ is a permutation of S_d (its inverse being simply $\sigma \mapsto \tau^{-1}\sigma$), thus the last sum equals $\sum_{\sigma\in S_d} \varepsilon(\sigma)\sigma(f) = A(f)$. We conclude that

$$\varepsilon(\tau)\tau(A(f)) = A(f)$$

and the result follows, since $\varepsilon(\tau)^{-1} = \varepsilon(\tau)$. □

A crucial property of alternating d-linear forms, which actually characterizes them, is

Theorem 7.9. *Let $f : V^d \to W$ be an alternating d-linear form. If $x_1, x_2, \ldots, x_d \in V$ are linearly dependent, then $f(x_1, x_2, \ldots, x_d) = 0$.*

Proof. Since $x_1, \ldots, x_d$ are linearly dependent, some x_i lies in the span of $(x_j)_{j\neq i}$, say

$$x_i = \sum_{j\neq i} a_j x_j$$

for some scalars a_j. Then using the d-linearity of f, we obtain

$$f(x_1, \ldots, x_d) = \sum_{j\neq i} a_j f(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_d).$$

As f is alternating, each of the terms $f(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_d)$ is zero, since $x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_d$ are not pairwise distinct. Thus $f(x_1, \ldots, x_d) = 0$. □

7.1.1 Problems for Practice

Let F be a field and let $V_1, \ldots, V_d$ be finite dimensional vector spaces over F. We define the **tensor product** $V_1 \otimes \ldots \otimes V_d$ **of** $V_1, \ldots, V_d$ as the set of multilinear maps $f : V_1^* \times \ldots \times V_d^* \to F$, where V_i^* is the dual of V_i.

1. Check that $V_1 \otimes \ldots \otimes V_d$ is a vector subspace of the vector space of all maps $f : V_1^* \times \ldots \times V_d^* \to F$.
2. If $v_i \in V_i$ for all $1 \leq i \leq d$, define a map $v_1 \otimes \ldots \otimes v_d : V_1^* \times \ldots \times V_d^* \to F$ by

$$(v_1 \otimes \ldots \otimes v_d)(f_1, \ldots, f_d) = f_1(v_1) f_2(v_2) \ldots f_d(v_d)$$

for $f_i \in V_i^*$.

a) Prove that $v_1 \otimes \ldots \otimes v_d \in V_1 \otimes \ldots \otimes V_d$ (elements of $V_1 \otimes \ldots \otimes V_d$ of the form $v_1 \otimes \ldots \otimes v_d$ are called **pure tensors**).
b) Is the map $V_1 \times \ldots \times V_d \to V_1 \otimes \ldots \otimes V_d$ sending $(v_1, \ldots, v_d)$ to $v_1 \otimes \ldots \otimes v_d$ linear? Is it multilinear?
c) Is every element of $V_1 \otimes \ldots \otimes V_d$ a pure tensor?

3. For each $1 \leq i \leq d$ let $(e_{i,j})_{1 \leq j \leq n_i}$ be a basis of V_i. Let $(e^*_{i,j})_{1 \leq j \leq n_i}$ be the associated dual basis of V_i^*.

a) Prove that for any $f \in V_1 \otimes \ldots \otimes V_d$ we have

$$f = \sum_{j_1=1}^{n_1} \ldots \sum_{j_d=1}^{n_d} f(e^*_{1,j_1}, \ldots, e^*_{d,j_d}) e_{1,j_1} \otimes \ldots \otimes e_{d,j_d}.$$

b) Prove that the family of pure tensors $e_{1,j_1} \otimes \ldots \otimes e_{d,j_d}$, where $1 \leq j_1 \leq n_1, \ldots, 1 \leq j_d \leq n_d$ forms a basis of $V_1 \otimes \ldots \otimes V_d$.
c) Prove that

$$\dim(V_1 \otimes \ldots \otimes V_d) = \dim V_1 \cdot \ldots \cdot \dim V_d.$$

4. Prove that $V_1 \otimes \ldots \otimes V_d$ has the following **universal property**: for any vector space W over F and any multilinear map $f : V_1 \times \ldots \times V_d \to W$ there is a unique **linear** map $g : V_1 \otimes \ldots \otimes V_d \to W$ such that

$$g(v_1 \otimes \ldots \otimes v_d) = f(v_1, \ldots, v_d)$$

for all $v_i \in V_i$, $1 \leq i \leq d$.
5. Prove that there is an isomorphism $(V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes V_2 \otimes V_3$ sending $(v_1 \otimes v_2) \otimes v_3$ to $v_1 \otimes v_2 \otimes v_3$ for all $v_1 \in V_1, v_2 \in V_2, v_3 \in V_3$.
6. Prove that there is an isomorphism $V_1^* \otimes V_2^* \to (V_1 \otimes V_2)^*$.
7. Prove that there is an isomorphism $V_1^* \otimes V_2 \to \mathrm{Hom}(V_1, V_2)$ sending $f_1 \otimes v_2$ to the map $v_1 \mapsto f_1(v_1)v_2$ for all $f_1 \in V_1^*$ and $v_2 \in V_2$. We recall that $\mathrm{Hom}(V_1, V_2)$ is the vector space of linear maps between V_1 and V_2.

7.2 Determinant of a Family of Vectors, of a Matrix, and of a Linear Transformation

Let V be a vector space over F, of dimension $n \geq 1$. Let $(v_1, v_2, \ldots, v_n)$ be an n-tuple of vectors in V forming a basis of V. **The order of $v_1, v_2, \ldots, v_n$ will be very important in the sequel**, so one should not consider only the set $\{v_1, \ldots, v_n\}$, but the n-tuple $(v_1, \ldots, v_n)$.

Consider the dual basis $v_1^*, \ldots, v_n^*$ of the dual space V^*. Recall that v_i^* is the linear form on V such that

$$v_i^*(x_1v_1 + \ldots + x_nv_n) = x_i$$

for all $x_1, \ldots, x_n \in F$. That is, $v_i^*(v)$ is the ith coordinate of v when expressed as a linear combination of $v_1, \ldots, v_n$.

By Problem 7.2 the map

$$f : V^n \to F, \quad (x_1, \ldots, x_n) \to v_1^*(x_1) \ldots v_n^*(x_n)$$

is a n-linear form. By Problem 7.8, the map

$$A(f) : V^n \to F, \quad A(f)(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

is an antisymmetric n-linear form.

Definition 7.10. Let f be as above and let $x_1, \ldots, x_n \in V$. We call $A(f)(x_1, \ldots, x_n)$ the **determinant of** $x_1, \ldots, x_n$ **with respect to** $(v_1, \ldots, v_n)$ and denote it $\det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n)$.

Remark 7.11. 1) By definition we have

$$\det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) v_1^*(x_{\sigma(1)}) \ldots v_n^*(x_{\sigma(n)}). \tag{7.2}$$

In other words, if we write

$$x_i = \sum_{j=1}^{n} a_{ji} v_j$$

for some scalars $a_{ji} \in F$ (which we can always do, since $v_1, \ldots, v_n$ is a basis of V), then

$$\det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}.$$

2) We claim that $\det_{(v_1,\ldots,v_n)}(v_1, \ldots, v_n) = 1$. Indeed, suppose that $v_1^*(v_{\sigma(1)}) \ldots v_n^*(v_{\sigma(n)})$ is a nonzero term appearing in the right-hand side of relation (7.2). Then $v_i^*(v_{\sigma(i)})$ is nonzero for all $i \in [1, n]$, which forces $\sigma(i) = i$ for all i. Thus the only nonzero term appearing in the right-hand side of (7.2) is the one corresponding to $\sigma = \mathrm{id}$, which is clearly equal to 1. This proves the claim.

3) The **geometric interpretation** of the determinant is as follows: consider $F = \mathbf{R}$ and let $e_1, e_2, \ldots, e_n$ be the canonical basis of $\mathbf{R}^n$. If $x_1, x_2, \ldots, x_n$ are vectors in $\mathbf{R}^n$, we write $\det(x_1, x_2, \ldots, x_n)$ instead of $\det_{(e_1,e_2,\ldots,e_n)}(x_1, x_2, \ldots, x_n)$. We can associate to the vectors $x_1, x_2, \ldots, x_n$ the parallelepiped

$$\mathcal{P}(x_1, x_2, \ldots, x_n) = \{a_1x_1 + a_2x_2 + \ldots + a_nx_n | a_1, \ldots, a_n \in [0, 1]\}.$$

For instance, if $x_i = e_i$ for all i, then the associated parallelepiped is the hypercube $[0,1]^n$. The geometric interpretation of $\det(x_1, x_2, \ldots, x_n)$ is given by the fundamental equality

$$|\det(x_1, x_2, \ldots, x_n)| = \mathrm{vol}(\mathcal{P}(x_1, x_2, \ldots, x_n)),$$

the volume being taken here with respect to the Lebesgue measure on $\mathbf{R}^n$ (this is the usual area/volume when $n = 2/n = 3$).

Example 7.12. Consider the vector space $V = F^2$ over F and let e_1, e_2 be the canonical basis of V. For any vectors $x_1 = \begin{bmatrix} a \\ b \end{bmatrix}$ and $x_2 = \begin{bmatrix} c \\ d \end{bmatrix}$ in V we have

$$\det_{(e_1,e_2)}(x_1, x_2) = ad - bc.$$

For instance

$$\det_{(e_1,e_2)}\left(\begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}\right) = 4 - 2 \cdot 3 = -2.$$

Here is the first big theorem concerning determinants:

Theorem 7.13. *Let $v_1, \ldots, v_n$ be a basis of a vector space V over F. The determinant map $\det_{(v_1,\ldots,v_n)} : V^d \to F$ with respect to this basis is n-linear and alternating.*

Proof. Denote $f = \det_{(v_1,\ldots,v_n)}$. By Definition 7.10 and the discussion preceding it we know that f is n-linear and antisymmetric. If $F \in \{\mathbf{Q}, \mathbf{R}, \mathbf{C}\}$, then Problem 7.6 shows that f is alternating. Let us give a proof which works for any field F (the reader interested only in fields such as $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}$ may skip the following technical proof).

Let $x_1, \ldots, x_n \in V$ and suppose that they are not pairwise distinct, say $x_i = x_j$ for some $i < j$. Let $\tau = (i, j)$, a transposition and let A_n be the set of even permutations in S_n, that is those permutations σ for which $\varepsilon(\sigma) = 1$. Since $\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma) = -\varepsilon(\sigma)$ for all $\sigma \in S_n$, we deduce that $S_n = A_n \cup \tau A_n$ (disjoint union) and using formula (7.2) we can write

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in A_n} v_1^*(x_{\sigma(1)}) \ldots v_n^*(x_{\sigma(n)}) - \sum_{\sigma \in A_n} v_1^*(x_{\tau\sigma(1)}) \ldots v_n^*(x_{\tau\sigma(n)}).$$

We claim that $x_{\tau\sigma(k)} = x_{\sigma(k)}$ for all k and $\sigma \in A_n$, which clearly shows that $f(x_1, \ldots, x_n) = 0$. The claim is clear if $\sigma(k) \notin \{i, j\}$, as then $\tau\sigma(k) = \sigma(k)$. Suppose that $\sigma(k) = i$, then $\tau\sigma(k) = j$ and the claim comes down to $x_j = x_i$, which holds by assumption. The argument being similar for $\sigma(k) = j$, the theorem is proved. □

The second big theorem in the theory of determinants and multilinear maps is the following:

Theorem 7.14. *Let $(v_1, \ldots, v_n)$ be an n-tuple of vectors of V, forming a basis of V. If $f : V^n \to F$ is any alternating n-linear form, then*

$$f = f(v_1, \ldots, v_n) \cdot \det_{(v_1,\ldots,v_n)}$$

Proof. Let $x_1, \ldots, x_n$ be vectors in V and write

$$x_i = a_{i1}v_1 + a_{i2}v_2 + \ldots + a_{in}v_n$$

for some scalars a_{ij}. By part 1) of Remark 7.11 we have

$$\det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}.$$

On the other hand, repeatedly using the n-linearity of f, we can write

$$f(x_1, \ldots, x_n) = f(a_{11}v_1 + \ldots + a_{1n}v_n, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_{1i} f(v_i, x_2, \ldots, x_n)$$

$$= \sum_{i,j=1}^{n} a_{1i}a_{2j} f(v_i, v_j, x_3, \ldots, x_n) = \ldots = \sum_{i_1,\ldots,i_n=1}^{n} a_{1i_1}a_{2i_2} \ldots a_{ni_n} f(v_{i_1}, \ldots, v_{i_n}).$$

Now, since f is alternating, we have $f(v_{i_1}, \ldots, v_{i_n}) = 0$ unless $i_1, \ldots, i_n$ are pairwise distinct, i.e., unless there is a permutation $\sigma \in S_n$ such that $\sigma(k) = i_k$ for $1 \leq k \leq n$. We conclude that

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} a_{1\sigma(1)} \ldots a_{n\sigma(n)} f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}).$$

Since f is antisymmetric (by Problem 7.5 and the alternating property of f), we can further rewrite the last equality as

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)} f(v_1, \ldots, v_n) =$$

$$\det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n) f(v_1, \ldots, v_n),$$

and the result follows. □

Let us record two important consequences of Theorem 7.14

Corollary 7.15. *Let V be a vector space of dimension $n \geq 1$. The vector space of n-linear alternating forms $f : V^n \to F$ has dimension* 1.

Proof. Consider a basis $v_1, \ldots, v_n$ of V and let $f = \det_{(v_1,\ldots,v_n)}$. By Theorem 7.13, the map f is an alternating n-linear form. By part 2) of Remark 7.11 we have $f(v_1, \ldots, v_n) = 1$, thus f is nonzero. On the other hand, Theorem 7.14 shows that any alternating n-linear form differs by a scalar from $\det_{(v_1,\ldots,v_n)}$. The result follows. □

Corollary 7.16. *Given a basis $v_1, v_2, \ldots, v_n$ of a vector space V over F, there is a unique n-linear alternating form $f : V^n \to F$ such that $f(v_1, v_2, \ldots, v_n) = 1$. This form is given by $f = \det_{(v_1,v_2,\ldots,v_n)}$.*

Proof. Uniqueness follows directly from Theorem 7.14. The existence has already been established during the proof of the last corollary. □

Theorem 7.14 can also be used to establish a criterion to decide when a family of vectors forms a basis of a finite dimensional vector space: it all comes down to computing determinants, and we will see quite a few methods to compute them in the next sections (however, in practice it the method explained before Problem 4.34 and based on row-reduction is the most efficient one).

Corollary 7.17. *Let V be a vector space of dimension n over F and let $x_1, x_2, \ldots, x_n \in V$. The following assertions are equivalent:*

a) $x_1, x_2, \ldots, x_n$ form a basis of V (or, equivalently, they are linearly independent).
b) For any basis $v_1, v_2, \ldots, v_n$ we have

$$\det_{(v_1,v_2,\ldots,v_n)}(x_1, x_2, \ldots, x_n) \neq 0.$$

c) There is a basis $v_1, v_2, \ldots, v_n$ such that

$$\det_{(v_1,v_2,\ldots,v_n)}(x_1, x_2, \ldots, x_n) \neq 0.$$

Proof. Suppose that a) holds and let $v_1, \ldots, v_n$ be a basis of V. By Theorem 7.14 applied to $f = \det_{(x_1,\ldots,x_n)}$ we have

$$\det_{(x_1,\ldots,x_n)}(x_1, \ldots, x_n) = \det_{(x_1,\ldots,x_n)}(v_1, \ldots, v_n) \cdot \det_{(v_1,\ldots,v_n)}(x_1, \ldots, x_n).$$

By Remark 7.11 the left-hand side is 1, thus both factors in the right-hand side are nonzero, establishing b). It is clear that b) implies c), so assume that c) holds and let us prove a). Since $\dim V = n$, it suffices to check that $x_1, x_2, \ldots, x_n$ are linearly independent. If this is not the case, we deduce from Theorems 7.14 and 7.9 that $\det_{(v_1,v_2,\ldots,v_n)}(x_1, x_2, \ldots, x_n) = 0$, a contradiction. □

Problem 7.18. Let V be a finite dimensional F-vector space, let $e_1, \ldots, e_n$ be a basis of V and let $T : V \to V$ be a linear transformation. Prove that for all $v_1, \ldots, v_n \in V$ we have

$$\sum_{i=1}^{n} \det(v_1, \ldots, v_{i-1}, T(v_i), v_{i+1}, \ldots, v_n) = \mathrm{Tr}(T) \cdot \det(v_1, \ldots, v_n),$$

where all determinants are computed with respect to the basis $e_1, \ldots, e_n$ and where $\mathrm{Tr}(T)$ is the trace of the matrix of T with respect to the basis $e_1, \ldots, e_n$.

Solution. Consider the map

$$\varphi : V^n \to F, \quad \varphi(v_1, \ldots, v_n) = \sum_{i=1}^{n} \det(v_1, \ldots, v_{i-1}, T(v_i), v_{i+1}, \ldots, v_n).$$

This map is a sum of n-linear maps, thus it is n-linear. Moreover, it is alternating. Indeed, assume for example that $v_1 = v_2$. Then $\det(v_1, \ldots, v_{i-1}, T(v_i), v_{i+1}, \ldots, v_n) = 0$ for $i > 2$ and

$$\det(T(v_1), v_2, \ldots, v_n) + \det(v_1, T(v_2), \ldots, v_n) =$$

$$\det(T(v_1), v_1, v_3, \ldots, v_n) + \det(v_1, T(v_1), v_3, \ldots, v_n) = 0,$$

since the determinant is antisymmetric.

Since the space of n-linear alternating forms on V is one-dimensional, it follows that we can find a scalar $\alpha \in F$ such that

$$\varphi(v_1, \ldots, v_n) = \alpha \det(v_1, \ldots, v_n)$$

for all $v_1, \ldots, v_n$. Choose $v_1 = e_1, \ldots, v_n = e_n$ and let $A = [a_{ij}]$ be the matrix of T with respect to $e_1, \ldots, e_n$. Then the right-hand side equals α, while the left-hand side equals

$$\sum_{i=1}^{n} \det(e_1, \ldots, e_{i-1}, \sum_{j=1}^{n} a_{ji} e_j, e_{i+1}, \ldots, e_n) =$$

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{ji} \det(e_1, \ldots, e_{i-1}, e_j, e_{i+1}, \ldots, e_n) = \sum_{i=1}^{n} a_{ii},$$

the last equality being a consequence of the fact that the determinant map is alternating. Since $\sum_{i=1}^{n} a_{ii} = \mathrm{Tr}(T)$, we conclude that $\alpha = \mathrm{Tr}(T)$ and we are done. □

Remark 7.19. $\mathrm{Tr}(T)$ is actually **independent of the choice of the basis** $e_1, \ldots, e_n$ and it is called the **trace of** T. To prove the independence with respect to the choice of the basis, we need to prove that for all $A \in M_n(F)$ and all $P \in \mathrm{GL}_n(F)$ we have

$$\mathrm{Tr}(A) = \mathrm{Tr}(PAP^{-1}).$$

By a fundamental property of the trace map (which the reader can check without any difficulty) we have

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$

for all matrices $A, B \in M_n(F)$. Thus

$$\mathrm{Tr}(PAP^{-1}) = \mathrm{Tr}((PA)P^{-1}) = \mathrm{Tr}(P^{-1}(PA)) = \mathrm{Tr}((P^{-1}P)A) = \mathrm{Tr}(A).$$

Consider a vector space V of dimension $n \geq 1$ and a linear transformation $T : V \to V$. If $f : V^n \to F$ is an n-linear form, then one can easily check that

- the map
$$T_f : V^n \to F, \quad (x_1, \ldots, x_n) \mapsto f(T(x_1), \ldots, T(x_n))$$
is also an n-linear form.
- If f is alternating, then so is T_f.

Using these observations, we will prove the following fundamental theorem:

Theorem 7.20. *Let V be a vector space of dimension $n \geq 1$ over F. For any linear transformation $T : V \to V$ there is a unique scalar* $\det T \in F$ *such that*

$$f(T(x_1), T(x_2), \ldots, T(x_n)) = \det T \cdot f(x_1, x_2, \ldots, x_n) \tag{7.3}$$

for all n-linear alternating forms $f : V^n \to F$ and all $x_1, x_2, \ldots, x_n \in V$.

Proof. Fix a basis $v_1, v_2, \ldots, v_n$ of V and denote $f_0 = \det_{(v_1,\ldots,v_n)}$. By Theorem 7.13 and Remark 7.11 f_0 is n-linear, alternating and we have $f_0(v_1, \ldots, v_n) = 1$.

Since $(x_1, \ldots, x_n) \to f_0(T(x_1), \ldots, T(x_n))$ is n-linear and alternating, it must be a scalar multiple of f_0, thus we can find $\det T \in F$ such that

$$f_0(T(x_1), \ldots, T(x_n)) = \det T \cdot f_0(x_1, \ldots, x_n)$$

for all $x_1, \ldots, x_n \in V$. Since any n-linear alternating form f is a scalar multiple of f_0 (Corollary 7.15), it follows that relation (7.3) holds for any such map f (since by definition of $\det T$ it holds for f_0), which establishes the existence part of the theorem. Uniqueness is much easier: if relation (7.3) holds for all f and all $x_1, \ldots, x_n$, choosing $f = f_0$ and $x_i = v_i$ for all i yields

$$\det T = f_0(T(v_1), \ldots, T(v_n)),$$

which clearly shows that $\det T$ is unique. □

Definition 7.21. The scalar $\det T$ is called the **determinant of the linear transformation** T.

Note that the end of the proof of Theorem 7.20 gives an explicit formula

$$\det T = \det_{(v_1,\ldots,v_n)}(T(v_1), \ldots, T(v_n)) \tag{7.4}$$

and this for **any choice** of the basis $v_1, \ldots, v_n$ of V. In particular, the right-hand side is independent of the choice of the basis!

Moreover, this allows us to express $\det T$ in terms of the matrix A_T of T with respect to the basis $v_1, \ldots, v_n$. Recall that $A_T = [a_{ij}]$ with

$$T(v_i) = \sum_{j=1}^{n} a_{ji} v_j.$$

Following the proof of Theorem 7.14 (i.e., using the fact that $\det_{(v_1,\ldots,v_n)}$ is n-linear and alternating, thus antisymmetric), we obtain

$$\det_{(v_1,\ldots,v_n)}(T(v_1), \ldots, T(v_n)) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}.$$

The right-hand side is expressed purely in terms of the matrix A_T, which motivates the following:

Definition 7.22. If $A = [a_{ij}] \in M_n(F)$, we define its determinant by

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}. \tag{7.5}$$

We also write $\det A$ as

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

Problem 7.23. Prove that the determinant of a diagonal matrix is the product of diagonal entries of that matrix. In particular $\det I_n = 1$.

Solution. Let $A = [a_{ij}]$ be a diagonal $n \times n$ matrix. Then

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}.$$

Consider a nonzero term in the previous sum, corresponding to a permutation σ. We have $a_{i\sigma(i)} \neq 0$ for all $i \in \{1, 2, \ldots, n\}$ and since A is diagonal, thus forces $\sigma(i) = i$ for all $i \in \{1, 2, \ldots, n\}$. It follows that the only possibly nonzero term in the above sum is the one corresponding to the identity permutation, which equals $a_{11} \ldots a_{nn}$, hence

$$\det A = a_{11} \ldots a_{nn},$$

as desired. □

Let us come back to our original situation: we have a vector space V over F, a linear transformation $T : V \to V$, a basis $v_1, \ldots, v_n$ of V and the matrix A_T of T with respect to this basis. The previous discussion gives

$$\det T = \det A_T \tag{7.6}$$

Note that the left-hand side is completely intrinsic to T by Theorem 7.20, in particular it is independent of the choice of $v_1, \ldots, v_n$. On the other hand, the matrix A_T certainly depends on the choice of the basis $v_1, \ldots, v_n$. The miracle is that while A_T depends on choices, its determinant does not! Let us glorify this observation, since this is a very important result:

Theorem 7.24. *If $A \in M_n(F)$, then $\det A = \det(PAP^{-1})$ for any invertible matrix $P \in \mathrm{GL}_n(F)$. In other words, similar matrices have the same determinant.*

We can turn this discussion upside down: start now with any matrix $A \in M_n(F)$ and let $T : F^n \to F^n$ be the linear transformation sending $X \in F^n$ to AX. Then A is the matrix of T with respect to the canonical basis $e_1, \ldots, e_n$ of F^n and the previous discussion shows that $\det A = \det T$. We deduce from Theorem 7.20 that

$$f(AX_1, AX_2, \ldots, AX_n) = \det A \cdot f(X_1, \ldots, X_n)$$

for all n-linear alternating forms $f : (F^n)^n \to F$.

7.2.1 Problems for Practice

1. Check that the general definition of the determinant of a matrix matches the definition of the determinant of a matrix $A \in M_2(\mathbf{C})$ as seen in the chapter concerned with square matrices of order 2.
2. Recall that a permutation matrix is a matrix $A \in M_n(\mathbf{R})$ having precisely one nonzero entry in each row and column, and this nonzero entry is equal to 1. Prove that the determinant of a permutation matrix is equal to 1 or -1.
3. Let $A = [a_{ij}] \in M_n(\mathbf{C})$ and let $B = [(-1)^{i+j} a_{ij}] \in M_n(\mathbf{C})$. Compare $\det A$ and $\det B$.
4. Generalize the previous problem as follows: let z be a complex number and let $A = [a_{ij}] \in M_n(\mathbf{C})$ and $B = [z^{i+j} a_{ij}] \in M_n(\mathbf{C})$. Express $\det B$ in terms of $\det A$ and z.
5. (The Wronskian) Let $f_1, f_2, \ldots, f_n$ be real-valued maps on some open interval I of $\mathbf{R}$. Assume that each of these maps is differentiable at least $n-1$ times. For $x \in I$ let $W(f_1, \ldots, f_n)(x)$ be the determinant of the matrix $A = [f_i^{(j-1)}(x)]_{1 \le i,j \le n}$, where $f_i^{(j)}$ is the jth derivative of f_i (with the convention that $f_i^{(0)} = f_i$). The map $x \mapsto W(f_1, \ldots, f_n)(x)$ is called the **Wronskian of** $f_1, \ldots, f_n$.

a) Take $n = 2$ and $f_1(x) = e^{ax}$, $f_2(x) = e^{bx}$ for two real numbers a, b. Compute the Wronskian of f_1, f_2.
b) Prove that if $f_1, \ldots, f_n$ are linearly dependent, then

$$W(f_1, \ldots, f_n) = 0.$$

6. Consider a matrix-valued map $A : I \to M_n(\mathbf{R})$, $A(t) = [a_{ij}(t)]$, where $a_{ij} : I \to \mathbf{R}$ are differentiable maps on some open interval I of $\mathbf{R}$. Let B_k be the matrix obtained by replacing all entries in the kth row of A by their derivatives. Prove that for all $t \in I$

$$\det(A(t)) = \sum_{k=1}^{n} \det(B_k(t)).$$

In the next problems V is a vector space of dimension $n \geq 1$ over a field $F \in \{\mathbf{R}, \mathbf{C}\}$. If p is a nonnegative integer, we let $\wedge^p V^*$ be the vector space of all p-linear alternating forms $\omega : V^p = V \times \ldots \times V \to F$, with the convention that $\wedge^0 V = F$.

7. Prove that $\wedge^p V^* = 0$ for $p > n$.
8. Prove that if W is a finite dimensional vector space over F and if $f : V \to W$ is a linear map, then f induces a linear map $f^* : \wedge^p W^* \to \wedge^p V^*$ defined by

$$f^*(\omega)(v_1, \ldots, v_p) = \omega(f(v_1), \ldots, f(v_p)).$$

9. Prove that if $g : W \to Z$ is a linear map from W to another finite dimensional vector space Z over F, then

$$(g \circ f)^* = f^* \circ g^*$$

as maps $\wedge^p Z^* \to \wedge^p V^*$.

If $\omega \in \wedge^p V^*$ and $\eta \in \wedge^q V^*$, we define the **exterior product** $\omega \wedge \eta$ of ω and η as the map $\omega \wedge \eta : V^{p+q} \to F$ defined by

$$(\omega \wedge \eta)(v_1, \ldots, v_{p+q}) = \frac{1}{p!q!} \sum_{\sigma \in S_{p+q}} \varepsilon(\sigma) \omega(v_{\sigma(1)}, \ldots, v_{\sigma(p)}) \cdot \eta(v_{\sigma(p+1)}, \ldots, v_{\sigma(p+q)}).$$

10. Prove that $\omega \wedge \eta \in \wedge^{p+q} V^*$.
11. Prove that

$$\omega \wedge \eta = (-1)^{pq} \eta \wedge \omega.$$

12. Check that for all $\omega_1 \in \wedge^p V^*$, $\omega_2 \in \wedge^q V^*$ and $\omega_3 \in \wedge^r V^*$ we have

$$(\omega_1 \wedge \omega_2) \wedge \omega_3 = \omega_1 \wedge (\omega_2 \wedge \omega_3).$$

We define $\omega_1 \wedge \omega_2 \wedge \ldots \wedge \omega_r$ by induction on r as follows:

$$\omega_1 \wedge \ldots \wedge \omega_r = (\omega_1 \wedge \omega_2 \wedge \ldots \wedge \omega_{r-1}) \wedge \omega_r.$$

13. Check that for all $\omega_1, \ldots, \omega_p \in V^* = \wedge^1 V^*$ and all $v_1, \ldots, v_p \in V$ we have

$$(\omega_1 \wedge \ldots \wedge \omega_p)(v_1, \ldots, v_p) = \det(\omega_i(x_j)).$$

The right-hand side is by definition the determinant of the matrix $A = [\omega_i(x_j)] \in M_p(F)$.

14. Prove that $\omega_1, \ldots, \omega_p \in V^* = \wedge^1 V^*$ are linearly independent if and only if

$$\omega_1 \wedge \omega_2 \wedge \ldots \wedge \omega_p \neq 0.$$

15. Let $\omega_1, \ldots, \omega_n$ be a basis of V. Prove that the family $(\omega_{i_1} \wedge \ldots \wedge \omega_{i_p})_{1 \leq i_1 < \ldots < i_p \leq n}$ forms a basis of $\wedge^p V^*$ and deduce that

$$\dim \wedge^p V^* = \binom{n}{p} := \frac{n!}{p!(n-p)!}.$$

7.3 Main Properties of the Determinant of a Matrix

We reach now the heart of this chapter: establishing the main properties of the determinant map that was introduced in the previous section. We have fortunately developed all the necessary theory to be able to give clean proofs of all important properties of determinants.

A first very important result is the **homogeneity of the determinant map**: **if we multiply all entries of a matrix $A \in M_n(F)$ by a scalar $\lambda \in F$, then the determinant gets multiplied by λ^n.**

Proposition 7.25. *We have* $\det(\lambda A) = \lambda^n \det A$ *for all* $A \in M_n(F)$ *and all* $\lambda \in F$.

Proof. Write $A = [a_{ij}]$, then $\lambda A = [\lambda a_{ij}]$, hence by definition

$$\det(\lambda A) = \sum_{\sigma \in S_n} \varepsilon(\sigma)(\lambda a_{1\sigma(1)}) \cdot \ldots \cdot (\lambda a_{n\sigma(n)}) =$$

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) \lambda^n a_{1\sigma_1} \cdot \ldots \cdot a_{n\sigma(n)} = \lambda^n \cdot \det A,$$

as desired. □

Problem 7.26. Prove that for any $A \in M_n(\mathbf{C})$ we have

$$\det(\overline{A}) = \overline{\det A},$$

where the entries of $\overline{A}$ are the complex conjugates of the entries of A.

Solution. Let $A = [a_{ij}]$, then $\overline{A} = [\overline{a_{ij}}]$ and so

$$\det(\overline{A}) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \overline{a_{1\sigma(1)}} \cdot \ldots \cdot \overline{a_{n\sigma(n)}} =$$

$$\sum_{\sigma \in S_n} \varepsilon(\sigma) \overline{a_{1\sigma(1)} \ldots a_{n\sigma(n)}} = \overline{\sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}} = \overline{\det A}.$$

□

The main property of the determinant is its **multiplicative character**.

Theorem 7.27. *For all linear transformations T_1, T_2 on a finite dimensional vector space V we have*

$$\det(T_1 \circ T_2) = \det T_1 \cdot \det T_2.$$

Proof. Let $v_1, \ldots, v_n$ be a basis of V. By Theorem 7.20 we have

$$\det(T_1 \circ T_2) = \det_{(v_1,\ldots,v_n)}(T_1(T_2(v_1)), \ldots, T_1(T_2(v_n)))$$

$$= \det T_1 \cdot \det_{(v_1,\ldots,v_n)}(T_2(v_1), \ldots, T_2(v_n)).$$

Relation (7.4) shows that

$$\det_{(v_1,\ldots,v_n)}(T_2(v_1), \ldots, T_2(v_n)) = \det T_2.$$

Combining these two equalities yields the desired result. □

Combining the previous theorem and relation (7.6) we obtain the following fundamental theorem, which would be quite a pain in the neck to prove directly from the defining relation (7.5).

Theorem 7.28. *For all matrices $A, B \in M_n(F)$ we have*

$$\det(AB) = \det A \cdot \det B.$$

Proof. Let $V = F^n$ and let $T_1 : V \to V$ be the linear transformation sending $X \in V$ to AX. Define similarly T_2 replacing A by B. If S is a linear transformation on V, let A_S be the matrix of S with respect to the canonical basis of $V = F^n$. Then $A = A_{T_1}$, $B = A_{T_2}$ and $AB = A_{T_1 \circ T_2}$. The result follows directly from the previous theorem and relation (7.6). □

Problem 7.29. An invertible matrix $A \in M_n(\mathbf{R})$ has the property that both A and A^{-1} have integer entries. Prove that $\det A \in \{-1, 1\}$.

Solution. We have $A \cdot A^{-1} = I_n$, so using the fact that the determinant is multiplicative and that $\det I_n = 1$ (which follows straight from the definition of the determinant of a matrix), we obtain

$$1 = \det I_n = \det(A \cdot A^{-1}) = \det A \cdot \det(A^{-1}).$$

Next, recalling the definition of the determinant of a matrix, we notice that if all entries of the matrix are integers, then the determinant of the matrix is an integer (since it is obtained by taking sums and differences of products of the entries of the matrix). Since A and A^{-1} have by hypothesis integer entries, it follows that $\det A$ and $\det A^{-1}$ are two integers, whose product equals 1. Thus $\det A$ is a divisor of 1 and necessarily $\det A \in \{-1, 1\}$. □

Remark 7.30. A much more remarkable result is the following kind of converse: suppose that $A \in M_n(\mathbf{R})$ is a matrix with integer entries. If $\det A \in \{-1, 1\}$, then A^{-1} has integer entries. This is fairly difficult to prove with the tools we have introduced so far! The reader might try to do the case $n = 2$, which is not so difficult.

We can use the previous theorem and Corollary 7.17 to obtain a beautiful characterization of invertible matrices. The result is stunningly simple to state.

Theorem 7.31. *A matrix $A \in M_n(F)$ is invertible if and only if* $\det A \neq 0$.

Proof. Suppose that A is invertible, so there is a matrix $B \in M_n(F)$ such that $AB = BA = I_n$. Taking the determinant yields $\det A \cdot \det B = 1$, thus $\det A \neq 0$.

Conversely, suppose that $\det A \neq 0$ and let $e_1, \ldots, e_n$ be the canonical basis of F^n, and $C_1, \ldots, C_n \in F^n$ the columns of A. Then $\det A = \det_{(e_1,\ldots,e_n)}(C_1, \ldots, C_n)$ is nonzero, thus by Corollary 7.17 the vectors $C_1, \ldots, C_n$ are linearly independent. This means that the linear map $\varphi : F^n \to F^n$ sending X to AX is injective, and so invertible. Let ψ be its inverse and let B be the matrix of ψ in the canonical basis of F^n. The equalities $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}$ yield $AB = BA = I_n$, thus A is invertible. □

Problem 7.32. Let A and B be invertible $n \times n$ matrices with real entries, where n is an odd positive integer. Show that $AB + BA$ is nonzero.

Solution. Suppose that $AB + BA = O_n$, thus $AB = -BA$. Taking the determinant, we deduce that

$$\det(AB) = (-1)^n \det BA = -\det BA.$$

On the other hand, $\det(AB) = \det A \det B = \det(BA)$, thus the previous equality yields $2 \det A \det B = 0$. This contradicts the hypothesis that A and B are invertible. □

Problem 7.33. Let A and B be two square matrices with real coefficients. If A and B commute, prove that

$$\det(A^2 + B^2) \geq 0.$$

Solution. Since A and B commute, we have

$$A^2 + B^2 = (A + iB)(A - iB).$$

Thus

$$\det(A^2 + B^2) = \det(A + iB)\det(A - iB).$$

But using Problem 7.26 we obtain

$$\det(A - iB) = \det(\overline{A + iB}) = \overline{\det(A + iB)},$$

thus

$$\det(A^2 + B^2) = |\det(A + iB)|^2 \geq 0,$$

as desired. □

Problem 7.34. Let n be an odd integer and let $A, B \in M_n(\mathbf{R})$ be matrices such that $A^2 + B^2 = O_n$. Prove that $AB - BA$ is not invertible.

Solution. Consider the equality

$$(A + iB)(A - iB) = A^2 + B^2 + i(BA - AB) = i(BA - AB).$$

Taking the determinant yields

$$\det(A + iB)\det(A - iB) = i^n \det(BA - AB).$$

Suppose that $\det(AB - BA) \neq 0$ and note that since A, B have real entries, we have by Problem 7.26

$$\det(A - iB) = \det(\overline{A + iB}) = \overline{\det(A + iB)}$$

and so

$$|\det(A + iB)|^2 = i^n \det(BA - AB).$$

Since $\det(AB - BA)$ is nonzero, we deduce that i^n is real, contradicting the hypothesis that n is odd. Thus

$$\det(AB - BA) = 0$$

and the result follows. □

Remark 7.35. An alternate solution goes as follows. Note that we have

$$(A + iB)(A - iB) = A^2 + B^2 + i(BA - AB) = i(BA - AB)$$

and

$$(A - iB)(A + iB) = A^2 + B^2 - i(BA - AB) = -i(BA - AB).$$

Since

$$\det((A + iB)(A - iB)) = \det(A + iB)\det(A - iB) = \det((A - iB)(A + iB)),$$

and n is odd, we conclude that

$$i^n \det(BA - AB) = (-i)^n \det(BA - AB) = -i^n \det(BA - AB)$$

and hence $\det(BA - AB) = 0$.

Problem 7.36. Let p, q be real numbers such that the equation $x^2 + px + q = 0$ has no real solutions. Prove that if n is odd, then the equation $X^2 + pX + qI_n = O_n$ has no solution in $M_n(\mathbf{R})$.

Solution. Suppose that $X^2 + pX + qI_n = O_n$ for some $X \in M_n(\mathbf{R})$. We can write this equation as

$$\left(X + \frac{p}{2} I_n\right)^2 = \frac{p^2 - 4q}{4} I_n.$$

Taking the determinant, we deduce that

$$\left(\frac{p^2 - 4q}{4}\right)^n = \left(\det\left(X + \frac{p}{2} I_n\right)\right)^2 \geq 0.$$

This is impossible, since by assumption $p^2 < 4q$ and n is odd. □

Another important property of the determinant of a matrix is its behavior with respect to the transpose operation. Recall that if $A = [a_{ij}] \in M_n(F)$, then its transpose ${}^tA$ is the matrix defined by ${}^tA = [a_{ji}]$.

Theorem 7.37. *For all matrices $A \in M_n(F)$ we have*

$$\det A = \det({}^tA).$$

Proof. By formula (7.5) applied to ${}^tA$ we have

$$\det({}^tA) = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(n)n}.$$

For any permutation σ we have

$$a_{\sigma(1)1}\ldots a_{\sigma(n)n} = a_{1\sigma^{-1}(1)}\ldots a_{n\sigma^{-1}(n)},$$

since $a_{i\sigma^{-1}(i)} = a_{\sigma(j)j}$ with $j = \sigma^{-1}(i)$ (and when i runs over $\{1, 2, \ldots, n\}$, so does j). Using this relation and the observation that $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1} = \varepsilon(\sigma)$, we obtain[2]

$$\det({}^tA) = \sum_{\sigma\in S_n} \varepsilon(\sigma^{-1})a_{1\sigma^{-1}(1)}\ldots a_{n\sigma^{-1}(n)} =$$

$$= \sum_{\sigma\in S_n} \varepsilon(\sigma)a_{1\sigma(1)}\ldots a_{n\sigma(n)} = \det A.$$

The result follows. □

Problem 7.38. Let A be a skew-symmetric matrix (recall that this means that $A + {}^tA = O_n$) of odd order with real or complex coefficients. Prove that $\det(A) = 0$.

Solution. By hypothesis we have ${}^tA = -A$. Since $\det(A) = \det({}^tA)$, it follows that

$$\det(A) = \det({}^tA) = \det(-A) = (-1)^n \det(A) = -\det(A).$$

Thus $\det(A)$ must be 0. □

Problem 7.39. Let A be a matrix of odd order. Show that

$$\det(A - {}^tA) = 0.$$

Solution. We have

$${}^t(A - {}^tA) = {}^tA - {}^t({}^tA) = {}^tA - A = -(A - {}^tA),$$

thus the matrix $A - {}^tA$ is skew-symmetric and its determinant must be 0 by Problem 7.38. □

Problem 7.40. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be complex numbers. Compute the determinant

$$\begin{vmatrix} a_1 + b_1 & b_1 & \ldots & b_1 \\ b_2 & a_2 + b_2 & \ldots & b_2 \\ \ldots & \ldots & \ldots & \ldots \\ b_n & b_n & \ldots & a_n + b_n \end{vmatrix}.$$

[2]Note that when σ runs over S_n, so does σ^{-1}.

Solution. Let A be the matrix whose determinant we need to evaluate. We have

$$\det A = \det({}^t A)$$

and the columns of ${}^t A$ are the vectors $a_1 e_1 + b_1 v, \ldots, a_n e_n + b_n v$, where $e_1, \ldots, e_n$ is the canonical basis of $\mathbf{C}^n$ and v is the vector all of whose coordinates are equal to 1. We deduce that[3]

$$\det({}^t A) = \det(a_1 e_1 + b_1 v, \ldots, a_n e_n + b_n v).$$

Using the fact that the determinant map is multilinear and alternating, we obtain

$$\det({}^t A) = \det(a_1 e_1, \ldots, a_n e_n) + \sum_{i=1}^{n} \det(a_1 e_1, \ldots, a_{i-1} e_{i-1}, b_i v, a_{i+1} e_{i+1}, \ldots, a_n e_n).$$

Indeed, note that $\det(x_1, \ldots, x_n) = 0$ if at least two of the vectors $x_1, \ldots, x_n$ are multiples of v. We conclude that

$$\det({}^t A) = a_1 \ldots a_n + \sum_{i=1}^{n} a_1 \ldots a_{i-1} b_i a_{i+1} \ldots a_n \det(e_1, \ldots, e_{i-1}, v, e_{i+1}, \ldots, e_n).$$

Since $v = e_1 + \ldots + e_n$ and the determinant map is multilinear and alternating, we have

$$\det(e_1, \ldots, e_{i-1}, v, e_{i+1}, \ldots, e_n) = \det(e_1, \ldots, e_n) = 1$$

for all i. We conclude that

$$\det A = a_1 \ldots a_n + \sum_{i=1}^{n} b_i \cdot \prod_{k \neq i} a_k.$$

□

Recall that a matrix $A \in M_n(F)$ is called **upper-triangular** if all entries of A below the main diagonal are 0, that is $a_{ij} = 0$ whenever $i > j$. Similarly, A is called **lower-triangular** if all entries above the main diagonal are 0, that is $a_{ij} = 0$ whenever $i < j$. The result of the following computation is absolutely crucial: **the determinant of an upper-triangular or lower-triangular square matrix is simply the product of the diagonal entries**. One can hardly underestimate the power of this innocent-looking statement.

[3] We simply write det instead of $\det_{(e_1,\ldots,e_n)}$.

Theorem 7.41. *If $A = [a_{ij}] \in M_n(F)$ is upper-triangular or lower triangular, then*

$$\det A = \prod_{i=1}^{n} a_{ii}.$$

Proof. The argument being identical in the lower-triangular case, let us assume that A is upper-triangular. Consider a nonzero term $\varepsilon(\sigma)a_{1\sigma(1)}\ldots a_{n\sigma(n)}$ appearing in the right-hand side of formula (7.4). Then each $a_{i\sigma(i)}$ is nonzero and so necessarily $i \leq \sigma(i)$ for all i. But since $\sum_{i=1}^{n} i = \sum_{i=1}^{n} \sigma(i)$ (as σ is a permutation), all the previous inequalities must be equalities. Thus σ is the identity permutation and the corresponding term is $a_{11}\ldots a_{nn}$. Since all other terms are 0, the theorem is proved. □

Problem 7.42. For $1 \leq i, j \leq n$ we let a_{ij} be the number of common positive divisors of i and j, and we let $b_{ij} = 1$ if j divides i, and $b_{ij} = 0$ otherwise.

a) Prove that $A = B \cdot {}^tB$, where $A = [a_{ij}]$ and $B = [b_{ij}]$.
b) What can you say about the shape of the matrix B?
c) Compute $\det A$.

Solution. a) Let us fix $i, j \in \{1, 2, \ldots, n\}$ and compute, using the product rule

$$(B \cdot {}^tB)_{ij} = \sum_{k=1}^{n} b_{ik} b_{jk}.$$

Consider a nonzero term $b_{ik}b_{jk}$ in the previous sum. Since b_{ik} and b_{jk} are nonzero, k must divide both i and j, that is k is a common positive divisor of i and j. Conversely, if k is a common positive divisor of i and j, then $b_{ik} = b_{jk} = 1$. We deduce that the only nonzero terms in the sum are those corresponding to common positive divisors of i and j, and each such nonzero term equals 1. Thus $(B \cdot {}^tB)_{ij}$ is the number of common positive divisors of i and j, which by definition of A is simply a_{ij}. Since i, j were arbitrary, we deduce that $A = B \cdot {}^tB$.

b) If $i < j$ are between 1 and n, then certainly j cannot divide i and so $b_{ij} = 0$. Thus $b_{ij} = 0$ whenever $i < j$, which means that B is lower-triangular. We can say a little more: since i divides i for all $i \in \{1, 2, \ldots, n\}$, we have $b_{ii} = 1$, thus all diagonal terms of B are equal to 1.

c) Since the determinant is multiplicative and since $\det B = \det({}^tB)$, we have (using part a))

$$\det A = \det(B \cdot {}^tB) = (\det B)^2.$$

We can now use part b) and the previous theorem to conclude that $\det B = 1$ and so

$$\det A = 1.$$

□

The next theorem (which can be very useful in practice) would also be quite painful to prove directly by manipulating the complicated expression defining the determinant of a matrix. The theory of alternating multilinear forms makes the proof completely transparent.

Theorem 7.43 (Block-Determinants). *Let $A \in M_n(F)$ be a matrix given in block form*

$$A = \begin{bmatrix} B & D \\ O_{q,p} & C \end{bmatrix},$$

where $B \in M_p(F)$, $C \in M_q(F)$ (with $p + q = n$) and $D \in M_{p,q}(F)$. Then

$$\det A = \det B \cdot \det C.$$

Proof. Consider the map

$$\varphi : (F^p)^p \to F, \quad \varphi(X_1, \ldots, X_p) = \begin{vmatrix} X & D \\ O_{q,p} & C \end{vmatrix},$$

where $X \in M_p(F)$ is the matrix with columns $X_1, \ldots, X_p$. The determinant map on $(F^n)^n$ (with respect to the canonical basis of F^n) being linear with respect to each variable, φ is p-linear. Moreover, φ is alternating: if $X_i = X_j$ for some $i \neq j$, then columns i and j in the matrix $\begin{bmatrix} X & D \\ O_{q,p} & C \end{bmatrix}$ are equal and so this matrix has determinant 0.

Now, applying Theorem 7.14 to the canonical basis of F^p, we obtain

$$\varphi(X) = \begin{vmatrix} X & D \\ O_{q,p} & C \end{vmatrix} = \det X \cdot \begin{vmatrix} I_p & D \\ O_{q,p} & C \end{vmatrix}$$

for all $X \in M_p(F)$. The same game played with the q-linear alternating form $Y \to \begin{vmatrix} I_p & D \\ O_{q,p} & Y \end{vmatrix}$ yields

$$\begin{vmatrix} I_p & D \\ O_{q,p} & Y \end{vmatrix} = \det Y \cdot \begin{vmatrix} I_p & D \\ O_{q,p} & I_q \end{vmatrix}.$$

Thus

$$\det A = \det B \det C \begin{vmatrix} I_p & D \\ O_{q,p} & I_q \end{vmatrix} = \det B \det C,$$

the last equality being a consequence of the fact that the matrix $\begin{bmatrix} I_p & D \\ O_{q,p} & I_q \end{bmatrix}$ is upper-triangular with diagonal entries equal to 1, thus its determinant equals 1. □

Problem 7.44. Let $A \in M_n(\mathbf{C})$ and let $T : M_n(\mathbf{C}) \to M_n(\mathbf{C})$ be the map defined by $T(X) = AX$. Find the determinant of T.

Solution. Let $(E_{ij})_{1 \leq i,j \leq n}$ be the canonical basis of $M_n(\mathbf{C})$. Note that

$$T(E_{ij}) = AE_{ij} = \sum_{k=1}^{n} a_{ki} E_{kj},$$

as shows a direct inspection of the product AE_{ij}. We deduce that the matrix of T with respect to the basis $E_{11}, \ldots, E_{n1}, E_{12}, \ldots, E_{n2}, \ldots, E_{1n}, \ldots, E_{nn}$ is a block-diagonal matrix with n diagonal blocks equal to A. It follows from Theorem 7.43 that

$$\det T = (\det A)^n.$$

□

7.3.1 Problems for Practice

1. A 5×5 matrix A with real entries has determinant 2. Compute the determinant of $2A, -3A, A^2, -A^3, ({}^tA)^2$.
2. Prove that the determinant of an orthogonal matrix $A \in M_n(\mathbf{R})$ equals -1 or 1. We recall that A is orthogonal if $A \cdot {}^tA = I_n$.
3. a) A matrix $A \in M_n(\mathbf{R})$ satisfies $A^3 = I_n$. What are the possible values of $\det A$?
   b) Answer the same question with $\mathbf{R}$ replaced by $\mathbf{C}$.
   c) Answer the same question with $\mathbf{R}$ replaced by $\mathbf{F}_2$.
4. Prove that for all $A \in M_n(\mathbf{R})$ we have

$$\det(A \cdot {}^tA) \geq 0.$$

5. If $A = [a_{ij}] \in M_n(\mathbf{C})$, define $A^* = [\overline{a_{ji}}] \in M_n(\mathbf{C})$.
   a) Express $\det(A^*)$ in terms of $\det A$.
   b) Prove that $\det(A \cdot A^*) \geq 0$.
6. Let T be a linear transformation on a finite dimensional vector space V. Suppose that $V = V_1 \oplus V_2$ for some subspaces V_1, V_2 which are stable under T. Let T_1, T_2 be the restrictions of T to V_1, V_2. Prove that

$$\det T = \det T_1 \cdot \det T_2.$$

7. The entries of a matrix $A \in M_n(\mathbf{R})$ are equal to -1 or 1. Prove that 2^{n-1} divides $\det A$.

8. Prove that for any matrix $A \in M_n(\mathbf{R})$ we have

   a) $\det(A^2 + I_n) \geq 0$.
   b) $\det(A^2 + A + I_n) \geq 0$.

9. Prove that if $A, B \in M_n(\mathbf{R})$ are matrices which commute, then

$$\det(A^2 + AB + B^2) \geq 0.$$

10. Let $A, B, C \in M_n(\mathbf{R})$ be pairwise commuting matrices. Prove that

$$\det(A^2 + B^2 + C^2 - AB - BC - CA) \geq 0.$$

    Hint: express $A^2 + B^2 + C^2 - AB - BC - CA$ simply in terms of the matrices $X = A - B$ and $Y = B - C$.

11. Let $A \in M_n(\mathbf{C})$ and consider the matrix

$$B = \begin{bmatrix} I_n & A \\ A & I_n \end{bmatrix}.$$

    a) Prove that $\det B = \det(I_n - A) \cdot \det(I_n + A)$. Hint: start by proving the equality

$$\begin{bmatrix} I_n & A \\ A & I_n \end{bmatrix} = \begin{bmatrix} I_n & O_n \\ A & I_n - A^2 \end{bmatrix} \cdot \begin{bmatrix} I_n & A \\ O_n & I_n \end{bmatrix}.$$

    b) If B is invertible, prove that $I_n - A^2$ is invertible and compute the inverse of B in terms of A and the inverse of $I_n - A^2$.

12. Prove that for all matrices $A, B \in M_n(\mathbf{R})$ we have

$$\begin{vmatrix} A & -B \\ B & A \end{vmatrix} = |\det(A + iB)|^2.$$

13. Let $A, B \in M_n(\mathbf{R})$ be matrices such that $A^2 + B^2 = AB$ and $AB - BA$ is invertible.

    a) Let $j = e^{\frac{2i\pi}{3}}$, so that $j^2 + j + 1 = 0$. Check that

$$(A + jB)(A + j^{-1}B) = j(BA - AB).$$

    b) Prove that n is a multiple of 3.

14. (Matrices differing by a rank one matrix) Let $A \in GL_n(F)$ be an invertible matrix and $v, w \in M_{n,1}(F)$ be vectors thought of as $n \times 1$ matrices.

    a) Show that

$$\det(A - v \cdot {}^t w) = \det(A)(1 - {}^t w A^{-1} v),$$

where we think of the 1×1 matrix ${}^t wA^{-1}v$ as a scalar.
Hint. One way to prove this formula is to justify the block matrix formula

$$\begin{bmatrix} 1 - {}^t wA^{-1}v\ {}^t w \\ 0 \qquad\quad A \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ A^{-1}v & I_n \end{bmatrix} = \begin{bmatrix} 1 & {}^t w \\ v & A \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ v & I_n \end{bmatrix} \cdot \begin{bmatrix} 1 & {}^t w \\ 0 & A - v \cdot {}^t w \end{bmatrix}.$$

b) If furthermore ${}^t wA^{-1}v \neq 1$, show that

$$(A - v \cdot {}^t w)^{-1} = A^{-1} + \frac{1}{1 - {}^t wA^{-1}v} A^{-1}v \cdot {}^t wA^{-1}.$$

15. (Determinants of block matrices) Let $X \in M_n(F)$ be a matrix given in block form

$$X = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where $A \in M_p(F)$, $B \in M_{p,q}(F)$, $C \in M_{q,p}(F)$, $D \in M_q(F)$, and $p+q = n$. If A is invertible, show that

$$\det(X) = \det(A) \det(D - CA^{-1}B).$$

Hint. Generalize the block matrix formula from the preceding problem.

16. (Smith's determinant) For $1 \leq i, j \leq n$ let x_{ij} be the greatest common divisor of i and j. The goal of this problem is to compute $\det X$, where $X = [x_{ij}]_{1 \leq i,j \leq n}$.

Let φ be Euler's totient function (i.e., $\varphi(1) = 1$ and, for $n \geq 2$, $\varphi(n)$ is the number of positive integers less than n and relatively prime to n). Define $y_{ij} = \varphi(j)$ if j divides i, and $y_{ij} = 0$ otherwise. Also, let $b_{ij} = 1$ if j divides i and 0 otherwise.

a) Prove that $X = Y\,{}^t B$, where $Y = [y_{ij}]$ and $B = [b_{ij}]$.
b) Prove that

$$\det X = \varphi(1)\varphi(2)\ldots\varphi(n).$$

7.4 Computing Determinants in Practice

If $n = 2$, then S_2 contains only the permutations $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, hence we get

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

a formula which we have extensively used in the chapter devoted to square matrices of order 2. The value of the determinant of a matrix of order two may be remembered by the array

$$\begin{vmatrix} a_{11} & \searrow & a_{12} \\ & & \\ a_{21} & & a_{22} \end{vmatrix}_{+}^{-} = a_{11}a_{22} - a_{12}a_{21}$$

If $n = 3$, then S_3 contains six permutations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The first three permutations are even and the last three are odd. In this case we get

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31}$$
$$- a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

The value of the determinant of order three may be remembered using a particular scheme similar to that used for determinants of order two:

$$\begin{array}{ccccc|cc} a_{11} & & a_{12} & & a_{13} & a_{11} & a_{12} \\ & \searrow & & \swarrow & & \swarrow & \nearrow \\ a_{21} & & a_{22} & & a_{23} & a_{21} & a_{22} \\ & \swarrow & & \searrow & & \searrow & \searrow \\ a_{31} & & a_{32} & & a_{33} & a_{31} & a_{32} \end{array} = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32}$$
$$+ a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31}$$
$$- a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}$$

i.e., the first two columns of the determinant are repeated at its right, the products of the three elements along the arrows running downward and to the right are noted as well as the negative of the products of the three elements along the arrows running upward and to the right. The algebraic sum of these six products is the value of the determinant.

For example, applying this scheme we get

$$\begin{vmatrix} 1 & 4 & 0 \\ -1 & 2 & 1 \\ 2 & 0 & 1 \end{vmatrix} \begin{matrix} 1 & 4 \\ \searrow & \nearrow \\ -1 & 2 \\ \nearrow & \searrow \\ 2 & 0 \end{matrix} = (2) + 8 - 0 - 0 - 0 - (-4) = 14$$

Problem 7.45. Compute the determinant

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

Solution. Using the rule described above, we obtain

$$\begin{vmatrix} 1 & 2 & 3 \\ 2 & -3 & 5 \\ 3 & 1 & -2 \end{vmatrix} = 6 + 30 + 6 + 27 - 5 + 8 = 72.$$

□

Problem 7.46. Consider the invertible matrix

$$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}.$$

Find the determinant of the inverse of A.

Solution. It is useless to compute A^{-1} explicitly in order to solve the problem. Indeed, since $A \cdot A^{-1} = I_3$, we have $\det A \cdot \det(A^{-1}) = 1$ and so

$$\det(A^{-1}) = \frac{1}{\det A}.$$

It suffices therefore to compute $\det A$. Now, using the previous rule, we obtain

$$\det A = 4 + 1 + 1 - 1 - 2 - 2 = 1.$$

Thus

$$\det(A^{-1}) = 1.$$

□

No such easy rules exist for matrices of size at least 4. In practice, the following properties of the determinant allow computing a large quantity of determinants (the elements $R_1, R_2, \ldots, R_n$ below are the rows of the matrix whose determinant we are asked to compute or study).

1. If every element of a row of a determinant of order n is multiplied by the scalar λ, then the value of the determinant is multiplied by λ.
2. If two rows of a determinant are interchanged, then the determinant gets multiplied by -1. More generally, we have the following formula where σ is any permutation in S_n

$$\det \begin{bmatrix} R_{\sigma(1)} \\ R_{\sigma(2)} \\ \vdots \\ R_{\sigma(n)} \end{bmatrix} = \varepsilon(\sigma) \det \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}.$$

3. Adding a scalar multiple of a row of a determinant to **another row** does not change the value of the determinant: for $j \neq k$ and $\lambda \in F$ we have

$$\det \begin{bmatrix} R_1 \\ \vdots \\ R_j + \lambda R_k \\ \vdots \\ R_n \end{bmatrix} = \det \begin{bmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{bmatrix}$$

4. A very useful property is that the determinant of an upper (or lower) **triangular** matrix is simply the product of its diagonal entries.

Note that the operations involved are the elementary row operations studied in Chap. 3. This gives us a practical way of computing determinants, known as the **Gaussian elimination algorithm for determinants**: start with the matrix A whose determinant we want to evaluate and perform Gaussian reduction in order to bring it to its reduced row-echelon form. This will require several elementary operations on the rows of the matrix A, which come down to multiplying A by a sequence of elementary matrices $E_1, \ldots, E_k$ on the left. Thus at the end we obtain

$$E_1 E_2 \ldots E_k A = A_{ref},$$

where A_{ref} is the reduced row-echelon form of A. Taking determinants gives

$$\det(E_1) \cdot \det(E_2) \cdot \ldots \cdot \det E_k \cdot \det A = \det A_{ref}.$$

Since A_{ref} is upper-triangular, its determinant is simply the product of its diagonal entries (in particular if some diagonal entry equals 0, then $\det A = 0$). Also, the

previous rules 1–3 allow us to compute very easily each of the factors $\det E_1$, $\det E_2$,..., $\det E_k$. We can neglect those matrices E_i which correspond to transvections, as their determinant is 1. Next, if E_i corresponds to multiplication of a row by a scalar λ, then $\det E_i = \lambda$, and if E_i corresponds to a permutation of two rows, then $\det E_i = -1$. Thus, in practice we simply follow the Gaussian reduction to bring the matrix to its reduced row-echelon form, and keep in mind to multiply at each step the value of the determinant by the corresponding constant, which depends on the operation performed as explained before.

Remark 7.47. a) Note that since $\det({}^t A) = \det A$ for all $A \in M_n(F)$, all previous properties referring to rows of a matrix (or determinant) still hold when the word row is replaced with the word column.

b) For any particular problem an intelligent human being can probably do better than the naive Gaussian elimination. The most likely way is by being opportunistic to produce more zeroes in the matrix with carefully placed row and/or column operations. Two more systematic ways are:

- If there is some linear dependence among the columns (or rows) then the determinant vanishes, which gives an early exit to the algorithm. Note that this is the case if a column (or row) consists entirely of zeros, or if there are two equal columns or two equal rows.
- Since we can easily compute the determinant of an upper-triangular matrix, we do not need to fully reduce, just get down to a triangular matrix.

c) There are some extra rules one could exploit (they are however more useful in theoretical questions):

- If a column is decomposed as the sum of two column vectors, then the determinant is the sum of the corresponding two determinants, i.e.

$$\det\left[\, c_1 \; c_2 \; \ldots \; c_k' + c_k'' \; \ldots \; c_n \,\right]$$

$$= \det\left[\, c_1 \; c_2 \; \ldots \; c_k' \; \ldots \; c_n \,\right] + \det\left[\, c_1 \; c_2 \; \ldots \; c_k'' \; \ldots \; c_n \,\right].$$

  A similar statement applies to rows.
- If $A \in M_n(\mathbf{C})$, then the determinant of the conjugate matrix of A equals the conjugate of determinant of A, i.e.

$$\det \overline{A} = \overline{\det A}.$$

- For $A, B \in M_n(F)$ we have

$$\det(A \cdot B) = \det A \cdot \det B.$$

- If $A \in M_n(F)$ and $\lambda \in F$, then

$$\det(\lambda A) = \lambda^n \det A.$$

Problem 7.48. Prove that for all real numbers a, b, c we have

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ b+c & c+a & a+b \end{vmatrix} = 0.$$

Solution. Adding the second row to the third row yields

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ b+c & c+a & a+b \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a+b+c & a+b+c & a+b+c \end{vmatrix}.$$

Since the third row is proportional to the first row, this last determinant vanishes. □

Problem 7.49. Let a, b, c be complex numbers. By computing the determinant of the matrix

$$A = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix}$$

in two different ways, prove that

$$a^3 + b^3 + c^3 - 3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca).$$

Solution. First, we can compute $\det A$ using the rule described in the beginning of this section. We end up with

$$\det A = -abc + abc + abc - a^3 - b^3 - c^3 = -(a^3+b^3+c^3-3abc).$$

On the other hand, we can add all columns to the first column and obtain

$$\det A = \begin{vmatrix} a+b+c & b & c \\ a+b+c & c & a \\ a+b+c & a & b \end{vmatrix} = (a+b+c)\begin{vmatrix} 1 & b & c \\ 1 & c & a \\ 1 & a & b \end{vmatrix}.$$

The last determinant can be computed using the rule described in the beginning of the section. We obtain

$$\begin{vmatrix} 1 & b & c \\ 1 & c & a \\ 1 & a & b \end{vmatrix} = bc + ab + ca - c^2 - a^2 - b^2 = -(a^2+b^2+c^2-ab-bc-ca).$$

Thus

$$\det A = -(a+b+c)(a^2+b^2+c^2-ab-bc-ca).$$

Comparing the two expressions for $\det A$ yields the desired result. □

Problem 7.50. Prove that

$$\begin{vmatrix} b_1+c_1 & c_1+a_1 & a_1+b_1 \\ b_2+c_2 & c_2+a_2 & a_2+b_2 \\ b_3+c_3 & c_3+a_3 & a_3+b_3 \end{vmatrix} = 2 \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

for all real numbers $a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3$.

Solution. Performing the indicated operations on the corresponding matrices, we have the following chain of equalities:

$$\begin{vmatrix} b_1+c_1 & c_1+a_1 & a_1+b_1 \\ b_2+c_2 & c_2+a_2 & a_2+b_2 \\ b_3+c_3 & c_3+a_3 & a_3+b_3 \end{vmatrix} \overset{C_1 \to C_1 - C_2}{=\!=} \begin{vmatrix} b_1-a_1 & c_1+a_1 & a_1+b_1 \\ b_2-a_2 & c_2+a_2 & a_2+b_2 \\ b_3-a_3 & c_3+a_3 & a_3+b_3 \end{vmatrix}$$

$$\overset{C_1 \to C_1 - C_3}{=\!=} \begin{vmatrix} -2a_1 & c_1+a_1 & a_1+b_1 \\ -2a_2 & c_2+a_2 & a_2+b_2 \\ -2a_3 & c_3+a_3 & a_3+b_3 \end{vmatrix} = -2 \begin{vmatrix} a_1 & c_1+a_1 & a_1+b_1 \\ a_2 & c_2+a_2 & a_2+b_2 \\ a_3 & c_3+a_3 & a_3+b_3 \end{vmatrix}$$

$$\begin{matrix} C_2 \to C_2 - C_1 \\ =\!= \\ C_3 \to C_3 - C_1 \end{matrix} -2 \begin{vmatrix} a_1 & c_1 & b_1 \\ a_2 & c_2 & b_2 \\ a_3 & c_3 & b_3 \end{vmatrix} = 2 \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

The result follows. □

Remark 7.51. An alternate and shorter solution to the previous problem is to note that

$$\begin{bmatrix} b_1+c_1 & c_1+a_1 & a_1+b_1 \\ b_2+c_2 & c_2+a_2 & a_2+b_2 \\ b_3+c_3 & c_3+a_3 & a_3+b_3 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Problem 7.52. Compute $\det A$, where $x_1, \ldots, x_n$ are real numbers and

$$A = \begin{bmatrix} 1+x_1 & x_2 & x_3 & \ldots & x_n \\ x_1 & 1+x_2 & x_3 & \ldots & x_n \\ \ldots & & & & \\ x_1 & x_2 & x_3 & \ldots & 1+x_n \end{bmatrix}.$$

Solution. We start by adding all the other columns to the first column, and factoring out $1 + x_1 + \ldots + x_n$. We obtain

$$\det A = (1 + x_1 + \ldots + x_n) \begin{vmatrix} 1 & x_2 & \ldots & x_n \\ 1 & 1+x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ 1 & x_2 & \ldots & 1+x_n \end{vmatrix}.$$

In this new determinant, from each row starting with the second we subtract the first row. We end up with

$$\det A = (1 + x_1 + x_2 + \ldots + x_n) \begin{vmatrix} 1 & x_2 & \ldots & x_n \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix}.$$

The last determinant is that of an upper-triangular matrix with diagonal entries equal to 1, thus it equals 1. We conclude that

$$\det A = 1 + x_1 + x_2 + \ldots + x_n.$$

□

Problem 7.53. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be the matrix defined by

$$a_{ij} = \begin{cases} n+1, \text{ if } i = j \\ 1, \quad \text{if } i \neq j. \end{cases}$$

Compute $\det A$.

Solution. The matrix A can be written in the form

$$A = \begin{bmatrix} n+1 & 1 & \ldots & 1 \\ 1 & n+1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \ldots & n+1 \end{bmatrix}.$$

Adding all columns of A to the first column we obtain

$$\det A = \begin{vmatrix} 2n & 1 & \ldots & 1 \\ 2n & n+1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 2n & 1 & \ldots & n+1 \end{vmatrix} = 2n \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & n+1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \ldots & n+1 \end{vmatrix}.$$

The last determinant can be computed by subtracting the first column from each of the other columns, and noting that the resulting matrix is lower-triangular. We obtain

$$\det A = 2n \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & n+1 & \ldots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \ldots & n+1 \end{vmatrix} = 2n \begin{vmatrix} 1 & 0 & \ldots & 0 \\ 1 & n & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \ldots & n \end{vmatrix}$$

$$= 2n(1 \cdot n \cdot n \ldots n) = 2n \cdot n^{n-1} = 2n^n.$$

□

Remark 7.54. The previous two problems are special cases of Problem 7.40.

Problem 7.55. Prove that for all real numbers a, b, c

$$\begin{vmatrix} \cos^2 a & \sin^2 a & \cos 2a \\ \cos^2 b & \sin^2 b & \cos 2b \\ \cos^2 c & \sin^2 c & \cos 2c \end{vmatrix} = 0.$$

Solution. We have

$$\begin{vmatrix} \cos^2 a & \sin^2 a & \cos 2a \\ \cos^2 b & \sin^2 b & \cos 2b \\ \cos^2 c & \sin^2 c & \cos 2c \end{vmatrix} = \begin{vmatrix} \cos^2 a - \sin^2 a & \sin^2 a & \cos 2a \\ \cos^2 b - \sin^2 b & \sin^2 b & \cos 2b \\ \cos^2 c - \sin^2 c & \sin^2 c & \cos 2c \end{vmatrix}$$

$$= \begin{vmatrix} \cos 2a & \sin^2 a & \cos 2a \\ \cos 2b & \sin^2 b & \cos 2b \\ \cos 2c & \sin^2 c & \cos 2c \end{vmatrix} = 0.$$

The result follows. □

Problem 7.56. Let $A \in M_n(\mathbf{R})$.

a) Show that if $n^2 - n + 1$ entries in A are equal to 0, then $\det(A) = 0$.
b) Show that one can choose A such that $\det A \neq 0$ and A has $n^2 - n + 1$ equal entries.
c) Show that if $n^2 - n + 2$ entries in A are equal, then $\det(A) = 0$.

Solution. a) We claim that the matrix A has a column consisting entirely of zeros, which implies $\det A = 0$. Indeed, if each column of A has at most $n - 1$ zeros, then A has at most $n(n-1)$ zero entries in total. This contradicts the hypothesis.
b) Consider the matrix A whose elements off the main diagonal are equal to 1 and the diagonal entries are $1, 2, \ldots, n$. Then $n^2 - n + 1$ entries are equal to 1, but $\det A \neq 0$. Indeed, subtracting the first row from each subsequent row yields an upper-triangular matrix with nonzero diagonal entries, thus invertible.
c) If $n^2 - n + 2$ entries in A are equal (say to some number a), then there are at most $n - 2$ entries of A that are not equal to a. Thus at most $n - 2$ columns of A contain an entry which is not equal to a. Said differently, at least 2 columns of A have all entries a. But then A has two equal columns and $\det(A) = 0$. □

Problem 7.57 (The Vandermonde Determinant). Let $a_1, a_2, \ldots, a_n$ be complex numbers. Prove that the determinant of the matrix $A = [a_i^{j-1}]_{1 \leq i,j \leq n}$ (where if necessary we interpret 0^0 as being 1) equals

$$\det(A) = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

Solution. Starting from the right-hand side and working left subtract a_1 times each column from the column to its right. This gives

$$\det A = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & (a_2-a_1) & (a_2-a_1)a_2 & \cdots & (a_2-a_1)a_2^{n-3} & (a_2-a_1)a_2^{n-2} \\ 1 & (a_3-a_1) & (a_3-a_1)a_3 & \cdots & (a_3-a_1)a_3^{n-3} & (a_3-a_1)a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & (a_n-a_1) & (a_n-a_1)a_n & \cdots & (a_n-a_1)a_n^{n-3} & (a_n-a_1)a_n^{n-2} \end{vmatrix}$$

$$= \begin{vmatrix} (a_2-a_1) & (a_2-a_1)a_2 & \cdots & (a_2-a_1)a_2^{n-3} & (a_2-a_1)a_2^{n-2} \\ (a_3-a_1) & (a_3-a_1)a_3 & \cdots & (a_3-a_1)a_3^{n-3} & (a_3-a_1)a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (a_n-a_1) & (a_n-a_1)a_n & \cdots & (a_n-a_1)a_n^{n-3} & (a_n-a_1)a_n^{n-2} \end{vmatrix}.$$

Factoring out $a_k - a_1$ from row k gives

$$\det A = \prod_{j=2}^{n}(a_j - a_1) \cdot \begin{vmatrix} 1 & a_2 & \cdots & a_2^{n-3} & a_2^{n-2} \\ 1 & a_3 & \cdots & a_3^{n-3} & a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-3} & a_n^{n-2} \end{vmatrix}.$$

This last determinant is of the same form as the original matrix, but of a smaller size, hence we are done using an easy induction on n. □

Problem 7.58 (The Cauchy Determinant). Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be complex numbers such that $a_i + b_j \neq 0$ for $1 \leq i, j \leq n$. Prove that the determinant of the matrix $A = [\frac{1}{a_i+b_j}]$ equals

$$\det A = \frac{\prod_{1\leq i<j\leq n}(a_j - a_i)(b_j - b_i)}{\prod_{i,j=1}^{n}(a_i + b_j)}.$$

Solution. Subtracting the last column from each of the first $n-1$ columns and using the identity

$$\frac{1}{a_i + b_j} - \frac{1}{a_i + b_n} = \frac{b_n - b_j}{(a_i + b_j)(a_i + b_n)}$$

to factor a $b_n - b_j$ out of the j-th column and a $\frac{1}{a_i+b_n}$ out of the i-th row yields

$$\det A = \frac{(b_n - b_1)\cdots(b_n - b_{n-1})}{(a_1 + b_n)\cdots(a_n + b_n)} \begin{vmatrix} \frac{1}{a_1+b_1} & \frac{1}{a_1+b_2} & \cdots & \frac{1}{a_1+b_{n-1}} & 1 \\ \frac{1}{a_2+b_1} & \frac{1}{a_2+b_2} & \cdots & \frac{1}{a_2+b_{n-1}} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{1}{a_n+b_1} & \frac{1}{a_n+b_2} & \cdots & \frac{1}{a_n+b_{n-1}} & 1 \end{vmatrix}.$$

Similarly, subtracting the last row from each of the first $n-1$ rows in the matrix appearing in the last equality and pulling out common factors, we obtain

$$\det A = \frac{\prod_{i=1}^{n-1}(b_n - b_i)(a_n - a_i)}{\prod_{i=1}^{n}(a_i + b_n)\prod_{i=1}^{n-1}(a_n + b_i)} \begin{vmatrix} \frac{1}{a_1+b_1} & \frac{1}{a_1+b_2} & \cdots & \frac{1}{a_1+b_{n-1}} & 0 \\ \frac{1}{a_2+b_1} & \frac{1}{a_2+b_2} & \cdots & \frac{1}{a_2+b_{n-1}} & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ \frac{1}{a_{n-1}+b_1} & \frac{1}{a_{n-1}+b_2} & \cdots & \frac{1}{a_{n-1}+b_{n-1}} & 0 \\ 1 & 1 & \ldots & 1 & 1 \end{vmatrix}.$$

Hence

$$\det A = \frac{\prod_{i=1}^{n-1}(b_n - b_i)(a_n - a_i)}{\prod_{i=1}^{n}(a_i + b_n)\prod_{i=1}^{n-1}(a_n + b_i)} \cdot \begin{vmatrix} \frac{1}{a_1+b_1} & \frac{1}{a_1+b_2} & \cdots & \frac{1}{a_1+b_{n-1}} \\ \frac{1}{a_2+b_1} & \frac{1}{a_2+b_2} & \cdots & \frac{1}{a_2+b_{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{a_{n-1}+b_1} & \frac{1}{a_{n-1}+b_2} & \cdots & \frac{1}{a_{n-1}+b_{n-1}} \end{vmatrix},$$

which allows us to conclude by induction on n, the last determinant being of the same form, but of smaller dimension. □

Another useful tool for computing determinants is the **Laplace expansion**. Consider a matrix $A \in M_n(F)$ with entries a_{ij}. The **minor** of a_{ij} is the determinant M_{ij} of the matrix obtained from A by deleting row i and column j. The **cofactor** of a_{ij} is $C_{ij} = (-1)^{i+j} M_{ij}$.

Example 7.59. The minor of a_{23} in

$$\begin{vmatrix} -2 & -1 & 0 \\ 1 & 2 & 3 \\ 4 & 0 & -2 \end{vmatrix}$$

is

$$M_{23} = \begin{vmatrix} -2 & -1 \\ 4 & 0 \end{vmatrix} = 4$$

and the cofactor of a_{23} is $C_{23} = (-1)^{2+3} M_{23} = -4$.

The cofactors play a key role, thanks to the following theorem, which shows that the computation of a determinant of order n may be reduced to the computation of n determinants of order $n-1$. If we use properties 1)–11) of determinants and we create some zeros on the kth line, then we only need the cofactors corresponding to the nonzero elements of this line, i.e., combining these methods we can reduce the volume of computations.

Theorem 7.60 (Laplace Expansion). *Let $A = [a_{ij}] \in M_n(F)$ be a matrix and let $C_{i,j}$ be the cofactor of a_{ij}.*

a) (expansion with respect to column j) For each $j \in \{1, 2, \ldots, n\}$ we have

$$\det A = \sum_{i=1}^{n} a_{ij} C_{ij}.$$

b) (expansion with respect to row i) For each $i \in \{1, 2, \ldots, n\}$ we have

$$\det A = \sum_{j=1}^{n} a_{ij} C_{ij}.$$

Proof. We will prove only part a), the argument being similar for part b) (alternatively, this follows from a) using that the determinant of a matrix equals the determinant of its transpose). Fix $j \in \{1, 2, \ldots, n\}$, let $B = (e_1, \ldots, e_n)$ be the canonical basis of F^n and let $C_1, \ldots, C_n \in F^n$ be the columns of A, so that $C_k = \sum_{i=1}^{n} a_{ik} e_i$ for all k. We deduce that

$$\det A = \det_B(C_1, .., C_n) = \det_B(C_1, \ldots, C_{j-1}, \sum_{i=1}^{n} a_{ij} e_i, C_{j+1}, \ldots, C_n)$$

$$= \sum_{i=1}^{n} a_{ij} \det_B(C_1, \ldots, C_{j-1}, e_i, C_{j+1}, \ldots, C_n).$$

It remains to see that $X_{ij} := \det_B(C_1, \ldots, C_{j-1}, e_i, C_{j+1}, \ldots, C_n)$ equals C_{ij}, the cofactor of a_{ij}. By a series of $n - j$ column interchanges, we can put the jth column of the determinant X_{ij} in the last position, and by a sequence of $n - i$ row interchanges we can put the ith row in the last position. We end up with

$$X_{ij} = (-1)^{n-i+n-j} \begin{vmatrix} a_{11} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1n} & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \\ a_{n1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{nn} & 0 \\ a_{i1} & \ldots & a_{i,j-1} & a_{i,j+1} & \ldots & a_{i,n} & 1 \end{vmatrix}.$$

The last determinant is precisely C_{ij}, thanks to Theorem 7.43. The result follows, since $(-1)^{n-i+n-j} = (-1)^{i+j}$. □

Example 7.61. Expanding with respect to the first row, we obtain

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

Problem 7.62. Let

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 \\ 2 & 2 & -2 & -2 \\ 3 & -1 & -1 & -1 \end{bmatrix}.$$

Compute

(a) $\det(A)$ (b) $\det(A^t A)$. (c) $\det(A + A)$. (d) $\det(A^{-1})$.

Solution. (a) Subtracting the second row from the first and expanding with respect to the first row yields

$$\det A = \begin{vmatrix} 0 & 0 & 0 & 4 \\ 1 & 1 & 1 & -3 \\ 2 & 2 & -2 & -2 \\ 3 & -1 & -1 & -1 \end{vmatrix} = -4 \begin{vmatrix} 1 & 1 & 1 \\ 2 & 2 & -2 \\ 3 & -1 & -1 \end{vmatrix}.$$

In the new determinant, subtract twice the first row from the second one, and add the first row to the last one. We obtain

$$\det A = -4 \begin{vmatrix} 1 & 1 & 1 \\ 0 & 0 & -4 \\ 4 & 0 & 0 \end{vmatrix}.$$

Expanding with respect to the last row yields

$$\det A = -4 \cdot 4 \cdot (-4) = 64.$$

(b) Since the determinant map is multiplicative and $\det A = \det({}^t A)$, we obtain

$$\det(A^t A) = \det A \cdot \det({}^t A) = (\det A)^2 = 64^2 = 4096.$$

(c) We have

$$\det(A + A) = \det(2A) = 2^4 \cdot \det(A) = 16 \cdot 64 = 1024.$$

(d) Finally,

$$\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{64}.$$

□

Problem 7.63. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a matrix with nonnegative entries such that the sum of the entries in each row does not exceed 1. Prove that $|\det A| \leq 1$.

Solution. We will prove the result by induction on n, the case $n = 1$ being clear. Assume that the result holds for $n - 1$ and let A be a matrix as in the statement of the problem. For $1 \leq i \leq n$ let A_i be the matrix obtained by deleting the first row and column i from A. Then

$$\det A = \sum_{i=1}^{n} (-1)^{i+1} a_{1i} \det A_i,$$

and by the inductive hypothesis applied to each A_i we have $|\det A_i| \leq 1$. We deduce that

$$|\det A| \leq \sum_{i=1}^{n} a_{1i} |\det A_i| \leq \sum_{i=1}^{n} a_{1i} \leq 1$$

and the result follows. □

We have already seen that a matrix $A \in M_n(F)$ is invertible if and only if $\det A \neq 0$. It turns out that we can actually compute the inverse of the matrix A by computing certain determinants. Before doing that, let us introduce a fundamental definition:

Definition 7.64. Let $A \in M_n(F)$ be a square matrix with entries in F. The **adjugate** matrix $\mathrm{adj}(A)$ is the matrix whose (i, j)-entry is the cofactor C_{ji} of a_{ji}. Thus $\mathrm{adj}(A)$ is the **transpose** of the matrix whose (i, j)-entry is the cofactor C_{ij} of a_{ij}.

We have the fundamental result:

Theorem 7.65. *If $A \in M_n(F)$ has nonzero determinant, then*

$$A^{-1} = \frac{1}{\det A} \mathrm{adj}(A).$$

Proof. It suffices to prove that $A \cdot \mathrm{adj}(A) = \det A \cdot I_n$. Using the multiplication rule, this comes down to checking that

$$\sum_{j=1}^{n} C_{k,j} a_{i,j} = \det A \cdot \delta_{ik}$$

for all $1 \leq i, k \leq n$, where δ_{ik} equals 1 if $i = k$ and 0 otherwise.

If $k = i$, this follows by Laplace expansion of $\det A$ with respect to the ith row, so suppose that $k \neq i$ and consider the matrix A' obtained from A by replacing its kth row with a copy of the ith row, so that rows i and k in A' coincide, forcing $\det A' = 0$. Using the Laplace expansion in A' with respect to the kth row and taking into account that the cofactors involved in the expression do not change when going from A to A' (as only the kth row of A is modified), we obtain

$$0 = \det A' = \sum_{j=1}^{n} a_{ij} C_{k,j}$$

and the result follows. □

The previous theorem does not give a practical way of computing the inverse of a matrix (this involves computing too many determinants), but it is very important from a theoretical point of view: for instance, it says that the entries of A^{-1} are rational functions of the entries of A (in particular they are continuous functions of the entries of A if A has real or complex coefficients). The practical way of computing the inverse of a matrix has already been presented in the chapter concerning linear systems and operations on matrices, so we will not repeat the discussion here.

7.4.1 Problems for Practice

1. Let x be a real number. Compute in two different ways the determinant

$$\begin{vmatrix} x & 1 & 1 \\ 1 & x & 1 \\ 1 & 1 & x \end{vmatrix}.$$

2. Let a, b, c be real numbers. Compute the determinant

$$\begin{vmatrix} a-b-c & 2a & 2a \\ 2b & b-c-a & 2b \\ 2c & 2c & c-a-b \end{vmatrix}.$$

3. Let x be a real number. Compute the determinant

$$\begin{vmatrix} \cos x & 0 & \sin x \\ 0 & 1 & 0 \\ -\sin x & 0 & \cos x \end{vmatrix}.$$

4. Let a, b, c be real numbers. Compute the determinant

$$\begin{vmatrix} a+1 & b+1 & c+1 \\ b+c & a+c & a+b \\ 1 & 1 & 1 \end{vmatrix}.$$

5. Let a, b, c be real numbers. Find a necessary and sufficient condition for the vanishing of the following determinant

$$\begin{vmatrix} (a+b)^2 & a^2 & b^2 \\ a^2 & (a+c)^2 & c^2 \\ b^2 & c^2 & (b+c)^2 \end{vmatrix}.$$

6. Let x, y, z be real numbers. By considering the matrices $\begin{bmatrix} 0 & y & z \\ z & x & 0 \\ y & 0 & x \end{bmatrix}$ and $\begin{bmatrix} 0 & z & y \\ y & x & 0 \\ z & 0 & x \end{bmatrix}$, compute the determinant

$$\begin{vmatrix} y^2+z^2 & xy & zx \\ xy & z^2+x^2 & yz \\ xz & yz & x^2+y^2 \end{vmatrix}.$$

7. Let x, y, z be real numbers. Compute

$$\begin{vmatrix} 1 & \cos x & \sin x \\ 1 & \cos(x+y) & \sin(x+y) \\ 1 & \cos(x+z) & \sin(x+z) \end{vmatrix}.$$

8. Compute $\det(A)$, where A is the $n \times n$ matrix

$$A = \begin{bmatrix} -1 & 1 & 1 \ldots & 1 \\ 1 & -1 & 1 \ldots & 1 \\ \ldots & & & \\ 1 & 1 & 1 \ldots & -1 \end{bmatrix}.$$

9. Let a, b, c, d be real numbers and consider the matrices

$$A = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}.$$

   a) Compute $\det B$.
   b) By considering the matrix AB, compute $\det A$.

10. Let a be a real number. Prove that for $n \geq 3$ we have $D_n = aD_{n-1} - D_{n-2}$, where

$$D_n = \begin{vmatrix} a & 1 & 0 & 0 & \ldots\ldots\ldots & 0 \\ 1 & a & 1 & 0 & \ldots\ldots\ldots & 0 \\ 0 & 1 & a & 1 & \ldots\ldots\ldots & 0 \\ 0 & 0 & 1 & a & \ldots\ldots\ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots\ldots\ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots\ 1 \quad a & 1 \\ 0 & 0 & 0 & 0 & \ldots\ 0 \quad 1 & a \end{vmatrix}$$

is the determinant of an $n \times n$ matrix.

11. Let $a, b, c \in \mathbf{R}$ and $x = a^2 + b^2 + c^2$, $y = ab + bc + ca$. Prove that

$$\begin{vmatrix} 1 & x & x & x \\ 1 & x+y & x+y & 2x \\ 1 & 2x & x+y & x+y \\ 1 & x+y & 2x & x+y \end{vmatrix} = (a^3 + b^3 + c^3 - 3abc)^2.$$

12. Compute $\det A$ in each of the following cases:

    (a) $a_{i,j} = \min(i, j)$, for $i, j = 1, \ldots, n$.
    (b) $a_{i,j} = \max(i, j)$, for $i, j = 1, \ldots, n$.
    (c) $a_{i,j} = |i - j|$, for $i, j = 1, \ldots, n$.

13. Let $n \geq 2$ and let $A = [a_{ij}] \in M_n(\mathbf{R})$ be the matrix defined by

$$a_{ij} = \begin{cases} 0, \text{ if } i = j \\ 1, \text{ if } i \neq j. \end{cases}$$

    a) Compute $\det A$.
    b) Prove that

$$A^{-1} = \frac{2-n}{n-1} I_n + \frac{1}{n-1} A.$$

14. Let $n \geq 3$ and let A be the $n \times n$ matrix whose (i, j)-entry is $a_{ij} = \cos \frac{2\pi(i+j)}{n}$ for $i, j \in [1, n]$. Find $\det(I_n + A)$.
15. Let A be a matrix of order 3.

    (a) If all the entries in A are 1 or -1 show that $\det(A)$ must be even integer and determine the largest possible value of $\det(A)$.
    (b) If all the entries in A are 1 or 0, determine the largest possible value of $\det(A)$.

16. Let $n > 2$ and let $x_1, \ldots, x_n$ be real numbers. Compute the determinant of the matrix whose entries are $\sin(x_i + x_j)$ for $1 \leq i, j \leq n$.
17. Let $A \in M_n(\mathbf{R})$ be the matrix whose (i, j)-entry is $a_{ij} = \frac{1}{i+j}$. Prove that

$$\det A = \frac{(1!2!\ldots, n!)^4}{(n!)^2 1!2!\ldots(2n)!}.$$

    Hint: use the Cauchy determinant.
18. Let V be the space of polynomials with real coefficients whose degree does not exceed n. Compute the determinant of the linear transformation T sending $P \in V$ to $P + P'$.

19. Prove that any matrix $A \in M_n(\mathbf{R})$ with determinant 1 is a product of matrices of the form $I_n + \lambda E_{ij}$, with $i \neq j \in [1, n]$ and $\lambda \in \mathbf{R}$. Hint: use elementary operations on rows and columns.
20. Let A be an invertible matrix with integer coefficients. Prove that A^{-1} has integer entries if and only if $\det A \in \{-1, 1\}$.
21. Let $A, B \in M_n(\mathbf{R})$ be matrices with integer entries such that $A, A + B, \ldots, A + 2nB$ are invertible and their inverses have integer entries. Prove that $A + (2n+1)B$ has the same property. Hint: prove first the existence of a polynomial P with integer coefficients such that $P(x) = \det(A + xB)$ for all $x \in \mathbf{R}$.
22. Let $A, B \in M_n(\mathbf{C})$ be matrices which commute. We want to prove that the adjugate matrices $\operatorname{adj}(A)$ and $\operatorname{adj}(B)$ also commute.

    a) Prove the desired result when A and B are invertible.
    b) By considering the matrices $A + \frac{1}{k} I_n$ and $B + \frac{1}{k} I_n$ for $k \to \infty$, prove the desired result in all cases.

23. Let $A \in M_n(\mathbf{C})$, with $n \geq 2$. Prove that

$$\det(\operatorname{adj}(A)) = (\det A)^{n-1}.$$

    Hint: start by proving the result when A is invertible, then in order to prove the general case consider the matrices $A + \frac{1}{k} I_n$ for $k \to \infty$.
24. (Dodgson condensation) Consider a 3×3 matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

    View this matrix as being composed of four 2×2 matrices (overlapping at a_{22}). Form a 2×2 matrix by taking the determinants of these four 2×2 matrices $\begin{bmatrix} NW & NE \\ SW & SE \end{bmatrix}$. Show that

$$\begin{vmatrix} NW & NE \\ SW & SE \end{vmatrix} = a_{22} \det(A).$$

25. (Dodgson condensation, continued) Choose your favorite 4×4 matrix $A = [a_{ij}]$ with $a_{22}, a_{23}, a_{32}, a_{33}$, and $a_{22}a_{33} - a_{23}a_{32}$ all nonzero.

    a) Compute $\det(A)$.
    b) View A as being composed of a 3×3 array of overlapping 2×2 matrices and compute the determinants of these 9 matrices. Write them in a 3×3 matrix B. View this 3×3 matrix as being composed of four overlapping 2×2 matrices. For each compute the determinant and divide by the entry of A the four had in common. Write the results in a 2×2 matrix C. Take the determinant of C and divide it by the central entry of B (the one common to the four determinants that make up C). Compare your result to the result of part (a).

Remark. This method of computing a determinant, due to Charles Dodgson, a.k.a. Lewis Carroll, extends to higher dimensions. It is best visualized if you imagine filling a pyramidal array of numbers. We start with an $(n+1)\times(n+1)$ array of all ones and we lay the $n \times n$ matrix whose determinant we want in the layer above, with each entry of A sitting between four of the ones. At each stage, we fill the next layer by computing the determinant of the 2×2 matrix formed by the four touching cells in the layer below and dividing by the entry two layer down directly below the cell. (Thus at the first stage there is a division by 1 that we neglected to mention above.) When you are done, the entry at the top of the pyramid will be the determinant. (There is a slight complication here. Following this procedure naively might result in dividing by zero. This is fixable, but makes the algorithm less pretty.)

7.5 The Vandermonde Determinant

If $A \in M_n(F)$, by definition

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}$$

is a polynomial expression in the entries of the matrix A. This suggests using properties of polynomials (such as degree, finiteness of the number of roots...) for studying determinants. This is a very fruitful idea and we will sketch in this section how it works.

We start with an absolutely fundamental computation, that of **Vandermonde determinants**. These determinants play a crucial role in almost all aspects of mathematics. We have already given a proof of the next theorem in Problem 7.57. Here we give a different proof.

Theorem 7.66. *Let F be a field and let $x_1, \ldots, x_n \in F$. Then*

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Proof. We will prove the statement by induction on n, the cases $n = 1$ and $n = 2$ being left to the reader. Assume that the result holds for $n-1$ (and for any choice of $x_1, \ldots, x_{n-1}$) and let $x_1, \ldots, x_n \in F$. If two of these elements are equal, the result is clear: the determinant we want to compute has two equal columns, so must vanish. So assume that $x_1, \ldots, x_n$ are pairwise distinct and consider the polynomial

$$P(X) = \begin{vmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-1} \\ 1 & X & \dots & X^{n-1} \end{vmatrix}.$$

Expanding with respect to the last row, we see that

$$P(X) = X^{n-1} \begin{vmatrix} 1 & x_1 & \dots & x_1^{n-2} \\ 1 & x_2 & \dots & x_2^{n-2} \\ \dots & \dots & \dots & \dots \\ 1 & x_{n-1} & \dots & x_{n-1}^{n-2} \end{vmatrix} + a_{n-2}X^{n-2} + \dots$$

for some $a_{n-2}, \dots, a_0 \in F$. Thus by the inductive hypothesis the leading coefficient of P is $\prod_{1 \le i < j \le n-1}(x_j - x_i) \neq 0$.

Let $i \in [1, n-1]$. Taking $X = x_i$, we obtain a determinant with two equal rows, which must therefore vanish. It follows that $P(x_1) = \dots = P(x_{n-1}) = 0$. Since P has degree $n-1$, leading coefficient $\prod_{1 \le i < j \le n-1}(x_j - x_i)$ and vanishes at $n-1$ distinct points $x_1, \dots, x_{n-1}$, we deduce that

$$P(X) = \prod_{1 \le i < j \le n-1} (x_j - x_i) \cdot \prod_{i=1}^{n-1} (X - x_i).$$

Plugging in $X = x_n$ yields the desired result. □

Remark 7.67. We call the determinant $\begin{vmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & x_n & \dots & x_n^{n-1} \end{vmatrix}$ the Vandermonde determinant associated with $x_1, \dots, x_n$. It follows from the previous theorem that the Vandermonde determinant associated with $x_1, \dots, x_n$ is nonzero if and only if $x_1, \dots, x_n$ are pairwise distinct. Vandermonde determinants are ubiquitous in mathematics and are closely related to the following fundamental problem: "for distinct complex numbers $x_1, \dots, x_n$ and arbitrary complex numbers $b_1, \dots, b_n$, find a polynomial $P(X)$ of degree at most $n-1$ such that $P(x_i) = b_i$." Written out as a linear system for the coefficients a_i of P yields the equation $Va = b$, where b is the column vector whose coordinates are the b_i's and V is the Vandermonde matrix associated with $x_1, \dots, x_n$ (thus $\det V$ is the Vandermonde determinant associated with $x_1, \dots, x_n$). The fact that the Vandermonde determinant is nonzero is equivalent to this problem having a unique solution. The unique solution of this problem (known as Lagrange interpolation) is given by

$$P(X) = \sum_{i=1}^{n} b_i \prod_{j \neq i} \frac{X - x_j}{x_i - x_j}.$$

Problem 7.68. Let a, b, c be nonzero real numbers. Prove that

$$\begin{vmatrix} a^2 & b^2 & c^2 \\ c^2 & a^2 & b^2 \\ ac & ab & bc \end{vmatrix} = (a^2 - bc)(b^2 - ca)(c^2 - ab).$$

Solution. Dividing all entries of the first column by a^2, all entries of the second column by b^2, and all entries of the third column by c^2, we obtain

$$\begin{vmatrix} a^2 & b^2 & c^2 \\ c^2 & a^2 & b^2 \\ ac & ab & bc \end{vmatrix} = (abc)^2 \begin{vmatrix} 1 & 1 & 1 \\ \left(\frac{c}{a}\right)^2 & \left(\frac{a}{b}\right)^2 & \left(\frac{b}{c}\right)^2 \\ \frac{c}{a} & \frac{a}{b} & \frac{b}{c} \end{vmatrix}$$

$$= -(abc)^2 \begin{vmatrix} 1 & 1 & 1 \\ \frac{c}{a} & \frac{a}{b} & \frac{b}{c} \\ \left(\frac{c}{a}\right)^2 & \left(\frac{a}{b}\right)^2 & \left(\frac{b}{c}\right)^2 \end{vmatrix}.$$

We recognize a Vandermonde determinant associated with $\frac{c}{a}, \frac{a}{b}, \frac{b}{c}$, thus we can further write

$$\begin{vmatrix} a^2 & b^2 & c^2 \\ c^2 & a^2 & b^2 \\ ac & ab & bc \end{vmatrix} = -(abc)^2 \left(\frac{b}{c} - \frac{c}{a}\right) \cdot \left(\frac{b}{c} - \frac{a}{b}\right) \cdot \left(\frac{a}{b} - \frac{c}{a}\right).$$

We have

$$\frac{b}{c} - \frac{c}{a} = -\frac{c^2 - ab}{ac}$$

and similar identities obtained by permuting a, b, c. We conclude that

$$\begin{vmatrix} a^2 & b^2 & c^2 \\ c^2 & a^2 & b^2 \\ ac & ab & bc \end{vmatrix} = (a^2 - bc)(b^2 - ca)(c^2 - ab).$$

□

Problem 7.69. Let F be a field and let $x_1, \ldots, x_n \in F$. Compute

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-2} & x_1^n \\ 1 & x_2 & \ldots & x_2^{n-2} & x_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & \ldots & x_n^{n-2} & x_n^n \end{vmatrix}.$$

Solution. Write

$$P(X) = (X - x_1)\ldots(X - x_n) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

for some scalars $a_0, \ldots, a_n \in F$, with $a_{n-1} = -(x_1 + \ldots + x_n)$. Next, add to the last column the first column multiplied by a_0, the second column multiplied by a_1,..., the $n-1$th column multiplied by a_{n-2}. The value of the determinant does not change, and since

$$x_i^n + a_{n-2}x_i^{n-2} + \ldots + a_0 = -a_{n-1}x_i^{n-1},$$

we deduce that

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-2} & x_1^n \\ 1 & x_2 & \ldots & x_2^{n-2} & x_1^n \\ \ldots & \ldots & \ldots & & \\ 1 & x_n & \ldots & x_n^{n-2} & x_n^n \end{vmatrix} = -a_{n-1} \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-2} & x_1^{n-1} \\ \ldots & \ldots & \ldots & & \\ 1 & x_n & \ldots & x_n^{n-2} & x_n^{n-1} \end{vmatrix}$$

$$= (\sum_{i=1}^{n} x_i) \prod_{1 \le i < j \le n} (x_j - x_i),$$

the last equality being a consequence of Theorem 7.66. □

Remark 7.70. An alternate solution is to remark that the desired determinant is the coefficient of X^{n-1} in the Vandermonde determinant

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^n \\ 1 & X & \cdots & X^n \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i) \cdot \prod_{k=1}^{n} (X - x_k).$$

Problem 7.71. Let $P_0, \ldots, P_{n-1}$ be monic polynomials with complex coefficients such that $\deg P_i = i$ for $0 \le i \le n-1$ (thus $P_0 = 1$). If $x_1, \ldots, x_n \in \mathbf{C}$, compute

$$\begin{vmatrix} P_0(x_1) & P_1(x_1) & \ldots & P_{n-1}(x_1) \\ P_0(x_2) & P_1(x_2) & \ldots & P_{n-1}(x_2) \\ \ldots & \ldots & \ldots & \ldots \\ P_0(x_n) & P_1(x_n) & \ldots & P_{n-1}(x_n) \end{vmatrix}.$$

Solution. Let A be the matrix whose determinant we want to compute and let us write

$$P_i(X) = X^i + c_{i,i-1}X^{i-1} + \ldots + c_{i,0}$$

for some complex numbers c_{ij}. The matrix A is then equal to

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & c_{1,0} & c_{2,0} & \dots & c_{n,0} \\ 0 & 1 & c_{2,1} & \dots & c_{n,1} \\ \vdots & \vdots & \vdots & \ddots & \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Since the second matrix is upper-triangular with diagonal entries equal to 1, its determinant equals 1. Using Theorem 7.66, we deduce that

$$\begin{vmatrix} P_0(x_1) & P_1(x_1) & \dots & P_{n-1}(x_1) \\ P_0(x_2) & P_1(x_2) & \dots & P_{n-1}(x_2) \\ \dots & \dots & \dots & \dots \\ P_0(x_n) & P_1(x_n) & \dots & P_{n-1}(x_n) \end{vmatrix} = \prod_{1 \le i < j \le n} (x_j - x_i).$$

□

Problem 7.72. For $0 < k < n$ compute $\det A$, where

$$A = \begin{bmatrix} 1^k & 2^k & 3^k & \dots & (n+1)^k \\ 2^k & 3^k & 4^k & \dots & (n+2)^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n+1)^k & (n+2)^k & (n+3)^k & \dots & (2n+1)^k \end{bmatrix}.$$

Solution. Consider the matrix

$$A_x = \begin{bmatrix} 1^k & 2^k & 3^k & \dots & n^k & (x+1)^k \\ 2^k & 3^k & 4^k & \dots & (n+1)^k & (x+2)^k \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n+1)^k & (n+2)^k & (n+3)^k & \dots & (2n)^k & (x+n+1)^k \end{bmatrix}$$

obtained from A by modifying its last column. Then $p(x) = \det(A_x)$ is a polynomial in the variable x, whose degree is at most $k < n$. Indeed, expanding the determinant of A_x with respect to the last column shows that $p(x)$ is a linear combination of $(x+1)^k, \dots, (x+n+1)^k$, each of which has degree k.

Next, observe that p vanishes at $0, 1, \dots, n-1$, since when $x \in \{0, 1, \dots, n-1\}$ the matrix A_x has two equal columns, thus $\det(A_x) = 0$. Since $\deg p < n$ and p has at least n distinct roots, it follows that p is the zero polynomial. In particular $p(n) = 0$, hence the determinant to be evaluated is 0. □

7.5.1 Problems for Practice

1. Given real numbers a, b, c, compute the determinant

$$\begin{vmatrix} b+c & a+c & a+b \\ b^2+c^2 & a^2+c^2 & a^2+b^2 \\ b^3+c^3 & a^3+c^3 & a^3+b^3 \end{vmatrix}.$$

2. Let a, b, c be real numbers. Compute

$$\begin{vmatrix} a+b & ab & a^2+b^2 \\ b+c & bc & b^2+c^2 \\ c+a & ca & c^2+a^2 \end{vmatrix}.$$

3. Let $z_1, \ldots, z_n$ be pairwise distinct complex numbers. Let $f_i : \mathbf{R} \to \mathbf{C}$ be the map $x \mapsto e^{z_i x}$. Prove that $f_1, \ldots, f_n$ are linearly independent over $\mathbf{C}$. Hint: if $\alpha_1 f_1 + \ldots + \alpha_n f_n = 0$, take successive derivatives of this relation and evaluate at $x = 0$.
4. a) Prove that for any positive integer n there is a polynomial T_n of degree n such that

$$T_n(\cos x) = \cos nx$$

for all real numbers x. This polynomial T_n is called the n**th Chebyshev polynomial**. For instance, $T_1(X) = X$, $T_2(X) = 2X^2 - 1$.

b) Let $x_1, \ldots, x_n$ be real numbers. Using part a), compute the determinant

$$\begin{vmatrix} 1 & \cos(x_1) & \cos(2x_1) & \ldots & \cos((n-1)x_1) \\ 1 & \cos(x_2) & \cos(2x_2) & \ldots & \cos((n-1)x_2) \\ \ldots & \ldots & \ldots & \ldots & \\ 1 & \cos(x_n) & \cos(2x_n) & \ldots & \cos((n-1)x_n) \end{vmatrix}.$$

5. Let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be complex numbers and let $k \in [0, n-1]$. Compute the determinant of the $n \times n$ matrix whose (i, j)-entry is $(x_i + y_j)^k$. Hint: use the binomial formula and write the matrix of the product of two simpler matrices, of Vandermonde type.
6. Let $a_0, a_1, \ldots, a_{n-1}$ be complex numbers and consider the matrix

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ \ldots & & & & \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{bmatrix}$$

obtained by cyclic permutations of the first row.

a) Let $z = e^{\frac{2i\pi}{n}}$ and consider the matrix $B = [z^{(i-1)(j-1)}]_{1\leq i,j\leq n}$. Compute the matrix AB.
b) Deduce that

$$\det A = \prod_{k=1}^{n} \left(\sum_{j=0}^{n-1} a_j z^{j(k-1)} \right).$$

7. Consider the "curve" $C = \{(1, t, t^2, \ldots, t^{n-1}) | t \in \mathbf{C}\}$ in $\mathbf{C}^n$, where n is a positive integer. Prove that any n pairwise distinct points of C form a basis of $\mathbf{C}^n$.
8. Using Vandermonde's determinant, prove that we cannot find finitely many maps $f_i, g_j : \mathbf{R} \to \mathbf{R}$ such that

$$e^{xy} = \sum_{i=1}^{n} f_i(x) g_i(y)$$

for all $x, y \in \mathbf{R}$.
9. Let $z_1, z_2, \ldots, n$ be complex numbers such that

$$z_1 + z_2 + \ldots + z_n = z_1^2 + z_2^2 + \ldots + z_n^2 = \ldots = z_1^n + z_2^n + \ldots + z_n^n = 0.$$

Prove that $z_1 = z_2 = \ldots = z_n = 0$.
10. Prove that there exists an infinite set of points

$$\ldots, \ P_{-3}, \ P_{-2}, \ P_{-1}, \ P_0, \ P_1, \ P_2, \ P_3, \ \ldots$$

in the plane with the following property: for any three distinct integers a, b, and c, points P_a, P_b, and P_c are collinear if and only if $a + b + c = 2014$. Hint: let P_n be the point with coordinates (x, x^3), where $x = n - \frac{2014}{3}$.

7.6 Linear Systems and Determinants

In this section we will use determinants to make a more refined study of linear systems. Before doing that, we will show that the computation of the rank of a matrix $A \in M_{m,n}(F)$ can be reduced to the computation of a certain number of determinants. This will be very important for applications to linear systems, but is not very useful in practice, since it is more practical to compute the rank of a matrix by computing its reduced echelon form (by definition of this form, the rank of A is simply the number of pivots).

Let $A \in M_{m,n}(F)$ be a matrix. Recall that a **sub-matrix** of A is a matrix obtained by deleting a certain number of rows and columns of A.

Theorem 7.73. *Let $A \in M_{m,n}(F)$ be a matrix of rank r. Then*

a) There is an invertible $r \times r$ sub-matrix in A.
b) For $k > r$, any $k \times k$ sub-matrix of A is not invertible.

In other words, the rank of A is the largest size of an invertible sub-matrix of A.

Proof. Let $A = [a_{ij}]$ and let $C_1, \ldots, C_n$ be the columns of A, so that

$$r = \dim \mathrm{Span}(C_1, \ldots, C_n).$$

Let d be the largest size of an invertible sub-matrix of A. We will prove separately the inequalities $d \geq r$ and $r \geq d$.

We start by proving the inequality $r \geq d$. Let B be an invertible $d \times d$ sub-matrix of A. Permuting the rows and columns of A (which does not change its rank), we may assume that B consists in the first d rows and columns of A. Then $C_1, \ldots, C_d$ are linearly independent (as any nontrivial linear relation between $C_1, \ldots, C_d$ would induce a nontrivial relation between the columns of B, contradicting the fact that B is invertible). But then

$$r = \dim \mathrm{Span}(C_1, \ldots, C_n) \geq \dim \mathrm{Span}(C_1, \ldots, C_d) = d.$$

Let us prove now that $r \leq d$. By definition of r, we know that we can find r columns of A which form a basis of the space generated by the columns of A. Let B be the $m \times r$ matrix obtained by deleting all other columns of A except for these r. Then B has rank r. But then ${}^tB$ also has rank r (because a matrix and its transpose have the same rank), thus the space generated by the rows of B has dimension r. In particular, we can find r rows of B which are linearly independent. The sub-matrix obtained from B by deleting all other rows except for these r is an invertible $r \times r$ sub-matrix of A, thud $d \geq r$. □

Problem 7.74. Let $v_1, \ldots, v_p \in F^n$ be vectors and let $A \in M_{n,p}(F)$ be the matrix whose columns are $v_1, \ldots, v_p$. Prove that $v_1, \ldots, v_p$ are linearly independent if and only if A has a $p \times p$ invertible sub-matrix.

Solution. $v_1, \ldots, v_p$ are linearly independent if and only if they form a basis of $\mathrm{Span}(v_1, \ldots, v_p)$ or equivalently if $\dim \mathrm{Span}(v_1, \ldots, v_p) = p$. Finally, this is further equivalent to $\mathrm{rank}(A) = p$. The result follows then directly from the previous theorem. □

Problem 7.75. Consider the vectors

$$v_1 = (1, x, 0, 1), \quad v_2 = (0, 1, 2, 1), \quad v_3 = (1, 1, 1, 1) \in \mathbf{R}^4.$$

Prove that for any choice of $x \in \mathbf{R}^4$ the vectors v_1, v_2, v_3 are linearly independent.

Solution. The matrix whose columns are v_1, v_2, v_3 is

$$A = \begin{bmatrix} 1 & 0 & 1 \\ x & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

By Problem 7.74 v_1, v_2, v_3 are linearly independent if and only if A has a 3×3 invertible sub-matrix. Such a matrix is obtained by deleting one row of A. Deleting the second row yields a sub-matrix whose determinant is

$$\begin{vmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{vmatrix} = -1,$$

thus the corresponding sub-matrix is invertible and the result follows. □

Thanks to the previous results, we can make a detailed study of linear systems. Consider the linear system

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \qquad\qquad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

with $A = [a_{ij}] \in M_{m,n}(F)$, $b = \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_m \end{bmatrix} \in F^m$ a given vector and unknowns $x_1, \ldots, x_n$. Let $X = \begin{bmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{bmatrix}$ and let $C_1, \ldots, C_n$ be the columns of A. Then the system can be written as

$$AX = b \quad \text{or} \quad x_1C_1 + \ldots + x_nC_n = b.$$

The first fundamental theorem of linear systems is the following:

Theorem 7.76 (Rouché–Capelli). *Consider the linear system above and let $[A, b] \in M_{m,n+1}(F)$ be the matrix obtained by adding a rightmost column to A, equal to b. Then*

a) The system is consistent[4] *if and only if* $\operatorname{rank}(A) = \operatorname{rank}[A, b]$.

b) Assume that the system is consistent and let X_0 *be a solution of it. Let* $\mathcal{S}_h$ *be the set of solutions of the associated homogeneous system.*[5] *Then the set of solutions of the original system is* $\{X_0 + X | X \in \mathcal{S}_h\}$ *and* $\mathcal{S}_h$ *is a vector space of dimension* $n - \operatorname{rank}(A)$ *over* F.

Proof. a) The system being equivalent to $b = x_1C_1 + \ldots + x_nC_n$, it is consistent if and only if b is a linear combination of $C_1, \ldots, C_n$, which is equivalent to $b \in \operatorname{Span}(C_1, \ldots, C_n)$. This is further equivalent to $\operatorname{Span}(C_1, \ldots, C_n) = \operatorname{Span}(C_1, \ldots, C_n, b)$ and finally

$$\dim \operatorname{Span}(C_1, \ldots, C_n) = \dim \operatorname{Span}(C_1, \ldots, C_n, b).$$

By definition, the left-hand side equals $\operatorname{rank}(A)$ and the right-hand side equals $\operatorname{rank}[A, b]$. The result follows.

b) By Proposition 3.2 we know that the set of solutions of the system is $\{X_0 + X | X \in \mathcal{S}_h\}$. It remains to prove that $\mathcal{S}_h$ is of dimension $n - \operatorname{rank}(A)$. But the corresponding homogeneous system can be written $AX = 0$, thus its set of solutions is the kernel of the map T sending $X \in F^n$ to $AX \in F^m$. By the rank-nullity theorem we deduce that

$$\dim \mathcal{S}_h = n - \dim \operatorname{Im}(T) = n - \operatorname{rank}(A)$$

and the theorem is proved. □

Let us take for simplicity $F = \mathbf{R}$ or $F = \mathbf{C}$ (the same argument will apply to any infinite field). It follows from the previous theorem that we have the following possibilities:

- the system has no solution. This happens precisely when A and $[A, b]$ do not have the same rank.
- the system has exactly one solution, which happens if and only if A has rank exactly n, or equivalently its columns are linearly independent.
- the system has more than 1 solution, and then it has infinitely many solutions. More precisely, the solutions depend on $n - \operatorname{rank}(A)$ parameters.

Here is an important consequence of the previous results:

Theorem 7.77. *Let* $A \in M_{m,n}(F)$ *and let* F_1 *be a field containing* F. *Consider the linear system* $AX = 0$. *If it has a nontrivial solution in* F_1^n, *then it has a nontrivial solution in* F^n.

Proof. Since the system has nontrivial solutions in F_1^n, A has rank $r < n$ seen as element of $M_{m,n}(F_1)$. But Theorem 7.73 shows that the rank of A seen as element of $M_{m,n}(F_1)$ or $M_{m,n}(F)$ is the same, thus using again the previous discussion we deduce that the system has nontrivial solutions in F^n. □

[4] Recall that this simply means that the system has at least one solution.

[5] This is the system $AX = 0$, i.e., it has the same unknowns, but b is equal to 0.

To make a deeper study of the linear system $AX = b$, assume that it is consistent and that A has rank r (therefore $[A, b]$ also has rank r). By Theorem 7.73 the matrix A has an invertible $r \times r$ sub-matrix. By permuting the equations and the unknowns of the system, we may assume that the sub-matrix consisting in the first r rows and columns of A is invertible. Then $x_1, \ldots, x_r$ are called the **principal unknowns** and the first r equations of the system are called the **principal equations**. All other equations can be deduced from the first r, so separating the principal and non-principal unknowns yields the equivalent system

$$\begin{cases} a_{11}x_1 + a_{12}x_2 & + \ldots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \ldots - a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 & + \ldots + a_{2r}x_r = b_2 - a_{2,r+1}x_{r+1} - \ldots - a_{2n}x_n \\ & \ldots \\ a_{r1}x_1 + a_{r2}x_2 & + \ldots + a_{rr}x_r = b_r - a_{r,r+1}x_{r+1} - \ldots - a_{rn}x_n \end{cases}$$

This a **Cramer system**, that is the number of unknowns (which are $x_1, \ldots, x_r$) equals the number of equations and the matrix of the system (which is $[a_{ij}]_{1 \leq i,j \leq r}$) is invertible. This kind of system has a unique solution, which can be expressed in terms of some determinants, as the following theorem shows:

Theorem 7.78. *Let $A = [a_{ij}]_{1 \leq i,j \leq n}$ be an invertible matrix in $M_n(F)$, let $b = \begin{bmatrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{bmatrix} \in F^n$ be a given vector and consider the system $AX = b$ with the unknowns $x_1, \ldots, x_n$. Then the system has a unique solution*

$$X = A^{-1}b$$

and we have for all $i \in [1, n]$

$$x_i = \frac{\Delta_i}{\Delta},$$

where $\Delta = \det A$ and Δ_i is the determinant of the matrix obtained from A by replacing the ith column with the vector b.

Proof. It is clear that the system $AX = b$ is equivalent to $X = A^{-1}b$ and so it has a unique solution. To prove the second part, let $e_1, \ldots, e_n$ be the canonical basis of F^n and write det instead of $\det_{(e_1,\ldots,e_n)}$. If $C_1, \ldots, C_n$ are the columns of A, then by definition

$$\Delta_i = \det(C_1, \ldots, C_{i-1}, b, C_{i+1}, \ldots, C_n).$$

Since $AX = b$, we have $x_1C_1 + \ldots + x_nC_n = b$. Since det is multilinear and alternating, we obtain

$$\Delta_i = \det(C_1, \ldots, C_{i-1}, \sum_{j=1}^{n} x_j C_j, C_{i+1}, \ldots, C_n) =$$

$$\sum_{j=1}^{n} x_j \det(C_1, \ldots, C_{i-1}, C_j, C_{i+1}, \ldots, C_n) = x_i \det(C_1, \ldots, C_{i-1}, C_i, C_{i+1}, \ldots, C_n)$$

$$= x_i \det A = x_i \Delta.$$

The result follows. □

Finally, we want to give another criterion for consistency. Recall that $A \in M_{m,n}(F)$ is the matrix of the system, that we assume $\operatorname{rank}(A) = r$ and (by permuting the unknowns and the equations) that the $r \times r$ sub-matrix of A consisting in the first r rows and columns of A is invertible.

Theorem 7.79. *Under the previous hypotheses, the system $AX = b \in F^m$ is consistent if and only if for all $k \in [r+1, m]$ we have*

$$\Delta_k = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2r} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \\ a_{r1} & a_{r2} & \ldots & a_{rr} & b_r \\ a_{k1} & a_{k2} & \ldots & a_{kr} & b_k \end{vmatrix} = 0.$$

Proof. If the system is consistent, then b is a linear combination of $C_1, \ldots, C_n$, so the last column of the matrix defining Δ_k is a linear combination of the other columns, thus $\Delta_k = 0$ and for all $k \in [r+1, m]$.

Conversely, assume that all determinants Δ_k are 0. Note that it makes sense to define Δ_k for $k \leq r$ by the same formula, and it is clear that we still have $\Delta_k = 0$ for $k \leq r$ (as the corresponding matrix has two equal rows). Expanding Δ_k with respect to its last row and denoting $\Delta_{r+1,1}, \ldots, \Delta_{r+1,r}$ the corresponding cofactors (which are independent of k) we obtain

$$\Delta_{r+1,1} a_{k1} + \cdots + \Delta_{r+1,r} a_{kr} + \det(a_{ij})_{1 \leq i,j \leq r} b_k = 0,$$

for all k and so

$$\Delta_{r+1,1} C_1 + \ldots + \Delta_{r+1,r} C_r + \det(a_{ij})_{1 \leq i,j \leq r} b = 0.$$

Since $\det(a_{ij})_{1 \leq i,j \leq r} \neq 0$ by assumption, this shows that $b \in \operatorname{Span}(C_1, \ldots, C_r)$ and so b is a linear combination of the columns of A, which means that the system is consistent. □

Let us see a few examples of explicit resolutions of linear systems using the above ideas. Actually for the first one the method of reduced echelon form is much more practical than the following. We strongly suggest the reader to compare the two methods.

Problem 7.80. a) Solve in real numbers the system

$$\begin{cases} x_1 + 3x_2 - 5x_3 = 4 \\ x_1 + 4x_2 - 8x_3 = 5 \\ -3x_1 - 7x_2 + 9x_3 = 6 \end{cases}$$

b) Solve the system

$$\begin{cases} x_1 + 3x_2 - 5x_3 = 4 \\ x_1 + 4x_2 - 8x_3 = 7 \\ -3x_1 - 7x_2 + 9x_3 = -6 \end{cases}$$

Solution. a) The matrix of the system is

$$A = \begin{bmatrix} 1 & 3 & -5 \\ 1 & 4 & -8 \\ -3 & -7 & 9 \end{bmatrix}$$

and one easily computes $\det A = 0$. Thus the system is not a Cramer system. Looking at the sub-matrix of A consisting in the first two rows and columns, we see that it is invertible. It follows that A has rank 2. The system is consistent if and only if

$$\operatorname{rank} \begin{bmatrix} 1 & 3 & -5 & 4 \\ 1 & 4 & -8 & 5 \\ -3 & -7 & 9 & 6 \end{bmatrix} = 2.$$

This means that all matrices obtained from this matrix by deleting one column have determinant 0. But one easily checks that the matrix obtained by deleting the second column is invertible, thus the system is not consistent and thus it has no solution.

b) The matrix of the system is the same. The system is consistent if and only if all matrices obtained by deleting one column from $\begin{bmatrix} 1 & 3 & -5 & 4 \\ 1 & 4 & -8 & 7 \\ -3 & -7 & 9 & -6 \end{bmatrix}$ have determinant 0. One easily checks that this is the case, thus the system will have infinitely many solutions. The principal unknowns are x_1, x_2 and the system is equivalent to

$$x_1 + 3x_2 = 5x_3 + 4, \quad x_1 + 4x_2 = 8x_3 + 7$$

and can be solved using Cramer's formulae or directly. One finds

$$x_2 = 3x_3 + 3, \quad x_1 = -4x_3 - 5.$$

We conclude that the solutions of the system are given by $(-4t - 5, 3t + 3, t)$ with $t \in \mathbf{R}$. □

Problem 7.81. Let a, b, c be given real numbers. Solve the linear system

$$\begin{cases} (b+c)x + by + cz = 1 \\ ax + (c+a)y + cz = 1 \\ ax + by + (a+b)z = 1 \end{cases}$$

□

Solution. The matrix of the system is

$$A = \begin{bmatrix} b+c & b & c \\ a & a+c & c \\ a & b & a+b \end{bmatrix}$$

and a brutal computation left to the reader shows that

$$\det A = 4abc.$$

We consider therefore two cases.

If $abc \neq 0$ the system is a Cramer system with a unique solution given by Cramer's formulae

$$x = \frac{\begin{vmatrix} 1 & b & c \\ 1 & a+c & c \\ 1 & b & a+b \end{vmatrix}}{4abc}, \quad y = \frac{\begin{vmatrix} b+c & 1 & c \\ a & 1 & c \\ a & 1 & a+b \end{vmatrix}}{4abc}, \quad z = \frac{\begin{vmatrix} b+c & b & 1 \\ a & a+c & 1 \\ a & b & 1 \end{vmatrix}}{4abc}.$$

In order to compute x explicitly, we subtract b times the first column from the second one, and c times the first column from the third one, ending up with

$$x = \frac{\begin{vmatrix} 1 & 0 & 0 \\ 1 & a+c-b & 0 \\ 1 & 0 & a+b-c \end{vmatrix}}{4abc} = \frac{(a+c-b)(a+b-c)}{4abc}$$

and we similarly obtain

$$y = \frac{(b+c-a)(b+a-c)}{4abc}, \quad z = \frac{(a+c-b)(b+c-a)}{4abc}.$$

In the second case we have $abc = 0$, that is A is not invertible. The system is consistent if and only if

$$\operatorname{rank}(A) = \operatorname{rank} \begin{bmatrix} b+c & b & c & 1 \\ a & a+c & c & 1 \\ a & b & a+b & 1 \end{bmatrix}.$$

While one can follow the discussion given in this chapter, it is much easier to deal with this case as follows: say without loss of generality that $a = 0$. The system becomes

$$\begin{cases} (b+c)x + by + cz = 1 \\ c(y+z) = 1 \\ b(y+z) = 1 \end{cases}$$

It is clear from the second and third equations that if the system is consistent, then necessarily $b = c$ and b is nonzero. So if $b \neq c$ or $bc = 0$, then the system has no solution in this case. Assume therefore that $b = c$ is nonzero. The system is equivalent to

$$\begin{cases} b(2x + y + z) = 1 \\ b(y+z) = 1 \end{cases}$$

making it clear that $x = 0$ and $y + z = \frac{1}{b}$. In this case the solutions of the system are given by $(0, y, \frac{1}{b} - y)$ with $y \in \mathbf{R}$. □

Problem 7.82. Let n be an integer greater than 1. Solve the linear system

$$\begin{cases} x_1 + & x_2 & + \ldots + & x_n = 1 \\ x_1 + & 2x_2 & + \ldots + & nx_n = 0 \\ & & \cdots & \\ x_1 + & 2^{n-1}x_2 & + \ldots + & n^{n-1}x_n = 0 \end{cases}$$

Solution. The matrix of the system is

$$A = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 2 & 3 & \ldots & n-1 & n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 2^{n-1} & 3^{n-1} & \ldots & (n-1)^{n-1} & n^{n-1} \end{bmatrix}$$

and it is invertible as its determinant is a Vandermonde determinant.

Therefore the system is a Cramer system and we have

$$x_i = \frac{\begin{vmatrix} 1 & 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & i-1 & 0 & i+1 & \ldots & n \\ \ldots & \ldots & \ldots & \ldots & & & & \\ 1 & 2^{n-1} & \ldots & (i-1)^{n-1} & 0 & (i+1)^{n-1} & \ldots & n^{n-1} \end{vmatrix}}{\det A}.$$

The numerator of the previous fraction is the Vandermonde determinant attached to $1, 2, \ldots, i-1, 0, i+1, \ldots, n$, while the denominator is the Vandermonde determinant attached to $1, 2, \ldots, i-1, i, i+1, \ldots, n$. Recalling that the Vandermonde determinant attached to $x_1, \ldots, x_n$ equals $\prod_{1 \le i < j \le n}(x_j - x_i)$ and canceling similar factors in the numerator and denominator, we end up with

$$x_i = \frac{\prod_{j=1}^{i-1}(0-j)\prod_{k=i+1}^{n} k}{\prod_{j=1}^{i-1}(i-j)\prod_{k=i+1}^{n}(k-i)} = (-1)^{i-1}\frac{(i-1)!n!}{(i-1)!i!(n-i)!}$$

$$= (-1)^{i-1}\frac{n!}{i!(n-i)!} = (-1)^{i-1}\binom{n}{i}$$

and so for $i \in [1, n]$

$$x_i = (-1)^{i-1}\binom{n}{i}.$$

□

Remark 7.83. An alternate solution goes as follows: write $P(T) = \sum_{k=1}^{n} x_k T^k$. Then the first equation reads $P(1) = 1$ and the rest read $P^{(k)}(1) = 0$ for $k = 1, \ldots, n-1$. Since we also have $P(0) = 0$ by construction, we see that the unique solution is $P(T) = 1 - (1-T)^n$ from which we read off the coefficients $x_k = (-1)^{k-1}\binom{n}{k}$.

Problem 7.84. Let $a_1, \ldots, a_n, b_1, \ldots, b_n$ be pairwise distinct complex numbers such that $a_i + b_j \neq 0$ for all $i, j \in [1, n]$. Find all complex numbers $x_1, \ldots, x_n$ such that for all $i \in [1, n]$ we have

$$\sum_{j=1}^{n} \frac{x_j}{a_i + b_j} = 1.$$

Solution. The determinant of the associated matrix is a Cauchy determinant and equals (by Problem 7.58)

$$\det A = \frac{\prod_{1 \le i < j \le n}(a_j - a_i)(b_j - b_i)}{\prod_{i,j \in [1,n]}(a_i + b_j)} \neq 0.$$

Thus the system has at most one solution. One could in principle argue as in the previous problem to find this solution, but there is a much more elegant (and very useful) technique that we prefer to present. Consider the rational function

$$F(X) = \sum_{j=1}^{n} \frac{x_j}{X + b_j}.$$

The system is equivalent to $F(a_1) = \ldots = F(a_n) = 1$. Write

$$F(X) = \frac{P(X)}{Q(X)}, \quad Q(X) = (X + b_1)\ldots(X + b_n)$$

for some polynomial P, and notice that $\deg P \leq n - 1$. The system becomes $P(a_j) = Q(a_j)$ for $1 \leq j \leq n$. Since $Q - P$ is a monic polynomial of degree n vanishing at $a_1, \ldots, a_n$ and since $a_1, \ldots, a_n$ are pairwise distinct, we deduce that the system is equivalent to

$$Q(X) - P(X) = \prod_{k=1}^{n} (X - a_k).$$

The conclusion is that $x_1, \ldots, x_n$ is a solution of the system if and only if

$$\sum_{j=1}^{n} \frac{x_j}{X + b_j} = \frac{\prod_{k=1}^{n}(X + b_k) - \prod_{k=1}^{n}(X - a_k)}{\prod_{k=1}^{n}(X + b_k)}.$$

In order to find each x_j, we multiply the previous relation by $X + b_j$ and then make X tend to $-b_j$. We deduce that

$$x_j = \lim_{x \to -b_j} \frac{\prod_{k=1}^{n}(X + b_k) - \prod_{k=1}^{n}(X - a_k)}{\prod_{k \neq j}(X + b_k)} = (-1)^{n-1} \frac{\prod_{k=1}^{n}(a_k + b_j)}{\prod_{k \neq j}(b_k - b_j)}.$$

It follows that the system has a unique solution, given by

$$x_j = (-1)^{n-1} \frac{\prod_{k=1}^{n}(a_k + b_j)}{\prod_{k \neq j}(b_k - b_j)}.$$

□

7.6.1 Problems for Practice

1. Let $A \in M_n(\mathbf{C})$ and let $B = \mathrm{adj}(A)$ be the adjugate matrix.
   a) Prove that if A is invertible, then so is B.
   b) Prove that if A has rank $n - 1$, then B has rank 1.
   c) Prove that if A has rank at most $n - 2$, then $B = O_n$.
2. Using the previous result, find all matrices $A \in M_n(\mathbf{C})$ which are equal to their adjugate matrix. Hint: the case $n = 2$ is special.

3. Let a, b be complex numbers and consider the matrix $A \in M_n(\mathbf{C})$ whose diagonal entries are all equal to a, and such that all other entries of A are equal to b.

   a) Compute $\det A$.
   b) Find the rank of A (you will need to distinguish several cases, according to the values of a and b).

4. Find real numbers a, b, c such that for all polynomials P with real coefficients and whose degree does not exceed 2 we have

$$\int_0^1 P(x)dx = aP(0) + bP(\frac{1}{2}) + cP(1).$$

5. Given real numbers a, b, c, u, v, w, solve the linear system

$$\begin{cases} ax - by = u \\ by - cz = v \\ cz - ax = w \end{cases}$$

6. Given a real number a, solve the linear system

$$\begin{cases} \frac{x}{1+a} + \frac{y}{1+2a} + \frac{z}{1+3a} = 1 \\ \frac{x}{2+a} + \frac{y}{2+2a} + \frac{z}{2+3a} = 1 \\ \frac{x}{3+a} + \frac{y}{3+2a} + \frac{z}{3+3a} = 1 \end{cases}$$

7. Let S_a be the linear system

$$\begin{cases} x - 2y + z = 1 \\ 3x + 2y - 2z = 2 \\ 2x - y + az = 3 \end{cases}$$

   a) Find all real numbers a for which the system has no solution.
   b) Find all real numbers a for which the system has a unique solution.
   c) Find all real numbers a for which the system has infinitely many solutions.

8. Given real numbers a, b, c, d, solve the linear system

$$\begin{cases} x + y + z = 1 \\ ax + by + cz = d \\ a^2x + b^2y + c^2z = d^2 \end{cases}$$

9. Given real numbers a, b, c, d, α, solve the linear system

$$\begin{cases} (1+\alpha)x + y + z + t = a \\ x + (1+\alpha)y + z + t = b \\ x + y + (1+\alpha)z + t = c \\ x + y + z + (1+\alpha)t = d \end{cases}$$

10. Find the necessary and sufficient condition satisfied by real numbers a, b, c for the system

$$\begin{cases} x - a(y+z) = 0 \\ y - b(x+z) = 0 \\ z - c(x+y) = 0 \end{cases}$$

to have a nontrivial solution.

11. Let a, b, c be pairwise distinct real numbers. Solve the system

$$\begin{cases} x + ay + a^2 z = a^3 \\ x + by + b^2 z = b^3 \\ x + cy + c^2 z = c^3 \end{cases}$$

12. Let a, b be complex numbers. Solve the linear system

$$\begin{cases} ax + y + z + t = 1 \\ x + ay + z + t = b \\ x + y + az + t = b^2 \\ x + y + z + at = b^3. \end{cases}$$

Chapter 8
Polynomial Expressions of Linear Transformations and Matrices

Abstract From a theoretical point of view, this chapter is the heart of the book. It uses essentially all results established before to prove a great deal of surprising results concerning matrices. This chapter makes heavy use of basic properties of polynomials which are used to study the eigenvalues and eigenvectors of matrices.

Keywords Minimal polynomial • Characteristic polynomial • Eigenvalue • Eigenvectors

From a theoretical point of view, we reach now the heart of the book. In this chapter we will use everything we have developed so far to study linear maps and matrices. To each matrix (or linear transformation of a finite dimensional vector space) we will associate two polynomials, the minimal and the characteristic polynomial. They are not enough to characterize the matrix up to similarity, but they give lots of nontrivial information about the matrix. We also associate a collection of scalars called eigenvalues of the matrix (if the field of scalars is $\mathbf{C}$, the eigenvalues are simply the roots of the characteristic polynomial) and a collection of subspaces indexed by the eigenvalues and called eigenspaces. An in-depth study of these objects yields many deep theorems and properties of matrices.

In this chapter we will make heavy use of basic properties of polynomials. We recalled them in the appendix concerning algebraic prerequisites, and we strongly advise the reader to make sure that he is familiar with these properties before starting reading this chapter. We fix a field F (the reader will not loose anything assuming that F is either $\mathbf{R}$ or $\mathbf{C}$).

8.1 Some Basic Constructions

Let V be a vector space over a field F, and let $T : V \to V$ be a linear transformation. We define a sequence $(T^i)_{i\geq 0}$ of linear transformations of V by the rule

$$T^0 = \mathrm{id}, \quad T^{i+1} = T \circ T^i$$

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_8

for $i \geq 0$, where id denotes the identity map (sending every vector v to v). In other words, T^i is the ith iterate of T, for instance

$$T^3(v) = T(T(T(v)))$$

for all $v \in V$.

If $P = a_0 + a_1X + \ldots + a_nX^n \in F[X]$ we define a linear transformation $P(T)$ of V by

$$P(T) := a_0T^0 + a_1T^1 + \ldots + a_nT^n.$$

The following result follows easily by unwinding definitions. We will use it constantly from now on, without further reference, thus the reader may want to take a break and check that he can actually prove it.

Proposition 8.1. *If $P_1, P_2 \in F[X]$ and T is a linear transformation of V, then*

a) $P_1(T) + P_2(T) = (P_1 + P_2)(T)$.
b) $P_1(T) \circ P_2(T) = (P_1P_2)(T)$.

We warn the reader that **we do not have** $P(T_1) + P(T_2) = P(T_1 + T_2)$ and $P(T_1) \circ P(T_2) = P(T_1 \circ T_2)$ in general. For instance, take $P(X) = X^2$ and $T_1 = T_2 = \mathrm{id}$, then

$$P(T_1) + P(T_2) = 2\mathrm{id} \neq 4\mathrm{id} = (T_1 + T_2)^2.$$

We invite the reader to find a counterexample for the equality $P(T_1) \circ P(T_2) = P(T_1 \circ T_2)$.

Definition 8.2. The F-algebra generated by the linear transformation T is the set

$$F[T] = \{P(T), P \in F[X]\}.$$

The following result follows directly from the previous proposition:

Proposition 8.3. *For all $x, y \in F[T]$ and $c \in F$ we have $x + cy \in F[T]$ and $x \circ y \in F[T]$. Thus $F[T]$ is a subspace of the space of linear transformations on V, which is stable by composition of linear transformations.*

Actually, the reader can easily check that $F[T]$ is the smallest subspace of the space of linear transformations on V which contains id, T and is closed under composition of linear transformations.

All previous constructions and results have analogues for matrices. Namely, if $A \in M_n(F)$ is a square matrix of order n with coefficients in F, we have the sequence $(A^i)_{i\geq 0}$ of successive powers of A, and we define for $P = a_0 + a_1X + \ldots + a_nX^n \in F[X]$

$$P(A) := a_0I_n + a_1A + \ldots + a_nA^n.$$

We have $P(A) \cdot Q(A) = (PQ)(A)$ for all polynomials P, Q and all matrices A. The algebra generated by A is defined by

$$F[A] = \{P(A), P \in F[X]\}.$$

It is a subspace of $M_n(F)$ which is stable under multiplication of matrices.

Remark 8.4. If A is the matrix of some linear transformation T of V in some basis of V, then $P(A)$ is the matrix of $P(T)$ in that basis.

Problem 8.5. a) Let $A, B \in M_n(F)$ be matrices, with B invertible. Prove that for any $P \in F[X]$ we have

$$P(BAB^{-1}) = BP(A)B^{-1}.$$

b) Prove that if $A, B \in M_n(F)$ are similar matrices, then $P(A)$ and $P(B)$ are similar matrices for all $P \in F[X]$.

Solution. a) Suppose first that $P(X) = X^k$ for some $k \geq 1$, we need to prove that $(BAB^{-1})^k = BA^kB^{-1}$. But using that $B^{-1}B = I_n$ several times, we obtain

$$(BAB^{-1})^k = BAB^{-1}BAB^{-1}\ldots BAB^{-1}$$

$$= BA^2B^{-1}BAB^{-1}\ldots BAB^{-1} = \ldots = BA^kB^{-1}.$$

In general, write $P(X) = a_0 + a_1X + \ldots + a_kX^k$, then

$$P(BAB^{-1}) = \sum_{i=0}^{k} a_i(BAB^{-1})^i = \sum_{i=0}^{k} a_i BA^i B^{-1}$$

$$= B(\sum_{i=0}^{k} a_i A^i)B^{-1} = BP(A)B^{-1}$$

and the problem is solved.

b) Write $A = CBC^{-1}$ for some invertible matrix C. Then by part a)

$$P(A) = P(CBC^{-1}) = CP(B)C^{-1},$$

thus $P(A)$ and $P(B)$ are similar. □

8.1.1 Problems for Practice

1. Prove Proposition 8.1.
2. Let

$$A = \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ -2 & 2 & -3 \end{bmatrix}.$$

Compute $P(A)$, where $P(X) = X^3 - X + 1$.

3. Let a, b, c be real numbers and let

$$A = \begin{bmatrix} 0 & -b & c \\ a & 0 & -c \\ -a & b & 0 \end{bmatrix}.$$

Compute $P(A)$, where

$$P(X) = X(X^2 + ab + bc + ca).$$

4. Prove that the matrix

$$A = \begin{bmatrix} 2 & 0 & 1 \\ -4 & 0 & -2 \\ -4 & 0 & -2 \end{bmatrix}$$

is nilpotent.

5. Let $A \in M_n(F)$ be a symmetric matrix. Prove that for all $P \in F[X]$ the matrix $P(A)$ is symmetric.
6. Let $A \in M_n(F)$ be a diagonal matrix. Prove that for all $P \in F[X]$ the matrix $P(A)$ is diagonal.
7. Let $A \in M_n(F)$ be an upper-triangular matrix. Prove that for all $P \in F[X]$ the matrix $P(A)$ is upper-triangular.
8. Let V be the vector space of smooth functions $f : \mathbf{R} \to \mathbf{R}$ and let $T : V \to V$ be the linear transformation sending $f \in V$ to its derivative f'. Can we find a nonzero polynomial $P \in \mathbf{R}[X]$ such that $P(T) = 0$?

8.2 The Minimal Polynomial of a Linear Transformation or Matrix

Let V be a finite dimensional vector space over F, say of dimension $n \geq 1$. We will be concerned with the following problem: given a linear transformation T of V, describe the polynomials $P \in F[X]$ for which $P(T) = 0$. Note that we can also ask the dual question: given a polynomial $P \in F[X]$, describe the linear transformations T for which $P(T) = 0$. This is more difficult to answer, and solving this problem actually requires the resolution of the first problem.

So let us start with a linear transformation T of V and consider the set

$$I(T) = \{P \in F[X], P(T) = 0\}.$$

A key observation is that $I(T)$ is not reduced to $\{0\}$. Indeed, the space of linear transformations on V has dimension n^2, thus the linear transformations $\mathrm{id}, T, T^2, \ldots, T^{n^2}$ cannot be linearly independent. Thus we can find $a_0, \ldots, a_{n^2}$ not all 0 such that

$$a_0 \mathrm{id} + a_1 T + \ldots + a_{n^2} T^{n^2} = 0$$

and then $a_0 + a_1 X + \ldots + a_{n^2} X^{n^2}$ is a nonzero element of $I(T)$.

Theorem 8.6. *There is a unique monic (nonzero) polynomial $\mu_T \in I(T)$ such that $I(T)$ is the set of multiples of μ_T in $F[X]$, i.e.*

$$I(T) = \mu_T \cdot F[X].$$

Proof. Proposition 8.1 implies that $I(T)$ is a subspace of $F[X]$ and that $PQ \in I(T)$ whenever $P \in I(T)$ and $Q \in F[X]$. Indeed,

$$(PQ)(T) = P(T) \circ Q(T) = 0 \circ Q(T) = 0.$$

The discussion preceding Theorem 8.6 shows that $I(T) \neq 0$. Let P be a nonzero polynomial of smallest degree in $I(T)$. Dividing P by its leading coefficient (the new polynomial is still in $I(T)$ and has the same degree as P), we may assume that P is monic. By the first paragraph, all multiples of P belong to $I(T)$. Conversely, let S be an element of $I(T)$ and write $S = QP + R$ with $Q, R \in F[X]$ and $\deg R < \deg P$. Note that $R = S - QP \in I(T)$ since $I(T)$ is a subspace of $F[X]$ and $S, QP \in I(T)$. If $R \neq 0$, then since $\deg R < \deg P$ we obtain a contradiction with the minimality of P. Thus $R = 0$ and P divides S. It follows that $I(T)$ is precisely the set of multiples of P and so we can take $\mu_T = P$.

Finally, we need to prove that μ_T is unique. If S had the same properties, then S would be a multiple of μ_T and μ_T would be a multiple of S. Since they are both monic, they must be equal. □

Definition 8.7. The polynomial μ_T is called the **minimal polynomial** of T.

Due to its importance, let us stress again the **properties of the minimal polynomial** μ_T:

- **it is monic and satisfies** $\mu_T(T) = 0$.
- **For any polynomial** $P \in F[X]$, **we have** $P(T) = 0$ **if and only if** μ_T **divides** P.

The whole theory developed above applies verbatim to matrices: if $A \in M_n(F)$, there is a unique **monic** polynomial $\mu_A \in F[X]$ with the following properties:

- $\mu_A(A) = O_n$ and
- If $P \in F[X]$, then $P(A) = O_n$ if and only if μ_A divides P.

Remark 8.8. If P is a polynomial and A is a matrix (or a linear transformation) satisfying $P(A) = O_n$, we will sometimes say that P kills A or that A is killed by P. Thus **the polynomials killing** A **are precisely the multiples of the minimal polynomial of** A**.**

The discussion preceding Theorem 8.6 shows that we can find a nonzero polynomial P of degree not exceeding n^2 such that $P(T) = 0$. Since μ_T divides P, it follows that $\deg \mu_T \leq n^2$. This bound is fairly weak and the goal of the next sections is to introduce a second polynomial canonically associated with T, the **characteristic polynomial** of T. This will be monic of degree n and will also vanish when evaluated at T. This will yield the inequality $\deg \mu_T \leq n$, which is essentially optimal.

Let us give a few examples of computations of minimal polynomials:

Example 8.9. Let F be a field. All matrices below are supposed to have entries in F.

a) The minimal polynomial of the matrix O_n is clearly $\mu_{O_n} = X$. More generally, the minimal polynomial of the scalar matrix cI_n is $X - c$.
b) Consider some elements $d_1, \ldots, d_n \in F$ and a diagonal matrix $A = [a_{ij}]$, with $a_{ii} = d_i$. The elements $d_1, \ldots, d_n$ are not necessarily pairwise distinct, so let us assume that $d_{i_1}, \ldots, d_{i_k}$ is the largest collection of pairwise distinct elements among $d_1, \ldots, d_n$. Note that for any polynomial $Q \in F[X]$ the matrix $Q(A)$ is simply the diagonal matrix with diagonal entries $Q(d_1), \ldots, Q(d_n)$. Thus $Q(A) = O_n$ if and only if $Q(d_i) = 0$ for $1 \leq i \leq n$. This happens if and only if $Q(d_{i_1}) = \ldots = Q(d_{i_k}) = 0$. Since $d_{i_1}, \ldots, d_{i_k}$ are pairwise distinct, this is further equivalent to $(X - d_{i_1}) \ldots (X - d_{i_k}) \mid Q$. Thus the minimal polynomial of A is

$$\mu_A(X) = (X - d_{i_1}) \ldots (X - d_{i_k}).$$

In particular, we see that $d_1, \ldots, d_n$ are pairwise distinct if and only if μ_A has degree n, in which case $\mu_A = \prod_{i=1}^{n} (X - d_i)$.
c) Suppose that $F = \mathbf{R}$ and that a matrix $A \in M_n(F)$ satisfies $A^2 + I_n = O_n$. What is the minimal polynomial μ_A of A? For sure it divides $X^2 + 1$, since $X^2 + 1$ vanishes at A. The only monic nonconstant divisor of $X^2 + 1$ in $\mathbf{R}[X]$ is $X^2 + 1$ itself, thus necessarily $\mu_A = X^2 + 1$.
d) With the tools introduced so far it is not easy at all to compute the minimal polynomial of a given matrix. We will introduce in the next sections another polynomial (called the characteristic polynomial of the matrix) which can be directly computed (via the computation of a determinant) from the matrix and which is always a multiple of the minimal polynomial. This makes the computation of the minimal polynomial much easier: one computes the characteristic polynomial P of the matrix, then looks at all possible monic divisors Q of P and checks which one kills the matrix and has the smallest degree. We will see later on that one does not really need to check all possible divisors, which makes the computation even more rapid.

Problem 8.10. Let T be a linear transformation on a finite dimensional F-vector space V and let $V = V_1 \oplus V_2$ be a decomposition of V into subspaces which are stable under T. Let P, P_1, P_2 be the minimal polynomials of $T, T|_{V_1}$ and $T|_{V_2}$ respectively. Prove that P is the least common multiple of P_1 and P_2.

Solution. Let Q be the least common multiple of P_1 and P_2. Since P kills T, it also kills $T|_{V_1}$ and $T|_{V_2}$, thus it is a multiple of P_1 and P_2. It follows that Q divides P. In order to prove that P divides Q, it suffices to prove that Q kills T. But since Q is a multiple of P_1 and P_1 kills $T|_{V_1}$, it follows that Q kills $T|_{V_1}$. Similarly, Q kills $T|_{V_2}$. Since $V = V_1 \oplus V_2$, we deduce that Q kills T and the result follows. $\square$

A natural and rather subtle problem is the following: suppose that $A \in M_n(\mathbf{Q})$ is a matrix with rational entries. We can definitely see A as a matrix with real entries, i.e., as an element of $M_n(\mathbf{R})$ or as a matrix with complex entries, i.e., as an element of $M_n(\mathbf{C})$. Thus we can attach to A three minimal polynomials! Fortunately, the following theorem shows that the three polynomials are actually one and the same: the minimal polynomial of a matrix does not depend on the field containing the entries of the matrix:

Theorem 8.11. *Let $F_1 \subset F_2$ be two fields and let $A \in M_n(F_1)$. Then the minimal polynomial of A seen as element of $M_n(F_1)$ and that of A seen as element of $M_n(F_2)$ coincide.*

Proof. Let μ_1 be the minimal polynomial of $A \in M_n(F_1)$ and μ_2 that of $A \in M_n(F_2)$. Since $F_1[X] \subset F_2[X]$, the polynomial μ_1 belongs to $F_2[X]$ and kills A, thus it must be a multiple of μ_2. In other words, μ_2 divides μ_1. Let $d_i = \deg \mu_i$. It suffices to prove that $d_2 \geq d_1$ and for this it suffices to prove that there is a nonzero polynomial $P \in F_1[X]$ of degree at most d_2 which vanishes at A (as such a polynomial is necessarily a multiple of μ_1). By hypothesis, we know that we have a relation

$$a_0 I_n + a_1 A + \ldots + a_{d_2} A^{d_2} = O_n$$

with $a_i \in F_2$ (namely the coefficients of μ_2). This is equivalent to n^2 linear homogeneous equations in the unknowns $a_0, \ldots, a_{d_2}$. The coefficients of these equations are entries of the matrices $I_n, A, \ldots, A^{d_2}$, so they belong to F_1. So we have a linear homogeneous system with coefficients in F_1 and having a nontrivial solution in F_2. Then it automatically has a nontrivial solution in F_1 (by Theorem 7.77), giving the desired polynomial P. □

We end this section with a series of problems related to the **pointwise minimal polynomial**. Let V be a finite dimensional vector space over a field F and let $T : V \to V$ be a linear transformation with minimal polynomial μ_T. For $x \in V$, consider

$$I_x = \{P \in F[X] | P(T)(x) = 0\}.$$

Note that the sum and difference of two elements of I_x is still in I_x.

Problem 8.12. Prove that there is a unique monic polynomial $\mu_x \in F[X]$ such that I_x is the set of multiples of μ_x in $F[X]$. Moreover, μ_x divides μ_T.

Solution. We may assume that $x \neq 0$. Note that $\mu_T \in I_x$, since $\mu_T(T) = 0$. Let μ_x be the monic polynomial of smallest degree which belongs to I_x. We will prove that $I_x = \mu_x F[X]$.

First, if $P \in \mu_x F[X]$, then $P = \mu_x Q$ for some $Q \in F[X]$ and

$$P(T)(x) = Q(T)(\mu_x(T)(x)) = Q(T)(0) = 0,$$

thus $P \in I_x$. This shows that $\mu_x F[X] \subset I_x$.

Conversely, let $P \in I_x$ and, using the division algorithm let $P = Q\mu_x + R$ for some polynomials $Q, R \in F[X]$ such that $\deg R < \deg \mu_x$. Assume that $R \neq 0$. Since P and $Q\mu_x$ belong to I_x (the second one by the previous paragraph), we deduce that $R \in I_x$. Let a be the leading coefficient of R, then $\frac{1}{a}R$ is a monic polynomial belonging to I_x and with degree less than that of μ_x, a contradiction. Thus $R = 0$ and μ_x divides P, finishing the solution. □

Problem 8.13. Let T be a linear transformation on a finite dimensional vector space V over F, where F is an arbitrary field.

a) Prove that if $\mu_T = P^k Q$ with $k \geq 1$, $P \in F[X]$ irreducible and Q relatively prime to P, then we can find $x \in V$ such that $\mu_x = P^k$.
b) Prove that if $x_1, x_2 \in V$ are such that μ_{x_1} and μ_{x_2} are relatively prime, then $\mu_{x_1+x_2} = \mu_{x_1}\mu_{x_2}$.
c) Conclude that there is always a vector $x \in V$ such that $\mu_x = \mu_T$.

Solution. a) Suppose on the contrary that $\mu_x \neq P^k$ for all $x \in V$. Let $x \in V$. Then by hypothesis $(P^k Q)(T)(x) = 0$. Hence $v = Q(T)(x)$ lies in the kernel of $P^k(T)$ and so μ_v divides P^k. Since $\mu_v \neq P^k$ and P is irreducible, μ_v divides P^{k-1} and so $P^{k-1}(T)(v) = 0$, that is $(P^{k-1}Q)(T)(x) = P^{k-1}(T)(v) = 0$. But since x was arbitrary, this means $\mu_T | P^{k-1}Q$, a contradiction.

b) Let $P_1 = \mu_{x_1}$ and $P_2 = \mu_{x_2}$, and let $P = P_1P_2$. Since P is a multiple of both P_1 and P_2, we deduce that $P(T)$ vanishes at both x_1 and x_2, thus it vanishes at $x_1 + x_2$ and so $\mu_{x_1+x_2} \mid P$.

On the other hand, $\mu_{x_1+x_2}(T)(x_1 + x_2) = 0$, thus

$$(P_1\mu_{x_1+x_2})(T)(x_1) + (P_1\mu_{x_1+x_2})(T)(x_2) = 0.$$

The first term in the sum is 0, since $P_1(T)(x_1) = 0$, thus the second term must be 0, which means that $\mu_{x_2} = P_2 \mid P_1\mu_{x_1+x_2}$. Since P_1 and P_2 are relatively prime, it follows that P_2 divides $\mu_{x_1+x_2}$ and by symmetry P_1 also divides $\mu_{x_1+x_2}$. Using again that P_1 and P_2 are relatively prime, we conclude that $P = P_1P_2$ divides $\mu_{x_1+x_2}$. Combining this with the divisibility $\mu_{x_1+x_2} \mid P$ and using that $\mu_{x_1+x_2}$ and P are both monic, the result follows.

c) Consider the decomposition $\mu_T = P_1^{k_1} \ldots P_r^{k_r}$ of μ_T into irreducible polynomials. Here $P_1, \ldots, P_r$ are pairwise relatively prime irreducible polynomials and k_i are positive integers. By part a) we can find $x_i \in V$ such that $\mu_{x_i} = P_i^{k_i}$. Applying successively part b), we obtain

$$\mu_{x_1+\ldots+x_r} = \mu_{x_1} \ldots \mu_{x_r} = P_1^{k_1} \ldots P_r^{k_r} = \mu_T$$

and so we can take $x = x_1 + \ldots + x_r$.

□

Problem 8.14. Let V_x be the span of $x, T(x), T^2(x), \ldots$. Prove that V_x is a subspace of V of dimension $\deg \mu_x$, stable under T.

Solution. It is clear that V_x is a subspace of V, stable under T. Let $d = \deg \mu_x$. We will prove that $x, T(x), \ldots, T^{d-1}(x)$ form a basis of V_x, which will yield the desired result.

Suppose first that $a_0 x + a_1 T(x) + \ldots + a_{d-1} T^{d-1}(x) = 0$ for some scalars $a_0, \ldots, a_{d-1}$, not all of them equal to 0. The polynomial $P = a_0 + a_1 X + \ldots + a_{d-1} X^{d-1}$ is then nonzero and belongs to I_x (i.e., $P(T)(x) = 0$). Thus P is a multiple of μ_x, which is impossible as it is nonzero and its degree is less than that of μ_x. Thus $x, T(x), \ldots, T^{d-1}(x)$ are linearly independent over F.

Let W be the span of $x, T(x), \ldots, T^{d-1}(x)$. We claim that W is stable under T. It suffices to check that $T^d(x)$ belongs to W. But since $\mu_x(T)(x) = 0$ and μ_x is monic of degree d, we know that there are scalars $b_0, \ldots, b_{d-1}$ such that

$$T^d(x) + b_{d-1} T^{d-1}(x) + \ldots + b_0 x = 0.$$

This relation shows that $T^d(x)$ is a linear combination of $x, T(x), \ldots, T^{d-1}(x)$ and so it belongs to W.

Now, since W is stable under T and contains x, it must contain all $T^k(x)$ for $k \geq 0$, thus W must also contain V_x. It follows that $x, T(x), \ldots, T^{d-1}(x)$ is a generating subset of V_x and the proof is finished, since we have already shown that this set is linearly independent. □

8.2.1 Problems for Practice

1. Compute the minimal polynomial of the following matrices:

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

2. Compute the minimal polynomial of the matrix $A \in M_n(\mathbf{R})$ all of whose entries are equal to 1.
3. Let $A \in M_n(\mathbf{C})$. Prove that

$$\dim \operatorname{Span}(I_n, A, A^2, \ldots) = \deg \mu_A.$$

4. Find a matrix $A \in M_2(\mathbf{R})$ whose minimal polynomial is

   a) $X^2 - 3X + 2$.
   b) X^2.
   c) $X^2 + 1$.

5. Let V be a finite dimensional vector space over F and let $T : V \to V$ be an invertible linear transformation. Prove that $T^{-1} \in F[T]$.

6. For which positive integers n can we find a matrix $A \in M_n(\mathbf{R})$ whose minimal polynomial is $X^2 + 1$?
7. Compute the minimal polynomial of the projection/symmetry of $\mathbf{C}^n$ onto a subspace along a complementary subspace.
8. Let $T : M_n(\mathbf{C}) \to \mathbf{C}$ be the map sending a matrix to its transpose. Find the minimal polynomial of T.
9. Let $T : M_n(\mathbf{C}) \to \mathbf{C}$ be the map sending a matrix $A = [a_{ij}]$ to the matrix $\overline{A} = [\overline{a_{ij}}]$, where $\bar{z}$ is the complex conjugate of z. Find the minimal polynomial of T.
10. Describe the minimal polynomial of a matrix $A \in M_n(\mathbf{C})$ of rank 1.

8.3 Eigenvectors and Eigenvalues

Let V be a vector space over a field F and let T be a linear transformation of V. In this section we will be interested in those $\lambda \in F$ for which $\lambda \cdot \mathrm{id} - T$ is **not** invertible. The following definition is fundamental.

Definition 8.15. An **eigenvalue** of T is a scalar $\lambda \in F$ such that $\lambda \cdot \mathrm{id} - T$ is not invertible. An **eigenvector** of T corresponding to the eigenvalue λ (or **λ-eigenvector**) is any nonzero element of the space $\ker(\lambda \cdot \mathrm{id} - T)$, which is called the **eigenspace** corresponding to λ (or the **λ-eigenspace**).

Thus a λ-eigenvector v is by definition **nonzero** and satisfies

$$T(v) = \lambda v,$$

and the λ-eigenspace consists of the vector 0 and all λ-eigenvectors.

We have the analogous definition for matrices:

Definition 8.16. Let $A \in M_n(F)$ be a square matrix. A scalar $\lambda \in F$ is called an **eigenvalue of** A if there is a nonzero vector $X \in F^n$ such that $AX = \lambda X$. In this case, the subspace

$$\ker(\lambda I_n - A) := \{X \in F^n \mid AX = \lambda \cdot X\}$$

is called the **λ-eigenspace of** A.

It is an easy but important exercise for the reader to check that the two definitions are compatible, in the following sense: let V be finite dimensional and let $T : V \to V$ be a linear transformation. Choose any basis of V and let A be the matrix of T with respect to this basis. Then the eigenvalues of T are exactly the eigenvalues of A.

Example 8.17. Consider the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Let us find the eigenvalues and the eigenspaces of A, **if we consider A as a matrix with complex entries.** Let λ be an eigenvalue and let X be a nonzero vector such that $AX = \lambda X$. If x_1, x_2 are the coordinates of X, the condition $AX = \lambda X$ is equivalent to the equations

$$-x_2 = \lambda x_1, \quad x_1 = \lambda x_2.$$

We deduce that

$$-x_2 = \lambda^2 x_2.$$

If $x_2 = 0$, then $x_1 = 0$ and $X = 0$, a contradiction. Thus $x_2 \neq 0$ and necessarily $\lambda^2 = -1$, that is $\lambda \in \{-i, i\}$. Conversely, i and $-i$ are both eigenvalues, since we can choose $x_2 = 1$ and $x_1 = \lambda$ as a solution of the previous system. Actually the λ-eigenspace is given by

$$\ker(\lambda I_2 - A) = \{(\lambda x_2, x_2) | x_2 \in \mathbf{C}\}$$

and it is the line spanned by $v = (\lambda, 1) \in \mathbf{C}^2$. Thus seen as a complex matrix, A has two eigenvalues $\pm i$, and the eigenspaces are the lines spanned by $(i, 1)$ and $(-i, 1)$.

We see now A as a matrix with real entries and we ask the same question. Letting $\lambda \in \mathbf{R}$ be an eigenvalue and X an eigenvector as above, the same computations yield

$$(\lambda^2 + 1)x_2 = 0.$$

Since λ is real, $\lambda^2 + 1$ is nonzero and so $x_2 = 0$, then $x_1 = 0$ and $X = 0$. The conclusion is that **seen as a matrix with real entries, A has no eigenvalue, thus no eigenspace.** This example shows that **eigenvalues and eigenspaces are very sensitive to the field of scalars**.

Given a matrix $A \in M_n(F)$, how can we find its eigenvalues and its eigenspaces? The first part is much harder than the second one. Indeed, finding eigenspaces is equivalent to solving linear systems of the form $AX = \lambda X$, which is not (too) difficult. On the other hand, finding eigenvalues comes down to solving polynomial equations, which is quite hard (but can be done approximately with the help of a computer as long as we are not interested in exact formulae). In practice (and for reasonably sized matrices) we use the following fundamental observation in order to compute eigenvalues:

Proposition 8.18. *A scalar $\lambda \in F$ is an eigenvalue of $A \in M_n(F)$ if and only if*

$$\det(\lambda I_n - A) = 0.$$

Proof. $\lambda I_n - A$ is not invertible if and only if its determinant vanishes. The result follows. □

Let us come back to our problem of computing the eigenvalues of a matrix. If we know that

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

where $a_{ij} \in F$ for $i, j = 1, 2, \dots, n$, then the proposition says that we can find the eigenvalues of A by solving the polynomial equation

$$\begin{vmatrix} \lambda - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \dots & -a_{2n} \\ \dots & \dots & \dots & \dots \\ -a_{n1} & -a_{n2} & \dots & \lambda - a_{nn} \end{vmatrix} = 0$$

in F. This is a polynomial equation of degree n. If the degree is greater than 4, there is no general solution in terms of radicals (of course, there are instances in which one can solve the equations in terms of radicals, but most of the time this will not happen).

Example 8.19. Let us find the eigenvalues of $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$. We start by simplifying the equation

$$\begin{vmatrix} \lambda - 1 & 0 & 0 \\ 0 & \lambda & 1 \\ 0 & -1 & \lambda \end{vmatrix} = 0.$$

Expanding with respect to the first column and doing the computations, we obtain the equivalent equation

$$(\lambda - 1)(\lambda^2 + 1) = 0.$$

Next, we recall that eigenvalues are sensitive to the field of scalars. Since nothing was said about the field of scalars in this problem, we consider two cases. If we take the field of scalars to be $\mathbf{C}$, then the eigenvalues are $1, \pm i$, which are the complex solutions of the equation $(\lambda - 1)(\lambda^2 + 1) = 0$. If the field of scalars is $\mathbf{R}$, then the only eigenvalue of A is 1.

Remark 8.20. Let us mention two important and interesting consequences of Proposition 8.18 and the discussion following it:

- For any matrix $A \in M_n(F)$, A **and its transpose** ${}^tA$ **have the same eigenvalues**. Indeed, for $\lambda \in F$ we have

$$\det(\lambda I_n - {}^tA) = \det({}^t(\lambda I_n - A)) = \det(\lambda I_n - A),$$

thus $\det(\lambda I_n - A) = 0$ if and only if $\det(\lambda I_n - {}^tA) = 0$.

- **Any matrix $A \in M_n(F)$ has finitely many eigenvalues**, since they are all solutions of a polynomial equation of degree n, namely $\det(\lambda I_n - A) = 0$. Actually, since a polynomial of degree n has at most n distinct roots, we deduce that **any matrix $A \in M_n(F)$ has at most n eigenvalues**.

We can restate part of the previous remark in terms of linear transformations:

Corollary 8.21. *Let V be a **finite dimensional** vector space over F and let $T : V \to V$ be a linear transformation. Then T has only finitely many (actually at most* $\dim V$*) distinct eigenvalues.*

Remark 8.22. On the other hand, a linear transformation on an infinite dimensional vector space may very well have infinitely many eigenvalues. Consider for instance the space V of all smooth functions $f : \mathbf{R} \to \mathbf{R}$, and consider the map $T : V \to V$ sending f to its derivative. Then $f_a : x \mapsto e^{ax}$ is an eigenvector with eigenvalue a for all $a \in \mathbf{R}$, thus any real number is an eigenvalue for T.

The following important problem shows that it is very easy to describe the eigenvalues of an upper-triangular matrix:

Problem 8.23. Let $A = [a_{ij}]$ be an upper-triangular matrix in $M_n(F)$. Prove that the eigenvalues of A are precisely its diagonal elements.

Solution. By definition, $\lambda \in F$ is an eigenvalue of A if and only if $\lambda I_n - A$ is not invertible. The matrix $\lambda I_n - A$ is also upper-triangular, with diagonal elements $\lambda - a_{ii}$. But an upper-triangular matrix is invertible if and only if its diagonal entries are nonzero (because its determinant equals the product of the diagonal entries by Theorem 7.41). The result follows.

Problem 8.24. Find the eigenvalues of A^6, where

$$A = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 0 & \frac{1}{10} & 3 & 6 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 2 \end{bmatrix} \in M_4(\mathbf{R}).$$

Solution. It is useless to compute explicitly A^6: by the product rule for matrices, the product of two upper-triangular matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ is an upper-triangular matrix with diagonal entries $a_{ii}b_{ii}$. It follows that A^6 is an upper-triangular matrix with diagonal entries $1, 1/10^6, 0, 64$. By the previous problem, these are also the eigenvalues of A^6. □

The next important result says that **eigenvectors corresponding to different eigenvalues are linearly independent**.

Theorem 8.25. *Let $\lambda_1, \ldots, \lambda_k$ be pairwise distinct eigenvalues of a linear transformation T. Then the λ_i-eigenspaces of T are in direct sum position.*

Proof. By definition, we need to prove that if $T(v_i) = \lambda_i v_i$ and $v_1 + \ldots + v_k = 0$, then $v_1 = \ldots = v_k = 0$. We will prove this by induction on k. The result is clear when $k = 1$, so assume that it holds for $k-1$ and let us prove it for k. We have

$$0 = T(v_1 + \ldots + v_k) = T(v_1) + \ldots + T(v_k) = \lambda_1 v_1 + \ldots + \lambda_k v_k,$$

which combined with the relation $\lambda_k v_1 + \ldots + \lambda_k v_k = 0$ yields

$$0 = (\lambda_k - \lambda_1)v_1 + \ldots + (\lambda_k - \lambda_{k-1})v_{k-1} = 0.$$

The inductive hypothesis implies that $(\lambda_k - \lambda_i)v_i = 0$ for $1 \leq i < k$. Since $\lambda_k \neq \lambda_i$, this forces $v_i = 0$ for $1 \leq i < k$. But then automatically $v_k = 0$, since $v_1 + \ldots + v_k = 0$. The inductive step being proved, the problem is solved. □

Problem 8.26. Let λ be an eigenvalue of a linear map $T : V \to V$, where V is a vector space over F and let P be a polynomial with coefficients in F. Prove that $P(\lambda)$ is an eigenvalue of $P(T)$.

Solution. The hypothesis yields the existence of a nonzero vector $v \in V$ such that $T(v) = \lambda v$. By induction, we obtain $T^k(v) = \lambda^k v$ for $k \geq 1$. Indeed, if $T^k(v) = \lambda^k v$, then

$$T^{k+1}(v) = T(T^k(v)) = T(\lambda^k v) = \lambda^k T(v) = \lambda^{k+1} v.$$

We deduce that if $P(X) = a_n X^n + \ldots + a_1 X + a_0$, then

$$P(T)(v) = a_n T^n(v) + \ldots + a_1 T(v) + a_0 v$$

$$= a_n \lambda^n v + \ldots + a_0 v = P(\lambda)v$$

and so $P(\lambda)$ is an eigenvalue of $P(T)$. □

The following consequence of the previous problem is very useful in practice:

Problem 8.27. Let $A \in M_n(\mathbf{C})$ be a matrix and let $P \in \mathbf{C}[X]$ be a polynomial such that $P(A) = O_n$. Prove that any eigenvalue λ of A satisfies $P(\lambda) = 0$.

Solution. By the previous problem, $P(\lambda)$ is an eigenvalue of $P(A) = O_n$. Since 0 is the only eigenvalue of O_n, we deduce that $P(\lambda) = 0$. □

In particular, we obtain the following:

Theorem 8.28. *Let $T : V \to V$ be a linear transformation on a **finite-dimensional** vector space V over F. Then the eigenvalues of T are precisely the roots **in** F of the minimal polynomial μ_T of T.*

Proof. Since $\mu_T(T) = 0$, the previous problem shows that all eigenvalues of T are roots of μ_T. Conversely, let $\lambda \in F$ be a root of μ_T and assume that λ is not

an eigenvalue of T. Thus $T - \lambda\mathrm{id}$ is invertible. Since $\mu_T(\lambda) = 0$, we can write $\mu_T(X) = (X - \lambda)Q(X)$ for some $Q \in F[X]$. Since $\mu_T(T) = 0$, we deduce that

$$(T - \lambda\mathrm{id}) \circ Q(T) = 0.$$

As $T - \lambda\mathrm{id}$ is invertible, the last relation is equivalent to $Q(T) = 0$. Hence μ_T divides Q, which is absurd. The problem is solved. □

The next problem is a classical result, which gives rather interesting bounds on the eigenvalues of a matrix.

Problem 8.29 (Gershgorin Discs). Let $A = [a_{ij}] \in M_n(\mathbf{C})$ be a matrix and let

$$R_i = \sum_{\substack{1 \le j \le n \\ j \ne i}} |a_{ij}|.$$

a) Prove that if $|a_{ii}| > R_i$ for all i, then A is invertible.
b) Deduce that any eigenvalue of A belongs to the set

$$\bigcup_{i=1}^{n} \{z \in \mathbf{C} | |z - a_{ii}| \le R_i\}.$$

c) Give a geometric interpretation of the result established in part b).

Solution. a) Suppose that A is not invertible, thus we can find a nonzero vector $X \in \mathbf{C}^n$, with coordinates $x_1, x_2, \ldots, x_n$, such that $AX = 0$. Let i be an index such that

$$|x_i| = \max_{1 \le j \le n} |x_j|.$$

The ith equation of the linear system $AX = 0$ reads

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = 0,$$

or equivalently

$$a_{ii}x_i = -\sum_{j \ne i} a_{ij}x_j.$$

Using the triangular inequality, i.e., $|z_1 + \ldots + z_n| \le |z_1| + \ldots + |z_n|$, valid for all complex numbers $z_1, \ldots, z_n$), we deduce that

$$|a_{ii}||x_{ii}| = |\sum_{j \ne i} a_{ij}x_j| \le \sum_{j \ne i} |a_{ij}||x_j|.$$

Since $|x_j| \leq |x_i|$ for all j, we can further write

$$|a_{ii}||x_i| \leq \sum_{j \neq i} |a_{ij}||x_i| = R_i|x_i|.$$

Note that $x_i \neq 0$, since otherwise $|x_j| \leq |x_i| = 0$ for all j, thus $x_j = 0$ for all j, contradicting the fact that $X \neq 0$. Thus we can divide by $|x_i|$ the previous inequality and obtain

$$|a_{ii}| \leq R_i,$$

which contradicts the assumption of the problem. Hence A is invertible.

b) Let λ be an eigenvalue of A and let $B = A - \lambda I_n$. Write $B = [b_{ij}]$, with $b_{ij} = a_{ij}$ when $i \neq j$ and $b_{ii} = a_{ii} - \lambda$. Since B is not invertible, part a) ensures the existence of an index i such that $|b_{ii}| \leq \sum_{i \neq j} |b_{ij}|$. This can be also written as

$$|a_{ii} - \lambda| \leq R_i$$

and shows that

$$\lambda \in \bigcup_{i=1}^{n} \{z \in \mathbf{C} || z - a_{ii}| \leq R_i\}.$$

c) The set $\{z \in \mathbf{C} || z - a_{ii}| \leq R_i\}$ is the closed disc centered at a_{ii} and having radius R_i. Thus part b) says that the eigenvalues of A are located in a union of discs centered at the diagonal entries of A and whose radii are $R_1, \ldots, R_n$. □

Remark 8.30. Consider

$$C_i = \sum_{j \neq i} |a_{ji}|.$$

Applying the result established before to ${}^tA$ (which has the same eigenvalues as A) we obtain that the eigenvalues of A are also located in

$$\bigcup_{i=1}^{n} \{z \in \mathbf{C} || z - a_{ii}| \leq C_i\}.$$

8.3.1 Problems for Practice

1. Find the eigenvalues and the eigenvectors of the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix} \in M_3(\mathbf{C}).$$

2. Let V be the set of matrices $A \in M_2(\mathbf{C})$ with the property that $\begin{bmatrix} 1 \\ 2 \end{bmatrix}$ is an eigenvector of A. Prove that V is vector subspace of $M_2(\mathbf{C})$ and give a basis for V.
3. Let e_1, e_2, e_3, e_4 be the standard basis of $\mathbf{C}^4$ and consider the set V of those matrices $A \in M_4(\mathbf{C})$ with the property that e_1, e_2 are both eigenvectors of A. Prove that V is a vector subspace of $M_4(\mathbf{C})$ and compute its dimension.
4. Find all matrices $A \in M_3(\mathbf{C})$ for which the vector $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ is an eigenvector with eigenvalue 2.
5. Find the eigenvalues of the matrix $A \in M_n(\mathbf{R})$ all of whose entries are equal to 2.
6. Find all real numbers x for which the matrix $A = \begin{bmatrix} 1 & x \\ 2 & 1 \end{bmatrix} \in M_2(\mathbf{R})$ has
   a) two distinct eigenvalues.
   b) no eigenvalue.
7. Let V be the space of all polynomials with real coefficients. Let T be the linear transformation on V sending $P(X)$ to $P(1 - X)$. Describe the eigenvalues of T. Hint: what is $T \circ T$?
8. A matrix $A \in M_n(\mathbf{R})$ is called **stochastic** if $a_{ij} \geq 0$ for all $i, j \in [1, n]$ and $\sum_{j=1}^{n} a_{ij} = 1$ for all $i \in [1, n]$.
   a) Prove that 1 is an eigenvalue of any stochastic matrix.
   b) Prove that any complex eigenvalue λ of a stochastic matrix satisfies $|\lambda| \leq 1$.
9. Consider the map $T : \mathbf{R}[X] \to \mathbf{R}[X]$ sending a polynomial $P(X)$ to $P(3X)$.
   a) Prove that T is a bijective linear transformation, thus its inverse T^{-1} exists and is linear.
   b) Find the eigenvalues of T.
   c) Deduce that there is no polynomial $P \in \mathbf{R}[X]$ such that
   $$T^{-1} = P(T).$$
10. Let $A, B \in M_n(\mathbf{C})$ be matrices such that
    $$AB - BA = B.$$
    a) Prove that $AB^k - B^k A = kB^k$ for all $k \geq 1$.
    b) Deduce that B is nilpotent. Hint: consider the eigenvalues of the map $T : M_n(\mathbf{C}) \to M_n(\mathbf{C})$ given by $T(X) = AX - XA$.

11. Let V be the space of continuous real-valued maps on $[0, 1]$. Define a map $T : V \to V$ by

$$T(f)(x) = \int_0^1 \min(x, t) f(t) dt$$

for $f \in V$.

a) Justify that T is well defined and a linear transformation on V.
b) Is V finite dimensional?
c) Find the eigenvalues and describe the corresponding eigenspaces of T.

12. Let V be the space of polynomials with real coefficients whose degree does not exceed n and let $T : V \to V$ be the map defined by

$$T(P) = P(X) - (1 + X)P'(X).$$

a) Explain why T is a linear transformation on V.
b) Find the eigenvalues of T.

13. Let V be the space of all sequences $(x_n)_{n\geq 1}$ of real numbers. Let T be the map which associates to a sequence $(x_n)_{n\geq 1}$ the sequence whose general term is $\frac{x_1+2x_2+\ldots+nx_n}{n^2}$ (for $n \geq 1$).

a) Prove that T is a linear transformation on V.
b) Find the eigenvalues and the corresponding eigenspaces of T.

14. Let V be the vector space of polynomials with real coefficients and let $T : V \to V$ be the map sending a polynomial P to

$$T(P) = (X^2 - 1)P''(X) + XP'(X).$$

a) Prove that T is a linear map.
b) What are the eigenvalues of T?

15. a) Let $A \in M_n(\mathbf{C})$ be a matrix with **complex entries**, let $P \in \mathbf{C}[X]$ be a nonconstant polynomial and let μ be an eigenvalue of $P(A)$. Prove that there is an eigenvalue λ of A such that $P(\lambda) = \mu$ (this gives a converse of the result proved in Problem 8.26 for matrices with complex entries). Hint: factor the polynomial $P(X)-\mu$ as $c\prod_{i=1}^{d}(X-z_i)$ for some nonzero constant c and some complex numbers $z_1, \ldots, z_d$, and prove that at least one of the matrices $A - z_1 I_n, \ldots, A - z_d I_n$ is not invertible.

b) By considering the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, prove that the result established in part a) is false if we replace $\mathbf{C}$ with $\mathbf{R}$.

c) Suppose that a **positive** real number λ is an eigenvalue of A^2, where $A \in M_n(\mathbf{R})$ is a matrix. Prove that $\sqrt{\lambda}$ or $-\sqrt{\lambda}$ is an eigenvalue of A.

16. Let $A \in M_n(\mathbf{R})$ be a matrix and let

$$B = \begin{bmatrix} 0 & A \\ A & 2A \end{bmatrix}.$$

Express the eigenvalues of B in terms of those of A.

17. Consider the matrix

$$A = \begin{bmatrix} 2 & -1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 2 & -1 \\ 0 & 0 & 0 & \dots & 0 & -1 & 2 \end{bmatrix} \in M_n(\mathbf{C}).$$

Prove that the eigenvalues of A are $4\sin^2\left(\frac{j\pi}{2n+2}\right)$ for $1 \leq j \leq n$.

8.4 The Characteristic Polynomial

We saw in the previous section that finding the eigenvalues of a matrix $A \in M_n(F)$ comes down to solving the polynomial equation

$$\det(\lambda I_n - A) = 0$$

in F. In this section we will study in greater detail the polynomial giving rise to this equation.

By construction, the determinant of a matrix is a polynomial expression with integer coefficients in the entries of that matrix. The following theorem refines this observation a little bit.

Theorem 8.31. *Consider two matrices $A, B \in M_n(F)$. There is a polynomial $P \in F[X]$ such that for all $x \in F$ we have*

$$P(x) = \det(xA + B).$$

Denoting this polynomial $P(X) = \det(XA + B)$, we have

$$\det(XA + B) = \det(A)X^n + \alpha_{n-1}X^{n-1} + \ldots + \alpha_1 X + \det B$$

for some polynomial expressions $\alpha_1, \ldots, \alpha_{n-1}$ with integer coefficients in the entries of A and B.

Proof. Define P by

$$P(X) = \sum_{\sigma \in S_n} \varepsilon(\sigma)(a_{1\sigma(1)}X + b_{1\sigma(1)})\ldots(a_{n\sigma(n)}X + b_{n\sigma(n)}).$$

It is clear on the definition that P is a polynomial whose coefficients are polynomial expressions with integer coefficients in the entries of A and B. It is also clear that $P(x) = \det(xA + B)$ for $x \in F$. The constant term is given by plugging in $X = 0$ and thus equals $\det B$. Moreover, for each $\sigma \in S_n$ we have

$$\varepsilon(\sigma)(a_{1\sigma(1)}X + b_{1\sigma(1)})\ldots(a_{n\sigma(n)}X + b_{n\sigma(n)}) = \varepsilon(\sigma)a_{1\sigma(1)}\ldots a_{n\sigma(n)}X^n + \ldots,$$

all terms but the first in the right-hand side having degree at most $n-1$. Taking the sum over σ, we see that $P(X)$ starts with $\det A \cdot X^n$, all other terms having degree at most $n-1$. The result follows. □

It follows from the theorem that if A, B have integer (respectively rational) entries, then $\det(XA + B)$ has integer (respectively rational) coefficients.

Armed with the previous results, we introduce the following

Definition 8.32. The **characteristic polynomial** of the matrix $A \in M_n(F)$ is the polynomial $\chi_A \in F[X]$ defined by

$$\chi_A(X) = \det(X \cdot I_n - A).$$

Problem 8.33. Find the characteristic polynomial and the eigenvalues of the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & -1 & 0 \\ 0 & 7 & 0 & 6 \\ 0 & 0 & 3 & 0 \end{bmatrix} \in M_4(\mathbf{R}).$$

Solution. We compute using Laplace expansion with respect to the first row

$$\chi_A(X) = \det(XI_4 - A) = \begin{vmatrix} X & -1 & 0 & 0 \\ -2 & X & 1 & 0 \\ 0 & -7 & X & -6 \\ 0 & 0 & -3 & X \end{vmatrix} =$$

$$X \begin{vmatrix} X & 1 & 0 \\ -7 & X & -6 \\ 0 & -3 & X \end{vmatrix} + \begin{vmatrix} -2 & 1 & 0 \\ 0 & X & -6 \\ 0 & -3 & X \end{vmatrix} =$$

$$X(X^3 - 11X) - 2(X^2 - 18) = X^4 - 13X^2 + 36.$$

In order to find the eigenvalues of A, we need to find the real solutions of the equation

$$x^4 - 13x^2 + 36 = 0.$$

Letting $y = x^2$ we obtain the quadratic equation

$$y^2 - 13y + 36 = 0$$

with solutions $y_1 = 4$ and $y_2 = 9$. Solving the equations $x^2 = 4$ and $x^2 = 9$ yields the eigenvalues $\pm 2, \pm 3$ of A. □

Problem 8.34. Find the characteristic polynomial and the eigenvalues of the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \in M_3(\mathbf{F}_2).$$

Solution. We will constantly use that $-1 = 1$ in $\mathbf{F}_2$. We obtain

$$\chi_A(X) = \det(XI_3 - A) = \det(XI_3 + A) =$$

$$\begin{vmatrix} X & 1 & 1 \\ 1 & X & 1 \\ 1 & 1 & X+1 \end{vmatrix} = \begin{vmatrix} 1+X & 0 & 1 \\ 1+X & X+1 & 1 \\ 0 & X & X+1 \end{vmatrix}.$$

the equality being obtained by adding the second column to the first one and the third column to the second one. Now

$$\begin{vmatrix} 1+X & 0 & 1 \\ 1+X & X+1 & 1 \\ 0 & X & X+1 \end{vmatrix} =$$

$$(X+1)\begin{vmatrix} 1 & 0 & 1 \\ 1 & X+1 & 1 \\ 0 & X & X+1 \end{vmatrix} = (X+1)(X+1)^2 = (X+1)^3.$$

Thus

$$\chi_A(X) = (X+1)^3$$

and consequently the unique eigenvalue of A is 1. □

In the following more theoretical exercises, we will

- compute the characteristic polynomial for a rather large class of matrices: upper-triangular, nilpotent, companion matrices, etc.
- establish a few basic properties of the characteristic polynomial which turn out to be important in practice or in theoretical problems.

For upper-triangular matrices the characteristic polynomial can be read off directly from the diagonal entries:

Problem 8.35. Let $A = [a_{ij}]$ be an upper-triangular matrix (so that $a_{ij} = 0$ whenever $i > j$). Prove that

$$\chi_A(X) = \prod_{i=1}^{n}(X - a_{ii}).$$

Solution. The matrix $XI_n - A$ is again upper-triangular, with diagonal entries equal to $X - a_{ii}$. The result follows directly from Theorem 7.41.

□

Recall that ${}^tA$ is the transpose of the matrix A.

Problem 8.36. Prove that A and ${}^tA$ have the same characteristic polynomial when $A \in M_n(F)$.

Solution. Indeed ${}^t(XI_n - A) = XI_n - {}^tA$. Since a matrix and its transpose have the same determinant (Theorem 7.37), we have

$$\chi_A(X) = \det(XI_n - A) = \det({}^t(XI_n - A)) = \det(XI_n - {}^tA) = \chi_{{}^tA}(X),$$

as desired. □

Problem 8.37. Prove that the characteristic polynomial χ_A of A is of the form

$$\chi_A(X) = X^n - \mathrm{Tr}(A)X^{n-1} + \ldots + (-1)^n \det A.$$

Solution. Let us come back to the definition

$$\det(X \cdot I_n - A) = \sum_{\sigma \in S_n} \varepsilon(\sigma)(X\delta_{1\sigma(1)} - a_{1\sigma(1)})\ldots(X\delta_{n\sigma(n)} - a_{n\sigma(n)}).$$

A brutal expansion shows that

$$(X\delta_{1\sigma(1)} - a_{1\sigma(1)})\ldots(X\delta_{n\sigma(n)} - a_{n\sigma(n)}) = X^n \prod_{i=1}^{n} \delta_{i\sigma(i)} -$$

$$X^{n-1} \sum_{j=1}^{n} (\prod_{k \neq j} \delta_{k\sigma(k)}) a_{j\sigma(j)} + \ldots.$$

Note that $\prod_{i=1}^{n} \delta_{i\sigma(i)}$ is nonzero only for the identity permutation, in which case it equals 1. This already shows that $\chi_A(X)$ is monic of degree n. It is clear that its constant term is $\chi_A(0) = \det(-A) = (-1)^n \det A$ (all these results also follow straight from Theorem 8.31).

Next, if $j \in \{1, 2, \ldots, n\}$, then $\prod_{k \neq j} \delta_{k\sigma(k)}$ is nonzero only when $\sigma(k) = k$ for all $k \neq j$, but then automatically $\sigma(j) = j$ (as σ is a permutation) and so σ is the identity permutation. Thus the coefficient of X^{n-1} is nonzero in $(X\delta_{1\sigma(1)} - a_{1\sigma(1)}) \ldots (X\delta_{n\sigma(n)} - a_{n\sigma(n)})$ if and only if σ is the identity permutation, in which case this coefficient equals $-\sum_{j=1}^{n} a_{jj} = -\mathrm{Tr}(A)$. This shows that the coefficient of X^{n-1} in $\chi_A(X)$ is $-\mathrm{Tr}(A)$. □

Problem 8.38. Let $A \in M_n(F)$ be a nilpotent matrix.

a) Prove that

$$\chi_A(X) = X^n.$$

b) Prove that $\mathrm{Tr}(A^k) = 0$ for all $k \geq 1$.

Solution. a) Note that by definition there is a positive integer k such that $A^k = O_n$. Then

$$X^k I_n = X^k I_n - A^k = (XI_n - A)(X^{k-1} I_n + X^{k-2} A + \ldots + A^{k-1}).$$

Taking determinants yields

$$X^{nk} = \chi_A(X) \cdot \det(X^{k-1} I_n + \ldots + A^{k-1}).$$

The right-hand side is the product of two polynomials (again by the polynomial nature of the determinant). We deduce that $\chi_A(X)$ divides the monomial X^{nk}. Since moreover $\chi_A(X)$ is monic of degree n (by Problem 8.37), it follows that $\chi_A(X) = X^n$.

b) Replacing A with A^k (which is also nilpotent), we may assume that $k = 1$. We need to prove that $\mathrm{Tr}(A) = 0$. But by part a) $\chi_A(X) = X^n$, thus the coefficient of X^{n-1} in $\chi_A(X)$ is 0. By the previous problem, this coefficient equals $-\mathrm{Tr}(A)$, thus $\mathrm{Tr}(A) = 0$. □

The following computation will play a fundamental role in the next section, which deals with the Cayley–Hamilton theorem. It also shows that any monic polynomial of degree n with coefficients in F is the characteristic polynomial of some matrix in $M_n(F)$.

Problem 8.39. Let $a_0, a_1, \ldots, a_{n-1} \in F$ and let

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \end{bmatrix}.$$

Prove that

$$\chi_A = X^n - a_{n-1}X^{n-1} - \ldots - a_0.$$

Solution. Let $P = X^n - a_{n-1}X^{n-1} - \ldots - a_1X - a_0$. Consider the matrix

$$B = XI_n - A = \begin{bmatrix} X & 0 & 0 & \ldots & 0 & -a_0 \\ -1 & X & 0 & \ldots & 0 & -a_1 \\ 0 & -1 & X & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ 0 & 0 & 0 & \ldots & -1 & X - a_{n-1} \end{bmatrix}.$$

Adding to the first row of B the second row multiplied by X, the third row multiplied by X^2,..., the nth row multiplied by X^{n-1} we obtain the matrix

$$C = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & P \\ -1 & X & 0 & \ldots & 0 & -a_1 \\ 0 & -1 & X & \ldots & 0 & -a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \\ 0 & 0 & 0 & \ldots & -1 & X - a_{n-1} \end{bmatrix}.$$

We have $\chi_A = \det B = \det C$ and, expanding $\det C$ with respect to the first row, we obtain

$$\det C = (-1)^{n+1}P \cdot \begin{vmatrix} -1 & X & \ldots & 0 \\ 0 & -1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 \end{vmatrix} = (-1)^{n+1}P(-1)^{n-1} = P,$$

observing that the matrix whose determinant we need to evaluate is upper-triangular with diagonal entries -1. The result follows. □

Recall that two matrices $A, B \in M_n(F)$ are called similar if they represent the same linear transformation of F^n in possibly different bases of this F-vector space. Equivalently, A and B are similar if there is $P \in \mathrm{GL}_n(F)$ such that $B = PAP^{-1}$, i.e., they are conjugated by an invertible matrix. A fundamental property is that **the characteristic polynomial is invariant under similarity of matrices**. More precisely:

Theorem 8.40. *Two similar matrices have the same characteristic polynomial.*

Proof. Suppose that A and B are similar, thus we can find an invertible matrix $P \in M_n(F)$ such that $B = PAP^{-1}$. Note that

$$XI_n - B = XPP^{-1} - PAP^{-1} = P(XI_n - A)P^{-1}.$$

Now, we will take for granted that the determinant is still defined and multiplicative for matrices with entries in $F[X]$ (recall that $F[X]$ is the set of polynomials in one variable with coefficients in F). The existence is easy, since one can simply define in the usual way

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

for a matrix $A = [a_{ij}]$ with entries in $F[X]$. The fact that the determinant is multiplicative is trickier (the hardest case being the case when F is a finite field) and we will take it for granted.

Consider then $P, XI_n - A, XI_n - B$ as matrices with entries in $F[X]$. The inverse of P in $M_n(F)$ is also an inverse of P in $M_n(F[X])$, thus P is invertible considered as a matrix in $M_n(F[X])$. The multiplicative character of the determinant map yields

$$\chi_B(X) = \det(XI_n - B) = \det(P) \cdot \det(XI_n - A) \cdot \det(P)^{-1}$$

$$= \det(XI_n - A) = \chi_A(X),$$

as desired. □

Problem 8.41. Prove that if $A, B \in M_n(F)$, then AB and BA have the same characteristic polynomial. You may assume for simplicity that $F = \mathbf{R}$ or $F = \mathbf{C}$.

Solution. If A is invertible, then AB and BA are similar, as

$$AB = ABAA^{-1} = A(BA)A^{-1}.$$

The previous theorem yields the result in this case.

Suppose now that A is not invertible. As A has only finitely many eigenvalues (Corollary 8.21) and since F is infinite, there are infinitely many $\lambda \in F$ such that $A_\lambda := \lambda \cdot I_n - A$ is invertible. By the first paragraph for all such λ we have

$$\det(A_\lambda B) = \det(BA_\lambda).$$

This can be written as

$$\det(\lambda B - AB) = \det(\lambda B - BA).$$

Both sides are polynomials in λ. Since they agree on infinitely many values of λ, these polynomials are equal. In particular, they agree on $\lambda = 0$, which is exactly the desired result. □

Remark 8.42. The previous proof crucially uses the fact that F is infinite. The same result is true if $F = \mathbf{F}_2$ (or more generally any field), but the proof requires more tools from algebra.

The previous theorem shows that the following definition makes sense.

Definition 8.43. Let V be a finite dimensional F-vector space. The **characteristic polynomial** χ_T of the linear transformation T of V is the characteristic polynomial of the matrix of T in any basis.

Problem 8.44. Let $T : \mathbf{R}^3 \to \mathbf{R}^3$ be the linear transformation defined by

$$T(x_1, x_2, x_3) = (x_1 - 2x_2 + x_3, x_2 - x_3, x_1).$$

Compute the characteristic polynomial of T.

Solution. The matrix of T with respect to the canonical basis is

$$A = \begin{bmatrix} 1 & -2 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Thus

$$\chi_T(X) = \chi_A(X) = \begin{vmatrix} X-1 & 2 & -1 \\ 0 & X-1 & 1 \\ -1 & 0 & X \end{vmatrix} =$$

$$(X-1)\begin{vmatrix} X-1 & 1 \\ 0 & X \end{vmatrix} - \begin{vmatrix} 2 & -1 \\ X-1 & 1 \end{vmatrix} = X^3 - 2X^2 - 1.$$

□

Problem 8.45. Let $T : V \to V$ be a linear transformation on a finite dimensional vector space and let W be a subspace of V which is stable under T. Let T_1 be the restriction of T to W. Prove that χ_{T_1} divides χ_T.

Solution. Choose a basis $w_1, \ldots, w_k$ of W and complete it to a basis $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$ of V. Since W is stable under T the matrix of T with respect to the basis $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$ is of the form $\begin{bmatrix} A & * \\ 0 & B \end{bmatrix}$, where $A \in M_k(F)$ is the matrix of T_1 with respect to $w_1, \ldots, w_k$. Using properties of block-determinants (more precisely Theorem 7.43) we obtain

$$\chi_T(X) = \chi_A(X) \cdot \chi_B(X)$$

and the result follows. □

The previous problem allows us to make the precise link between characteristic polynomial and eigenspaces: by construction the eigenvalues of a matrix can be recovered as the roots in F of the characteristic polynomial, but it is not clear how to deal with their possible multiplicities. Actually, there are two different (and important) notions of multiplicity:

Definition 8.46. Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V over F and let $\lambda \in F$ be an eigenvalue of T.

a) The **geometric multiplicity** of λ is the dimension of the F-vector space $\mathrm{Ker}(\lambda \cdot \mathrm{id} - T)$.
b) The **algebraic multiplicity** of λ is the multiplicity of λ as a root of the characteristic polynomial χ_T of T (i.e., the largest integer j such that $(X - \lambda)^j$ divides $\chi_T(X)$).

Of course, we have similar definitions for the multiplicities of an eigenvalue of a matrix: if $A \in M_n(F)$ and $\lambda \in F$ is an eigenvalue of A, the algebraic multiplicity of λ is the multiplicity of λ as a root of χ_A, while the geometric multiplicity of λ is $\dim \mathrm{Ker}(\lambda I_n - A)$. A good exercise for the reader is to convince himself that if A is the matrix of a linear transformation T with respect to any basis of V, then the corresponding multiplicities of λ for A and for T are the same.

Remark 8.47. The algebraic multiplicity and the geometric multiplicity are not always equal: consider the matrix $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. It has 0 as an eigenvalue with geometric multiplicity 1: indeed the system $AX = 0$ is equivalent to $x_2 = 0$, thus $\mathrm{Ker}(A)$ is the line spanned by the first vector of the canonical basis of F^2. On the other hand, the characteristic polynomial of A is $\chi_A(X) = X^2$, thus the algebraic multiplicity of 0 is 2. If the algebraic multiplicity of an eigenvalue λ coincides with its geometric multiplicity, we will simply refer to this common value as the multiplicity of λ.

Problem 8.48. Consider the matrix

$$A = \begin{bmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{bmatrix} \in M_3(\mathbf{R}).$$

a) Find the characteristic polynomial and the eigenvalues of A.
b) For each eigenvalue λ of A, find the algebraic and the geometric multiplicity of λ.

Solution. a) Adding the second and third column to the first one yields

$$\chi_A(X) = \begin{vmatrix} X-8 & 1 & 5 \\ 2 & X-3 & -1 \\ -4 & 1 & X+1 \end{vmatrix} = \begin{vmatrix} X-2 & 1 & 5 \\ X-2 & X-3 & -1 \\ X-2 & 1 & X+1 \end{vmatrix}$$

$$= (X-2) \begin{vmatrix} 1 & 1 & 5 \\ 1 & X-3 & -1 \\ 1 & 1 & X+1 \end{vmatrix}.$$

To compute the last determinant, subtract the first row from the second and the third row, then expand with respect to the first column. We obtain in the end

$$\chi_A(X) = (X-2)(X-4)^2.$$

The eigenvalues of A are the real roots of χ_A, thus they are 2 and 4.

b) Since $\chi_A(X) = (X-2)(X-4)^2$, it follows that 2 has algebraic multiplicity 1 and 4 has algebraic multiplicity 2. To find the geometric multiplicity of 2, we determine the 2-eigenspace by solving the system $AX = 2X$. The reader will check without difficulty that the system is equivalent to $x = y = z$ (where x, y, z are the coordinates of X), thus the 2-eigenspace is one-dimensional and the geometric multiplicity of the eigenvalue 2 is 1 (we could have done this without any computation if we knew the theorem below). For the eigenvalue 4, we proceed similarly by solving the system $AX = 4X$. An easy computation shows that the system is equivalent to $y = -x$ and $z = x$, thus the 4-eigenspace is also one-dimensional and so the geometric multiplicity of the eigenvalue 4 is also 1. □

As we have already seen, algebraic multiplicity and geometric multiplicity are not the same thing. The next result gives however precious information concerning the link between the two notions.

Theorem 8.49. *Let $A \in M_n(F)$ and let $\lambda \in F$ be an eigenvalue of A. Then the geometric multiplicity of λ does not exceed its algebraic multiplicity. In particular, if the algebraic multiplicity of λ is* 1*, then its geometric multiplicity equals* 1.

Proof. Let $V = F^n$ and let T be the linear map on V attached to A. Let $W = \ker(\lambda I_n - A) = \ker(\lambda \mathrm{id} - T)$. Then W is stable under T, thus by Problem 8.45 (and letting $T|_W$ be the restriction of T to W) $\chi_{T|_W}$ divides χ_T. On the other hand, $T|_W$ is simply multiplication by λ on W, thus

$$\chi_{T|_W}(X) = (X-\lambda)^{\dim W}.$$

It follows that $(X-\lambda)^{\dim W}$ divides $\chi_A(X) = \chi_T(X)$ and the result follows. □

The result established in the next problem is very important in applications:

Problem 8.50. Let $A \in M_n(\mathbf{C})$ be a matrix with **complex** entries. Let $\mathrm{Sp}(A)$ be the set of eigenvalues of A (we call $\mathrm{Sp}(A)$ the **spectrum** of A) and, for $\lambda \in \mathrm{Sp}(A)$, let m_λ be the algebraic multiplicity of λ.

a) Explain the equality of polynomials

$$\chi_A(X) = \prod_{\lambda \in \mathrm{Sp}(A)} (X-\lambda)^{m_\lambda}.$$

b) Prove that

$$\mathrm{Tr}(A) = \sum_{\lambda \in \mathrm{Sp}(A)} m_\lambda \lambda.$$

In other words, **the trace of a complex matrix is the sum of its eigenvalues, counted with their algebraic multiplicities.**

c) Prove that

$$\det A = \prod_{\lambda \in \mathrm{Sp}(A)} \lambda^{m_\lambda},$$

that is **the determinant of a matrix is the product of its eigenvalues, counted with their algebraic multiplicities.** □

Solution. a) It is clear by definition of algebraic multiplicities that $\prod_{\lambda \in \mathrm{Sp}(A)} (X - \lambda)^{m_\lambda}$ divides $\chi_A(X)$ (this holds for a matrix with coefficients in any field). To prove the opposite divisibility (which allows us to conclude since both polynomials are monic), we will crucially exploit the fact that the matrix has complex entries and that $\mathbf{C}$ is algebraically closed. In particular, we know that χ_A splits in $\mathbf{C}[X]$ into a product of linear factors $X - z$. Any such z is an eigenvalue of A, since $\det(zI_n - A) = 0$. Hence $z \in \mathrm{Sp}(A)$ and by definition its multiplicity as root of $\chi_A(X)$ is m_z. The result follows.

b) The coefficient of X^{n-1} in $\prod_{\lambda \in \mathrm{Sp}(A)} (X - \lambda)^{m_\lambda}$ is $-\sum_{\lambda \in \mathrm{Sp}(A)} m_\lambda \lambda$. On the other hand, the coefficient of X^{n-1} in χ_A equals $-\mathrm{Tr}(A)$ by Problem 8.37. The result follows from a).

c) Taking $X = 0$ in the equality established in a) and using the fact that $\chi_A(0) = (-1)^n \det A$ and that $\sum_{\lambda \in \mathrm{Sp}(A)} m_\lambda = n$, we obtain

$$(-1)^n \det A = \chi_A(0) = \prod_{\lambda \in \mathrm{Sp}(A)} (-\lambda)^{m_\lambda} = (-1)^n \prod_{\lambda \in \mathrm{Sp}(A)} \lambda^{m_\lambda}.$$

The result follows by dividing by $(-1)^n$. □

Remark 8.51. If we replace $\mathbf{C}$ with $\mathbf{R}$ or $\mathbf{Q}$ the result is completely false: it may even happen that $\mathrm{Sp}(A)$ is empty! Indeed, consider for instance the matrix $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Here is a nice application of the previous problem.

Problem 8.52. a) Let $A \in M_n(\mathbf{R})$ be a matrix such that

$$A^2 - 3A + 2I_n = 0.$$

Prove that $\det A \in \{1, 2, 4, \ldots, 2^n\}$.

b) Let $k \in \{1, 2, 4, \ldots, 2^n\}$. Construct a matrix $A \in M_n(\mathbf{R})$ such that $A^2 - 3A + 2I_n = 0$ and $\det A = k$.

Solution. a) By Problem 8.27 for any complex eigenvalue λ of A we have $\lambda^2 - 3\lambda + 2 = 0$, that is $(\lambda - 1)(\lambda - 2) = 0$. It follows that each complex eigenvalue of A is either 1 or 2. Since $\det A$ is the product of all complex eigenvalues of A (counted with their algebraic multiplicities), the result follows.

b) Write $k = 2^p$ with $p \in \{0, 1, \ldots, n\}$. Then a diagonal matrix A having p diagonal entries equal to 2 and the other diagonal entries equal to 1 is a solution of the problem. □

8.4.1 Problems for Practice

1. Find the characteristic polynomial and the eigenvalues of the matrix

$$A = \begin{bmatrix} 3 & 0 & -1 \\ 2 & 4 & 2 \\ -1 & 0 & 3 \end{bmatrix} \in M_3(\mathbf{R}).$$

2. Find the characteristic polynomial and the eigenvalues of the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \in M_4(\mathbf{F}_2).$$

3. a) Give an example of a matrix $A \in M_4(\mathbf{R})$ whose characteristic polynomial equals $X^4 - X^3 + 1$.
   b) Is there a matrix $A \in M_3(\mathbf{Q})$ whose characteristic polynomial equals $X^3 - \sqrt{2}$? Give an example of such a matrix in $M_3(\mathbf{R})$.
4. For each of the matrices below, compute its characteristic and minimal polynomial

   a)

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

   b)

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

Then find their eigenvalues and the corresponding eigenspaces, by considering these matrices as matrices with rational entries. Then do the same by considering these matrices as matrices with real (and finally with complex) entries.

5. Let $n \geq 2$ and let

$$A = \begin{bmatrix} 1 & 2 & 2 & \dots & 2 & 2 \\ 2 & 1 & 2 & \dots & 2 & 2 \\ 2 & 2 & 1 & \dots & 2 & 2 \\ \dots & \dots & \dots & \dots & \dots & \\ 2 & 2 & 2 & \dots & 2 & 1 \end{bmatrix} \in M_n(\mathbf{R}).$$

   a) Compute the minimal polynomial and the characteristic polynomial of A.
   b) Describe the eigenvalues of A and the corresponding eigenspaces.

6. a) Let $A \in M_n(\mathbf{R})$ be the matrix associated with the projection of $\mathbf{R}^n$ onto a subspace W along a complementary subspace of W. Compute the characteristic polynomial of A in terms of n and $\dim W$.
   b) Answer the same question assuming that A is the matrix associated with the symmetry with respect to a subspace W along a complementary subspace of W.

7. Consider the following three 5×5 nilpotent matrices

$$A = \begin{bmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{bmatrix}, \; B = \begin{bmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \end{bmatrix}, \; C = \begin{bmatrix} 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&1 \\ 0&0&0&0&0 \end{bmatrix}.$$

   Since these matrices are nilpotent they all have characteristic polynomial $\chi_A(X) = \chi_B(X) = \chi_C(X) = X^5$.

   a) Compute the minimal polynomials of these matrices and use them to show that A is not similar to either B or C.
   b) Compute the dimensions of the kernels of these matrices and use them to show that B is not similar to A or C.

8. Let $A \in M_n(\mathbf{R})$ be a matrix such that $A^3 + I_n = 0$. Prove that $\mathrm{Tr}(A)$ is an integer.
9. Prove that any matrix $A \in M_n(\mathbf{R})$ is the sum of two invertible matrices.
10. Let $A \in M_n(\mathbf{C})$ be an invertible matrix. Prove that for all $x \neq 0$ we have

$$\chi_{A^{-1}}(x) = \frac{x^n}{\chi_A(0)} \chi_A(1/x).$$

11. Let $A = [a_{ij}] \in M_n(\mathbf{C})$ and let $\overline{A} = [\overline{a_{ij}}]$ be the matrix whose entries are the complex-conjugates of the entries of A. Prove that the characteristic polynomial of $A\overline{A}$ has real coefficients. Hint: use the fact that $A\overline{A}$ and $\overline{A}A$ have the same characteristic polynomial.
12. Let $A \in M_{n,p}(\mathbf{C})$ and $B \in M_{p,n}(\mathbf{C})$.

    a) Prove the following identities for $x \in \mathbf{C}$

$$\begin{bmatrix} xI_n & A \\ B & I_p \end{bmatrix} \cdot \begin{bmatrix} I_n & O_{n,p} \\ -B & I_p \end{bmatrix} = \begin{bmatrix} xI_n - AB & A \\ O_{p,n} & I_p \end{bmatrix}$$

    and

$$\begin{bmatrix} I_n & O_{n,p} \\ -B & xI_p \end{bmatrix} \cdot \begin{bmatrix} xI_n & A \\ B & I_p \end{bmatrix} = \begin{bmatrix} xI_n & A \\ O_{p,n} & xI_p - BA \end{bmatrix}.$$

    b) Deduce that

$$X^q \chi_{AB}(X) = X^p \chi_{BA}(X).$$

13. Let A and B be matrices in $M_3(\mathbf{C})$. Show that

$$\det(AB - BA) = \frac{1}{3}\mathrm{Tr}[(AB - BA)^3].$$

    Hint: if a, b, c are the eigenvalues of $AB - BA$, prove that $a + b + c = 0$ and then that

$$a^3 + b^3 + c^3 = 3abc.$$

14. Prove that for all $A, B \in M_n(\mathbf{C})$

$$\deg(\det(XA + B)) \leq \mathrm{rank}(A).$$

    Hint: if r is the rank of A, start by reducing the problem to the case $A = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \in M_n(\mathbf{C})$.
15. Let A, B, C and D be square matrices in $M_n(\mathbf{C})$ and let

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in M_{2n}(\mathbf{C}).$$

    a) Assume that $DC = CD$ and that D is invertible. Check the identity

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} D & O_n \\ -C & I_n \end{bmatrix} = \begin{bmatrix} AD - BC & B \\ O_n & D \end{bmatrix}$$

and deduce that

$$\det M = \det(AD - BC).$$

b) Assume that $DC = CD$, but not necessarily that D is invertible. Prove that

$$\det M = \det(AD - BC).$$

Hint: consider the matrix $D_x = xI_n + D$ with $x \in \mathbf{C}$.

c) By considering the matrices

$$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

prove that the result in part b) no longer holds if we drop the hypothesis $CD = DC$.

16. a) Find two matrices $A, B \in M_4(\mathbf{R})$ with the same characteristic and minimal polynomial, but which are not similar.
    b) Can we find two such matrices in $M_2(\mathbf{R})$?
17. Let $A = [a_{ij}] \in M_n(\mathbf{C})$ and let s_k be the sum of all $k \times k$ principal minors of A (thus s_1 is the sum of the diagonal entries of A, that is $\mathrm{Tr}(A)$, while s_n is $\det A$). Prove that

$$\chi_A(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \ldots + (-1)^n s_n.$$

Hint: use the multilinear character of the determinant map.

18. Let $V = M_n(\mathbf{R})$ and consider the linear transformation $T : V \to V$ defined by

$$T(A) = -A + \mathrm{Tr}(A) \cdot I_n.$$

a) Prove that V is the direct sum of the eigenspaces of T.
b) Compute the characteristic polynomial of T.

19. Let $V = M_n(\mathbf{R})$ and consider the linear transformation $T : V \to V$ sending A to ${}^t A$. Find the characteristic polynomial of T. Hint: what is $T \circ T$?

8.5 The Cayley–Hamilton Theorem

We now reach a truly beautiful result: **any matrix is killed by its characteristic polynomial**. Recall that χ_A denotes the characteristic polynomial of $A \in M_n(F)$.

Theorem 8.53 (Cayley–Hamilton). *For all matrices $A \in M_n(F)$ we have*

$$\chi_A(A) = O_n.$$

In other words, if $\chi_A(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, then

$$A^n + a_{n-1}A^{n-1} + \ldots + a_1 A + a_0 I_n = O_n.$$

There are quite a few (at least 30...) different proofs of this result, neither of them being straightforward. The reader should therefore start by finding the error in the following classical, but unfortunately wrong argument: since $\chi_A(X) = \det(XI_n - A)$, we have

$$\chi_A(A) = \det(AI_n - A) = \det(A - A) = \det(O_n) = 0.$$

Before moving to the rather technical proofs of the previous theorem, we take a break and focus on some applications:

Problem 8.54. Let $A \in M_n(F)$. Prove that the minimal polynomial of A divides the characteristic polynomial of A.

Solution. Since χ_A annihilates A by the Cayley–Hamilton theorem, it follows that μ_A divides χ_A.

□

Problem 8.55. Let $A \in M_n(F)$ be an invertible matrix. Prove that there are scalars $a_0, \ldots, a_{n-1} \in F$ such that

$$A^{-1} = a_0 I_n + a_1 A + \ldots + a_{n-1}A^{n-1}.$$

Solution. The characteristic polynomial of A is of the form $X^n + b_{n-1}X^{n-1} + \ldots + b_1 X + b_0$, with $b_0 = (-1)^n \det A$ nonzero. By the Cayley–Hamilton theorem

$$A^n + b_{n-1}A^{n-1} + \ldots + b_1 A + b_0 I_n = O_n.$$

Multiplying by $\frac{1}{b_0}A^{-1}$ we obtain

$$\frac{1}{b_0}A^{n-1} + \frac{b_{n-1}}{b_0}A^{n-2} + \ldots + \frac{b_1}{b_0}I_n + A^{-1} = O_n.$$

Thus we can take

$$a_0 = -\frac{b_1}{b_0}, \quad a_1 = -\frac{b_2}{b_0}, \ldots, \quad a_{n-1} = -\frac{1}{b_0}.$$

□

Problem 8.56. Let $A \in M_n(\mathbf{C})$ be a matrix. Prove that the following statements are equivalent:

a) A is nilpotent (recall that this means that $A^k = O_n$ for some $k \geq 1$).
b) The characteristic polynomial of A is X^n.
c) $A^n = O_n$.
d) The minimal polynomial of A is of the form X^k for some $k \geq 1$.

Solution. The fact that a) implies b) follows directly from part a) of Problem 8.38. That b) implies c) is a direct consequence of the Cayley–Hamilton theorem. If c) holds, then X^n kills A, thus the minimal polynomial of A divides X^n and is monic, thus necessarily of the form X^k for some $k \geq 1$, proving that c) implies d). Finally, since the monic polynomial of A kills A, it is clear that d) implies a). □

We will give two proofs of the Cayley–Hamilton theorem in this section. Neither of them really explains clearly what is happening (the second one does a much better job than the first proof from this point of view), but with the technology we have developed so far, we cannot do any better. We will see later on a much better proof,[1] which reduces (via a subtle but very useful density argument) the theorem to the case of diagonal matrices (which is immediate).

Let us give now the first proof of the Cayley–Hamilton theorem. Let $A \in M_n(F)$ and let $B = XI_n - A \in M_n(K)$, where $K = F(X)$ is the field of rational fractions[2] in the variable X, with coefficients in F. Consider the adjugate matrix $C = \text{adj}(B)$ of B. Its entries are given by determinants of $(n-1) \times (n-1)$-matrices whose entries are polynomials of degree ≤ 1 in X. Thus each entry of C is a polynomial of degree at most $n-1$ in X, with coefficients in F. Let

$$c_{ij} = c_{ij}^{(0)} + c_{ij}^{(1)} X + \ldots + c_{ij}^{(n-1)} X^{n-1}$$

be the (i, j)-entry of C, with $c_{ij}^{(0)}, \ldots, c_{ij}^{(n-1)} \in F$. Let $C^{(k)}$ be the matrix whose entries are the $c_{ij}^{(k)}$. Then

$$C = C^{(0)} + C^{(1)} X + \ldots + C^{(n-1)} X^{n-1}.$$

Next, recall that

$$B \cdot C = B \cdot \text{adj}(B) = \det B \cdot I_n = \chi_A(X) \cdot I_n.$$

Thus we have

$$(XI_n - A) \cdot (C^{(0)} + C^{(1)} X + \ldots + C^{(n-1)} X^{n-1}) = \chi_A(X) \cdot I_n.$$

[1] Which unfortunately works only when $F \subset \mathbf{C}$, even though one can actually deduce the theorem from this case.

[2] An element of K is a quotient $\frac{A}{B}$, where $A, B \in F[X]$ and $B \neq 0$.

Writing $\chi_A(X) = X^n + u_{n-1}X^{n-1} + \ldots + u_0 \in F[X]$, the previous equality becomes

$$-AC^{(0)} + (C^{(0)} - AC^{(1)})X + (C^{(1)} - AC^{(2)})X + \ldots + (C^{(n-2)} - AC^{(n-1)})X^{n-1}$$

$$+C^{(n-1)}X^n = u_0 I_n + u_1 I_n X + \ldots + u_{n-1} I_n X^{n-1} + I_n X^n.$$

Identifying coefficients yields

$$-AC^{(0)} = u_0 I_n, \quad C^{(0)} - AC^{(1)} = u_1 I_n, \ldots,$$

$$C^{(n-2)} - AC^{(n-1)} = u_{n-1} I_n, \quad C^{(n-1)} = I_n.$$

Dealing with these relations by starting with the last one and working backwards yields

$$C^{(n-1)} = I_n, \quad C^{(n-2)} = A + u_{n-1} I_n, \quad C^{(n-3)} = A^2 + u_{n-1} A + u_{n-2} I_n$$

and an easy induction gives

$$C^{(n-j-1)} = A^j + u_{n-1} A^{j-1} + \ldots + u_{n-j} I_n.$$

In particular

$$C^{(0)} = A^{n-1} + u_{n-1} A^{n-2} + \ldots + u_1 I_n.$$

Combining this with the relation $-AC^{(0)} = u_0 I_n$ finally yields

$$A^n + u_{n-1} A^{n-1} + \ldots + u_0 I_n = O_n,$$

that is $\chi_A(A) = O_n$.

As the reader can easily observe, though rather long, the proof is fairly elementary and based on very simple manipulations. It is not very satisfactory however, since it does not really show **why** the theorem holds.

We turn now to the second proof of the Cayley–Hamilton theorem. We will actually prove the following result, which is clearly equivalent (via the choice of a basis) to the Cayley–Hamilton theorem.

Theorem 8.57. *Let V be a finite dimensional vector space over F and let $T : V \to V$ be a linear map. Then $\chi_T(T) = 0$.*

Proof. The idea is to reduce the problem to linear maps for which we can compute easily χ_T. The details are a little bit more complicated than this might suggest...

Fix an $x \in V$. If m is a nonnegative integer, let

$$W_m = \mathrm{Span}(T^0(x), T^1(x), \ldots, T^m(x)).$$

Note that $W_0 \subset W_1 \subset \ldots \subset V$ and that $\dim W_m \leq \dim W_{m+1} \leq \dim V$ for all $m \geq 0$. Hence there must be some least m such that $\dim W_{m-1} = \dim W_m$. Since $W_{m-1} = W_m$, we must have $W_{m-1} = W_m$, in other words $T^m(x)$ lies in the subspace W_{m-1} and we can write $T^m(x)$ as a linear combination of $T^k(x)$ for $0 \leq k < m$, say

$$T^m(x) = \sum_{k=0}^{m-1} a_k T^k(x).$$

Note that this implies W_{m-1} is stable under T. Since m is minimal, the vectors $T^0(x), \ldots, T^{m-1}(x)$ must be linearly independent (a linear dependence among them would express a lower iterate as a linear combination of earlier iterates). Therefore they are a basis of W_{m-1} and with respect to this basis the matrix of $T_1 = T|_{W_{m-1}}$ is

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix}.$$

The characteristic polynomial of this matrix was computed in Problem 8.39 and it equals $X^m - a_{m-1}X^{m-1} - \cdots - a_0$. Hence

$$\chi_{T_1}(T)(x) = T^m(x) - \sum_{k=0}^{m-1} a_k T^k(x) = 0.$$

By Problem 8.45, since W_{m-1} is T-stable, the characteristic polynomial χ_{T_1} of T restricted to W_{m-1} divides χ_T. Therefore $\chi_T(T)(x) = 0$. Since x was arbitrary, we conclude that $\chi_T(T)$ vanishes when applied to any vector, that is, it is the zero linear map. □

8.5.1 Problems for Practice

1. Prove that for any $A = [a_{ij}] \in M_3(\mathbf{C})$ we have

$$A^3 - \mathrm{Tr}(A) \cdot A^2 + \mathrm{Tr}(\mathrm{adjA}) \cdot \mathrm{A} - \det \mathrm{A} \cdot \mathrm{I}_3 = 0.$$

2. Let $A \in M_3(\mathbf{R})$ be a matrix such that

$$\mathrm{Tr}(A) = \mathrm{Tr}(A^2) = 0.$$

Prove that $A^3 = \alpha I_3$ for some real number α.

3. Let $A, B \in M_3(\mathbf{C})$ be matrices such that the traces of AB and $(AB)^2$ are both 0. Prove that $(AB)^3 = (BA)^3$.
4. Let $A, B, C \in M_n(\mathbf{C})$ be matrices such that $AC = CB$ and $C \neq O_n$.

   a) Prove that for all polynomials $P \in \mathbf{C}[T]$ we have

   $$P(A)C = CP(B).$$

   b) By choosing a suitable polynomial P and using the Cayley–Hamilton theorem, deduce that A and B have a common eigenvalue.

5. Let $A, B \in M_n(\mathbf{C})$ be matrices such that $(AB)^n = O_n$. Prove that $(BA)^n = O_n$. Hint: prove first that $(BA)^{n+1} = O_n$, then use Problem 8.56.
6. Let $A \in M_n(\mathbf{C})$ be a matrix such that A and $3A$ are similar. Prove that $A^n = O_n$. Hint: similar matrices have the same characteristic polynomial. Also use Problem 8.56.
7. Let $A \in M_n(\mathbf{C})$. Prove that $A^n = O_n$ if and only if $\operatorname{Tr}(A^k) = 0$ for all $k \geq 1$. Hint: to establish the harder direction, prove that all eigenvalues of A must be 0 and use Problem 8.56.
8. Let V be a vector space of dimension n over a field F and let $T : V \to V$ be a linear transformation. The goal of this problem is to prove that the following assertions are equivalent:

   i) There exists a vector $x \in V$ such that $x, T(x), \ldots, T^{n-1}(x)$ forms a basis of V.
   ii) The minimal polynomial and the characteristic polynomial of T coincide.

   a) Assume that i) holds. Use Problem 8.14 to prove that $\deg \mu_T \geq n$ and conclude that ii) holds using the Cayley–Hamilton theorem.
   b) Assume that ii) holds. Using Problems 8.13 and 8.14, explain why we can find $x \in V$ such that $x, T(x), T^2(x), \ldots$ span V. Conclude that i) holds.

9. Let $n \geq 1$ and let $A, B \in M_n(\mathbf{Z})$ be matrices with integer entries. Suppose that $\det A$ and $\det B$ are relatively prime. Prove that we can find matrices $U, V \in M_n(\mathbf{Z})$ such that $AU + BV = I_n$.

Chapter 9
Diagonalizability

Abstract The main focus is on diagonalizable matrices, that is matrices similar to a diagonal one. We completely characterize these matrices and use this to complete the proof of Jordan's classification theorem for arbitrary matrices with complex entries. Along the way, we prove that diagonalizable matrices with complex entries are dense and use this to give a clean proof of the Cayley–Hamilton theorem.

Keywords Diagonalizable • Trigonalizable • Jordan block • Jordan's classification

In this chapter we will apply the results obtained in the previous chapter to study matrices which are as close as possible to diagonal ones. The diagonal matrices are fairly easy to understand and so are matrices similar to diagonal matrices. These are called diagonalizable matrices and play a fundamental role in linear algebra. For instance, we will prove that diagonalizable matrices form a dense subset of $M_n(\mathbf{C})$ (i.e., any matrix in $M_n(\mathbf{C})$ can be approximated to arbitrary precision with a diagonalizable matrix) and we will use this result to give a very simple proof of the Cayley–Hamilton theorem over $\mathbf{C}$, by reducing it to the case of diagonal matrices (which is trivial). Also, we will prove that any matrix $A \in M_n(\mathbf{C})$ is the commuting sum of a nilpotent and of a diagonalizable matrix, showing once more the importance of diagonalizable (and nilpotent) matrices. We then use the classification of nilpotent matrices obtained in the chapter concerned with duality to prove the general form of Jordan's theorem, classifying **all** matrices in $M_n(\mathbf{C})$ up to similarity. Along the way, we give applications to the resolution of linear differential equations (of any order) with constant coefficients, as well as to linear recurrence sequences.

A large part of the chapter is devoted to finding intrinsic properties and characterizations of diagonalizable matrices. In this chapter F will be a field, but the reader will not loose anything by assuming that F is either $\mathbf{R}$ or $\mathbf{C}$.

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_9

9.1 Upper-Triangular Matrices, Once Again

Recall that a matrix $A = [a_{ij}] \in M_n(F)$ is called upper-triangular if $a_{ij} = 0$ whenever $i > j$, that is all entries of A below the main diagonal are zero. We have already established quite a few results about upper-triangular matrices, which make this class of matrices rather easy to understand. For instance, we have already seen that the upper-triangular matrices form a vector subspace of $M_n(F)$ which is closed under multiplication. Moreover, it is easy to compute the eigenvalues of an upper-triangular matrix: simply look at the diagonal entries! It is therefore easy to compute the characteristic polynomial of such a matrix: if $A = [a_{ij}]$ is an upper-triangular matrix, then its characteristic polynomial

$$\chi_A(X) = \prod_{i=1}^{n}(X - a_{ii}).$$

Before dealing with diagonalizable matrices, we will focus on the **trigonalizable** ones, i.e., matrices $A \in M_n(F)$ which are similar to an upper-triangular matrix. We will need an important definition:

Definition 9.1. A polynomial $P \in F[X]$ is **split over** F if it is of the form

$$P(X) = c(X - a_1)\dots(X - a_n)$$

for some scalars $c, a_1, \dots, a_n \in F$ (not necessarily distinct).

For instance, $X^2 + 1$ is not split over $\mathbf{R}$ since it has no real root, but it is split over $\mathbf{C}$, since $X^2+1 = (X+i)(X-i)$. On the other hand, the polynomial X^2-3X+2 is split over $\mathbf{R}$, since it factors as $(X-1)(X-2)$. It is pointless to look for a polynomial in $\mathbf{C}[X]$ which is not split, due to the following amazing theorem of Gauss:

Theorem 9.2 (The Fundamental Theorem of Algebra). *Any polynomial $P \in \mathbf{C}[X]$ is split over $\mathbf{C}$.*

This theorem is usually stated as: $\mathbf{C}$ is an algebraically closed field, that is any nonconstant polynomial equation with complex coefficients has at least one complex solution. The previous theorem is actually equivalent to this usual version of Gauss' theorem (and it is a good exercise for the reader to prove the equivalence of these two statements).

By the previous discussion, the characteristic polynomial of an upper-triangular matrix is split over F. Since the characteristic polynomials of two similar matrices are equal, we deduce that the characteristic polynomial of any trigonalizable matrix is split over F.

Problem 9.3. Give an example of a matrix $A \in M_2(\mathbf{R})$ which is not trigonalizable in $M_2(\mathbf{R})$.

Solution. Since the characteristic polynomial of a trigonalizable matrix is split over $\mathbf{R}$, it suffices to find a matrix $A \in M_2(\mathbf{R})$ whose characteristic polynomial is not split over $\mathbf{R}$. Consider the matrix

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

Its characteristic polynomial is $X^2 + 1$, which is not split over $\mathbf{R}$. Thus A is not trigonalizable in $M_2(\mathbf{R})$. □

The following fundamental theorem gives an intrinsic characterization of trigonalizable matrices.

Theorem 9.4. *Let $A \in M_n(F)$ be a matrix. Then the following assertions are equivalent:*

a) The characteristic polynomial of A is split over F.
b) A is similar to an upper-triangular matrix in $M_n(F)$.

Proof. The discussion preceding the theorem shows that b) implies a). We will prove the converse by induction on n. It is clearly true for $n = 1$, so assume that $n \geq 2$ and that the statement holds for $n - 1$.

Choose a root $\lambda \in F$ of the characteristic polynomial χ_A of A (we can do it, thanks to the hypothesis that χ_A is split over F), and choose a nonzero vector $v \in F^n$ such that $Av = \lambda v$. Since $v \neq 0$, we can complete v_1 to a basis $v_1, \ldots, v_n$ of $V = F^n$. The matrix of the linear transformation T attached to A with respect to the basis $v_1, \ldots, v_n$ is of the form

$$\begin{bmatrix} \lambda & * \\ 0 & B \end{bmatrix}$$

for some $B \in M_{n-1}(F)$. Thus we can find an invertible matrix P_1 such that

$$P_1 A P_1^{-1} = \begin{bmatrix} \lambda & * \\ 0 & B \end{bmatrix}$$

for some $B \in M_{n-1}(F)$. Since similar matrices have the same characteristic polynomial, we obtain

$$\chi_A(X) = \chi_{P_1 A P_1^{-1}}(X) = (X - \lambda)\chi_B(X),$$

the last equality being a consequence of Theorem 7.43. It follows that χ_B is split over F. Since $B \in M_{n-1}(F)$, we can apply the inductive hypothesis and find an invertible matrix $Q \in M_{n-1}(F)$ such that QBQ^{-1} is upper-triangular. Let $P_2 = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$, then $P_2 \in M_n(F)$ is invertible (again by Theorem 7.43 we have $\det P_2 = \det Q \neq 0$) and

$$P_2(P_1AP_1^{-1})P_2^{-1} = \begin{bmatrix} \lambda & * \\ 0 & QBQ^{-1} \end{bmatrix}$$

is upper-triangular. Setting $P = P_2P_1$, the matrix PAP^{-1} is upper-triangular, as desired. □

Combining the previous two theorems, we obtain the following very important result:

Corollary 9.5. *For any matrix $A \in M_n(\mathbf{C})$ we can find an invertible matrix $P \in M_n(\mathbf{C})$ and an upper-triangular matrix $T \in M_n(\mathbf{C})$ such that $A = PTP^{-1}$. Thus any matrix $A \in M_n(\mathbf{C})$ is trigonalizable in $M_n(\mathbf{C})$.*

Proof. By Gauss' theorem the characteristic polynomial χ_A of A is split over $\mathbf{C}$. The result follows from Theorem 9.4. □

As a beautiful application of Corollary 9.5, let us give yet another proof of the Cayley–Hamilton theorem for matrices in $M_n(\mathbf{C})$ (the result applies of course to matrices in $M_n(\mathbf{Q})$ or $M_n(\mathbf{R})$). Recall that this theorem says that $\chi_A(A) = O_n$ for any matrix $A \in M_n(\mathbf{C})$, where χ_A is the characteristic polynomial of A. We will prove this in two steps: first, we reduce to the case when A is upper-triangular, then we prove the theorem in this case by a straightforward argument.

Let $A \in M_n(\mathbf{C})$ be a matrix and let P be an invertible matrix such that the matrix $T = PAP^{-1}$ is upper-triangular. We want to prove that $\chi_A(A) = O_n$, but

$$\chi_A(A) = \chi_A(P^{-1}TP) = P^{-1}\chi_A(T)P = P^{-1}\chi_T(T)P,$$

the last equality being a consequence of the fact that A and T are similar, thus have the same characteristic polynomial. Hence it suffices to prove that $\chi_T(T) = O_n$, in other words, we may and will assume that A is upper-triangular.

Let $e_1, \dots, e_n$ be the canonical basis of $\mathbf{C}^n$ and consider the polynomials

$$Q_k(X) = \prod_{i=1}^{k}(X - a_{ii}),$$

so that $Q_n = \chi_A$ (since A is upper-triangular). We claim that $Q_k(A)e_i = 0$ for $1 \le i \le k$ and for all $1 \le k \le n$. Accepting this for a moment, it follows that $Q_n(A)e_i = 0$ for all $1 \le i \le n$, that is $\chi_A(A)e_i = 0$ for all $1 \le i \le n$, which is exactly saying that $\chi_A(A) = O_n$.

It remains to prove the claim, and we will do this by induction on k. If $k = 1$, we need to check that $Q_1(A)e_1 = 0$, that is $(A - a_{11}I_n)e_1 = 0$, or equivalently that the first column of $A - a_{11}I_n$ is zero, which is clear since A is upper-triangular. Assume now that $Q_k(A)e_i = 0$ for $1 \le i \le k$, and let us prove that $Q_{k+1}(A)e_i = 0$ for $1 \le i \le k+1$. If $1 \le i \le k$, then $Q_k(A)e_i = 0$ yields

$$Q_{k+1}(A)e_i = (A - a_{k+1,k+1}I_n)Q_k(A)e_i = 0.$$

If $i = k + 1$, then

$$Q_{k+1}(A)e_i = Q_k(A)(A - a_{k+1,k+1}I_n)e_i =$$

$$Q_k(A)(Ae_i - a_{k+1,k+1}e_i) = -\sum_{i=1}^{k} a_{i,k+1}Q_k(A)e_i = 0,$$

since $Q_k(A)e_i = 0$ for $1 \leq i \leq k$. The inductive step is established and the claim is proved.

Problem 9.6. Let $A \in M_n(\mathbf{C})$ and let $Q \in \mathbf{C}[X]$ be a polynomial. If the characteristic polynomial of A equals $\prod_{i=1}^{n}(X - \lambda_i)$, prove that the characteristic polynomial of $Q(A)$ equals $\prod_{i=1}^{n}(X - Q(\lambda_i))$.

Solution. By the previous corollary we can write $A = PTP^{-1}$ for some $P \in \mathrm{GL}_n(\mathbf{C})$ and some upper-triangular matrix T. The characteristic polynomial of T is the same as that of A, and it is also equal to $\prod_{i=1}^{n}(X - t_{ii})$ if $T = [t_{ij}]$. Thus the diagonal entries of T are $\lambda_1, \ldots, \lambda_n$ (up to a permutation). Next, $Q(A) = PQ(T)P^{-1}$ and the characteristic polynomial of $Q(A)$ is the same as that of $Q(T)$. But $Q(T)$ is again upper-triangular, with diagonal entries $Q(\lambda_1), \ldots, Q(\lambda_n)$, so

$$\chi_{Q(A)} = \chi_{Q(T)} = \prod_{i=1}^{n}(X - Q(\lambda_i)).$$

□

Problem 9.7. Let $A \in M_n(\mathbf{C})$ have eigenvalues $\lambda_1, \ldots, \lambda_n$ (counted with their algebraic multiplicities). Prove that for all $Q \in \mathbf{C}[X]$ we have

$$\det Q(A) = \prod_{i=1}^{n} Q(\lambda_i), \quad \mathrm{Tr}(Q(A)) = \sum_{i=1}^{n} Q(\lambda_i).$$

Solution. Simply combine the previous problem with Problem 8.50. □

9.1.1 Problems for Practice

1. For each of the following matrices decide whether A is trigonalizable over $\mathbf{R}$ or not:

   a) $A = \begin{bmatrix} 1 & 2 & 1 \\ 3 & 2 & 2 \\ 0 & 1 & 1 \end{bmatrix}$.

   b) $A = \begin{bmatrix} 1 & 4 \\ 2 & 5 \end{bmatrix}$

2. Find all real numbers x for which the matrix $A = \begin{bmatrix} x & 1 \\ x-1 & 2+x \end{bmatrix}$ is trigonalizable in $M_2(\mathbf{R})$.
3. Find an upper-triangular matrix which is similar to the matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}.$$

4. Find an upper-triangular matrix which is similar to the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix}.$$

5. A matrix $A \in M_3(\mathbf{C})$ has eigenvalues $1, 2, -1$. Find the trace and the determinant of $A^3 + 2A + I_3$.
6. Let $A \in M_n(F)$ be a matrix. Prove that A is nilpotent if and only if A is similar to an upper-triangular matrix all of whose diagonal entries are 0.
7. Let $A, B \in M_n(\mathbf{C})$ be matrices such that $AB = BA$.

   a) Prove that each eigenspace of B is stable under the linear transformation attached to A.
   b) Deduce that A and B have a common eigenvector.
   c) Prove by induction on n that there is an invertible matrix P such that PAP^{-1} and PBP^{-1} are both upper-triangular.

8. Let $A, B \in M_n(\mathbf{C})$ be two matrices. Recall that the Kronecker or tensor product of A and B is the matrix $A \otimes B \in M_{n^2}(\mathbf{C})$ defined by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \dots & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nn}B \end{bmatrix}.$$

   We recall that

$$(A \otimes B) \cdot (A' \otimes B') = (AA') \otimes (BB')$$

   for all matrices $A, A', B, B' \in M_n(\mathbf{C})$.

   a) Consider two invertible matrices P, Q such that $P^{-1}AP$ and $Q^{-1}BQ$ are upper-triangular. Prove that $(P \otimes Q)^{-1}(A \otimes B)(P \otimes Q)$ is also upper-triangular and describe its diagonal entries in terms of the eigenvalues of A and B.

b) Deduce that if

$$\chi_A(X) = \prod_{i=1}^{n}(X - \lambda_i) \quad \text{and} \quad \chi_B(X) = \prod_{i=1}^{n}(X - \mu_i)$$

then

$$\chi_{A\otimes B}(X) = \prod_{i=1}^{n}\prod_{j=1}^{n}(X - \lambda_i\mu_j).$$

9.2 Diagonalizable Matrices and Linear Transformations

Diagonal matrices are fairly easy to understand and study. In this section we study those matrices which are as close as possible to being diagonal: the matrices which are similar to a diagonal matrix. We fix a field F. All vector spaces will be considered over F and will be finite-dimensional.

Definition 9.8. a) A matrix $A \in M_n(F)$ is called **diagonalizable** if it is similar to a diagonal matrix in $M_n(F)$.

b) A linear transformation $T : V \to V$ on a vector space V is called **diagonalizable** if its matrix in some basis of V is diagonal.

Thus a matrix $A \in M_n(F)$ is diagonalizable if and only if we can write

$$A = PDP^{-1}$$

for some invertible matrix $P \in M_n(F)$ and some diagonal matrix $D = [d_{ij}] \in M_n(F)$. Note that any matrix which is similar to a diagonalizable matrix is itself diagonalizable. In particular, if T is a diagonalizable linear transformation, then the matrix of T with respect to **any** basis of V is still diagonalizable (but **not** diagonal in general).

We can give a completely intrinsic characterization of diagonalizable linear transformations, with no reference to a choice of basis or to matrices:

Theorem 9.9. *A linear transformation $T : V \to V$ on a vector space V is diagonalizable if and only if there is a basis of V consisting of eigenvectors of T.*

Proof. Suppose that T is diagonalizable. Thus there is a basis $v_1, \ldots, v_n$ of V such that the matrix A of T with respect to this basis is diagonal. If $(a_{ii})_{1\le i\le n}$ are the diagonal entries of A, then by definition $T(v_i) = a_{ii}v_i$ for all $1 \le i \le n$, thus $v_1, \ldots, v_n$ is a basis of V consisting of eigenvectors for T.

Conversely, suppose that there is a basis $v_1, \ldots, v_n$ of V consisting of eigenvectors for T. If $T(v_i) = d_i v_i$, then the matrix of T with respect to $v_1, \ldots, v_n$ is diagonal, thus T is diagonalizable. □

Remark 9.10. One can use these ideas to find an **explicit way to diagonalize a matrix A. If $A \in M_n(F)$ is diagonalizable, then we find a basis of $V = F^n$ consisting of eigenvectors and we let P be the matrix whose columns are this basis. Then $P^{-1}AP = D$ is diagonal and $A = PDP^{-1}$.**

Remark 9.11. Suppose that A is diagonalizable and write $A = PDP^{-1}$ for some diagonal matrix D and some invertible matrix P.

a) The characteristic polynomials of A and D are the same, since A and D are similar. We deduce that

$$\prod_{i=1}^{n}(X - d_{ii}) = \chi_A(X).$$

In particular, the diagonal entries of D are (up to a permutation) the eigenvalues of A (counted with algebraic multiplicities). This is very useful in practice.

b) Let λ be an eigenvalue of A. Then the algebraic multiplicity of λ equals the number of indices $i \in [1, n]$ for which $d_{ii} = \lambda$ (this follows from a)). On the other hand, the geometric multiplicity of λ as eigenvalue of A or D is the same (since $X \mapsto P^{-1}X$ induces an isomorphism between $\mathrm{Ker}(\lambda I_n - A)$ and $\mathrm{Ker}(\lambda I_n - D)$, thus these two spaces have the same dimension). But it is not difficult to see that the geometric multiplicity of λ as eigenvalue of D is the number of indices $i \in [1, n]$ for which $d_{ii} = \lambda$, since the system $DX = \lambda X$ is equivalent to the equations $(d_{ii} - \lambda)x_i = 0$ for $1 \leq i \leq n$. We conclude that **for a diagonalizable matrix, the algebraic multiplicity of any eigenvalue equals its geometric multiplicity**.

Problem 9.12. Show that

$$A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$$

is not diagonalizable when $a \neq 0$.

Solution. Suppose that A is diagonalizable and write $A = PDP^{-1}$ with P invertible and D diagonal. Since A is upper-triangular with diagonal entries equal to 1, we deduce that the eigenvalues of A are equal to 1. By the previous remark the diagonal entries of D must all be equal to 1 and so $D = I_n$. But then $A = PI_nP^{-1} = I_n$, a contradiction. □

Problem 9.13. Prove that the only nilpotent and diagonalizable matrix $A \in M_n(F)$ is the zero matrix.

Solution. Suppose that A is diagonalizable and nilpotent and write $A = PDP^{-1}$. By Problem 8.38 and the previous remark we obtain

$$X^n = \chi_A(X) = \prod_{i=1}^{n}(X - d_{ii}).$$

Thus $d_{ii} = 0$ for all i and then $D = O_n$ and $A = PO_nP^{-1} = O_n$. □

The study of diagonalizable matrices is more involved than that of trigonalizable ones. Before proving the main theorem characterizing diagonalizable matrices, we will prove a technical result, which is extremely useful in other situations as well (the reader will find two more beautiful applications of this result in the next section).

Let $k > 1$ be an integer and let $P_1, \ldots, P_k$ pairwise relatively prime polynomials in $F[X]$. Denote $P = P_1 \ldots P_k$ the product of these k polynomials.

Problem 9.14. Let $Q_i = \frac{P}{P_i}$. Prove that $Q_1, \ldots, Q_k$ are relatively prime, i.e., there is no nonconstant polynomial Q dividing all $Q_1, \ldots, Q_k$.

Solution. Suppose there is an irreducible polynomial Q that divides Q_i for all i. Since $Q|Q_1 = P_2 \cdots P_k$, we deduce that Q divides P_j for some $j \in \{2, \ldots, k\}$. But since Q divides Q_j, it also divides P_i for some $i \neq j$, contradicting that P_i and P_j are relatively prime. □

Note that it is definitely **not true** that $Q_1, \ldots, Q_k$ are themselves pairwise relatively prime: if $k > 2$, then both Q_1 and Q_2 are multiples of P_k.

The technical result we need is the following:

Theorem 9.15. *Suppose that T is a linear transformation on some F-vector space V (not necessarily finite dimensional). Then for any pairwise relatively prime polynomials $P_1, \ldots, P_k \in F[X]$ we have*

$$\ker P(T) = \bigoplus_{i=1}^{k} \ker P_i(T),$$

where $P = P_1 P_2 \ldots P_k$.

Proof. Consider the polynomials $Q_i = \frac{P}{P_i}$ as in the previous problem. Since they are relatively prime, Bezout's lemma[1] yields the existence of polynomials $R_1, \ldots, R_k$ such that

$$Q_1 R_1 + \ldots + Q_k R_k = 1 \tag{9.1}$$

Since P_i divides P, it follows that $\ker P_i(T) \subset \ker P(T)$ for all $i \in [1, k]$. On the other hand, take $x \in \ker P(T)$ and let $x_i = (Q_i R_i)(T)(x)$. Then relation (9.1) shows that

$$x = x_1 + x_2 + \ldots + x_k.$$

[1]This lemma says that if $A, B \in F[X]$ are relatively prime polynomials, then we can find polynomials $U, V \in F[X]$ such that $AU + BV = 1$. This easily yields the following more general statement: if $P_1, \ldots, P_k$ are polynomials whose greatest common divisor is 1, then we can find polynomials $U_1, \ldots, U_k$ such that $U_1 P_1 + \ldots + U_k P_k = 1$.

Moreover, $P_i(T)(x_i) = (P_i Q_i R_i)(T)(x)$ and $P_i Q_i R_i$ is a multiple of P. Since $x \in \ker P(T) \subset \ker(P_i Q_i R_i)(T)$, it follows that $x_i \in \ker P_i(T)$, and since $x = x_1 + \ldots + x_k$, we conclude that

$$\ker P(T) = \sum_{i=1}^{k} \ker P_i(T).$$

It remains to prove that if $x_i \in \ker P_i(T)$ and $x_1 + \ldots + x_k = 0$, then $x_i = 0$ for all $i \in [1, k]$. We have

$$Q_1(T)(x_1) + Q_1(T)(x_2) + \ldots + Q_1(T)(x_k) = 0.$$

But $Q_1(T)(x_2) = \ldots = Q_1(T)(x_k) = 0$, since Q_1 is a multiple of $P_2, \ldots, P_k$ and $P_2(T)(x_2) = \ldots = P_k(T)(x_k) = 0$. Thus $Q_1(T)(x_1) = 0$ and similarly $Q_j(T)(x_j) = 0$ for $1 \leq j \leq k$. But then

$$x_1 = (R_1 Q_1)(T)(x_1) + \ldots + (R_k Q_k)(T)(x_k) = 0$$

and similarly we obtain $x_2 = \ldots = x_k = 0$. The theorem is proved. □

We are now ready to prove the fundamental theorem concerning diagonalizable linear transformations.

Theorem 9.16. *Let V be a finite dimensional vector space over F and let $T : V \to V$ be a linear transformation. The following assertions are equivalent:*

a) T is diagonalizable.
b) There is a polynomial $P \in F[X]$ which splits over F and has pairwise distinct roots, such that $P(T) = 0$.
c) The minimal polynomial μ_T of T splits over F and has pairwise distinct roots.
d) Let $\mathrm{Sp}(T) \subset F$ be the set of eigenvalues of T. Then

$$\bigoplus_{\lambda \in \mathrm{Sp}(T)} \ker(T - \lambda \cdot \mathrm{id}) = V.$$

Proof. We start by proving that a) implies b). Choose a basis in which T is represented by the diagonal matrix D. Let P be the polynomial whose roots are the distinct diagonal entries of D. Then $P(T)$ is represented by the diagonal matrix $P(D)$ with entries $P(d_{ii}) = 0$. Thus $P(T) = 0$.

That b) implies c) is clear since the minimal polynomial of T will divide P and hence it splits over F, with distinct roots.

That c) implies d) is just Theorem 9.15 applied to P the minimal polynomial of T and P_i its linear factors.

Finally, to see that d) implies a), write $\mathrm{Sp}(T) = \{\lambda_1, \ldots, \lambda_k\}$ and choose a basis $v_1, \ldots, v_n$ of V obtained by patching a basis of $\ker(T - \lambda_1 \cdot \mathrm{id})$, followed by a basis of $\ker(T - \lambda_2 \cdot \mathrm{id}), \ldots$, followed by a basis of $\ker(T - \lambda_k \cdot \mathrm{id})$. Then $v_1, \ldots, v_n$ form a basis of eigenvectors of T, thus a) holds by Theorem 9.9. □

Remark 9.17. a) If T is a diagonalizable linear transformation, then example 8.9 shows that the minimal polynomial of T is

$$\mu_T(X) = \prod_{\lambda \in \mathrm{Sp}(T)} (X - \lambda),$$

the product being taken all eigenvalues of T, counted **without** multiplicities. Taking the same product, but counting multiplicities (algebraic or geometric, they are the same) of eigenvalues this time, we obtain the characteristic polynomial of T.

b) If T is any linear transformation on a finite dimensional vector space V, then T is diagonalizable if and only if the sum of the dimensions of the eigenspaces of T equals $\dim V$, i.e.,

$$\sum_{\lambda \in \mathrm{Sp}(T)} \dim \ker(T - \lambda \cdot \mathrm{id}) = \dim V.$$

Indeed, this follows from the theorem and the fact that the subspaces $\ker(T - \lambda \cdot \mathrm{id})$ are always in direct sum position.

c) Suppose that T is diagonalizable. For each $\lambda \in \mathrm{Sp}(T)$ let π_λ be the projection on the subspace $\ker(T - \lambda \cdot \mathrm{id})$. Then

$$T = \sum_{\lambda \in \mathrm{Sp}(T)} \lambda \pi_\lambda.$$

This follows from $\oplus_{\lambda \in \mathrm{Sp}(T)} \ker(T - \lambda \cdot \mathrm{id}) = V$ and the fact that if

$$v = \sum_{\lambda \in \mathrm{Sp}(T)} v_\lambda \quad \text{with} \quad v_\lambda \in \ker(T - \lambda \cdot \mathrm{id}),$$

then

$$T(v) = \sum_{\lambda \in \mathrm{Sp}(T)} T(v_\lambda) = \sum_{\lambda \in \mathrm{Sp}(T)} \lambda v_\lambda = \sum_{\lambda \in \mathrm{Sp}(T)} \lambda \pi_\lambda(v).$$

Due to its importance, we will restate the previous theorem in terms of matrices:

Theorem 9.18. *Let $A \in M_n(F)$. Then the following assertions are equivalent:*

a) A is diagonalizable in $M_n(F)$.
b) If $\mathrm{Sp}(A)$ is the set of eigenvalues of A, then

$$\bigoplus_{\lambda \in \mathrm{Sp}(A)} \ker(\lambda I_n - A) = F^n.$$

c) The minimal polynomial μ_A of A is split over F, with pairwise distinct roots.
d) There is a polynomial $P \in F[X]$ which is split over F, with pairwise distinct roots and such that $P(A) = O_n$.

In the following problems the reader will have the opportunity to check the comprehension of the various statements involved in the previous theorem.

Problem 9.19. Explain why the matrix A with real entries is diagonalizable in each of the following two cases.

(a) The matrix A has characteristic polynomial

$$X^3 - 3X^2 + 2X.$$

(b)

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 & 4 \end{bmatrix}.$$

Solution. (a) We have

$$X^3 - 3X^2 + 2X = X(X^2 - 3X + 2) = X(X-1)(X-2),$$

which is split, with distinct roots. Since this polynomial kills A (by the Cayley–Hamilton theorem), the result follows from the implication "b) implies a)" in Theorem 9.16. We can also argue directly, as follows: if v_1, v_2, v_3 are eigenvectors corresponding to the eigenvalues $0, 1, 2$, then v_1, v_2, v_3 are linearly independent (since the eigenvalues are distinct) and thus must form a basis of $\mathbf{R}^3$. Thus A is diagonalizable (by Theorem 9.9 and the discussion preceding it).

(b) We have

$$\chi_A(X) = \det(XI_5 - A) = (X-1)(X-3)(X-4)[(X-3)(X-4) - 2]$$

$$= (X-1)(X-3)(X-4)(X^2-7X+10) = (X-1)(X-2)(X-3)(X-4)(X-5).$$

This polynomial is split with distinct roots, so the same argument as in part a) yields the result. □

Problem 9.20. Consider the matrix

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

a) Is A diagonalizable in $M_3(\mathbf{C})$?
b) Is A diagonalizable in $M_3(\mathbf{R})$?

Solution. One easily finds that the characteristic polynomial of A is $\chi_A(X) = X^3 - 1$. This polynomial is split with distinct roots in $\mathbf{C}[X]$, thus A is diagonalizable in $M_3(\mathbf{C})$. On the other hand, A is not diagonalizable in $M_3(\mathbf{R})$, since its characteristic polynomial does not split in $\mathbf{R}[X]$. □

Problem 9.21. Let

$$A = \begin{bmatrix} -7 & -16 & 4 \\ 6 & 13 & -2 \\ 12 & 16 & 1 \end{bmatrix} \in M_3(\mathbf{R})$$

(a) Prove that $\lambda = 5$ is an eigenvalue of A.
(b) Diagonalize A, if possible.

Solution. (a) We have

$$A - 5I = \begin{bmatrix} -12 & -16 & 4 \\ 6 & 8 & -2 \\ 12 & 16 & -4 \end{bmatrix}$$

and the last row is the opposite of the first row. Thus $A - 5I$ is not invertible and 5 is an eigenvalue of A.

(b) We take advantage of part a) and study the 5-eigenspace of A. This is described by the system of equations

$$\begin{cases} -12x - 16y + 4z = 0 \\ 6x + 8y - 2z = 0 \\ 12x + 16y - 4z = 0 \end{cases}$$

As we have already remarked in part a), the first and the third equations are equivalent. The system is then equivalent (after dividing the first equation by 4 and the second one by 2) to

$$\begin{cases} -3x - 4y + z = 0 \\ 3x + 4y - z = 0 \end{cases}$$

Again, the first and second equations are equivalent. Thus the 5-eigenspace is

$$\ker(A - 5I) = \{(x, y, 3x + 4y) | x, y \in \mathbb{R}\}$$

and this is a two-dimensional vector space, with a basis given by

$$v_1 = (1, 0, 3), \quad v_2 = (0, 1, 4).$$

We deduce that 5 has algebraic multiplicity at least 2. Since the sum of the complex eigenvalues of A equals the trace of A, which is $-7 + 13 + 1 = 7$, we deduce that -3 is another eigenvalue of A, and the corresponding eigenspace is a line. Solving the system $AX = -3X$ yields the solution $(-2, 1, 2)$. We deduce that a diagonalization of A is given by

$$A = \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 3 & 4 & 2 \end{bmatrix} \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & -3 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 3 & 4 & 2 \end{bmatrix}^{-1}. \qquad \square$$

Problem 9.22. Consider the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{bmatrix} \in M_3(\mathbf{R}).$$

Is this matrix diagonalizable?

Solution. We start by computing the characteristic polynomial

$$\chi_A(X) = \begin{vmatrix} X & -1 & 0 \\ 4 & X-4 & 0 \\ 2 & -1 & X-2 \end{vmatrix} = (X-2) \begin{vmatrix} X & -1 \\ 4 & X-4 \end{vmatrix} =$$

$$(X-2)(X^2 - 4X + 4) = (X-2)^3.$$

Thus 2 is an eigenvalue of A with algebraic multiplicity 3. If A is diagonalizable, then 2 would have geometric multiplicity 3, that is $\mathrm{Ker}(A - 2I_3)$ would be three dimensional and $A = 2I_3$. Since this is certainly not the case, it follows that A is not diagonalizable. $\square$

Problem 9.23. Find all values of $a \in \mathbf{R}$ for which the matrix

$$A = \begin{bmatrix} 2 & 1 & -2 \\ 1 & a & -1 \\ 1 & 1 & -1 \end{bmatrix} \in M_3(\mathbf{R})$$

is diagonalizable.

Solution. As usual, we start by computing the characteristic polynomial $\chi_A(X)$ of A. Adding the first column to the third one, then subtracting the first row from the third one, we obtain

$$\chi_A(X) = \begin{vmatrix} X-2 & -1 & 2 \\ -1 & X-a & 1 \\ -1 & -1 & X+1 \end{vmatrix} =$$

$$\begin{vmatrix} X-2 & -1 & X \\ -1 & X-a & 0 \\ 1-X & 0 & 0 \end{vmatrix} = X(X-1)(X-a).$$

If $a \notin \{0, 1\}$, then $\chi_A(X)$ is split with distinct roots and since it kills A (by the Cayley–Hamilton theorem), we deduce that A is diagonalizable.

Suppose that $a = 0$, thus 0 is an eigenvalue of A with algebraic multiplicity 2. Let us find its geometric multiplicity, which comes down to solving the system $AX = 0$. This system reads to

$$\begin{cases} 2x_1 + x_2 - 2x_3 = 0 \\ x_1 - x_3 = 0 \\ x_1 + x_2 - x_3 = 0 \end{cases}$$

and its solutions are $(x_1, 0, x_1)$ with $x_1 \in \mathbf{R}$. As this space is one dimensional, we deduce that the geometric multiplicity of 0 is 1 and so A is not diagonalizable.

If $a = 1$, a similar argument shows that 1 is an eigenvalue with algebraic multiplicity 2 and with geometric multiplicity 1, thus A is not diagonalizable. All in all, the answer of the problem is: all $a \in \mathbf{R} \setminus \{0, 1\}$. □

Problem 9.24. Diagonalize, if possible, the matrix

$$A = \begin{bmatrix} 4 & 0 & -2 \\ 2 & 5 & 4 \\ 0 & 0 & 5 \end{bmatrix} \in M_3(\mathbf{R})$$

Solution. We start by computing the characteristic polynomial of A:

$$\begin{vmatrix} X-4 & 0 & 2 \\ -2 & X-5 & -4 \\ 0 & 0 & X-5 \end{vmatrix} = (X-5) \begin{vmatrix} X-4 & 0 \\ -2 & X-5 \end{vmatrix} = (X-4)(X-5)^2.$$

We deduce that A has two eigenvalues, namely 4 with algebraic multiplicity 1 and 5 with algebraic multiplicity 2. Next, we study separately the corresponding eigenspaces. Since 4 has algebraic multiplicity 1, we already know that the 4-eigenspace will be a line. To find it, we write the condition $AX = 4X$ as the system

$$\begin{cases} 4x - 2z = 4x \\ 2x + 5y + 4z = 4y \\ 5z = 4z \end{cases}$$

This system can easily be solved: the last equation gives $z = 0$, the first one becomes tautological and the second one gives $y = -2x$. Thus the 4-eigenspace is the line spanned by $v_1 = (1, -2, 0)$.

Next, we study the 5-eigenspace. Write the equation $AX = 5X$ as the system

$$\begin{cases} 4x - 2z = 5x \\ 2x + 5y + 4z = 5y \\ 5z = 5z \end{cases}$$

The last equation is tautological. The first equation gives $x = -2z$ and the second one becomes then tautological. Thus the solutions of the system are $(-2z, y, z) = y(0, 1, 0) + z(-2, 0, 1)$ with $y, z \in \mathbf{R}^2$. We deduce that the 5-eigenspace is two-dimensional, with a basis given by $v_2 = (0, 1, 0)$ and $v_3 = (-2, 0, 1)$.

Since the sum of the dimensions of the eigenspaces equals $3 = \dim \mathbf{R}^3$, we deduce that A is diagonalizable and v_1, v_2, v_3 form a basis of eigenvectors. The matrix P whose columns are the coordinates of v_1, v_2, v_3 with respect to the canonical basis is

$$P = \begin{bmatrix} 1 & 0 & -2 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We have

$$A = PDP^{-1}, \quad \text{with} \quad D = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix}. \qquad \square$$

We end this section with some more theoretical exercises.

Problem 9.25. Let T be a diagonalizable linear transformation on a finite dimensional vector space V over a field F. Let W be a subspace of V which is stable under T. Prove that $T|_W : W \to W$ is diagonalizable.

Solution. Since $T : V \to V$ is diagonalizable, there is a polynomial $P \in F[X]$ of the form $P = (X - \lambda_1) \dots (X - \lambda_k)$ with $\lambda_1, \dots, \lambda_k \in F$ pairwise distinct, such that $P(T) = 0$. Since $P(T)(v) = 0$ for all $v \in V$, we have $P(T)(w) = 0$ for all $w \in W$. Thus $P(T|_W) = 0$ and so $T|_W$ is diagonalizable by Theorem 9.16. $\square$

The result established in the next problem is very useful in many situations.

Problem 9.26. Let V be a finite dimensional vector space over a field F and let $T_1, T_2 : V \to V$ be linear transformations of V. Prove that if T_1 and T_2 commute, then any eigenspace of T_2 is stable under T_1.

Solution. Let $\lambda \in F$ be an eigenvalue of T_2 and let $E_\lambda = \ker(\lambda \cdot \mathrm{id} - T_2)$ be the corresponding eigenspace. If $v \in E_\lambda$, then $T_2(v) = \lambda v$, thus

$$T_2(T_1(v)) = T_1(T_2(v)) = T_1(\lambda v) = \lambda T_1(v)$$

and so $T_1(v) \in E_\lambda$. The result follows. $\square$

Problem 9.27. Let V be a finite dimensional vector space over a field F and let $T_1, T_2 : V \to V$ be diagonalizable linear transformations of V. Prove that T_1 and T_2 commute if and only if they are simultaneously diagonalizable.

Solution. Suppose first that T_1 and T_2 are simultaneously diagonalizable. Thus there is a basis B of V in which the matrices of T_1 and T_2 are diagonal, say D_1 and D_2. We clearly have $D_1D_2 = D_2D_1$, thus the matrices of $T_1 \circ T_2$ and $T_2 \circ T_1$ coincide in this basis and so $T_1 \circ T_2 = T_2 \circ T_1$.

Conversely, suppose that T_1 and T_2 commute. Let $\lambda_1, \ldots, \lambda_k$ be the distinct eigenvalues of T_1 and let $W_i = \ker(T_1 - \lambda_i)$ be the corresponding eigenspaces. Since T_1 is diagonalizable, we have $V = W_1 \oplus \ldots \oplus W_k$. Since T_1 and T_2 commute, T_2 leaves each W_i invariant by Problem 9.26. Since T_2 is diagonalizable, so is its restriction to W_i, by Problem 9.25. Thus there is a basis B_i of W_i consisting of eigenvectors for $T_2|_{W_i}$. Consider the basis B' consisting of all vectors in $B_1 \cup \ldots \cup B_k$. Then B' consists of eigenvectors for both T_1 and T_2 (this is clear for T_2, and holds for T_1 since T_1 acts on W_i by the scalar λ_i). Thus the matrices of T_1 and T_2 in the basis B' are both diagonal and the result follows. □

Problem 9.28. Let A be an invertible matrix with complex coefficients and let $d \geq 1$. Prove that A is diagonalizable if and only if A^d is diagonalizable. What happens if we don't assume that A is invertible?

Solution. Suppose that A is diagonalizable, thus there is an invertible matrix P such that PAP^{-1} is a diagonal matrix. Then $(PAP^{-1})^d = PA^dP^{-1}$ is also a diagonal matrix, hence A^d is diagonalizable. This implication does not require the hypothesis that A is invertible.

Suppose now that A^d is diagonalizable and that A is invertible. Since A^d is diagonalizable and invertible, its minimal polynomial is of the form $(X-\lambda_1)\ldots(X-\lambda_k)$ with $\lambda_1, \ldots, \lambda_k$ pairwise distinct and nonzero. Consider the polynomial $P(X) = (X^d - \lambda_1)\ldots(X^d - \lambda_k)$. Since each of the polynomials $X^d - \lambda_1, \ldots, X^d - \lambda_k$ has pairwise distinct roots and since these polynomials are pairwise relatively prime, their product P has pairwise distinct roots. Since $P(A) = 0$, we deduce that A is diagonalizable.

Finally, if we only assume that A^d is diagonalizable and A is not invertible, then one of the eigenvalues of A is 0. Hence one of the factors of the matrix $P(X)$ above becomes X^d. Since this does not have distinct roots the proof breaks down. Indeed A need not be diagonalizable in this case. For instance, consider the matrix $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. This matrix satisfies $A^2 = 0$, thus A^2 is certainly diagonalizable. However, A is not diagonalizable. Indeed, if this was the case, then A would necessarily be the zero matrix, since its eigenvalues are all 0. Hence for the more difficult implication one cannot drop the hypothesis that A is invertible. □

Problem 9.29. Let A be a matrix with real entries such that $A^3 = A^2$.

a) Prove that A^2 is diagonalizable.
b) Find A if its trace equals the number of columns of A.

Solution. a) The hypothesis yields $A^4 = A^3 = A^2$, thus $(A^2)^2 = A^2$. It follows that A^2 is killed by the polynomial $X(X-1)$, which has pairwise distinct and real roots. Thus A^2 is diagonalizable.

b) Let n be the number of columns of A. The trace of A equals n, and this is also the sum of the complex eigenvalues of A, counted with their algebraic multiplicities. By hypothesis each eigenvalue λ satisfies $\lambda^3 = \lambda^2$, thus $\lambda \in \{0, 1\}$. Since the n eigenvalues add up to n, it follows that all of them are equal to 1. Thus all eigenvalues of A^2 are 1 and using part a) we deduce that $A^2 = I_n$. Combining this with the hypothesis yields $A \cdot I_n = I_n$ and then $A = I_n$, which is the unique solution of the problem.

□

Problem 9.30. Let $A_1 \in M_p(F)$ and $A_2 \in M_q(F)$ and let

$$A = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix} \in M_{p+q}(F).$$

Prove that A is diagonalizable if and only if A_1 and A_2 are diagonalizable.

Solution. If $P \in F[X]$ is a polynomial, then

$$P(A) = \begin{bmatrix} P(A_1) & 0 \\ 0 & P(A_2) \end{bmatrix}.$$

If A is diagonalizable, then we can find a polynomial P which splits over F into a product of distinct linear factors and which kills A. By the previous formula, P also kills A_1 and A_2, which must therefore be diagonalizable.

Suppose now that A_1 and A_2 are diagonalizable, thus we can find polynomials P_1, P_2 which split over F into products of distinct linear factors and which kill A_1 and A_2 respectively. Let P be the least common multiple of P_1 and P_2. Then P splits into a product of distinct linear factors and kills A, which is therefore diagonalizable.

An alternative solution is based on the study of eigenspaces of A. Namely, it is not difficult to see that for any $\lambda \in F$ we have

$$\ker(A - \lambda I_{p+q}) = \ker(A_1 - \lambda I_p) \oplus \ker(A_2 - \lambda I_q).$$

Now a matrix $X \in M_n(F)$ is diagonalizable if and only if $\oplus_{\lambda \in F} \ker(X - \lambda I_n) = F^n$, from where the result follows easily. □

9.2.1 Problems for Practice

1. a) Diagonalize the matrix

$$A = \begin{bmatrix} -1 & 2 \\ 4 & 1 \end{bmatrix}$$

in $M_2(\mathbf{C})$.

b) Do the same by considering A as an element of $M_2(\mathbf{R})$.

2. For each matrix A below, decide if A is diagonalizable. Explain your reasoning. If A is diagonalizable, find an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$.

   (a)

$$A = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 1 & 0 & 5 \end{bmatrix} \in M_3(\mathbf{R})$$

   (b)

$$A = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 5 & 0 \\ 1 & 0 & 5 \end{bmatrix} \in M_3(\mathbf{R})$$

3. a) Let $a_1, \ldots, a_n$ be complex numbers and let $A = [a_i a_j]_{1 \le i,j \le n} \in M_n(\mathbf{C})$. When is A diagonalizable?
   b) Let $a_1, \ldots, a_n$ be real numbers and let $A = [a_i a_j]_{1 \le i,j \le n} \in M_n(\mathbf{R})$. When is A diagonalizable?
4. Let A be the $n \times n$ matrix all of whose entries are equal to 1. Prove that $A \in M_n(\mathbf{R})$ is diagonalizable and find its eigenvalues.
5. Compute the nth power of the matrix

$$A = \begin{bmatrix} 1 & 3 & 3 \\ 3 & 1 & 3 \\ 3 & 3 & 1 \end{bmatrix}.$$

   Hint: diagonalize A.
6. Find all differentiable maps $x, y, z : \mathbf{R} \to \mathbf{R}$ such that $x(0) = 1$, $y(0) = 0$, $z(0) = 0$ and

$$x' = y + z, \quad y' = x + z, \quad z' = x - 3y + 4z.$$

   Hint: the matrix $A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -3 & 4 \end{bmatrix}$ has an eigenvalue equal to -1. Use this to diagonalize A. How is this related to the original problem?
7. Let V be a finite dimensional vector space over $\mathbf{C}$ and let $T : V \to V$ be a linear transformation.

   a) Prove that if T is diagonalizable, then T^2 is diagonalizable and $\ker T = \ker T^2$.
   b) Prove that if T^2 is diagonalizable and $\ker T = \ker T^2$, then T is diagonalizable.

8. Let $A, B \in M_n(F)$ be matrices such that A is invertible and AB is diagonalizable. Prove that BA is also diagonalizable. What happens if we don't assume that A is invertible?
9. Find all matrices $A \in M_3(\mathbf{R})$ such that

$$A^2 = \begin{bmatrix} 9 & 0 & 0 \\ 1 & 4 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Hint: start by diagonalizing the matrix $\begin{bmatrix} 9 & 0 & 0 \\ 1 & 4 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ and prove that any solution of the problem is diagonalizable and commutes with this matrix.

10. Let $A \in M_n(\mathbf{C})$ be a matrix such that $A^d = I_n$ for some positive integer d. Prove that

a) A is diagonalizable with eigenvalues dth roots of unity.
b) Deduce that

$$\dim \ker(A - I_n) = \frac{1}{d} \sum_{i=1}^{d} \mathrm{Tr}(A^i).$$

11. Let $\mathcal{F}$ be an arbitrary family of diagonalizable matrices in $M_n(\mathbf{C})$. Suppose that $AB = BA$ for all $A, B \in \mathcal{F}$. Prove that there is an invertible matrix P such that PAP^{-1} is diagonal for all $A \in \mathcal{F}$. Hint: proceed by induction on n and use Problem 9.26 and the arguments in the solution of Problem 9.27.
12. (Functions of a diagonalizable matrix) Let $A \in M_n(F)$ be a diagonalizable matrix with $A = PDP^{-1}$ and D diagonal with diagonal entries d_{ii}. Let $f : F \to F$ be any function and let $f(D)$ be the diagonal matrix with (i, i) entry $f(d_{ii})$. Define $f(A) = Pf(D)P^{-1}$.

a) Prove that $f(A)$ is well defined. That is, if we diagonalize A in a different way, we will get the same matrix $f(A)$. (Hint: there is a polynomial p with $p(d_{ii}) = f(d_{ii})$.)
b) Prove that if A is diagonalizable over $F = \mathbf{R}$ and m is odd, then there is a diagonalizable matrix B with $B^m = A$.

13. Let $A, B \in M_n(\mathbf{R})$ be diagonalizable matrices such that

$$AB^5 = B^5A.$$

Write $B = PDP^{-1}$ with P invertible and D diagonal.

a) Let $C = P^{-1}AP$. Prove that $CD^5 = D^5C$.
b) Prove that $CD = DC$. Hint: use the injectivity of the map $x \to x^5$ ($x \in \mathbf{R}$).
c) Deduce that $AB = BA$.

14. Let $A \in M_n(\mathbf{C})$ and let $B = \begin{bmatrix} A & A \\ 0 & A \end{bmatrix} \in M_{2n}(\mathbf{C})$.

    a) Prove that for all $P \in \mathbf{C}[X]$ we have

    $$P(B) = \begin{bmatrix} P(A) & AP'(A) \\ 0 & P(A) \end{bmatrix}.$$

    b) Deduce that B is diagonalizable if and only if $A = O_n$.

15. Find all matrices $A \in M_n(\mathbf{R})$ such that $A^5 = A^2$ and the trace of A equals n. Hint: prove that all complex eigenvalues of A are equal to 1 and then that A is diagonalizable in $M_n(\mathbf{C})$.
16. Let $A, B \in M_n(\mathbf{R})$ be diagonalizable matrices such that $A^5 = B^5$. Prove that $A = B$. Hint: use problems 13 and 9.27.
17. Let V be a finite dimensional $\mathbf{C}$-vector space and let $T : V \to V$ be a linear transformation such that any subspace of V which is stable under T has a complement which is stable under T. Prove that T is diagonalizable.
18. Let V be a finite dimensional vector space over some field F and let $T : V \to V$ be a diagonalizable linear transformation on V. Let $C(T)$ be the set of linear transformations $S : V \to V$ such that $S \circ T = T \circ S$.

    a) Prove that a linear transformation $S : V \to V$ belongs to $C(T)$ if and only if S leaves invariant each eigenspace of T.
    b) Let m_λ be the algebraic multiplicity of the eigenvalue λ of T. Prove that $C(T)$ is an F-vector space of dimension $\sum_\lambda m_\lambda^2$, the sum being taken over all eigenvalues λ of T.
    c) Suppose that the eigenvalues of T are pairwise distinct. Prove that $\mathrm{id}, T, T^2, \ldots, T^{n-1}$ form a basis of $C(T)$ as F-vector space.

9.3 Some Applications of the Previous Ideas

In this section we would like to come back to the technical result given by Theorem 9.15 and give some further nice applications of it. First of all, we will apply it to the resolution of **linear differential equations with constant coefficients.**

Consider the following classical problem in real analysis: given complex numbers $a_0, a_1, \ldots, a_{n-1}$ and an open interval I in $\mathbf{R}$, find all smooth functions $f : I \to \mathbf{C}$ such that

$$f^{(n)}(x) + a_{n-1} f^{(n-1)}(x) + \ldots + a_1 f'(x) + a_0 f(x) = 0 \tag{9.2}$$

for all $x \in I$. Here $f^{(i)}$ is the ith derivative of f.

It follows from elementary calculus that any solution of Eq. (9.2) is smooth, i.e., infinitely differentiable. Let V be the space of smooth functions $f : I \to \mathbf{C}$.

Note that V is an infinite dimensional vector space over $\mathbf{C}$, but we had no finiteness assumption in Theorem 9.15, so we can use it for this vector space. Consider the linear transformation T sending a map f in V to its derivative

$$T : V \to V, \quad T(f) = f'.$$

Then $T^k(f) = f^{(k)}$ for all $k \geq 0$, thus solving Eq. (9.2) is equivalent to finding $\ker P(T)$, where

$$P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

is the characteristic polynomial of Eq. (9.2). Since we work over the complex numbers, we can factor

$$P(X) = \prod_{i=1}^{d} (X - z_i)^{k_i}$$

for some positive integers $k_1, \ldots, k_d$ and some pairwise distinct complex numbers $z_1, \ldots, z_d$. By Theorem 9.15 we have

$$\ker P(T) = \bigoplus_{i=1}^{d} \ker(T - z_i \cdot \mathrm{id})^{k_i}$$

so it suffices to understand $\ker(T - z \cdot \mathrm{id})^k$, where z is a complex number and k is a positive integer. Let $g \in V$ be the map

$$g(x) = e^{zx},$$

so that $g' = zg$. Then for any $f \in V$ we have

$$(T - z \cdot \mathrm{id})(fg) = (fg)' - zfg = f'g,$$

thus by an immediate induction

$$(T - z \cdot \mathrm{id})^k (fg) = f^{(k)} g.$$

Take $h \in \ker(T - z \cdot \mathrm{id})^k$ and let $f = h/g$ (note that g has no complex zero). Then the previous computation gives $f^{(k)} = 0$, that is f is a polynomial map of degree less than k. Conversely, the same computation shows that any such f gives rise to an element of $\ker(T - z \cdot \mathrm{id})^k$ (if multiplied by g). We conclude that $\ker(T - z \cdot \mathrm{id})^k$ consists of the maps $x \mapsto g(x)P(x)$, with P a polynomial of degree $\leq k - 1$ with complex coefficients, a basis of $\ker(T - z \cdot \mathrm{id})^k$ being given by the maps $x \mapsto x^j e^{zx}$, where $0 \leq j \leq k - 1$.

Putting everything together, we obtain the following:

Theorem 9.31. *Let $a_0, \ldots, a_{n-1}$ be complex numbers and write*

$$X^n + a_{n-1}X^{n-1} + \ldots + a_0 = \prod_{i=1}^{d} (X - z_i)^{k_i}.$$

a) The complex-valued solutions of the differential equation

$$f^{(n)} + a_{n-1} f^{(n-1)} + \ldots + a_1 f' + a_0 f = 0$$

are the maps of the form

$$x \mapsto f(x) = \sum_{i=1}^{d} e^{z_i x} P_i(x),$$

where P_i is a polynomial with complex coefficients whose degree does not exceed $k_i - 1$.

b) The set of complex-valued solutions of the previous differential equation is a vector space of dimension $n = k_1 + \ldots + k_d$ over $\mathbf{C}$, a basis being given by the maps $x \mapsto x^j e^{z_i x}$, where $1 \leq i \leq d$ and $0 \leq j < k_i$.

We consider now the discrete analogue of the previous problem, namely **linear recurrence sequences**. Let $a_0, \ldots, a_{d-1}$ be complex numbers and consider the set $\mathcal{S}$ of sequences $(x_n)_{n \geq 0}$ of complex numbers such that

$$x_{n+d} = a_0 x_n + a_1 x_{n+1} + \ldots + a_{d-1} x_{n+d-1}$$

for all $n \geq 0$.

First of all, it is clear that an element of $\mathcal{S}$ is uniquely determined by its first d terms $x_0, \ldots, x_{d-1}$. In other words, the map

$$\mathcal{S} \to \mathbf{C}^d, \quad (x_n)_{n \geq 0} \mapsto (x_0, x_1, \ldots, x_{d-1}),$$

which is clearly linear, is bijective and so an isomorphism of vector spaces. We deduce that

$$\dim \mathcal{S} = d.$$

We would like to describe explicitly the elements of $\mathcal{S}$. We proceed as above, by working in the big space V of all sequences $(x_n)_{n \geq 0}$ of complex numbers and considering the shift map

$$T : V \to V, \quad T((x_n)_{n \geq 0}) = (x_{n+1})_{n \geq 0}.$$

Note that T is clearly a linear map and that

$$T^k((x_n)_{n\geq 0}) = (x_{n+k})_{n\geq 0}.$$

It follows that

$$\mathcal{S} = \ker P(T), \quad \text{where} \quad P(X) = X^d - a_{d-1}X^{d-1} - \ldots - a_0$$

is the **characteristic polynomial of the recurrence relation**. As before, factorizing

$$P(T) = \prod_{i=1}^{p} (X - z_i)^{k_i}$$

we obtain using Theorem 9.15 that

$$\mathcal{S} = \bigoplus_{i=1}^{p} \ker(T - z_i \cdot \mathrm{id})^{k_i}$$

and so the problem is reduced to understanding the space $\ker(T - z \cdot \mathrm{id})^k$ where z is a complex number and k is a positive integer.

Let us start with the case $z = 0$, i.e., understanding $\ker T^k$. We have $T^k((x_n)_{n\geq 0}) = 0$ if and only if $x_{n+k} = 0$ for all $n \geq 0$, i.e., the sequence $x_0, x_1, \ldots$ becomes the zero sequence starting with index k. A basis of $\ker T^k$ is given by the sequences $x^{(0)}, \ldots, x^{(k-1)}$, where $x^{(j)}$ is the sequence whose jth term is 1 and all other terms 0.

Assume now that $z \neq 0$. Let $x = (x_n)_{n\geq 0}$ be any sequence in V and define a new sequence $y = (y_n)_{n\geq 0}$ by

$$y_n = \frac{x_n}{z^n}$$

for $n \geq 0$. One can easily check by induction on j that

$$(T - z \cdot \mathrm{id})^j(x) = (z^{n+j}(T - \mathrm{id})^j(y)_n)_{n\geq 0},$$

where $(T - \mathrm{id})^j(y)_n$ is the nth component of the sequence $(T - \mathrm{id})^j(y)$. It follows that

$$x \in \ker(T - z \cdot \mathrm{id})^k \quad \text{if and only if} \quad y \in \ker(T - \mathrm{id})^k.$$

We are therefore reduced to understanding $\mathrm{Ker}(T - \mathrm{id})^k$. If $k = 1$, a sequence $x = (x_n)_{n\geq 0}$ is in $\mathrm{Ker}(T - \mathrm{id})^k$ if and only if $x_{n+1} - x_n = 0$ for $n \geq 0$, i.e., x is a constant sequence. If $k = 2$, a sequence $x = (x_n)_{n\geq 0}$ is in $\mathrm{Ker}(T - \mathrm{id})^k$ if and only

if $(T - \mathrm{id})(x)$ is a constant sequence, i.e., the sequence $(x_{n+1} - x_n)_{n\geq 0}$ is constant, that is x is an arithmetic sequence or equivalently

$$x_n = an + b$$

for some complex numbers a, b. In general, we have

Proposition 9.32. *If k is a positive integer, then $\ker(T-\mathrm{id})^k$ is the set of sequences of the form*

$$x_n = a_0 + a_1 n + \ldots + a_{k-1} n^{k-1}$$

with $a_0, \ldots, a_{k-1} \in \mathbf{C}$, a basis of it being given by the sequences

$$x^{(j)} = (n^j)_{n\geq 0}$$

for $0 \leq j \leq k-1$ (with the convention that $0^0 = 1$).

Proof. It suffices to prove that the sequences $x^{(0)}, \ldots, x^{(k-1)}$ form a basis of $\ker(T - \mathrm{id})^k$.

First, we prove that $x^{(0)}, \ldots, x^{(k-1)}$ are linearly independent. Indeed, if not, then we can find complex numbers $u_0, \ldots, u_{k-1}$, not all 0, such that for all $n \geq 0$

$$u_0 + u_1 n + \ldots + u_{k-1} n^{k-1} = 0.$$

The polynomial $u_0 + u_1 X + \ldots + u_{k-1} X^{k-1}$ is then nonzero and has infinitely many roots, a contradiction.

Next, we prove that $x^{(j)} \in \ker(T - \mathrm{id})^k$ for $0 \leq j \leq k-1$, by induction on k. This is clear for $k = 1$, and assuming that it holds for $k-1$, it suffices (thanks to the inductive hypothesis and the inclusion $\ker(T-\mathrm{id})^{k-1} \subset \ker(T-\mathrm{id})^k$) to check that $x^{(k-1)} \in \ker(T - \mathrm{id})^k$, or equivalently that

$$(T - \mathrm{id})x^{(k-1)} = ((n+1)^{k-1} - n^{k-1})_{n\geq 0} \in \ker(T - \mathrm{id})^{k-1}.$$

But the binomial theorem shows that $((n+1)^{k-1} - n^{k-1})_{n\geq 0}$ is a linear combination of $x^{(0)}, \ldots, x^{(k-2)}$, which all belong to $\ker(T - \mathrm{id})^{k-1}$ by the inductive hypothesis, hence the inductive step is proved.

To conclude, it suffices to prove that $\dim \ker(T - \mathrm{id})^k \leq k$ for all k, which we do again by induction on k. This has already been seen for $k = 1$, and if it holds for $k-1$, then the rank-nullity theorem applied to the map

$$T - \mathrm{id} : \ker(T - \mathrm{id})^k \to \ker(T - \mathrm{id})^{k-1}$$

yields

$$\dim \ker(T - \mathrm{id})^k \leq \dim \ker(T - \mathrm{id}) + \dim \ker(T - \mathrm{id})^{k-1}.$$

Now $\dim\ker(T-\mathrm{id}) \leq 1$ and by induction $\dim\ker(T-\mathrm{id})^{k-1} \leq k-1$, hence $\dim\ker(T-\mathrm{id})^k \leq k$ and the inductive step is completed. The proposition is finally proved. □

We can now put everything together and the previous discussion yields the following beautiful:

Theorem 9.33. *Let $a_0, \ldots, a_{d-1}$ be complex numbers. Consider the polynomial*

$$P(X) = X^d - a_{d-1}X^{d-1} - \ldots - a_0 = \prod_{i=1}^{p}(X - z_i)^{k_i}$$

and assume for simplicity that $a_0 \neq 0$, so that all z_i are nonzero.

Let $\mathcal{S}$ be the set of sequences $(x_n)_{n\geq 0}$ of complex numbers such that

$$x_{n+d} = a_0x_n + a_1x_{n+1} + \ldots + a_{d-1}x_{n+d-1}$$

for all $n \geq 0$.

a) A sequence $(x_n)_{n\geq 0}$ is in $\mathcal{S}$ if and only if there are polynomials Q_i with complex coefficients, of degree not exceeding $k_i - 1$, such that for all n

$$x_n = Q_1(n)z_1^n + \ldots + Q_p(n)z_p^n.$$

b) $\mathcal{S}$ is a vector space of dimension d over $\mathbf{C}$, a basis being given by the sequences $(z_i^n n^j)_{1\leq i\leq p, 0\leq j<k_i}$.

We promised that we will use the ideas developed in this chapter to give a very natural and simple proof of the Cayley–Hamilton theorem for matrices with complex entries. It is now time to honor our promise! We will need some topological preliminaries, however...

A sequence of matrices $(A_k)_{k\geq 0}$ in $M_n(\mathbf{C})$ **converges** to a matrix $A \in M_n(\mathbf{C})$ (which we denote by $A_k \to A$) if for all $i, j \in [1, n]$ the sequence with general term the (i, j)-entry of A_k converges (as a sequence of complex numbers) to the (i, j)-entry of A. Equivalently, the sequence $(A_k)_{k\geq 0}$ converges to A if for all $\varepsilon > 0$ we have

$$\max_{1\leq i,j\leq n} |(A_k)_{ij} - A_{ij}| < \varepsilon$$

for all k large enough (depending on ε). We leave it to the reader to check that if $A_k \to A$ and $B_k \to B$, then $A_k + B_k \to A + B$ and $A_k \cdot B_k \to A \cdot B$. Finally, a subset S of $M_n(\mathbf{C})$ is **dense** in $M_n(\mathbf{C})$ if for any matrix $A \in M_n(\mathbf{C})$ there is a sequence of elements of S which converges to A. That is, any matrix in $M_n(\mathbf{C})$ is the limit of a suitable sequence of matrices in S.

The following fundamental result makes the importance of diagonalizable matrices fairly clear.

Theorem 9.34. *The set of diagonalizable matrices in $M_n(\mathbf{C})$ is dense in $M_n(\mathbf{C})$. In other words, any matrix $A \in M_n(\mathbf{C})$ is the limit of a sequence of diagonalizable matrices.*

Proof. Suppose first that T is an upper-triangular matrix with entries t_{ij}. Consider the sequence T_k of matrices, where all entries of T_k except the diagonal ones are equal to the corresponding entries in T, and for which the diagonal entries of T_k are $t_{ii} + \frac{1}{k^i}$. Clearly, $\lim_{k\to\infty} T_k = T$. We claim that if k is large enough, then T_k is diagonalizable. It suffices to check that the eigenvalues of T_k are pairwise distinct. But since T_k is upper-triangular, its eigenvalues are the diagonal entries. Thus it suffices to check that for k large enough the numbers $t_{11} + \frac{1}{k}, t_{22} + \frac{1}{k^2}, \ldots, t_{nn} + \frac{1}{k^n}$ are pairwise distinct, which is clear.

Now let $A \in M_n(\mathbf{C})$ be an arbitrary matrix. By Corollary 9.5 we can write $A = PTP^{-1}$ for some invertible matrix P and some upper-triangular matrix T. By the previous paragraph, there is a sequence D_k of diagonalizable matrices which converges to T. Then $D'_k := PD_kP^{-1}$ is a sequence of diagonalizable matrices which converges to A. Thus any matrix is a limit of diagonalizable matrices and the theorem is proved. □

Remark 9.35. a) We can restate the theorem as follows: given any matrix $A = [a_{ij}] \in M_n(\mathbf{C})$ and any $\varepsilon > 0$, we can find a diagonalizable matrix $B = [b_{ij}] \in M_n(\mathbf{C})$ such that

$$\max_{1\le i,j\le n} |a_{ij} - b_{ij}| < \varepsilon.$$

b) This result is completely **false** over the real numbers: the diagonalizable matrices in $M_n(\mathbf{R})$ are not dense in $M_n(\mathbf{R})$. The reason is that the characteristic polynomial of a diagonalizable matrix is split. One can prove that if $\lim_{n\to\infty} A_n = A$ and A_n is diagonalizable for all n, then the characteristic polynomial of A is split. Conversely, if this happens, then A is trigonalizable in $M_n(\mathbf{R})$ and the proof of the previous theorem easily yields that A is a limit of diagonalizable matrices in $M_n(\mathbf{R})$. We deduce that the trigonalizable matrices in $M_n(\mathbf{R})$ are precisely the limits of sequences of diagonalizable matrices in $M_n(\mathbf{R})$. In other words, a matrix $A \in M_n(\mathbf{R})$ is trigonalizable if and only if it can be approximated to any precision by a diagonalizable matrix in $M_n(\mathbf{R})$.

Using the previous theorem, we can give a very simple and natural proof of the Cayley–Hamilton theorem.

Theorem 9.36 (Cayley–Hamilton). *For any matrix $A \in M_n(\mathbf{C})$ we have $\chi_A(A) = O_n$, that is A is annihilated by its characteristic polynomial.*

Proof. If A is diagonal, the result is clear: if $a_1, \ldots, a_n$ are the diagonal entries of A, then $\chi_A(X) = (X - a_1)\ldots(X - a_n)$ and clearly this polynomial annihilates A (since it vanishes at $a_1, \ldots, a_n$).

Next, suppose that A is diagonalizable. Thus we can write $A = PDP^{-1}$ for an invertible matrix P and a diagonal matrix D. Since A and D are similar, we have $\chi_A = \chi_D$. So we need to check that $\chi_D(A) = O_n$. But

$$\chi_D(A) = \chi_D(PDP^{-1}) = P\chi_D(D)P^{-1} = O_n,$$

the last equality being a consequence of the first paragraph and the equality $\chi_D(PDP^{-1}) = P\chi_D(D)P^{-1}$ being a consequence of linearity and of the equality $(PDP^{-1})^k = PD^kP^{-1}$ for all $k \geq 0$.

Finally, let $A \in M_n(\mathbf{C})$ be arbitrary. By Theorem 9.34 there is a sequence $(A_k)_{k\geq 1}$ of diagonalizable matrices such that $A_k \to A$. The coefficients of χ_{A_k} are polynomial expressions in the coefficients of A_k and since $\lim_{k\to\infty} A_k = A$, it follows that the coefficient of X^d in χ_{A_k} converges to the coefficient of X^d in χ_A for all $d \leq n$. Now write

$$\chi_{A_k}(X) = a_0(k) + a_1(k)X + \ldots + a_n(k)X^n, \quad \chi_A(X) = a_0 + a_1X + \ldots + a_nX^n.$$

By the previous paragraph we know that

$$a_0(k)I_n + a_1(k)A_k + \ldots + a_n(k)A_k^n = O_n$$

for all k. Passing to the limit and using the fact that $A_k^i \to A^i$ and $a_i(k) \to a_i$ for all $i \geq 0$, we deduce that

$$\chi_A(A) = a_0I_n + a_1A + \ldots + a_nA^n =$$
$$\lim_{k\to\infty}(a_0(k)I_n + a_1(k)A_k + \ldots + a_n(k)A_k^n) = O_n,$$

finishing the proof of the theorem. □

Remark 9.37. a) The second half of the proof of the previous theorem essentially proves that if a polynomial equation on $\mathbf{C}^{n^2}$ holds on a dense subset, then it holds everywhere. The reader is strongly advised to convince himself that he can adapt the argument to prove this very useful result.

b) In fact by using some deep facts from algebra one can show that the Cayley–Hamilton theorem for the field $\mathbf{C}$ just proven implies the Cayley–Hamilton theorem over an arbitrary field. One first needs to know that one can choose n^2 elements x_{ij} of $\mathbf{C}$ such that there is no polynomial equation with integer coefficients (in n^2 variables) satisfied by the x_{ij} (this is a generalization of a transcendental number which is a number that satisfies no polynomial equation with integer coefficients). Then since the Cayley–Hamilton theorem holds for the matrix with entries x_{ij}, we conclude that each coefficient of the Cayley–Hamilton theorem gives a polynomial identity in n^2 indeterminates which holds over the integers. Second, one needs to know that for any field F and any n^2 elements a_{ij} of F there is a morphism (a map respecting addition and multiplication) from $\mathbf{Z}[x_{11}, \ldots, x_{nn}]$ to F taking x_{ij} to a_{ij}. Thus each coefficient also vanishes in F for the matrix $A = (a_{ij})$ and the Cayley–Hamilton theorem holds for F.

We will end this chapter by explaining how we can combine the ideas seen so far with Jordan's Theorems 6.40 and 6.41 to obtain a classification up to similarity of **all** matrices $A \in M_n(\mathbf{C})$ (Theorems 6.40 and 6.41 classified nilpotent matrices up to similarity).

Suppose that V is a finite dimensional vector space over a field F and that $T : V \to V$ is a **trigonalizable** linear transformation on V. Recall that this is equivalent to saying that the characteristic polynomial of T is split over F. For instance, if $F = \mathbf{C}$, then any linear transformation on V is trigonalizable. Let

$$\chi_T(X) = \prod_{i=1}^{d} (X - \lambda_i)^{k_i}$$

be the factorization of the characteristic polynomial of T, with $\lambda_1, \ldots, \lambda_d \in F$ pairwise distinct and $k_1, \ldots, k_d$ positive integers. Thus k_i is the algebraic multiplicity of the eigenvalue λ_i.

By the Cayley–Hamilton theorem $\chi_T(T) = 0$, thus Theorem 9.15 yields

$$V = \bigoplus_{i=1}^{d} \ker(T - \lambda_i \cdot \mathrm{id})^{k_i}.$$

We call the subspace

$$C_i = \ker(T - \lambda_i \cdot \mathrm{id})^{k_i}$$

the **characteristic subspace of** λ_i. Note that the λ_i-eigenspace is a subspace of C_i and that the previous relation can be written as

$$V = \bigoplus_{i=1}^{d} C_i.$$

Since T commutes with $(T - \lambda_i \cdot \mathrm{id})^{k_i}$, T leaves invariant $C_i = \ker(T - \lambda_i \cdot \mathrm{id})^{k_i}$, thus **each characteristic subspace C_i is stable under T.**

Let T_i be the restriction of $T - \lambda_i \cdot \mathrm{id}$ to C_i. By definition, $T_i^{k_i} = 0$, thus T_i is a nilpotent transformation on C_i, of index not exceeding k_i. Thus T_i is classified up to similarity by a Jordan matrix, that is there is a basis $\mathcal{B}_i$ of C_i in which the matrix of T_i is

$$\begin{bmatrix} J_{k_{1,i}} & 0 & \ldots & 0 \\ 0 & J_{k_{2,i}} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_{r_i,i}} \end{bmatrix}$$

for a sequence $k_{1,i} \geq \ldots \geq k_{r_i,i}$ of positive integers adding up to $\dim C_i$. We recall that

$$J_k = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

is the Jordan block of size k.

Definition 9.38. If $\lambda \in F$, we let

$$J_n(\lambda) = \lambda \cdot I_n + J_n \in M_n(F)$$

the **Jordan block of size n associated with λ.**

The previous discussion naturally leads to

Theorem 9.39 (Jordan). *Let $T : V \to V$ be a **trigonalizable** linear transformation on a finite dimensional vector space. Then there is a basis of V in which the matrix of T is of the form*

$$\begin{bmatrix} J_{k_1}(\lambda_1) & 0 & \ldots & 0 \\ 0 & J_{k_2}(\lambda_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d}(\lambda_d) \end{bmatrix}$$

for some positive integers $k_1, \ldots, k_d$ adding up to n and some $\lambda_1, \ldots, \lambda_d \in F$.

Proof. With notations as above, we found a basis $\mathcal{B}_i$ of C_i in which the matrix of the restriction of T to C_i is $J_{\dim C_i}(\lambda_i)$. Patching these bases $\mathcal{B}_i$ yields a basis of V in which the matrix of T has the desired form. □

We can restate the previous theorem in terms of matrices:

Theorem 9.40 (Jordan). *Any **trigonalizable** matrix $A \in M_n(F)$ is similar to a matrix of the form*

$$\begin{bmatrix} J_{k_1}(\lambda_1) & 0 & \ldots & 0 \\ 0 & J_{k_2}(\lambda_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d}(\lambda_d) \end{bmatrix}$$

for some positive integers $k_1, \ldots, k_d$ adding up to n and some $\lambda_1, \ldots, \lambda_d \in F$.

The story isn't quite finished: we would like to know when two block-diagonal matrices as in the theorem are similar, in other words we would like to know if $\lambda_1, \ldots, \lambda_d$ and $k_1, \ldots, k_d$ are determined by the similarity class of the matrix

$$\begin{bmatrix} J_{k_1}(\lambda_1) & 0 & \ldots & 0 \\ 0 & J_{k_2}(\lambda_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d}(\lambda_d) \end{bmatrix}. \qquad (\star)$$

Suppose that A is a matrix similar to the matrix ($\star$). Then the characteristic polynomial of A is

$$\chi_A(X) = \prod_{i=1}^{d} \chi_{J_{k_i}}(\lambda_i)(X).$$

Now, since J_n is nilpotent we have $\chi_{J_n}(X) = X^n$ and so

$$\chi_{J_n(\lambda)}(X) = (X - \lambda)^n.$$

It follows that

$$\chi_A(X) = \prod_{i=1}^{d} (X - \lambda_i)^{k_i}$$

and so necessarily $\lambda_1, \ldots, \lambda_d$ are all eigenvalues of A. **Note that we did not assume that $\lambda_1, \ldots, \lambda_d$ are pairwise distinct**, thus we cannot conclude from the previous equality that $k_1, \ldots, k_d$ are the algebraic multiplicities of the eigenvalues of A. This is not true in general: **several Jordan blocks corresponding to a given eigenvalue may appear**. The problem of uniqueness is completely solved by the following:

Theorem 9.41. *Suppose that a matrix $A \in M_n(F)$ is similar to*

$$\begin{bmatrix} J_{k_1}(\lambda_1) & 0 & \ldots & 0 \\ 0 & J_{k_2}(\lambda_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & J_{k_d}(\lambda_d) \end{bmatrix}$$

for some positive integers $k_1, \ldots, k_d$ adding up to n and some $\lambda_1, \ldots, \lambda_d \in F$. Then

a) Each λ_i is an eigenvalue of A.
b) For each eigenvalue λ of A and each positive integer m, the number of Jordan blocks $J_m(\lambda)$ among $J_{k_1}(\lambda_1), \ldots, J_{k_d}(\lambda_d)$ is

$$N_m(\lambda) = \operatorname{rank}(A - \lambda I_n)^{m+1} - 2\operatorname{rank}(A - \lambda I_n)^m + \operatorname{rank}(A - \lambda I_n)^{m-1}$$

and depends only on the similarity class of A.

Proof. We have already seen part a). The proof of part b) is very similar to the solution of Problem 6.43. More precisely, let $B = A - \lambda I_n$ and observe that B^m is similar to $\begin{bmatrix} (J_{k_1}(\lambda_1) - \lambda I_{k_1})^m & 0 & \dots & 0 \\ 0 & (J_{k_2}(\lambda_2) - \lambda I_{k_2})^m & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (J_{k_d}(\lambda_d) - \lambda I_{k_d})^m \end{bmatrix}$, thus

$$\operatorname{rank}(B^m) = \sum_{i=1}^{d} \operatorname{rank}(J_{k_i}(\lambda_i) - \lambda I_{k_i})^m.$$

Now, the rank of $(J_n(\lambda) - \mu I_n)^m$ is

- n if $\lambda \neq \mu$, as in this case

$$J_n(\lambda) - \mu I_n = J_n + (\lambda - \mu) I_n$$

  is invertible,
- $n - m$ for $\lambda = \mu$ and $m \leq n$, as follows from Problem 6.42.
- 0 for $\lambda = \mu$ and $m > n$, as $J_n^n = O_n$.

Hence, if $N_m(\lambda)$ is the number of Jordan blocks $J_m(\lambda)$ among $J_{k_1}(\lambda_1), \dots, J_{k_d}(\lambda_d)$, then

$$\operatorname{rank}(B^m) = \sum_{\substack{\lambda_i = \lambda \\ k_i \geq m}} (k_i - m) + \sum_{\lambda_i \neq \lambda} k_i,$$

then subtracting these relations for $m - 1$ and m yields

$$\operatorname{rank}(B^{m-1}) - \operatorname{rank}(B^m) = \sum_{\substack{\lambda_i = \lambda \\ k_i \geq m}} 1$$

and finally

$$\operatorname{rank}(B^{m-1}) - 2\operatorname{rank}(B^m) + \operatorname{rank}(B^{m+1}) = (\operatorname{rank}(B^{m-1}) - \operatorname{rank}(B^m)) -$$
$$(\operatorname{rank}(B^m) - \operatorname{rank}(B^{m+1})) = \sum_{\substack{\lambda_i = \lambda \\ k_i = m}} 1 = N_m(\lambda),$$

as desired. □

Note that if an eigenvalue λ has algebraic multiplicity 1, then there is a single Jordan block attached to λ, and it has size 1.

Example 9.42. Consider the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -2 \end{bmatrix}.$$

We compute $\chi_A(X)$ by expanding $\det(XI_5 - A)$ with respect to the third row and obtain (using again an expansion with respect to the second row in the new determinant)

$$\chi_A(X) = X \begin{vmatrix} X-1 & 0 & 0 & -2 \\ 0 & X & 0 & 0 \\ 0 & -1 & X & 0 \\ 1 & 0 & 0 & X+2 \end{vmatrix} = X^2 \begin{vmatrix} X-1 & 0 & 2 \\ 0 & X & 0 \\ 1 & 0 & X+2 \end{vmatrix}$$

$$= X^3 \begin{vmatrix} X-1 & -2 \\ 1 & X+2 \end{vmatrix} = X^4(X+1).$$

The eigenvalue -1 has algebraic multiplicity 1, thus there is a single Jordan block associated with this eigenvalue, of size 1. Let us deal now with the eigenvalue 0, which has algebraic multiplicity 4. Let N_m be the number of Jordan blocks of size m associated with this eigenvalue. By the previous theorem

$$N_1 = \operatorname{rank}(A^2) - 2\operatorname{rank}(A) + 5,$$

$$N_2 = \operatorname{rank}(A^3) - 2\operatorname{rank}(A^2) + \operatorname{rank}(A)$$

and so on. One easily checks that A has rank 3. Next, one computes

$$A^2 = \begin{bmatrix} -1 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -2 \end{bmatrix}.$$

Note that A^2 has rank 2 (it is apparent that a basis of the space spanned by its rows is given by the first and fourth row) and A^3 has rank 1. Thus

$$N_1 = 2 - 2 \cdot 3 + 5 = 1,$$

thus there is one Jordan block of size 1 and

$$N_2 = 1 - 2 \cdot 2 + 3 = 0,$$

thus there is no Jordan block of size 2. Since the sum of the sizes of the Jordan blocks associated with the eigenvalue 0 is 4, and since we already know that there is a block of size 1 and no block of size 2, we deduce that there is one block of size 3 and so the Jordan canonical form of A is

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

9.3.1 Problems for Practice

1. Given a real number ω and two real numbers a, b, find all twice differentiable functions $f : \mathbf{R} \to \mathbf{R}$ satisfying $f(0) = a$, $f'(0) = b$ and

$$f'' + \omega^2 f = 0$$

2. Find all smooth functions $f : \mathbf{R} \to \mathbf{R}$ such that $f(0)=1$, $f'(0)=0$, $f''(0)=0$ and

$$f''' + f'' + f' + f = 0.$$

3. Let V be a finite dimensional F-vector space and let $T : V \to V$ be a linear transformation such that $T^3 = \mathrm{id}$.

   a) Prove that $V = \mathrm{Ker}(T - \mathrm{id}) \oplus \mathrm{Ker}(T^2 + T + \mathrm{id})$.
   b) Prove that

$$\mathrm{rank}(T - \mathrm{id}) = \dim \mathrm{Ker}(T^2 + T + \mathrm{id}).$$

   c) Deduce that

$$V = \mathrm{Ker}(T - \mathrm{id}) \oplus \mathrm{Im}(T - \mathrm{id}).$$

4. Describe the sequences $(x_n)_{n \geq 0}$ of complex numbers such that

$$x_{n+4} + x_{n+3} - x_{n+1} - x_n = 0$$

   for all $n \geq 0$.
5. Find the Jordan canonical form of the matrix

$$A = \begin{bmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{bmatrix}.$$

6. Compute the Jordan canonical form of the matrix

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

7. Consider the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

   a) Prove that $A^3 = O_3$ and find the characteristic polynomial of A.
   b) Find the Jordan canonical form of A.

8. What are the possible Jordan forms of a matrix whose characteristic polynomial is $(X-1)(X-2)^2$?
9. Consider a matrix $A \in M_6(\mathbf{C})$ of rank 4 whose minimal polynomial is $X(X-1)(X-2)^2$.

   a) What are the eigenvalues of A?
   b) Is A diagonalizable?
   c) What are the possible forms of the Jordan canonical form of A?

10. Prove that any matrix similar to a matrix of the form

$$\begin{bmatrix} J_{k_1}(\lambda_1) & 0 & \dots & 0 \\ 0 & J_{k_2}(\lambda_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{k_d}(\lambda_d) \end{bmatrix}$$

    is trigonalizable (this is a converse to Jordan's theorem).
11. a) What is the minimal polynomial of $J_n(\lambda)$ when $\lambda \in \mathbf{C}$ and $n \geq 1$?
    b) Explain how we can compute the minimal polynomial of a matrix in terms of its Jordan canonical form.

12. Prove that two matrices $A, B \in M_n(\mathbf{C})$ are similar if and only if $P(A)$ and $P(B)$ have the same rank for all polynomials $P \in \mathbf{C}[X]$.
13. Use Jordan's theorem to prove that any matrix $A \in M_n(\mathbf{C})$ is similar to its transpose.
14. a) Prove that if $A \in M_n(\mathbf{C})$ is similar to $2A$, then A is nilpotent.
    b) Use Jordan's theorem to prove that if $A \in M_n(\mathbf{C})$ is nilpotent then A is similar to $2A$.
15. Let $T : V \to V$ be a trigonalizable linear transformation on a finite dimensional vector space V over a field F. Let

$$\chi_T(T) = \prod_{i=1}^{d} (X - \lambda_i)^{k_i}$$

be the factorization of its characteristic polynomial and let

$$C_i = \ker(T - \lambda_i \cdot \mathrm{id})^{k_i}$$

be the characteristic subspace of λ_i.

a) Prove that $\ker(T - \lambda_i \cdot \mathrm{id})^k = C_i$ for all $k \geq k_i$. Hint: use Theorem 9.15 to show that $V = \ker(T - \lambda_i \cdot \mathrm{id})^k \oplus \oplus_{j \neq i} C_j$, then take dimensions.
b) Prove that

$$\dim C_i = k_i.$$

Hint: consider the matrix of T with respect to a basis of V obtained by patching a basis of C_i and a basis of a complementary subspace of C_i. What is its characteristic polynomial?
c) Prove that the smallest positive integer k for which

$$\ker(T - \lambda_i \cdot \mathrm{id})^k = C_i$$

is the multiplicity of λ_i as root of the minimal polynomial of T.

16. (The Dunford–Jordan decomposition) a) Using Jordan's theorem, prove that any trigonalizable linear transformation $T : V \to V$ on a finite dimensional vector space is the sum of a diagonalizable and of a nilpotent transformation, the two transformations commuting with each other.

    b) State the result obtained in a) in terms of matrices.
    b) Conversely, prove the sum of a nilpotent and of a diagonalizable transformations which commute with each other is trigonalizable.

17. (More on the Dunford–Jordan decomposition) Let $T : V \to V$ be a trigonalizable linear transformation with

$$\chi_T(T) = \prod_{i=1}^{d} (X - \lambda_i)^{k_i}$$

as in Problem 15. Let C_i be the characteristic subspace of the eigenvalue λ_i. We define the λ_i**-spectral projection** π_{λ_i} as the projection of V onto C_i along $\oplus_{j\neq i} C_j$. Thus by definition if $v \in V$ is written as $v_1 + \ldots + v_d$ with $v_i \in C_i$, then

$$\pi_{\lambda_i}(v) = c_i.$$

a) Use the proof of Theorem 9.15 to show that

$$\pi_{\lambda_i} \in F[T].$$

b) Let

$$D = \sum_{i=1}^{d} \lambda_i \cdot \pi_{\lambda_i}.$$

Prove that D is a diagonalizable linear transformation on V, that $N = T - D$ is nilpotent and $N \circ D = D \circ N$. Thus D, N give a Dunford–Jordan decomposition of T.

c) Prove that D and N are in $F[T]$.

d) Deduce from part c) that if D' is diagonalizable, N' is nilpotent, D' and N' commute and $D' + N' = T$, then $D' = D$ and $N' = N$. In other words, the pair (D, N) in the Jordan–Dunford decomposition is unique.

e) Find the Dunford–Jordan decomposition of the matrices

$$A = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & -3 \\ 1 & -1 & -6 \\ -1 & 2 & 5 \end{bmatrix}.$$

Chapter 10
Forms

Abstract This chapter has a strong geometrical flavor. It starts with a discussion of bilinear and quadratic forms and uses this to introduce Euclidean spaces and establish their main geometric properties. This is in turn applied to linear algebra, leading to a classification of symmetric and orthogonal matrices with real entries.

Keywords Quadratic form • Bilinear form • Polar form • Euclidean space • Inner-product • Positive-definite matrix • Orthogonal projection • Gram–Schmidt algorithm

The goal of this last chapter is to make a rather detailed study of Euclidean spaces over the real numbers. Euclidean spaces make the link between linear algebra, geometry and analysis. They are therefore of fundamental importance. The geometric insight they offer also reveals unexpected and deep properties of symmetric and orthogonal matrices. Thus on the one hand proving the fundamental theorems concerning Euclidean spaces will use essentially everything we have developed so far, so this is also an opportunity to see real applications of linear algebra, on the other hand the geometry of Euclidean spaces helps discovering and proving many interesting properties of matrices! Among the important topics discussed in this chapter, we mention: basic properties of bilinear and quadratic forms, orthogonality and inequalities in Euclidean spaces, orthogonal projections and their applications to minimization problems, orthogonal bases and their applications, for instance to Fourier analysis, the classification of isometries (i.e., linear transformations preserving distance) of an Euclidean space, the classification of symmetric matrices, and its applications to matrix inequalities, norms, etc. In all this chapter we work with the field $F = \mathbf{R}$ of real numbers. Many exercises (left to the reader) are devoted to the analogous theory over the field of complex numbers.

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_10

10.1 Bilinear and Quadratic Forms

We have already introduced the notion of d-linear form on a vector space in the chapter devoted to determinants. We will be concerned with a special case of this notion, and for the reader's convenience we will give the detailed definition in this special case:

Definition 10.1. Let V be a vector space over $\mathbf{R}$. A **bilinear form** on V is a map $b : V \times V \to \mathbf{R}$ such that

- For all $x \in V$ the map $b(x, \cdot) : V \to \mathbf{R}$ sending v to $b(x, v)$ is linear.
- For all $y \in V$ the map $b(\cdot, y) : V \to \mathbf{R}$ sending v to $b(v, y)$ is linear.

The bilinear form b is called **symmetric** if $b(x, y) = b(y, x)$ for all $x, y \in V$.

Remark 10.2. If $x_1, \ldots, x_n \in V, y_1, \ldots, y_m \in V$ and $a_1, \ldots, a_n, c_1, \ldots, c_m \in \mathbf{R}$, then for any bilinear form b on V we have

$$b(\sum_{i=1}^{n} a_i x_i, \sum_{j=1}^{m} c_j y_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i c_j b(x_i, y_j) \tag{10.1}$$

In particular, **if V is finite dimensional and if $e_1, \ldots, e_n$ is a basis of V, then b is uniquely determined by its values at the pairs (e_i, e_j) with** $1 \leq i, j \leq n$ (i.e., if b, b' are bilinear forms on V and $b(e_i, e_j) = b'(e_i, e_j)$ for all $1 \leq i, j \leq n$, then $b = b'$).

Example 10.3. a) If $a_1, \ldots, a_n$ are real numbers and $V = \mathbf{R}^n$, then setting for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$

$$b(x, y) = a_1 x_1 y_1 + \ldots + a_n x_n y_n$$

yields a symmetric bilinear form on V. The choice $a_1 = \ldots = a_n = 1$ is particularly important and in this case we call b the **canonical inner product on $\mathbf{R}^n$.**

b) Consider the space V of continuous, real-valued functions on $[-1, 1]$. Then

$$b(f, g) = \int_{-1}^{1} f(x)g(x)dx$$

is a symmetric bilinear form on V, as the reader can easily check.

c) Let V be the space $M_n(\mathbf{R})$ of $n \times n$ matrices with real entries, and consider the map $b : V \times V \to \mathbf{R}$ defined by

$$b(A, B) = \mathrm{Tr}(AB).$$

Then b is a symmetric bilinear form on V. A slightly different and more commonly used variant is

$$b'(A, B) = \mathrm{Tr}(A^t B).$$

The reason why b' is preferred to b is that one can easily check that if $A = [a_{ij}]$ and $B = [b_{ij}]$, then

$$b'(A, B) = \sum_{i,j=1}^{n} a_{ij} b_{ij},$$

that is if we identify $V = \mathbf{R}^{n^2}$ via the canonical basis of V, then b' becomes identified with the canonical inner product on $\mathbf{R}^{n^2}$.

d) Let V be the space of sequences $(x_n)_{n\geq 1}$ of real numbers for which $\sum_{n\geq 1} x_n^2$ is a convergent series. Define

$$b(x, y) = \sum_{n\geq 1} x_n y_n$$

for $x = (x_n)_{n\geq 1}$ and $y = (y_n)_{n\geq 1}$ in V. Note that the series $\sum_{n\geq 1} x_n y_n$ converges since it converges absolutely. Indeed, we have $(|x_n| - |y_n|)^2 \geq 0$ which can be written as

$$|x_n y_n| \leq \frac{x_n^2 + y_n^2}{2}$$

and by assumption the series with general term $\frac{x_n^2+y_n^2}{2}$ converges. One can easily check that b is a symmetric bilinear form on V.

e) Let V be the space of polynomials with real coefficients and, for $P, Q \in V$, define

$$b(P, Q) = \sum_{n\geq 1} \frac{P(n)Q(n)}{2^n}.$$

Note that the series converges absolutely, since $n^k/2^n = O(1/n^2)$ for all $k \geq 1$. Then b is a symmetric bilinear form.

It follows easily by unwinding definitions that the set of all bilinear forms on V is naturally a vector subspace of the vector space of all maps $V \times V \to \mathbf{R}$. Moreover, the subset of symmetric bilinear forms is a subspace of the space of all bilinear forms on V. To any bilinear form b one can attach a map of one variable

$$q : V \to \mathbf{R}, \quad q(x) = b(x, x).$$

This is called the **quadratic form attached to** b. Let us formally define quadratic forms:

Definition 10.4. A **quadratic form** on V is a map $q : V \to \mathbf{R}$ for which there is a bilinear form $b : V \times V \to \mathbf{R}$ such that $q(x) = b(x, x)$ for all $x \in V$.

A natural question is whether the bilinear form b attached to a quadratic form as in the previous definition is uniquely determined by the quadratic form. So the question is whether we can have two different bilinear forms b_1, b_2 such that

$$b_1(x, x) = b_2(x, x)$$

for all x. Stated differently, is there a nonzero bilinear form b such that $b(x, x) = 0$ for all $x \in V$? The answer is yes: consider the bilinear form $b : \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}$ defined by

$$b((x_1, y_1), (x_2, y_2)) = x_1 y_2 - x_2 y_1.$$

Clearly this is a nonzero bilinear form and $b(x, x) = 0$ for all x. On the other hand, **if we further impose that b should be symmetric, then we have uniqueness**, as shows the following fundamental:

Theorem 10.5. *For any quadratic form $q : V \to \mathbf{R}$ there is a unique **symmetric** bilinear form $b : V \times V \to \mathbf{R}$ such that $q(x) = b(x, x)$ for all $x \in V$. It is determined by the **polarization identity***

$$b(x, y) = \frac{q(x + y) - q(x) - q(y)}{2}.$$

Proof. Fix a quadratic form $q : V \to \mathbf{R}$. By hypothesis we can find a bilinear (but not necessarily symmetric) form B such that $q(x) = B(x, x)$ for all $x \in V$. Define a map $b : V \times V \to \mathbf{R}$ by

$$b(x, y) = \frac{q(x + y) - q(x) - q(y)}{2}.$$

We claim that b is a symmetric bilinear form and $b(x, x) = q(x)$. By definition, we have

$$b(x, y) = \frac{B(x + y, x + y) - B(x, x) - B(y, y)}{2}.$$

Since B is bilinear, we can write

$$B(x + y, x + y) = B(x, x) + B(x, y) + B(y, x) + B(y, y).$$

Thus

$$b(x, y) = \frac{B(x, y) + B(y, x)}{2}.$$

This makes it clear that $b(x,x) = B(x,x) = q(x)$ and that $b(x,y) = b(y,x)$ for all $x, y \in V$. It remains to see that b is bilinear. But for fixed x the maps $B(x,\cdot)$ and $B(\cdot,x)$ are linear (since B is bilinear), thus so is the map

$$b(x,\cdot) = \frac{B(x,\cdot) + B(\cdot,x)}{2}.$$

Similarly, $b(\cdot,x)$ is linear for all $x \in V$, establishing that b is bilinear and proving the claim.

Let us now show that b is unique. If b' is another bilinear symmetric form such that $b'(x,x) = q(x)$ for all x, then a computation as in the previous paragraph gives

$$q(x+y) = b'(x+y, x+y) =$$

$$b'(x,x) + 2b'(x,y) + b'(y,y) = q(x) + q(y) + 2b'(x,y),$$

thus necessarily $b'(x,y) = b(x,y)$ for all x, y, that is $b' = b$. □

Definition 10.6. If b is attached to q as in the previous theorem, we call b the **polar form** of q.

Example 10.7. a) Consider the space $V = \mathbf{R}^n$ and the map $q : \mathbf{R}^n \to \mathbf{R}$ defined by

$$q(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2.$$

Then q is a quadratic form and its polar form is

$$b((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = x_1 y_1 + \ldots + x_n y_n.$$

Indeed, let us compute for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$

$$\frac{q(x+y) - q(x) - q(y)}{2} = \frac{\sum_{i=1}^n (x_i + y_i)^2 - \sum_{i=1}^n x_i^2 - \sum_{i=1}^n y_i^2}{2}$$

$$= \sum_{i=1}^n x_i y_i.$$

The map $(x,y) \mapsto \sum_{i=1}^n x_i y_i$ being bilinear and symmetric, it follows on the one hand that q is a quadratic form and on the other hand that b is its polar form.

b) Consider the space V of continuous real-valued maps on $[0,1]$ and define $q : V \to \mathbf{R}$ by

$$q(f) = \int_0^1 f(x)^2 dx.$$

To see that q is a quadratic form and to find the polar form of f, we compute

$$\frac{q(f+g)-q(f)-q(g)}{2} = \frac{\int_0^1 (f(x)+g(x))^2 dx - \int_0^1 f(x)^2 dx - \int_0^1 g(x)^2 dx}{2}$$

$$= \int_0^1 f(x)g(x)dx.$$

Since the map b defined by $b(f,g) = \int_0^1 f(x)g(x)dx$ is bilinear and symmetric, it follows that q is a quadratic form with polar form b.

c) As a counter-example, consider the map $q : \mathbf{R}^2 \to \mathbf{R}$ defined by

$$q(x,y) = x^2 + 2y^2 + 3x.$$

We claim that q is not a quadratic form. Indeed, otherwise letting b its polar form we would have

$$b((x,y),(x,y)) = x^2 + 2y^2 + 3x$$

for all $x, y \in \mathbf{R}^2$. Replacing x by $-x$ and y by $-y$ and taking into account that b is bilinear, we obtain

$$x^2 + 2y^2 + 3x = b((x,y),(x,y)) = b(-(x,y),-(x,y)) =$$

$$b((-x,-y),(-x,-y)) = x^2 + 2y^2 - 3x,$$

thus $6x = 0$ and this for all $x \in \mathbf{R}$, which is plainly absurd.

The previous theorem establishes therefore a **bijection between quadratic forms and symmetric bilinear forms**: any symmetric bilinear form b determines a quadratic form $x \mapsto b(x,x)$, and any quadratic form determines a symmetric bilinear form, namely its polar form.

Problem 10.8. Let q be a quadratic form on V, with polar form b.

a) Prove that for all $x, y \in V$

$$b(x,y) = \frac{q(x+y)-q(x-y)}{4}.$$

b) (**Parallelogram law**) Prove that for all $x, y \in V$

$$q(x+y) + q(x-y) = 2(q(x) + q(y)).$$

c) (**Pythagorean theorem**) Prove that for all $x, y \in V$ we have $b(x, y) = 0$ if and only if

$$q(x + y) = q(x) + q(y).$$

Solution. a) By the polarization identity we have

$$q(x + y) = q(x) + q(y) + 2b(x, y)$$

and (noting that $q(-y) = q(y)$ and $b(x, -y) = -b(x, y)$)

$$q(x - y) = q(x) + q(y) - 2b(x, y).$$

Subtracting the two previous relations yields the desired result.

b) It suffices to add the two relations established in the proof of part a).

c) This follows directly from the polarization identity. □

Let us try to understand the quadratic forms on $\mathbf{R}^n$. If q is a quadratic form on $\mathbf{R}^n$ with polar form b, and if $e_1, \ldots, e_n$ is the canonical basis of $\mathbf{R}^n$, then for all $x = x_1e_1 + \ldots + x_ne_n \in \mathbf{R}^n$ we have, using Remark 10.2

$$q(x_1, \ldots, x_n) = b(x_1e_1 + \ldots + x_ne_n, x_1e_1 + \ldots + x_ne_n) =$$

$$\sum_{i,j=1}^{n} b(e_i, e_j)x_ix_j = \sum_{i,j=1}^{n} a_{ij}x_ix_j,$$

with $a_{ij} = b(e_i, e_j)$. Notice that since $b(e_i, e_j) = b(e_j, e_i)$, we have $a_{ij} = a_{ji}$, thus any quadratic form q on $\mathbf{R}^n$ can be written

$$q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j = \sum_{i=1}^{n} a_{ii}x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij}x_ix_j,$$

with $A = [a_{ij}]$ a symmetric matrix.

Conversely, if $A = [a_{ij}]$ is **any** matrix in $M_n(\mathbf{R})$ (not necessarily symmetric), then the map

$$q : \mathbf{R}^n \to \mathbf{R}, \quad q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$$

is a quadratic form on $\mathbf{R}^n$, with polar form

$$b((x_1, \ldots, x_n), (x_1', \ldots, x_n')) = \sum_{i,j=1}^{n} \frac{a_{ij}(x_ix_j' + x_jx_i')}{2}.$$

We leave this as an easy exercise for the reader. Notice that

$$q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j = \sum_{i,j=1}^{n} b_{ij} x_i x_j,$$

with

$$b_{ij} = \frac{a_{ij} + a_{ji}}{2},$$

and the matrix $B = [b_{ij}]$ is symmetric.

There is another natural way of constructing quadratic forms on $\mathbf{R}^n$: pick real numbers $\alpha_1, \ldots, \alpha_r$ and linear forms $l_1, \ldots, l_r$ on $\mathbf{R}^n$, and set

$$q(x) = \alpha_1 l_1(x)^2 + \ldots + \alpha_r l_r(x)^2.$$

Then q is a quadratic form on $\mathbf{R}^n$, with associated polar form given by

$$b(x, y) = \sum_{i=1}^{r} \alpha_i l_i(x) l_i(y),$$

as the reader can easily check. The following amazing result due to Gauss says that we obtain in this way all quadratic forms on $\mathbf{R}^n$. Moreover, Gauss described an algorithm which allows us to write a given quadratic form q in the form

$$q = \alpha_1 l_1^2 + \ldots + \alpha_r l_r^2,$$

with $l_1, \ldots, l_r$ linearly independent linear forms. This algorithm will be described in the (long) proof of the following theorem.

Theorem 10.9 (Gauss). *Let q be a quadratic form on $V = \mathbf{R}^n$. There are real numbers $\alpha_1, \ldots, \alpha_r$ and linearly independent linear forms $l_1, \ldots, l_r \in V^*$ such that for all $x \in V$*

$$q(x) = \alpha_1 l_1(x)^2 + \ldots + \alpha_r l_r(x)^2.$$

Before giving the proof of the theorem, let us make some further remarks on the statement. Of course, we may assume that $\alpha_i \neq 0$ for $1 \leq i \leq r$, otherwise simply delete the corresponding term $\alpha_i l_i^2$. Let I be the set of those i for which $\alpha_i > 0$ and let J be the set of those i for which $\alpha_i < 0$. Then

$$q(x) = \sum_{i \in I} (\sqrt{\alpha_i} l_i)^2(x) - \sum_{i \in J} (\sqrt{-\alpha_i} l_i)^2(x)$$

and defining

$$L_i = \sqrt{\alpha_i} l_i \quad \text{if} \quad i \in I \quad \text{and} \quad L_i = \sqrt{-\alpha_i} l_i \quad \text{if} \quad i \in J,$$

we obtain

$$q = \sum_{i \in I} L_i^2 - \sum_{i \in J} L_i^2.$$

Moreover, since $l_1, \ldots, l_r$ are linearly independent, so are $L_1, \ldots, L_r$. In other words, we can refine the previous theorem by asking that $\alpha_i \in \{-1, 1\}$ for all i. One can prove that the number of elements of I, J, as well as the number r are uniquely determined by q (this is **Sylvester's inertia theorem**). The pair $(|I|, |J|)$ consisting in the number of elements of I and J is called the **signature** of q. We call $|I| + |J| = r$ the **rank** of q (we will see another interpretation of r later on, which will also explain its name).

We will start now the **algorithmic** proof of Theorem 10.9, by induction on n. For $n = 1$ we can write $q(x_1) = \alpha_1 x_1^2$, where $x_1 \in \mathbf{R}$ and $\alpha_1 = q(1) \in \mathbf{R}$, so the result holds.

Assume now that the result holds for $n - 1$. We can write

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij} x_i x_j$$

for some scalars $a_{ij} \in \mathbf{R}$. We will discuss two cases:

- There is $i \in \{1, 2, \ldots, n\}$ such that $a_{ii} \neq 0$. Without loss of generality, we may assume that $a_{nn} \neq 0$. We consider $q(x_1, \ldots, x_n)$ as a quadratic polynomial in the variable x_n and complete the square, to obtain

$$q(x_1, \ldots, x_n) = a_{nn} x_n^2 + 2 \left(\sum_{i=1}^{n-1} a_{in} x_i \right) x_n + \sum_{i=1}^{n-1} a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n-1} a_{ij} x_i x_j =$$

$$a_{nn} \left(x_n + \sum_{i=1}^{n-1} \frac{a_{in}}{a_{nn}} x_i \right)^2 - a_{nn} \left(\sum_{i=1}^{n-1} \frac{a_{in}}{a_{nn}} x_i \right)^2 + \sum_{i=1}^{n-1} a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n-1} a_{ij} x_i x_j$$

$$= a_{nn} \left(x_n + \sum_{i=1}^{n-1} \frac{a_{in}}{a_{nn}} x_i \right)^2 + q'(x_1, \ldots, x_{n-1}),$$

where q' is a quadratic form on $\mathbf{R}^{n-1}$. By induction, we can write

$$q'(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{r} \alpha_i L_i(x_1, \ldots, x_{n-1})^2$$

for some linearly independent linear forms L_i in $x_1, \ldots, x_{n-1}$. Defining

$$l_{r+1}(x_1, \ldots, x_n) = x_n + \sum_{i=1}^{n-1} \frac{a_{in}}{a_{nn}} x_i, \quad \alpha_{r+1} = a_{nn}$$

and

$$l_i(x_1, \ldots, x_n) = L_i(x_1, \ldots, x_{n-1})$$

for $1 \leq i \leq r$ we obtain

$$q(x) = \sum_{i=1}^{r+1} \alpha_i l_i(x)^2$$

for all $x \in V$ and the inductive step is finished (we leave it to the reader to check that $l_1, \ldots, l_{r+1}$ are linearly independent).

- All $a_{ii} = 0$. If all $a_{ij} = 0$, then $q = 0$ and the result is clear. If not, without loss of generality we may assume that $a_{n-1,n} \neq 0$. We use the identity

$$axy + bx + cy = a\left(xy + \frac{b}{a}x + \frac{c}{a}y\right) = a\left(x + \frac{c}{a}\right)\left(y + \frac{b}{a}\right) - \frac{bc}{a}$$

to rewrite

$$q(x_1, \ldots, x_n) = 2a_{n-1,n}x_{n-1}x_n + 2\sum_{i=1}^{n-2} a_{in}x_i x_n$$

$$+2\sum_{i=1}^{n-2} a_{i,n-1}x_i x_{n-1} + 2\sum_{1 \leq i < j \leq n-2} a_{ij}x_i x_j =$$

$$2a_{n-1,n}\left(x_{n-1} + \sum_{i=1}^{n-2} \frac{a_{i,n}}{a_{n-1,n}}x_i\right) \cdot \left(x_n + \sum_{i=1}^{n-2} \frac{a_{i,n-1}}{a_{n-1,n}}x_i\right) + q'(x_1, \ldots, x_{n-2})$$

for some quadratic form q' on $\mathbf{R}^{n-2}$. Applying the inductive hypothesis, we can write

$$q'(x_1, \ldots, x_{n-2}) = \sum_{i=1}^{r} \alpha_i L_i(x_1, \ldots, x_{n-2})^2$$

for some linearly independent linear forms L_i of $x_1, \ldots, x_{n-2}$, as well as some scalars α_i. Using the identity

$$ab = \frac{(a+b)^2 - (a-b)^2}{4},$$

we obtain

$$2a_{n-1,n}\left(x_{n-1} + \sum_{i=1}^{n-2} \frac{a_{i,n}}{a_{n-1,n}} x_i\right) \cdot \left(x_n + \sum_{i=1}^{n-2} \frac{a_{i,n-1}}{a_{n-1,n}} x_i\right) =$$

$$\frac{a_{n-1,n}}{2}(l_{r+1}(x_1, \ldots, x_n)^2 - l_{r+2}(x_1, \ldots, x_n)^2),$$

where

$$l_{r+1}(x_1, \ldots, x_n) = x_{n-1} + x_n + \sum_{i=1}^{n-2} \frac{a_{i,n} + a_{i,n-1}}{a_{n-1,n}} x_i,$$

and

$$l_{r+2}(x_1, \ldots, x_n) = x_{n-1} - x_n + \sum_{i=1}^{n-2} \frac{a_{i,n} - a_{i,n-1}}{a_{n-1,n}} x_i.$$

All in all, setting

$$\alpha_{r+1} = -\alpha_{r+2} = \frac{a_{n-1,n}}{2}$$

we have

$$q(x) = \sum_{i=1}^{r+2} \alpha_i l_i(x)^2.$$

We leave it to the reader to check that $l_1, \ldots, l_{r+2}$ are linearly independent. This finishes the proof of Theorem 10.9.

Problem 10.10. Implement the algorithm described in the previous proof in each of the following cases:

a) q is the quadratic form on $\mathbf{R}^3$ defined by

$$q(x, y, z) = xy + yz + zx.$$

b) q is the quadratic form on $\mathbf{R}^3$ defined by

$$q(x, y, z) = (x - y)^2 + (y - z)^2 + (z - x)^2.$$

Solution. a) With the notations of the previous proof, we have $a_{ii} = 0$ for $1 \leq i \leq 3$, thus we are in the second case of the above proof. We focus on the nonzero term yz and we write

$$q(x, y, z) = (y + x)(z + x) - x^2.$$

Next, using the identity

$$ab = \frac{(a + b)^2 - (a - b)^2}{4}$$

we obtain

$$(y + x)(z + x) = \frac{(2x + y + z)^2 - (y - z)^2}{4}.$$

We conclude that

$$q(x, y, z) = \frac{1}{4}(2x + y + z)^2 - \frac{1}{4}(y - z)^2 - x^2$$

and one easily checks that the linear forms $2x + y + z$, $y - z$ and x are linearly independent.

b) It is tempting to say that q is already written in the desired form, but the problem is that the linear forms $x - y$, $y - z$, and $z - x$ are not linearly independent (they add up to 0). Therefore we write (by brutal expansion)

$$q(x, y, z) = (x - y)^2 + (y - z)^2 + (z - x)^2 =$$

$$2(x^2 + y^2 + z^2 - xy - yz - zx).$$

We are in the first case of the previous proof, so we focus on the term x^2 and try to complete the square:

$$q(x, y, z) = 2\left(x - \frac{y + z}{2}\right)^2 - \frac{(y + z)^2}{2} + 2y^2 + 2z^2 - 2yz =$$

$$2\left(x - \frac{y + z}{2}\right)^2 + \frac{3y^2 + 3z^2 - 6yz}{2} = 2\left(x - \frac{y + z}{2}\right)^2 + \frac{3}{2}(y - z)^2$$

and we easily check that the linear forms $x - \frac{y+z}{2}$ and $y - z$ are linearly independent. □

10.1.1 Problems for Practice

1. Prove that the map

$$b : \mathbf{R}^2 \times \mathbf{R}^2 \to \mathbf{R}, \quad b((x, y), (z, t)) = xt - yz$$

is a bilinear form on $\mathbf{R}^2$. Describe the associated quadratic form.

2. Consider the map $q : \mathbf{R}^4 \to \mathbf{R}$,

$$q(x, y, z, t) = xy + 2z^2 + tx - t^2.$$

a) Prove that q is a quadratic form and find its polar form.
b) Implement Gauss' algorithm and write q in the form $\sum_{i=1}^{r} \alpha_i l_i^2$ with real numbers α_i and linearly independent linear forms l_i.
c) What is the signature of q?

3. Use Gauss' algorithm to write each of the following quadratic forms as $\sum_{i=1}^{r} \alpha_i l_i^2$ with linearly independent linear forms $l_1, \ldots, l_r$ and scalars $\alpha_1, \ldots, \alpha_r$.

a) $q(x, y, z) = (x - 2y + z)^2 - (x - y)^2 + z^2$.
b) $q(x, y, z) = (x - 2y + z)^2 + (y - 2z + x)^2 - (z - 2x + y)^2$.
c) $q(x, y, z, t) = xy + yz + zt + tx$.
d) $q(x, y, z) = x^2 + xy + yz + zx$.

For each of these quadratic forms, find its signature and its rank.

4. a) If q is a quadratic form on $\mathbf{R}^n$, is it true that $\{x \in \mathbf{R}^n | q(x) = 0\}$ is a vector subspace of $\mathbf{R}^n$?
b) Describe geometrically $\{x \in \mathbf{R}^n | q(x) = 0\}$ if $q(x, y) = x^2 - 2y^2$, if $q(x, y) = x^2 + y^2$ and finally if $q(x, y, z) = x^2 + y^2 - z^2$.

5. Which of the following maps are quadratic forms:

a) $q : \mathbf{R}^3 \to \mathbf{R}$, $q(x, y, z) = x^2 + y^3 + z^2$.
b) $q : \mathbf{R}^4 \to \mathbf{R}$, $q(x, y, z, t) = xt - z^2 + zt - y$.
c) $q : \mathbf{R}^4 \to \mathbf{R}$, $q(x, y, z, t) = (x + z)(y + t)$?

6. Let V be the space of continuous real-valued maps on $[-1, 1]$ and consider the map $b : V \times V \to \mathbf{R}$ defined by

$$b(f, g) = \int_{-1}^{1} (1 - t^2) f(t) g(t) dt + f'(1) g'(1).$$

a) Prove that b is a symmetric bilinear form on V.
b) If q is the associated quadratic form, find those $f \in V$ for which $q(f) = 0$.

7. Let b be a bilinear form on a vector space V over $\mathbf{R}$. The **kernel of** b is the set $\ker b$ defined by

$$\ker b = \{x \in V | b(x, y) = 0 \quad \forall y \in V\}.$$

   a) Prove that $\ker b$ is a vector subspace of V.
   b) Find the kernel of the polar form of the quadratic form $q(x, y, z) = xy + yz + zx$ on $\mathbf{R}^3$.

8. If b is a bilinear form on a vector space V over $\mathbf{R}$, is it true that $\{(x, y) \in V \times V | b(x, y) = 0\}$ is a vector subspace of $V \times V$?
9. Let $V = M_n(\mathbf{R})$ and consider the map $q : V \to V$ defined by

$$q(A) = \mathrm{Tr}({}^tAA) + (\mathrm{Tr}(A))^2.$$

   Prove that q is a quadratic form on V and describe its polar form.

   One can define bilinear forms over $\mathbf{C}$, but they do not have all the properties one desires. Instead it is standard to take **sesquilinear forms** (sesqui- meaning one-and-a-half).

   Definition. Let V be a vector space over $\mathbf{C}$. A sesquilinear form on V is a map $\varphi : V \times V \to \mathbf{C}$ such that

   i) For all $x \in V$ the map $\varphi(x, \cdot) : V \to \mathbf{C}$ sending y to $\varphi(x, y)$ is linear.
   ii) For all $y \in V$ the map $\varphi(\cdot, y) : V \to \mathbf{C}$ sending x to the complex conjugate $\overline{\varphi(x, y)}$ of $\varphi(x, y) \in \mathbf{C}$ is linear.

   The sesquilinear form φ is called **conjugate symmetric** or **hermitian** if $\varphi(x, y) = \overline{\varphi(y, x)}$ for all $x, y \in V$.

   In the next problems V is a $\mathbf{C}$-vector space.
10. Prove that the set $\mathcal{S}(V)$ of sesquilinear forms on V is a vector subspace of the $\mathbf{C}$-vector space of all maps $\psi : V \times V \to \mathbf{C}$.
11. Prove that the set $H(V)$ of hermitian sesquilinear forms on V is a vector subspace of the $\mathbf{R}$-vector space $\mathcal{S}(V)$. Is $H(V)$ a $\mathbf{C}$-vector subspace of $\mathcal{S}(V)$?
12. Prove that we have a direct-sum decomposition of $\mathbf{R}$-vector spaces

$$\mathcal{S}(V) = H(V) \oplus iH(V).$$

13. Let φ be a hermitian sesquilinear form on V and consider the map $\Phi : V \to \mathbf{C}$ defined by

$$\Phi(x) = \varphi(x, x).$$

   A map $\Phi : V \to \mathbf{C}$ of this form is called a **hermitian quadratic form** and if $\Phi(x) = \varphi(x, x)$ for all $x \in V$, we call the hermitian sesquilinear form φ the **polar form** of Φ.

a) Prove that $\Phi(x) \in \mathbf{R}$ for all $x \in V$.
b) Prove that $\Phi(ax) = |a|^2\Phi(x)$ for all $a \in \mathbf{C}$ and $x \in V$.
c) Prove that for all $x, y \in V$ we have

$$\Phi(x + y) = \Phi(x) + \Phi(y) + 2\mathrm{Re}(\varphi(x, y)).$$

d) Deduce the polarization identity

$$\Phi(x + y) - \Phi(x - y) + i(\Phi(x + iy) - \Phi(x - iy)) = 4\varphi(y, x).$$

Conclude that the polar form of a quadratic hermitian form is unique.
e) Prove the parallelogram law

$$\Phi(x + y) + \Phi(x - y) = 2(\Phi(x) + \Phi(y)).$$

14. Let $V = \mathbf{C}^n$ and consider the map $\Phi : V \to \mathbf{R}$ defined by

$$\Phi(x_1, \ldots, x_n) = |x_1|^2 + |x_2|^2 + \ldots + |x_n|^2$$

for all $(x_1, \ldots, x_n) \in \mathbf{C}^n$. Prove that Φ is a hermitian quadratic form and find its polar form.
15. Let V be the space of continuous maps $f : [0, 1] \to \mathbf{C}$. Answer the same questions as in the previous problem for the map $\Phi : V \to \mathbf{R}$ defined by

$$\Phi(f) = \int_0^1 |f(t)|^2 dt.$$

16. Prove the complex analogue of Gauss' theorem: if Φ is a hermitian quadratic form on $\mathbf{C}^n$, then we can find $\alpha_1, \ldots, \alpha_r \in \{-1, 1\}$ and linearly independent linear forms $l_1, \ldots, l_r$ on $\mathbf{C}^n$ such that for all $x \in \mathbf{C}^n$

$$\Phi(x_1, \ldots, x_n) = \sum_{i=1}^{r} \alpha_i |l_i(x)|^2.$$

10.2 Positivity, Inner Products, and the Cauchy–Schwarz Inequality

A fundamental notion in the theory of bilinear and quadratic forms is that of positivity:

Definition 10.11. a) A symmetric bilinear form $b : V \times V \to \mathbf{R}$ is called **positive** if $b(x, x) \geq 0$ for all $x \in V$. We say that b is **positive definite** if $b(x, x) > 0$ for all nonzero vectors $x \in V$.

b) A quadratic form q on V is called **positive** (or **positive definite**) if its polar form is positive (or positive definite). Thus q is positive if $q(x) \geq 0$ for all $x \in V$, and positive definite if moreover we have equality only for the zero vector.

Problem 10.12. Which of the following quadratic forms are positive? Which ones are positive definite?

a) $q(x, y, z) = xy + yz + zx$.
b) $q(x, y, z) = x^2 + 2(y - z)^2 + 3(z - x)^2$.
c) $q(x, y, z) = x^2 + y^2 + z^2 - xy - yz - zx$.

Solution. a) We have to check whether $xy + yz + zx \geq 0$ for all real numbers x, y, z. This is definitely not the case, since taking $z = 0$ we would have $xy \geq 0$ for all $x, y \in \mathbf{R}$, which is definitely absurd. Thus q is not positive, and thus not positive definite either.

b) It is clear that $q(x, y, z) \geq 0$ for all $x, y, z \in \mathbf{R}$, since $q(x, y, z)$ is a sum of squares of real numbers. Thus q is positive. To see whether q is positive definite, we need to investigate when $q(x, y, z) = 0$. This forces

$$x = y - z = z - x = 0$$

and then $x = y = z = 0$. Thus q is positive definite.

c) We observe that

$$q(x, y, z) = \frac{(x - y)^2 + (y - z)^2 + (z - x)^2}{2} \geq 0$$

for all $x, y, z \in \mathbf{R}$, thus q is positive. Notice that q is not positive definite, since $q(1, 1, 1) = 0$, but $(1, 1, 1) \neq (0, 0, 0)$. □

We introduce now another fundamental concept, which will be constantly used in the sequel:

Definition 10.13. a) An **inner product** on a $\mathbf{R}$-vector space V is a symmetric positive definite bilinear form on V.

b) An **Euclidean space** is a finite dimensional $\mathbf{R}$-vector space V endowed with an inner product.

We warn the reader that some authors do not impose that an Euclidean space is finite dimensional. When dealing with inner products and Euclidean spaces, the notation $\langle x, y \rangle$ is preferred to $b(x, y)$ (where b is the inner product on V). If $\langle\ ,\ \rangle$ is an inner product on V, we let

$$||x|| = \sqrt{\langle x, x \rangle}$$

and we call $||x||$ the **norm of** x (the reason for this name will be given a bit later).

Remark 10.14. a) If V is an Euclidean space, then any subspace W of V is naturally an Euclidean space, when endowed with the restriction of the inner product on V to W: note that this restriction is still an inner product on W, by definition.

b) $\mathbf{R}^n$ endowed with the **canonical inner product**

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$$

is an Euclidean space. We leave it to the reader to check this assertion.

Problem 10.15. Let n be a positive integer and let V be the space of polynomials with real coefficients whose degree does not exceed n. Prove that

$$\langle P, Q \rangle = \sum_{i=0}^{n} P(i)Q(i)$$

defines an inner product on V.

Solution. First, it is clear that for any P the map $Q \mapsto \langle P, Q \rangle$ is linear, and similarly for any Q the map $P \mapsto \langle P, Q \rangle$ is linear. Next, we have

$$\langle P, P \rangle = \sum_{i=0}^{n} P(i)^2$$

and the last quantity is clearly nonnegative. Finally, assume that $\langle P, P \rangle = 0$ for some $P \in V$. Then $\sum_{i=0}^{n} P(i)^2 = 0$, which forces $P(i) = 0$ for all $0 \leq i \leq n$. Thus P has at least $n+1$ distinct roots and since $\deg P \leq n$, we deduce that $P = 0$. The result follows. □

Problem 10.16. Let V be the space of continuous real-valued maps on $[a, b]$ (where $a < b$ are fixed real numbers). Prove that the map $\langle\ ,\ \rangle$ defined by

$$\langle f, g \rangle = \int_a^b f(x)g(x)dx$$

is an inner product on V.

Solution. It is easy to see that $\langle\ ,\ \rangle$ is a symmetric bilinear form, it remains to check that it is positive definite. Since f^2 is a continuous nonnegative map, we have

$$\langle f, f \rangle = \int_a^b f(x)^2 dx \geq 0.$$

Suppose that $\langle f, f\rangle = 0$ and that f is nonzero. Thus there is $x_0 \in (a, b)$ such that $f(x_0) \neq 0$. By continuity we can find $\varepsilon > 0$ such that $(x_0 - \varepsilon, x_0 + \varepsilon) \subset [a, b]$ and $|f(x)| \geq \varepsilon$ for $x \in (x_0 - \varepsilon, x_0 + \varepsilon)$. It follows that

$$\langle f, f\rangle \geq \int_{x_0-\varepsilon}^{x_0+\varepsilon} \varepsilon^2 dx = 2\varepsilon^3 > 0$$

and the result follows. □

Problem 10.17. Let V be the space of smooth functions $f : [0, 1] \to \mathbf{R}$ such that $f(0) = f(1) = 0$. Prove that

$$\langle f, g\rangle = -\int_0^1 (f(x)g''(x) + f''(x)g(x))dx$$

defines an inner product on V.

Solution. Using integration by parts, we obtain

$$\langle f, g\rangle = -(fg' + f'g)|_0^1 + 2\int_0^1 f'(x)g'(x)dx = 2\int_0^1 f'(x)g'(x)dx.$$

The last formula makes it clear that $\langle\ ,\ \rangle$ is a symmetric bilinear form on V. It remains to see that it is positive definite. We have

$$\langle f, f\rangle = 2\int_0^1 (f'(x))^2 dx \geq 0,$$

with equality if and only if (by the previous problem) $f'(x) = 0$ for all x. This last condition is equivalent to saying that f is constant. But since f vanishes by assumption at 0, if f if constant then it must be the zero map. Thus $\langle f, f\rangle = 0$ implies $f = 0$, which yields the desired result. □

The fundamental result concerning positive symmetric bilinear forms is the

Theorem 10.18 (Cauchy–Schwarz Inequality). *Let $b : V \times V \to \mathbf{R}$ be a symmetric bilinear form and let q be its associated quadratic form.*

a) If b is positive, then for all $x, y \in V$ we have

$$b(x, y)^2 \leq q(x)q(y).$$

b) If moreover b is positive definite and if $b(x, y)^2 = q(x)q(y)$ for some $x, y \in V$, then x and y are linearly dependent.

Proof. a) Consider the map $F : \mathbf{R} \to \mathbf{R}$ given by

$$F(t) = q(x + ty).$$

Note that since b is bilinear and symmetric, we have

$$F(t) = b(x + ty, x + ty) = b(x, x) + b(x, ty) + b(ty, x) + b(ty, ty)$$

$$= q(x) + tb(x, y) + tb(x, y) + t^2 b(y, y) = q(x) + 2tb(x, y) + t^2 q(y).$$

Thus $F(t)$ is a quadratic polynomial function with leading coefficient $q(y) \geq 0$. Moreover, since b is positive, we have $F(t) \geq 0$ for all $t \in \mathbf{R}$. It follows that the discriminant of F is nonpositive, that is

$$4b(x, y)^2 - 4q(x)q(y) \leq 0.$$

But this is precisely the desired inequality (after division by 4).

b) Suppose that b is positive definite and that $b(x, y)^2 = q(x)q(y)$. We may assume that $y \neq 0$, so that $q(y) > 0$. Thus with the notations used in the proof of part a), the discriminant of F is 0. It follows that F has a unique real root, say t. Then $q(x+ty) = 0$ and since q is positive definite, this can only happen if $x+ty = 0$. Thus x and y are linearly dependent. □

The following result is a direct consequence of the previous theorem, but it is of fundamental importance:

Corollary 10.19. *If V is a vector space over $\mathbf{R}$ endowed with an inner product $\langle\ ,\ \rangle$, then for all $x, y \in V$ we have*

$$|\langle x, y\rangle| \leq ||x|| \cdot ||y||.$$

Example 10.20. a) Let $V = \mathbf{R}^n$ be endowed with the canonical inner product. The inequality $|\langle x, y\rangle| \leq ||x|| \cdot ||y||$ can be re-written (after squaring) as

$$(x_1 y_1 + \ldots + x_n y_n)^2 \leq (x_1^2 + \ldots + x_n^2)(y_1^2 + \ldots + y_n^2).$$

b) Let V be the space of continuous real-valued maps on $[a, b]$, where $a < b$ are real numbers. The map $\langle\ ,\ \rangle : V \times V \to \mathbf{R}$ defined by

$$\langle f, g\rangle = \int_a^b f(x)g(x)dx$$

is an inner product on V (see Problem 10.16) and the inequality in the corollary becomes (after squaring)

$$\left(\int_a^b f(x)g(x)dx\right)^2 \leq \left(\int_a^b f(x)^2 dx\right) \cdot \left(\int_a^b g(x)^2 dx\right).$$

Let V be a vector space over $\mathbf{R}$, endowed with an inner product $\langle\ ,\rangle$. By the previous corollary we have

$$-1 \leq \frac{\langle u, v\rangle}{\|u\|\|v\|} \leq 1 \text{ for all } u, v \in V - \{0\}.$$

Thus there exists a unique angle $\theta \in [0, \pi]$ satisfying

$$\cos\theta = \frac{\langle u, v\rangle}{\|u\|\|v\|}.$$

We define this angle θ to be **the angle between the vectors** u, v.

An important consequence of the Cauchy–Schwarz inequality is

Theorem 10.21 (Minkowski's Inequality). *Let V be a vector space over $\mathbf{R}$ and let q be a positive quadratic form on V. Then for all $x, y \in E$ we have*

$$\sqrt{q(x)} + \sqrt{q(y)} \geq \sqrt{q(x+y)}.$$

Proof. Squaring the inequality we obtain the equivalent one

$$q(x) + q(y) + 2\sqrt{q(x)q(y)} \geq q(x+y).$$

Letting b be the polar form of q, the polarization identity yields

$$q(x+y) = q(x) + q(y) + 2b(x, y).$$

Comparing this equality and the previous inequality, we obtain the equivalent form

$$\sqrt{q(x)q(y)} \geq b(x, y),$$

which, squared, is exactly the Cauchy–Schwarz inequality. □

Consider now an inner product $\langle\ ,\ \rangle$ on some $\mathbf{R}$-vector space V. Recall that we defined

$$||\cdot|| : V \to \mathbf{R}, \quad ||x|| = \sqrt{\langle x, x\rangle}.$$

Since an inner product is positive definite, we see that $||x|| \geq 0$ for all x, with equality if and only if $x = 0$. Also, since an inner product is a bilinear form, we have $||ax|| = |a|||x||$ for all $a \in \mathbf{R}$. Finally, Minkowski's inequality yields

$$||x + y|| \leq ||x|| + ||y||$$

for all $x, y \in V$. We call this inequality the **triangle inequality**.

A map $||\cdot|| : V \to \mathbf{R}$ satisfying the following properties:

- $||v|| \geq 0$ for all $v \in V$, with equality if and only if $v = 0$.

- $||av|| = |a| \cdot ||v||$ for all $v \in V$ and $a \in \mathbf{R}$.
- $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$

is called a **norm on** V. This explains why we called $||x||$ the norm of x.

Minkowski's inequality shows that any inner product on a vector space V over $\mathbf{R}$ naturally endows the space V with a norm $|| \cdot ||$. We can use this norm to define a **distance** $d : V \times V \to \mathbf{R}^+$ by

$$d(u, v) = ||u - v||.$$

One can check (see the exercise section) that for all $u, v, w \in V$ we have

$$d(u, v) + d(v, w) \geq d(u, w).$$

This construction is of fundamental importance, since it allows us to do analysis on V as we do it on $\mathbf{R}$. Note that if $V = \mathbf{R}^n$ with $n \leq 3$, endowed with its canonical inner product, then the distance obtained as above is really the Euclidean distance that we are used with on the line, in the plane and in three-dimensional space. For instance, the distance between the points $(1, 1)$ and $(2, 3)$ is

$$d((1, 1), (2, 3)) = \sqrt{(1 - 2)^2 + (1 - 3)^2} = \sqrt{5},$$

and this really corresponds to the geometric distance between these two points in the plane.

10.2.1 Practice Problems

In the following problems, whenever the inner product on $\mathbf{R}^n$ is not specified, it is implicitly assumed that we consider the canonical inner product on $\mathbf{R}^n$, defined by

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.$$

1. Let V be an $\mathbf{R}$-vector space endowed with an inner product $\langle \ , \ \rangle$. Recall that the distance between two points $x, y \in V$ is

   $$d(x, y) = \sqrt{\langle x - y, x - y \rangle}.$$

   Prove the **triangle inequality**

   $$d(x, y) + d(y, z) \geq d(x, z)$$

   for all $x, y, z \in V$.

2. a) What is the distance between the vectors $u = (1, 1, 1)$ and $v = (1, 2, 3)$ in $\mathbf{R}^3$?
   b) What are their respective norms?
   c) What is the angle between u and v?
3. Find the angle between the vectors $u = (1, 2)$ and $v = (1, -1)$ in $\mathbf{R}^2$.
4. Find the vectors v of norm 1 in $\mathbf{R}^3$ such that the angle between v and $(1, 1, 0)$ is $\frac{\pi}{4}$.
5. Among all vectors of the form $(1, x, 2, 1)$ with $x \in \mathbf{R}$, which vector is at smallest distance from $(0, 1, 1, 1)$?
6. Find all values of $\alpha \in \mathbf{R}$ for which the map $\langle\ ,\ \rangle : \mathbf{R}^4 \times \mathbf{R}^4 \to \mathbf{R}$ defined by

$$\langle (x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_3) \rangle = \alpha x_1 y_1 + 2x_2 y_2 + (1 - \alpha) x_3 y_3 + x_4 y_4$$

   is an inner product.
7. Prove that if $f : [a, b] \to \mathbf{R}$ is a continuous map, then

$$\left(\int_a^b f(t) dt \right)^2 \leq (b - a) \int_a^b f(t)^2 dt.$$

8. a) Prove that if $x_1, \ldots, x_n$ are positive real numbers, then

$$(x_1 + x_2 + \ldots + x_n) \cdot \left(\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} \right) \geq n^2.$$

   When do we have equality?
   b) Prove that if $f : [a, b] \to (0, \infty)$ is a continuous map, then

$$\int_a^b f(t) dt \cdot \int_a^b \frac{1}{f(t)} dt \geq (b - a)^2.$$

   When do we have equality?
9. Let $f : [0, 1] \to \mathbf{R}^+$ be a continuous map taking nonnegative values and let

$$x_n = \int_0^1 t^n f(t) dt.$$

   Prove that for all $n, p \geq 0$

$$x_{n+p} \leq \sqrt{x_{2n}} \cdot \sqrt{x_{2p}}.$$

10. Let V be a $\mathbf{C}$-vector space and let Φ be a hermitian quadratic form on V. Assume that Φ is positive definite, i.e., $\Phi(x) > 0$ for all nonzero vectors $x \in V$. Let φ be the polar form of Φ.

a) Prove the Cauchy–Schwarz inequality: for all $x, y \in V$ we have

$$|\varphi(x, y)|^2 \leq \Phi(x)\Phi(y),$$

with equality if and only if x, y are linearly dependent.

b) Prove Minkowski's inequality: for all $x, y \in V$ we have

$$\sqrt{\Phi(x)} + \sqrt{\Phi(y)} \geq \sqrt{\Phi(x+y)}.$$

11. Prove that there is no inner product $\langle\ ,\ \rangle$ on the space V of continuous real-valued maps on $[0, 1]$ such that for all $f \in V$ we have

$$\langle f, f \rangle = \sup_{x \in [0,1]} f(x)^2.$$

Hint: the parallelogram law.

10.3 Bilinear Forms and Matrices

From now on we will focus only on finite dimensional vector spaces V over $\mathbf{R}$. We have already seen that we can describe linear transformations on V in terms of matrices. We would like to have a similar description for bilinear forms.

Definition 10.22. Consider a basis $e_1, \ldots, e_n$ of V, and let b be a symmetric bilinear form on V. The **matrix of** b **with respect to the basis** $e_1, \ldots, e_n$ is the matrix $(b(e_i, e_j))_{1 \leq i,j \leq n}$.

b) If q is a quadratic form on V, the **matrix of** q **with respect to the basis** $e_1, \ldots, e_n$ is the matrix of its polar form with respect to $e_1, \ldots, e_n$.

Theorem 10.23. *Let V be a finite dimensional vector space and let $e_1, \ldots, e_n$ be a basis of V. Sending a symmetric bilinear form to its matrix with respect to $e_1, \ldots, e_n$ establishes an isomorphism of* $\mathbf{R}$*-vector spaces between the vector space of symmetric bilinear forms on V and the vector space of symmetric matrices in $M_n(\mathbf{R})$.*

Proof. It is clear that if A is the matrix of b and A' is the matrix of b', then $cA + A'$ is the matrix of $cb + b'$ for all scalars $c \in \mathbf{R}$. Also, since b is symmetric, we have $b(e_i, e_j) = b(e_j, e_i)$, thus the matrix of b is symmetric. Thus sending a symmetric bilinear form b to its matrix A with respect to $e_1, \ldots, e_n$ induces a linear map φ from symmetric bilinear forms on V to symmetric matrices $A \in M_n(\mathbf{R})$.

Injectivity of the map φ follows directly from Remark 10.2, so it remains to prove that φ is surjective. Start with any symmetric matrix $A = [a_{ij}]$. If $x = x_1 e_1 + \ldots + x_n e_n$ and $y = y_1 e_1 + \ldots + y_n e_n$ are vectors in V, define

$$b(x, y) = \sum_{i,j=1}^{n} a_{ij} x_i y_j.$$

It is easy to see that b is a symmetric bilinear form whose matrix in the basis $e_1, \ldots, e_n$ is precisely A. □

A natural question is the following: what is **explicitly** the inverse of the isomorphism given by the previous theorem? Fortunately, this has already been answered during the proof: it is the map sending a symmetric matrix $A = [a_{ij}]$ to the bilinear form b defined by

$$b(x_1e_1 + \ldots + x_ne_n, y_1e_1 + \ldots + y_ne_n) = \sum_{i,j=1}^{n} a_{ij}x_iy_j.$$

This formula does not come out of nowhere, but it is imposed by Remark 10.2. Also, note that the right-hand side of the previous equality can be written as ${}^tXAY$, where X, Y are the column vectors whose coordinates are $x_1, \ldots, x_n$, respectively $y_1, \ldots, y_n$. Here we consider ${}^tX$ as a $1 \times n$ matrix and of Y as a $n \times 1$ matrix, so that ${}^tXAY$ is a 1×1 matrix, that is a real number. We obtain the following characterization of the matrix of b with respect to the basis $e_1, \ldots, e_n$.

Theorem 10.24. *Let $e_1, e_2, \ldots, e_n$ be a basis of V and let b be a symmetric bilinear form on V. The matrix of b with respect to $e_1, \ldots, e_n$ is the unique symmetric matrix $A \in M_n(\mathbf{R})$ such that*

$$b(x, y) = {}^tXAY$$

for all vectors $x, y \in V$ (where X, Y are the column vectors whose coordinates are those of x, y with respect to $e_1, \ldots, e_n$).

Remark 10.25. Keep the hypotheses and notations of the previous theorem and discussion. If q is the quadratic form attached to b, then

$$q(x_1e_1 + \ldots + x_ne_n) = {}^tXAX = \sum_{i,j=1}^{n} a_{ij}x_ix_j = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{1 \le i < j \le n} a_{ij}x_ix_j,$$

the last equality being a consequence of the equality $a_{ij} = a_{ji}$ for $i < j$. The presence of the factor 2 is quite often a source of errors when dealing with the link between quadratic forms and matrices. Indeed, it is quite tempting (and this happens quite often!) to say that the quadratic form associated with the matrix $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is

$$q(x_1, x_2) = x_1x_2,$$

which is **wrong**: the quadratic form associated with A is

$$q(x_1, x_2) = 2x_1x_2.$$

An even more common mistake is to say that the matrix associated with the quadratic form

$$q(x, y, z) = xy + yz + zx$$

on $\mathbf{R}^3$ is $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. Actually, the correct matrix is $\begin{bmatrix} 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix}$, since the polar form of q is the bilinear form b defined by

$$b((x, y, z), (x', y', z')) = \frac{x'y + y'x + x'z + z'x + y'z + z'y}{2}.$$

Armed with Theorem 10.24, it is not difficult to understand how the matrix of a bilinear form varies when we vary the basis. More precisely, consider two bases $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n$ of V and let A, A' be the matrices of a symmetric bilinear form b with respect to these bases. If $x = x_1e_1 + \ldots + x_ne_n = x'_1e'_1 + \ldots + x'_ne'_n$ is a vector in V, let X (respectively X') be the column vector whose coordinates are $x_1, \ldots, x_n$ (respectively $x'_1, \ldots, x'_n$). Then

$$b(x, y) = {}^tXAY = {}^tX'A'Y'.$$

Letting P be the change of basis matrix from $e_1, \ldots, e_n$ to $e'_1, \ldots, e'_n$ (recall that the columns of P are the coordinates of $e'_1, \ldots, e'_n$ when expressed in terms of $e_1, \ldots, e_n$), we have

$$X = PX', \quad Y = PY'.$$

It follows that

$${}^tX'A'Y' = b(x, y) = {}^tXAY = {}^t(PX')APY' = {}^t(X'){}^tPAPY'$$

and we obtain the following

Theorem 10.26. *Suppose that a symmetric bilinear form b has matrix A with respect to a basis $e_1, \ldots, e_n$ of V. Let $e'_1, \ldots, e'_n$ be another basis of V and let P be the change of basis matrix from $e_1, \ldots, e_n$ to $e'_1, \ldots, e'_n$. Then the matrix of b with respect to $e'_1, \ldots, e'_n$ is*

$$A' = {}^tPAP.$$

The previous theorem suggests the following

Definition 10.27. Two symmetric matrices $A, B \in M_n(\mathbf{R})$ are called **congruent** if they are the matrices of some symmetric bilinear form in two bases of F^n.

Equivalently, A and B are congruent if there is an invertible matrix $P \in M_n(F)$ such that $B = {}^tPAP$.

By definition, the congruence relation is an equivalence relation on the set of symmetric matrices $A \in M_n(\mathbf{R})$, that is:

- any matrix A is congruent to itself (this is clear).
- If A is congruent to B, then B is congruent to A: indeed, if $B = {}^tPAP$, then $A = {}^t(P^{-1})BP^{-1}$.
- If A is congruent to B and B is congruent to C, then A is congruent to C. Indeed, if $B = {}^tPAP$ and $C = {}^tQBQ$, then $C = {}^t(PQ)A(PQ)$.

Note that two congruent matrices have the same rank. This allows us to define the **rank of a symmetric bilinear form** as the rank of its matrix in any basis of the surrounding space (the previous discussion shows that it is independent of the choice of the basis). Note that we **cannot** define the determinant of a symmetric bilinear form in a similar way: if A and B are congruent matrices, then it is **not true** that $\det A = \det B$. All we can say is that if $B = {}^tPAP$, then

$$\det B = \det({}^tP) \det A \det P = \det A \cdot (\det P)^2,$$

thus $\det A$ and $\det B$ differ by the square of a nonzero real number. In particular, they have the **same sign**. The **discriminant** of a symmetric bilinear form is defined to be the sign of the determinant of its matrix in a basis of the surrounding space (it is independent of the choice of the basis).

The fundamental theorem concerning the congruence relation is the following consequence of Theorem 10.9:

Theorem 10.28 (Gauss). *Any symmetric matrix $A \in M_n(\mathbf{R})$ is congruent to a diagonal matrix.*

Proof. Consider the associated quadratic form q on $V = \mathbf{R}^n$

$$q(X) = {}^tXAX, \quad i.e., \quad q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j.$$

By Theorem 10.26, it suffices to prove the existence of a basis of $\mathbf{R}^n$ with respect to which the matrix of q is diagonal (as then A will be congruent to the corresponding diagonal matrix).

By Theorem 10.9 we know that we can find real numbers $\alpha_1, \ldots, \alpha_r$ and linearly independent linear forms $l_1, \ldots, l_r \in V^*$ such that

$$q(X) = \sum_{i=1}^{r} \alpha_i l_i(X)^2$$

for all $X \in V$. Complete the family $(l_1, \ldots, l_r)$ to a basis $(l_1, \ldots, l_n)$ of V^*. By Theorem 6.13 there is a basis $(e_1, \ldots, e_n)$ of V whose dual basis is $(l_1, \ldots, l_n)$. Thus, if $X = x_1 e_1 + \ldots + x_n e_n \in V$, then

$$q(X) = \sum_{i=1}^{r} \alpha_i l_i(X)^2 = \sum_{i=1}^{r} \alpha_i x_i^2,$$

so that the matrix of q with respect to the basis $(e_1, \ldots, e_n)$ is the diagonal matrix D with diagonal entries $\alpha_1, \ldots, \alpha_r$. □

Remark 10.29. The proof also shows the following interesting fact: if q is a quadratic form on $\mathbf{R}^n$ with polar form b, then we can find a basis $f_1, \ldots, f_n$ of $\mathbf{R}^n$ such that

$$b(f_i, f_j) = 0 \quad \text{for all} \quad 1 \leq i \neq j \leq n.$$

Such a basis is called a q-**orthogonal basis of** $\mathbf{R}^n$. We can even impose that $q(f_i) \in \{-1, 0, 1\}$ for all $1 \leq i \leq n$. Indeed, as in the above proof we can write

$$q(X) = \sum_{i=1}^{r} \alpha_i l_i(X)^2$$

and by the discussion following Theorem 10.9 we can even ensure that $\alpha_i \in \{-1, 1\}$ for all $1 \leq i \leq r$. If $e_1, \ldots, e_n$ is a basis as in the above proof, then

$$q(X) = \sum_{i=1}^{r} \alpha_i x_i^2$$

for $X = x_1 e_1 + \ldots + x_n e_n$, thus

$$b(X, Y) = \sum_{i=1}^{n} \alpha_i x_i y_i$$

with $\alpha_i = 0$ for $r < i \leq n$. It follows that we can take $f_i = e_i$ for $1 \leq i \leq n$.

We introduce one more definition before ending this section:

Definition 10.30. A symmetric matrix $A \in M_n(\mathbf{R})$ is called **positive** if ${}^t XAX \geq 0$ for all $X \in \mathbf{R}^n$. It is called **positive definite** if ${}^t XAX > 0$ for all nonzero vectors $X \in \mathbf{R}^n$.

In other words, $A = [a_{ij}]$ is positive (respectively positive definite) if and only if the quadratic form associated with A, namely $(x_1, \ldots, x_n) \to \sum_{i,j=1}^{n} a_{ij} x_i x_j$, is positive (respectively positive definite). Any symmetric positive definite matrix A gives rise to an inner product $\langle\ ,\ \rangle_A$ on $\mathbf{R}^n$, defined by

$$\langle X, Y \rangle_A = \langle X, AY \rangle = {}^t XAY,$$

where $\langle\ ,\ \rangle$ is the canonical inner product on $\mathbf{R}^n$.

Note that if A is positive then letting $e_1, \ldots, e_n$ be the canonical basis of $\mathbf{R}^n$, we have

$$a_{ii} = {}^t e_i A e_i \geq 0,$$

and if A is positive definite then the inequality is strict. Also, note that any matrix congruent to a positive (respectively positive definite) symmetric matrix is itself positive (respectively positive definite), since

$${}^t X({}^t PAP)X = {}^t(PX)A(PX).$$

Problem 10.31. Let $A \in M_n(\mathbf{R})$ be any matrix.

a) Prove that ${}^t AA$ is symmetric and positive.
b) Prove that ${}^t AA$ is positive definite if and only if A is invertible.

Solution. Note that

$${}^t({}^t AA) = {}^t A \cdot {}^t({}^t A) = {}^t AA,$$

thus ${}^t AA$ is symmetric. Next, for all $X \in \mathbf{R}^n$ we have

$${}^t X({}^t AA)X = {}^t(AX)(AX) = ||AX||^2 \geq 0,$$

with equality if and only if $AX = 0$. Both a) and b) follow from these observations (and the fact that A is invertible if and only if $AX = 0$ implies $X = 0$). □

Remark 10.32. The same result holds with $A\,{}^t A$ instead of ${}^t AA$.

Remarkably, the converse of the result established in the previous problem holds:

Theorem 10.33. *Any symmetric positive matrix $A \in M_n(\mathbf{R})$ can be written as ${}^t BB$ for some matrix $B \in M_n(\mathbf{R})$.*

Proof. We use Gauss' Theorem 10.28. By that theorem, there is an invertible matrix P such that ${}^t PAP = D$ is a diagonal matrix. By the discussion preceding Problem 10.31 we know that D itself is positive and its diagonal coefficients d_{ii} are nonnegative. Hence we can write $D = {}^t D_1 D_1$ for a diagonal matrix D_1 whose diagonal entries are $\sqrt{d_{ii}}$. But then

$$A = {}^t P^{-1} D P^{-1} = {}^t P^{-1}\,{}^t D_1 D_1 P^{-1} = {}^t BB,$$

with $B = D_1 P^{-1}$. □

Problem 10.34. Let $(V, \langle\,,\,\rangle)$ be an Euclidean space and let $v_1, \ldots, v_n$ be a family of vectors in V. Let $A \in M_n(\mathbf{R})$ be the **Gram matrix** of the family, i.e., the matrix whose (i, j)-entry is $\langle v_i, v_j \rangle$.

a) Prove that A is symmetric positive.
b) Prove that A is positive definite if and only if $v_1, \ldots, v_n$ are linearly independent.

Solution. Again, it is clear that A is symmetric. For all $x_1, \ldots, x_n \in \mathbf{R}$ we have

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j = \sum_{i,j=1}^{n} x_i x_j \langle v_i, v_j \rangle =$$

$$\sum_{i=1}^{n} x_i \cdot \sum_{j=1}^{n} \langle v_i, x_j v_j \rangle = \sum_{i=1}^{n} \langle x_i v_i, \sum_{j=1}^{n} x_j v_j \rangle = || \sum_{i=1}^{n} x_i v_i ||^2 \geq 0,$$

with equality if and only if $\sum_{i=1}^{n} x_i v_i = 0$. The result follows. □

Problem 10.35. Let $n \geq 1$ and let $A = [a_{ij}] \in M_n(\mathbf{R})$ be defined by $a_{ij} = \min(i, j)$. Prove that A is symmetric and positive definite.

Solution. It is clear that the matrix is symmetric. Note that we can write

$$\min(i, j) = \sum_{k \leq i, k \leq j} 1.$$

Doing so and interchanging orders of summation, we see that

$$\sum_{i=1}^{n} \sum_{j=1}^{n} \min(i, j) x_i x_j = \sum_{k=1}^{n} \sum_{i=k}^{n} \sum_{j=k}^{n} x_i x_j = \sum_{k=1}^{n} \left(\sum_{i=k}^{n} x_i \right)^2.$$

This last expression is clearly nonnegative, and it equals 0 if and only if

$$x_1 + \cdots + x_n = 0, x_2 + \cdots + x_n = 0, \ \ldots \ , x_n = 0.$$

Subtracting each equation from the one before it, we see that the unique solution is $x_1 = x_2 = \cdots = x_n = 0$, which shows that the matrix is positive definite.

An alternative argument is to note that

$$\min(i, j) = \int_0^\infty f_i(x) f_j(x) dx,$$

where $f_i(x) = 1$ for $x \in [0, i]$ and $f_i(x) = 0$ for $x > i$ (i.e., f_i is the characteristic function of the interval $[0, i]$). It follows that A is the Gram matrix of the family $f_1, \ldots, f_n$, thus it is symmetric and positive. Since $f_1, \ldots, f_n$ are linearly independent (in the space of integrable functions on $[0, \infty)$), it follows that A is positive definite (all this uses Problem 10.34).

Yet another argument is to note that $A = {}^t BB$ where B is the upper triangular matrix all of whose nonzero coefficients are equal to 1. Since B is invertible, we deduce that A is positive definite by Problem 10.31. □

10.3.1 Problems for Practice

1. Consider the map $q : \mathbf{R}^3 \to \mathbf{R}$ defined by

$$q(x, y, z) = (x + 2y + 3z)^2 + (y + z)^2 - (y - z)^2.$$

   a) Prove that q is a quadratic form and find its polar form b.
   b) Is q positive definite?
   c) Give the matrix of q with respect to the canonical basis of $\mathbf{R}^3$.
   d) Consider the vectors

$$v_1 = (2, 0, 0), \quad v_2 = (-5, 1, 1), \quad v_3 = (1, 1, -1).$$

   Prove that (v_1, v_2, v_3) is a basis of $\mathbf{R}^3$ and find the matrix of b with respect to this basis.

2. Consider the map $q : \mathbf{R}^3 \to \mathbf{R}$ defined by

$$q(x, y, z) = x(x - y + z) - 2y(y + z).$$

   a) Prove that q is a quadratic form and find its polar form b.
   b) Find the matrix of q with respect to the canonical basis of $\mathbf{R}^3$.
   c) Find those vectors $v \in \mathbf{R}^3$ such that $b(v, w) = 0$ for all vectors $w \in \mathbf{R}^3$.

3. Consider the quadratic form q on $\mathbf{R}^3$ defined by

$$q(x, y, z) = 2x(x + y - z) + y^2 + z^2.$$

   a) Find the matrix of q with respect to the canonical basis of $\mathbf{R}^3$.
   b) Write q in the form $\sum_{i=1}^{r} \alpha_i l_i^2$ with $l_1, \ldots, l_r$ linearly independent linear forms.
   c) Find the rank, signature, and discriminant of q.
   d) Find a q-orthogonal basis of $\mathbf{R}^3$ and give the matrix of q with respect to this basis.

4. Is the matrix $A = [a_{ij}] \in M_n(\mathbf{R})$ with $a_{ij} = i \cdot j$ positive? Is it positive definite?
5. a) Prove that a symmetric positive definite matrix is invertible.
   b) Prove that a symmetric positive matrix is positive definite if and only if it is invertible.
6. All entries but the diagonal ones of the matrix $A \in M_n(\mathbf{R})$ are equal to -1, while all diagonal entries are equal to $n-1$. Is A positive? Is it positive definite?
7. Prove that any symmetric positive matrix $A \in M_n(\mathbf{R})$ is the Gram matrix of a family of vectors $v_1, \ldots, v_n \in \mathbf{R}^n$. Hint: use Theorem 10.33.
8. Let V be a $\mathbf{R}$-vector space endowed with an inner product $\langle\ ,\ \rangle$ and let $x_1, \ldots, x_n$ be vectors in V. The **Gram determinant** of $x_1, \ldots, x_n$, denoted $G(x_1, \ldots, x_n)$

is by definition the determinant of the Gram matrix $[\langle x_i, x_j \rangle]_{1 \leq i,j \leq n}$. Prove that $x_1, \ldots, x_n$ is linearly independent if and only if $G(x_1, \ldots, x_n) \neq 0$.

9. Compute the Gram determinant of the vectors

$$x_1 = (1, 2, 1), \quad x_2 = (-1, -1, 2), \quad x_3 = (1, 0, -1)$$

in $\mathbf{R}^3$. Are they linearly independent?

10. Prove that the matrix $A = [\frac{1}{i+j}]_{1 \leq i,j \leq n}$ is symmetric and positive (hint: what is $\int_0^1 t^{i+j-1} dt$?).

11. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a matrix such that $a_{ij} = 1$ for $i \neq j$, and $a_{ii} > 1$ for all $i \in [1, n]$. Prove that A is symmetric and positive definite.

12. Let n be a positive integer. Consider the space V of polynomials of degree at most n with real coefficients. Define a map

$$b : V \times V \to \mathbf{R}, \quad b(P, Q) = \int_0^1 tP(t)Q'(t)dt,$$

where Q' is the derivative of Q.

a) Prove that b is a bilinear form on V. Is it symmetric?

b) Let q be the quadratic form attached to b, so that $q(x) = b(x, x)$. Find the matrix of q with respect to the basis $1, X, \ldots, X^n$ of V.

13. In this long problem we establish the link between sesquilinear maps and matrices, extending thus the results of this section to finite dimensional $\mathbf{C}$-vector spaces. Let V be a finite dimensional $\mathbf{C}$-vector space and let $\mathcal{B} = (e_1, \ldots, e_n)$ be a basis of V. Recall that $\mathcal{S}(V)$ is the set of sesquilinear forms on V.

a) Let $\varphi \in \mathcal{S}(V)$ be a sesquilinear form on V. The **matrix of φ with respect to** $\mathcal{B}$ is the matrix $A = [a_{ij}] \in M_n(\mathbf{C})$ where $a_{ij} = \varphi(e_i, e_j)$ for $1 \leq i, j \leq n$. Prove that for all vectors $x, y \in V$ we have

$$\varphi(x, y) = X^* A Y,$$

where X, Y are the column vectors whose coordinates are the coordinates of x, y with respect to $\mathcal{B}$, and $X^* = {}^t\overline{X}$ is the row vector whose coordinates are the complex conjugates of the coordinates of x with respect to $\mathcal{B}$.

b) Prove that A is the unique matrix having the property stated in a).

c) Prove that the map sending $\varphi \in \mathcal{S}(V)$ to its matrix with respect to $\mathcal{B}$ is an isomorphism of $\mathbf{C}$-vector spaces between $\mathcal{S}(V)$ and $M_n(\mathbf{C})$.

d) Let $\varphi \in \mathcal{S}(V)$ and let A be its matrix with respect to $\mathcal{B}$. Prove that φ is hermitian if and only if A satisfies $A = \overline{{}^t A}$. Such a matrix is called **conjugate symmetric or hermitian**. **We usually write A^* instead of $\overline{{}^t A}$, so a matrix A is hermitian if and only if $A = A^*$.**

e) Let $\mathcal{B}'$ be another basis of V and let P be the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}'$. If $x, y \in V$, let X, Y (respectively X', Y') be the column vectors whose coordinates are the coordinates of x, y with respect to $\mathcal{B}$ (respectively $\mathcal{B}'$). Prove that if A (respectively A') is the matrix of φ with respect to $\mathcal{B}$ (respectively $\mathcal{B}'$), then

$$A' = P^* A P.$$

f) A hermitian matrix $A \in M_n(\mathbf{C})$ is called **positive** (respectively **positive definite**) if $X^* A X \geq 0$ for all $X \in \mathbf{C}^n$ (respectively if moreover $X^* A X \neq 0$ for $X \neq 0$). Prove that for any matrix $B \in M_n(\mathbf{C})$ the matrices $B^* B$ and $B B^*$ are hermitian positive, and they are hermitian positive definite if and only if B is invertible.

g) Prove that any hermitian positive matrix A can be written as $B B^*$ for some matrix $B \in M_n(\mathbf{C})$.

10.4 Duality and Orthogonality

Let b be a symmetric bilinear form on a vector space V over $\mathbf{R}$ (for now we don't assume that V is finite dimensional). For each $y \in V$ the map $x \to b(x, y)$ is by definition linear, thus it is a linear form on V. Letting V^* be the dual of V, we obtain therefore a map

$$\varphi_b : V \to V^*, \quad \varphi_b(y)(x) = b(x, y).$$

Since for all $x \in V$ the map $y \to b(x, y)$ is linear, it follows that φ_b is a linear map.

Problem 10.36. Suppose that V is finite dimensional and let $e_1, \ldots, e_n$ be a basis of V. Let $e_1^*, \ldots, e_n^*$ be the dual basis[1] of $e_1, \ldots, e_n$. Prove that the matrix of φ_b with respect to the bases $e_1, \ldots, e_n$ and $e_1^*, \ldots, e_n^*$ is the matrix of b in the basis $e_1, \ldots, e_n$.

Solution. For $x = x_1 e_1 + \ldots + x_n e_n \in V$ we have

$$\varphi_b(e_i)(x) = b(x, e_i) = x_1 b(e_1, e_i) + \ldots + x_n b(e_n, e_i)$$

$$= b(e_1, e_i) e_1^*(x) + \ldots + b(e_n, e_i) e_n^*(x).$$

Thus

$$\varphi_b(e_i) = b(e_1, e_i) e_1^* + \ldots + b(e_n, e_i) e_n^*.$$

[1] Recall that $e_i^*(e_j) = 1_{i=j}$, where $1_{i=j}$ equals 1 if $i = j$ and 0 otherwise.

The result follows. □

The following result, though very simple, is very useful:

Theorem 10.37 (Riesz's Representation Theorem). *If V is an Euclidean (thus finite dimensional) space with inner product $\langle\ ,\ \rangle$, then the map $\varphi_{\langle\ ,\ \rangle} : V \to V^*$ is an isomorphism. In other words, for any linear map $l : V \to \mathbf{R}$ there is a unique vector $v \in V$ such that $l(x) = \langle v, x\rangle$ for all $x \in V$.*

Proof. Since $\dim V = \dim V^*$, it suffices to prove that $\varphi_{\langle\ ,\ \rangle}$ is injective. Assume that $\varphi_{\langle\ ,\ \rangle}(x) = 0$ for some $x \in V$. Then by definition $\langle x, y\rangle = 0$ for all $y \in V$, in particular $\langle x, x\rangle = 0$. But then $||x||^2 = 0$, where $||\cdot||$ is the norm associated with the inner product, and so $x = 0$. □

Let V be again an arbitrary vector space over $\mathbf{R}$ and let b be a symmetric bilinear form on V.

Definition 10.38. a) Two vectors $x, y \in V$ are called **orthogonal** (with respect to b) if $b(x, y) = 0$.

b) The orthogonal $S^\perp$ of a subset S of V is the set of vectors $v \in V$ which are orthogonal to each element of S.

c) Two subsets S, T of V are called orthogonal if $S \subset T^\perp$, that is any element of S is orthogonal to any element of T.

Remark 10.39. Suppose that $\langle\ ,\ \rangle$ is an inner product on V, with associated norm $||\cdot||$ (thus $||x|| = \sqrt{\langle x, x\rangle}$). Then vectors $x, y \in V$ are orthogonal if and only if

$$||x + y||^2 = ||x||^2 + ||y||^2.$$

This is the **Pythagorean theorem** and follows directly from the polarization identity

$$||x + y||^2 = ||x||^2 + 2\langle x, y\rangle + ||y||^2.$$

Coming back to the general case, note that $b(x, y) = 0$ is equivalent to $\varphi_b(y)(x) = 0$, i.e., x and the linear form $\varphi_b(y)$ are orthogonal in the sense of duality. This allows us to use the results we have already established in the chapter concerned with duality to obtain information about symmetric bilinear forms. As a consequence, we obtain the following fundamental:

Theorem 10.40. *Let V be an Euclidean space and let W be a subspace of V. Then $W^\perp \oplus W = V$, in particular*

$$\dim W^\perp + \dim W = \dim V.$$

Moreover, $(W^\perp)^\perp = W$.

We can slightly refine the following theorem by allowing infinite dimensional ambient spaces and **finite dimensional subspaces therein**.

Theorem 10.41. *Let V be any* **R***-vector space endowed with an inner product and let W be a* ***finite dimensional*** *subspace of V. Then*

$$W \oplus W^{\perp} = V \quad \textit{and} \quad W^{\perp\perp} = W.$$

Proof. Let $\langle\ ,\ \rangle$ be the inner product on V, with associated norm $||\cdot||$. We start by proving that $W \oplus W^{\perp} = V$. If $x \in W \cap W^{\perp}$, then $\langle x, x\rangle = 0$, that is $||x||^2 = 0$, and so $x = 0$. Thus $W \cap W^{\perp} = \{0\}$. We still need to prove that $W + W^{\perp} = V$, so let $x \in V$ be arbitrary and consider the map $f : W \to \mathbf{R}$ defined by $f(y) = \langle x, y\rangle$. Then f is a linear form on W. Since W is an Euclidean space (for the inner product inherited from the one on V), by Theorem 10.37 there is a unique $z \in W$ such that $f(y) = \langle z, y\rangle$ for all $y \in W$. We deduce that $\langle x - z, y\rangle = 0$ for all $y \in W$, thus $x - z \in W^{\perp}$. Since $z \in W$, we conclude that $x \in W + W^{\perp}$ and the result follows.

It remains to prove that $W^{\perp\perp} = W$. By definition W is contained in $W^{\perp\perp}$, so let $x \in W^{\perp\perp}$. By the result established in the previous paragraph we can write $x = y + z$ with $y \in W$ and $z \in W^{\perp}$. Since $x \in W^{\perp\perp}$, we have $\langle x, z\rangle = 0$, thus $\langle y, z\rangle + ||z||^2 = 0$. But $y \in W$ and $z \in W^{\perp}$, thus $\langle y, z\rangle = 0$ and so $||z||^2 = 0$, then $z = 0$ and finally $x = y \in W$. □

Remark 10.42. **The hypothesis that W is finite dimensional is crucial in the previous theorem**. Indeed, consider the following situation: V is the space of continuous real-valued maps on $[0, 1]$ and W is the subspace consisting of maps f such that $f(0) = 0$. Endow V with the inner product given by

$$\langle f, g\rangle = \int_0^1 f(x)g(x)dx.$$

Then the orthogonal $W^{\perp}$ of W is reduced to $\{0\}$, thus we do not have $W \oplus W^{\perp} = V$ or $W^{\perp\perp} = W$. To prove that $W^{\perp} = \{0\}$, let $f \in W^{\perp}$. Note that the map g defined by $g(x) = xf(x)$ belongs to W and so $\langle f, g\rangle = 0$. This can be written as

$$\int_0^1 xf(x)^2 dx = 0.$$

Since the map $x \mapsto xf(x)^2$ is continuous, nonnegative, and with average 0, it is the 0 map and so $f(x) = 0$ for all $x \in (0, 1]$. By continuity, we deduce that $f = 0$.

The previous theorem has quite a lot of important applications in analysis, in particular concerning minimization problems. We will see a few examples in the sequel, but before that we introduce two very important definitions.

Definition 10.43. Let V be a **R**-vector space endowed with an inner product. Let W be a finite dimensional subspace of V. By Theorem 10.41 we have $V = W \oplus W^{\perp}$. The **orthogonal projection onto** W is the projection $p_W : V \to W$ onto W along $W^{\perp}$. In other words, for $x \in V$ $p_W(x)$ is the unique vector in W such that $x - p_W(x) \in W^{\perp}$.

Remark 10.44. Simply by definition we have

$$p_W(x) + p_{W^\perp}(x) = x$$

for all $x \in V$ and all subspaces W of V. This can be very useful in practice, since it might be easier to compute the orthogonal projection onto $W^\perp$ than that onto W.

Example 10.45. Endow $\mathbf{R}^3$ with the canonical inner product. Let $W = \{(0, 0, a_3) \mid a_3 \in \mathbf{R}\}$. Then the orthogonal complement $W^\perp$ is

$$W^\perp = \{(a_1, a_2, 0) \mid a_1, a_2 \in \mathbf{R}\}.$$

Note that W is the Cartesian z-axis and $W^\perp$ is the Cartesian xy-plane. The orthogonal projection P_W of $\mathbf{R}^3$ onto W is the map

$$P_W : \mathbf{R}^3 \to \mathbf{R}^3, \quad P_W(x, y, z) = (0, 0, z).$$

Problem 10.46. Let

$$v_1 = (1, -1, 0, 0) \quad \text{and} \quad v_2 = (1, 0, -1, 0).$$

Find the matrix of the orthogonal projection of $\mathbf{R}^4$ onto $W = \text{Span}(v_1, v_2)$.

Solution. Let $v \in \mathbf{R}^4$ and write $p_W(v) = av_1 + bv_2$ for some real numbers a, b. Since $v - p_W(v)$ is orthogonal to W, we have

$$\langle v - (av_1 + bv_2), v_1\rangle = \langle v - (av_1 + bv_2), v_2\rangle = 0,$$

which can also be written, taking into account that

$$||v_1||^2 = 2, \quad ||v_2||^2 = 2, \quad \langle v_1, v_2\rangle = 1,$$

as

$$2a + b = \langle v, v_1\rangle, \quad a + 2b = \langle v, v_2\rangle.$$

Solving the system yields

$$a = \langle v, \frac{2v_1 - v_2}{3}\rangle, \quad b = \langle v, \frac{2v_2 - v_1}{3}\rangle.$$

Since

$$\frac{2v_1 - v_2}{3} = \left(\frac{1}{3}, -\frac{2}{3}, \frac{1}{3}, 0\right), \quad \frac{2v_2 - v_1}{3} = \left(\frac{1}{3}, \frac{1}{3}, -\frac{2}{3}, 0\right),$$

we can easily compute the values $p_W(e_1), \ldots, p_W(e_4)$, where $e_1, \ldots, e_4$ is the canonical basis of $\mathbf{R}^4$. More precisely, we obtain for $v = v_1$ that $a = \frac{1}{3}$ and $b = \frac{1}{3}$, thus

$$p_W(e_1) = \frac{v_1 + v_2}{3} = \left(\frac{2}{3}, -\frac{1}{3}, -\frac{1}{3}, 0\right),$$

and similar arguments yield

$$p_W(e_2) = \frac{-2v_1 + v_2}{3} = \left(-\frac{1}{3}, \frac{2}{3}, -\frac{1}{3}, 0\right),$$

$$p_W(e_3) = \frac{v_1 - 2v_2}{3} = \left(-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}, 0\right)$$

and finally

$$p_W(e_4) = 0 \cdot v_1 + 0 \cdot v_2 = (0, 0, 0, 0).$$

We conclude that the desired matrix is

$$A = \begin{bmatrix} \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \qquad \square$$

Definition 10.47. Let V be an Euclidean space. A linear map $p : V \to V$ is called an **orthogonal projection** if there is a subspace W of V such that p is the orthogonal projection onto W.

The next theorem describes orthogonal projections as solutions to minimization problems. The result is absolutely fundamental:

Theorem 10.48. *Let V be a $\mathbf{R}$-vector space with an inner product $\langle\ ,\ \rangle$ and with associated norm $||\cdot||$. Let W be a finite dimensional subspace of V and let $v \in V$. Then $p_W(v)$ is the element of W at smallest distance from v, i.e.*

$$||v - p_W(v)|| = \min_{x \in W} ||x - v||.$$

Moreover, $p_W(v)$ is the unique element of W with this property.

Proof. Let $x \in W$ and apply the Pythagorean theorem (Remark 10.39; observe that $x - p_W(v) \in W$ and $v - p_W(v) \in W^{\perp}$) to obtain

$$||x - v||^2 = ||(x - p_W(v)) + (p_W(v) - v)||^2 =$$

$$||x - p_W(v)||^2 + ||p_W(v) - v||^2 \geq ||p_W(v) - v||^2.$$

This shows that $||x-v|| \geq ||p_W(v)-v||$ for al $v \in V$ and yields the first part of the theorem. For the second part, note that equality holds in the first offset equation if and only if $x = p_W(v)$. This finishes the proof of the theorem. □

Definition 10.49. With the notations of Theorem 10.48, we define the **distance from** v **to** W as

$$d(v,W) = ||v - p_W(v)|| = \min_{x \in W} ||x - v||.$$

Problem 10.50. Let V be a $\mathbf{R}$-vector space endowed with an inner product $\langle\ ,\ \rangle$ and let W be a finite dimensional subspace of V. Let $x_1, \ldots, x_n$ be a basis of W and let $v \in V$. Prove that

$$d(v,W)^2 = \frac{G(v, x_1, \ldots, x_n)}{G(x_1, \ldots, x_n)},$$

where $G(x_1, \ldots, x_n) = \det(\langle x_i, x_j \rangle)$ is the Gram determinant of the family $x_1, \ldots, x_n$.

Solution. Write $p_W(v) = a_1 x_1 + \ldots + a_n x_n$ for some real numbers $a_1, \ldots, a_n$. By definition

$$d(v,W)^2 = ||v - p_W(v)||^2 = \langle v - p_W(v), v \rangle = ||v||^2 - \langle v, p_W(v) \rangle,$$

thus

$$d(v,W)^2 + a_1 \langle v, x_1 \rangle + \ldots + a_n \langle v, x_n \rangle = ||v||^2.$$

Since

$$\langle v, x_i \rangle = \langle v - p_W(v), x_i \rangle + \langle p_W(v), x_i \rangle = \langle p_W(v), x_i \rangle$$

$$= a_1 \langle x_1, x_i \rangle + a_2 \langle x_2, x_i \rangle + \ldots + a_n \langle x_n, x_i \rangle,$$

we deduce that $d(v,W)^2$ and $a_1, \ldots, a_n$ are solutions of the linear system in the unknowns $t_0, \ldots, t_n$

$$\begin{cases} t_0 + t_1 \langle v, x_1 \rangle + \ldots + t_n \langle v, x_n \rangle = ||v||^2 \\ t_1 \langle x_1, x_1 \rangle + t_2 \langle x_1, x_2 \rangle + \ldots + t_n \langle x_1, x_n \rangle = \langle v, x_1 \rangle \\ \qquad\qquad \ldots \\ t_1 \langle x_1, x_n \rangle + t_2 \langle x_2, x_n \rangle + \ldots + t_n \langle x_n, x_n \rangle = \langle v, x_n \rangle \end{cases}$$

The result follows then straight from Cramer's rule. □

Problem 10.51. Consider the vectors

$$v_1 = \begin{bmatrix} 3 \\ 1 \\ -1 \\ 1 \end{bmatrix}, \qquad v_2 = \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \qquad \text{and} \qquad b = \begin{bmatrix} 3 \\ 1 \\ 5 \\ 1 \end{bmatrix}.$$

Find the distance from b to the space $W = \text{Span}(v_1, v_2)$.

Solution. We start by finding the orthogonal projection of b on W by writing

$$b = p_W(b) + u$$

with $\langle u, v_1 \rangle = \langle u, v_2 \rangle = 0$. Writing $p_W(b) = \alpha v_1 + \beta v_2$ we obtain

$$\alpha ||v_1||^2 + \beta \langle v_1, v_2 \rangle = \langle b, v_1 \rangle$$

and

$$\alpha \langle v_1, v_2 \rangle + \beta ||v_2||^2 = \langle b, v_2 \rangle,$$

which reduces to

$$12\alpha = 6, \quad 4\beta = 6.$$

We deduce that

$$p_W(b) = \frac{1}{2} v_1 + \frac{3}{2} v_2 = \begin{bmatrix} 3 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

and so

$$d(b, W) = ||b - p_W(b)|| =$$

$$\sqrt{(3-3)^2 + (1-(-1))^2 + (5-1)^2 + (1-(-1))^2} = \sqrt{24}.$$

Of course, one can also use the previous exercise, by computing (exercise left to the reader) $G(v_1, v_2) = 48$ and $G(b, v_1, v_2) = 32 \cdot 36$, then

$$d(b, W) = \sqrt{\frac{G(b, v_1, v_2)}{G(v_1, v_2)}} = \sqrt{24}.$$

However, we strongly advise the reader to redo every time the argument explained in the first part of the solution. □

Problem 10.52. Let n be a positive integer and let V be the vector space of polynomials with real coefficients whose degree does not exceed n. For $P, Q \in V$ define

$$\langle P, Q\rangle = \int_0^\infty P(x)Q(x)e^{-x}dx.$$

a) Explain why $\langle\ ,\ \rangle$ is a well-defined inner product on V.
b) Find

$$\min_{a_1,\ldots,a_n\in\mathbf{R}} \int_0^\infty (1 + a_1x + \ldots + a_nx^n)^2e^{-x}dx.$$

Solution. a) The definition makes sense, since x^ke^{-x} is integrable on $[0, \infty)$ for all $k \geq 0$. More precisely, we have the following classical result, which follows easily by induction on k combined with integration by parts

$$\int_0^\infty e^{-x}x^k dx = k!.$$

It is easy to see that $\langle\ ,\ \rangle$ is indeed an inner product: it is clearly symmetric and bilinear, and we have

$$\langle P, P\rangle = \int_0^\infty P(x)^2e^{-x}dx \geq 0.$$

If the last quantity equals 0, then so does $\int_0^1 e^{-x}P(x)^2dx \leq \int_0^\infty e^{-x}P(x)^2dx$. Since $x \mapsto e^{-x}P(x)^2$ is continuous, nonnegative, and with average value 0 on $[0, 1]$, it must be the zero map, thus P vanishes on $[0, 1]$ and so $P = 0$ (because P is a polynomial). This proves the claim that $\langle\ ,\ \rangle$ is an inner product.

b) Let W be the span of $X, X^2, \ldots, X^n$, then W is a subspace of V and the problem asks us to find

$$\inf_{P\in W} ||1 + P||^2 = d(-1, W)^2.$$

We know that the minimum value is attained when P is the orthogonal projection of -1 on W. This is characterized by $\langle P + 1, Q\rangle = 0$ for all $Q \in W$, or equivalently $\langle P + 1, X^k\rangle = 0$ for all $1 \leq k \leq n$. Using the identity

$$\int_0^\infty e^{-x}x^k dx = k!$$

and writing $P = a_1X + \ldots + a_nX^n$, we can rewrite the condition as

$$k! + \sum_{i=1}^{n} a_i(k+i)! = 0 \quad \text{or} \quad 1 + \sum_{i=1}^{n} a_i(k+1)\ldots(k+n) = 0.$$

Thus the polynomial $Q = 1 + \sum_{i=1}^{n} a_i(X+1)\ldots(X+i)$ vanishes at $1, 2, \ldots, n$ and since it has degree n and leading coefficient a_n, we must have

$$Q = a_n(X-1)\ldots(X-n).$$

We need to evaluate

$$d(-1, W)^2 = ||1 + P||^2 = \langle 1 + P, 1\rangle = 1 + \sum_{i=1}^{n} a_i i! = Q(0) = (-1)^n n! a_n.$$

Taking $X = -1$ in the equality

$$1 + \sum_{i=1}^{n} a_i(X+1)\ldots(X+n) = a_n(X-1)\ldots(X-n)$$

yields

$$1 = a_n(-1)^n(n+1)!.$$

We conclude that the answer of the problem is

$$(-1)^n n! a_n = n! \cdot \frac{1}{(n+1)!} = \frac{1}{n+1}.$$ □

10.4.1 Problems for Practice

Whenever it is not specified, the inner product on $\mathbf{R}^n$ is the canonical one.

1. Let

$$x_1 = \begin{bmatrix} 1 \\ 3 \\ -2 \end{bmatrix}, \qquad x_2 = \begin{bmatrix} 6 \\ 4 \\ 2 \end{bmatrix} \qquad \text{and} \qquad b = \begin{bmatrix} 4 \\ -2 \\ -3 \end{bmatrix}.$$

   Find the distance from b to the plane spanned by x_1 and x_2.
2. Determine the orthogonal projection of $b = (2, 1, 1)$ on the subspace spanned by $(1, 1, 1)$ and $(1, 0, 1)$.

3. Let W be the subspace of $\mathbf{R}^4$ spanned by $w = (1, -1, 1, -1)$. Find the orthogonal projection of $b = (3, 0, 3, -2)$ on the orthogonal complement $W^{\perp}$.
4. Consider the vector space V of continuous real-valued maps on $[0, 1]$, with the inner product defined by

$$\langle f, g \rangle = \int_0^1 f(x)g(x)dx.$$

Determine which of the functions $f(x) = x$ and $g(x) = x^3$ is closer (with respect to the distance associated with the norm induced by the inner product) to the function $h(x) = x^2$.

5. a) Let V be an Euclidean space and let T_1, T_2 be orthogonal projections such that $T_1 \circ T_2$ is a projection. Prove that $T_1 \circ T_2 = T_2 \circ T_1$. Hint: use Problem 14.
   b) Does this result remain true if we no longer assume that T_1 and T_2 are orthogonal projections, but only projections?
6. Let $a_1, \ldots, a_n$ be real numbers, not all of them equal to 0. Let H be the set of vectors $(x_1, \ldots, x_n) \in \mathbf{R}^n$ such that $a_1x_1 + \ldots + a_nx_n = 0$. Find the matrix of the orthogonal projection onto H with respect to the canonical basis of $\mathbf{R}^n$.
7. Let V be the vector space of polynomials with real coefficients whose degree does not exceed n. If $P = \sum_{i=0}^n a_i X^i \in V$ and $Q = \sum_{i=0}^n b_i X^i \in V$, define

$$\langle P, Q \rangle = \sum_{i=0}^{n} a_i b_i.$$

Let H be the subspace of polynomials in V vanishing at 1. Compute $d(X, H)$.

8. Let V be the set of polynomials with real coefficients and degree not exceeding 3. Find

$$\min_{P \in V} \int_{-\pi}^{\pi} |P(x) - \sin x|^2.$$

9. Find the vector in $\mathrm{Span}((1, 2, 1), (-1, 3, -4))$ which is closest (with respect to the Euclidean norm) to the vector $(-1, 1, 1)$.
10. Let $v_1 = (0, 1, 1, 0)$, $v_2 = (1, -1, 1, -1)$ in $\mathbf{R}^4$. Let W be the span of v_1, v_2.
    a) Find the matrix of the orthogonal projection of $\mathbf{R}^4$ onto W with respect to the canonical basis of $\mathbf{R}^4$.
    b) Compute the distance from $(1, 1, 1, 1)$ to W.
11. Let V be the space of smooth real-valued maps on $[0, 1]$, endowed with

$$\langle f, g \rangle = \int_0^1 f(x)g(x)dx + \int_0^1 f'(x)g'(x)dx.$$

a) Prove that $\langle\ ,\ \rangle$ is an inner product on V.
b) Let W_1 be the subspace of V consisting of maps f vanishing at 0 and 1. Let W_2 be the subspace of V consisting of maps f such that $f'' = f$. Prove that $W_1 \oplus W_2 = V$ and that W_1 and W_2 are orthogonal to each other.
c) Describe the orthogonal projection of V onto W_2.

12. Let $(V, \langle\ ,\ \rangle)$ be an Euclidean space and let $f : V \to V$ be a map such that $\langle f(x), y\rangle = \langle x, f(y)\rangle$ for all $x, y \in V$. Prove that f is linear.
13. Let V be an Euclidean space and let $T : V \to V$ be a linear map such that $T^2 = T$, i.e., T is a projection. Prove that the following statements are equivalent:

a) T is an orthogonal projection.
b) For all $x, y \in V$ we have $\langle T(x), y\rangle = \langle x, T(y)\rangle$.

14. Let V be an Euclidean space and let T be a linear transformation on V such that $T^2 = T$, i.e., T is a projection.

a) Suppose that T is an orthogonal projection. Using the Pythagorean theorem, prove that for all $x \in V$ we have

$$||T(x)|| \leq ||x||.$$

b) Conversely, suppose that $||T(x)|| \leq ||x||$ for all $x \in V$. Prove that $\langle x, y\rangle = 0$ for $x \in \ker T$ and $y \in \mathrm{Im}(T)$ (hint: use that $||T(x + cy)||^2 \leq ||x + cy||^2$ for all real numbers c) and deduce that T is an orthogonal projection.

10.5 Orthogonal Bases

Let V be a vector space over $\mathbf{R}$ endowed with an inner product $(x, y) \mapsto \langle x, y\rangle$, with associated norm $||\cdot||$ (recall that $||x|| = \sqrt{\langle x, x\rangle}$ for all $x \in V$).

Definition 10.53. a) A family $(v_i)_{i\in I}$ of vectors in V is called **orthogonal** if

$$\langle v_i, v_j\rangle = 0 \quad \text{for all} \quad i \neq j \in I.$$

It is called **orthonormal** if moreover $||v_i|| = 1$ for all $i \in I$. Thus the vectors in an orthonormal family of V have norm 1 and are pairwise orthogonal.
b) An **orthogonal basis** of V is a basis of V which is an orthogonal family.
c) An **orthonormal basis** of V is a basis which is an orthonormal family.

Note that the canonical basis of $\mathbf{R}^n$ is an orthonormal basis of $\mathbf{R}^n$ with respect to the canonical inner product on $\mathbf{R}^n$. In the following two exercises the reader will find two other very important examples of orthonormal families.

Problem 10.54. Let $x_0, \ldots, x_n$ be pairwise distinct real numbers and consider the space V of polynomials with real coefficients and degree not exceeding n, endowed

with

$$\langle P, Q\rangle = \sum_{i=0}^{n} P(x_i)Q(x_i).$$

Prove that $\langle\ ,\ \rangle$ is an inner product on V and that the family $(L_i)_{0\leq i\leq n}$ where

$$L_i(X) = \prod_{\substack{0\leq k\leq n\\ k\neq i}} \frac{X - x_k}{x_i - x_k}$$

is an orthonormal family in V.

Solution. Clearly $\langle\ ,\ \rangle$ is a symmetric bilinear form on V and for all $P \in V$ we have

$$\langle P, P\rangle = \sum_{i=0}^{n} P(x_i)^2 \geq 0,$$

with equality if and only if $P(x_i) = 0$ for $0 \leq i \leq n$. Since $x_0, \ldots, x_n$ are pairwise distinct and since $\deg P \leq n$, it follows that necessarily $P = 0$ and so $\langle\ ,\ \rangle$ is an inner product on V.

To prove the second assertion, let $i \neq j \in \{0, \ldots, n\}$ and let us compute

$$\langle L_i, L_j\rangle = \sum_{k=0}^{n} L_i(x_k)L_j(x_k).$$

Now, by construction we have

$$L_i(x_j) = \delta_{ij},$$

where $\delta_{ij} = 0$ if $i \neq j$ and 1 otherwise. Thus

$$\langle L_i, L_j\rangle = \sum_{k=0}^{n} \delta_{ik}\delta_{jk}.$$

If $i \neq j$, then $\delta_{ik}\delta_{jk} = 0$ for $0 \leq k \leq n$, thus $\langle L_i, L_j\rangle = 0$. If $i = j$, then $\delta_{ik}\delta_{jk} = 0$ for $k \neq i$ and 1 for $k = i$, thus $\langle L_i, L_i\rangle = 1$ and the result follows. □

Problem 10.55. Let V be the space of continuous 2π-periodic maps $f : \mathbf{R} \to \mathbf{R}$, endowed with the inner product

$$\langle f, g\rangle = \int_{-\pi}^{\pi} f(x)g(x)dx.$$

Let $c_n, s_n \in V$ be the maps defined by

$$c_n(x) = \cos(nx), \quad s_n(x) = \sin(nx).$$

Prove that the family

$$\mathcal{F} = \left\{ \frac{1}{\sqrt{2\pi}} \right\} \bigcup \left\{ \frac{1}{\sqrt{\pi}} c_n \,|\, n \geq 1 \right\} \bigcup \left\{ \frac{1}{\sqrt{\pi}} s_n \,|\, n \geq 1 \right\}$$

is an orthonormal family in V.

Solution. To simplify notations a little bit, let $C_0 = \frac{1}{\sqrt{2\pi}}$ and for $n \geq 1$

$$C_n = \frac{1}{\sqrt{\pi}} c_n, \quad S_n = \frac{1}{\sqrt{\pi}} s_n.$$

Clearly

$$||C_0||^2 = \int_{-\pi}^{\pi} \frac{1}{2\pi} dx = 1.$$

Next,

$$||C_n||^2 = \int_{-\pi}^{\pi} \frac{1}{\pi} \cos^2(nx) dx = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{1 + \cos(2nx)}{2} dx = 1,$$

since

$$\int_{-\pi}^{\pi} \cos(px) dx = 0 \quad \forall \quad p \in \mathbf{Z}^* \tag{10.2}$$

(a primitive of $\cos(px)$ is $\frac{1}{p} \sin(px)$ and this vanishes at π and $-\pi$). Similarly, we obtain that $||S_n|| = 1$, by using the identity

$$\sin^2(nx) = \frac{1 - \cos(2nx)}{2}.$$

Thus $||v|| = 1$ for all $v \in \mathcal{F}$.

It remains to check that elements of $\mathcal{F}$ are pairwise orthogonal. That C_0 is orthogonal to C_n and S_n for all $n \geq 1$ follows from relation (10.2) and its analogue

$$\int_{-\pi}^{\pi} \sin(px) = 0, \quad \forall \quad p \in \mathbf{Z} \tag{10.3}$$

Next, we check that C_n and C_m are orthogonal for $m \neq n$. This follows from the identity

$$\cos(nx)\cos(mx) = \frac{\cos((m-n)x) + \cos((m+n)x)}{2}$$

and relation (10.2). Similarly, the fact that S_n and S_m are orthogonal for $n \neq m$ is a consequence of the relations

$$\sin(nx)\sin(mx) = \frac{\cos((m-n)x) - \cos((m+n)x)}{2}$$

and (10.2). Finally, the fact that S_n and C_m are orthogonal for $n, m \geq 1$ follows from relations

$$\sin(nx)\cos(mx) = \frac{\sin((m+n)x) + \sin((n-m)x)}{2}$$

and (10.3). □

A fundamental property of orthonormal families is that they are linearly independent. More precisely

Proposition 10.56. *Let V be a vector space over $\mathbf{R}$ endowed with an inner product. Then any orthogonal family $(v_i)_{i\in I}$ of **nonzero** vectors in E is linearly independent.*

Proof. Suppose that $\sum_{i\in I} a_i v_i = 0$ for some scalars $a_i \in \mathbf{R}$, such that all but finitely many of them are 0. For $j \in I$ we have

$$\langle v_j, \sum_{i\in I} a_i v_i \rangle = 0.$$

By bilinearity, the left-hand side equals

$$\sum_{i\in I} a_i \langle v_j, v_i \rangle = a_j ||v_j||^2,$$

the last equality being a consequence of the fact that $(v_i)_{i\in I}$ is orthogonal. We deduce (thanks to the hypothesis that $v_j \neq 0$ for all j) that $a_j = 0$ for all $j \in I$ and the result follows. □

The following result is a direct consequence of the previous proposition:

Corollary 10.57. *An orthogonal family of nonzero vectors in an Euclidean space of dimension n has at most n elements. Moreover, it has n elements if and only if it is an orthogonal basis. **In particular, an orthonormal family of n vectors in an n-dimensional Euclidean space is automatically an orthonormal basis of that space.***

When we have an orthonormal basis $e_1, \ldots, e_n$ of an Euclidean space V, it is rather easy to write down the coordinates of a vector $v \in V$ with respect to this basis: these coordinates are simply $\langle v, e_i \rangle$ for $1 \leq i \leq n$. More precisely, we have the very important formula

$$v = \sum_{i=1}^{n} \langle v, e_i \rangle e_i \tag{10.4}$$

called the **Fourier decomposition of v with respect to the orthonormal basis** $e_1, \ldots, e_n$. In order to prove formula (10.4), write

$$v = \sum_{i=1}^{n} x_i e_i$$

for some real numbers x_i and observe that

$$\langle v, e_j \rangle = \sum_{i=1}^{n} \langle x_i e_i, e_j \rangle = \sum_{i=1}^{n} x_i \langle e_i, e_j \rangle = x_j$$

for all $1 \leq j \leq n$.

Let us come back for a moment to the setup and notations of Problem 10.54. Recall that we proved in that problem that the polynomials

$$L_i(X) = \prod_{\substack{0 \leq k \leq n \\ k \neq i}} \frac{X - x_k}{x_i - x_k}$$

for $0 \leq i \leq n$ form an orthonormal family in the space V of polynomials with real coefficients and degree at most n, endowed with the inner product defined by

$$\langle P, Q \rangle = \sum_{i=0}^{n} P(x_i) Q(x_i).$$

Since $\dim V = n+1$ and since the family $(L_i)_{0 \leq i \leq n}$ is orthonormal (Problem 10.54) and has $n + 1$ elements, Corollary 10.57 shows that this family is an orthonormal basis of V. Moreover, for each $P \in V$ the Fourier decomposition of P becomes

$$P = \sum_{i=0}^{n} \langle P, L_i \rangle L_i.$$

Note that

$$\langle P, L_i \rangle = \sum_{k=0}^{n} P(x_k) L_i(x_k) = P(x_i),$$

since $L_i(x_k) = 0$ for $i \neq k$ and 1 for $i = k$. We obtain in this way **Lagrange's interpolation formula: for all polynomials P of degree at most n we have**

$$P = \sum_{i=0}^{n} P(x_i) L_i = \sum_{i=0}^{n} P(x_i) \prod_{\substack{0 \leq k \leq n \\ k \neq i}} \frac{X - x_k}{x_i - x_k}.$$

Let us do now the same thing starting with Problem 10.55. Let $\mathcal{T}_n$ be the space of **trigonometric polynomials** of degree at most n. By definition,

$$\mathcal{T}_n = \text{Span}(c_0, c_1, \ldots, c_n, s_1, \ldots, s_n),$$

where we recall that

$$c_k(x) = \cos(kx), \quad s_k(x) = \sin(kx).$$

Thus an element of $\mathcal{T}_n$ is a continuous 2π-periodic map of the form

$$x \mapsto a_0 + \sum_{k=1}^{n} (a_k \cos(kx) + b_k \sin(kx))$$

with $a_k, b_k \in \mathbf{R}$. By Problem 10.55 the family

$$\mathcal{F}_n = \left\{ \frac{1}{\sqrt{2\pi}} \right\} \bigcup \left\{ \frac{1}{\sqrt{\pi}} c_k \,|\, 1 \leq k \leq n \right\} \bigcup \left\{ \frac{1}{\sqrt{\pi}} s_k \,|\, 1 \leq k \leq n \right\}$$

is orthonormal with respect to the inner product

$$\langle f, g \rangle = \int_{-\pi}^{\pi} f(x) g(x) dx$$

on $\mathcal{T}_n$. This family is therefore linearly independent in $\mathcal{T}_n$ and by definition it spans $\mathcal{T}_n$, hence it is an orthonormal basis of $\mathcal{T}_n$. If $f : \mathbf{R} \to \mathbf{R}$ is any continuous 2π-periodic map, we call the sum

$$S_n(f) = \sum_{g \in \mathcal{F}_n} \langle f, g \rangle g$$

the n**th partial Fourier series of** f. A small calculation shows that we can also write

$$S_n(f)(x) = \frac{a_0(f)}{2} + \sum_{k=1}^{n} \left(a_k(f) \cos(kx) + b_k(f) \sin(kx) \right),$$

where

$$a_m(f) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(mx)dx, \quad b_m(f) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(mx)dx$$

and the mth **Fourier coefficients of** f.

We can also rewrite the previous results in terms of the **complex Fourier coefficients**

$$c_m(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-imx}dx$$

of f. These are usually referred to simply as the Fourier coefficients of f. A nice exercise for the reader consists in checking that the partial Fourier series can also be expressed as

$$S_n(f)(x) = \sum_{k=-n}^{n} c_k(f)e^{ikx},$$

by first checking that for $m \geq 0$

$$c_m(f) = \frac{a_m(f) - ib_m(f)}{2}.$$

Note that relation (10.4) says that

$$f = S_n(f) \quad \text{if} \quad f \in \mathcal{T}_n,$$

but of course we do not have $f = S_n(f)$ for any continuous 2π-periodic function f. One may wonder what is the actual relationship between f and the partial Fourier series of f. The naive guess would be that

$$\lim_{n\to\infty} S_n(f)(x) = f(x)$$

for every continuous 2π-periodic map $f : \mathbf{R} \to \mathbf{R}$. This is not true, but there are many situations in which this is actually true: a deep theorem in Fourier analysis due to Dirichlet says that if f and its derivative are piecewise continuous, then for all x we have

$$\lim_{n\to\infty} S_n(f)(x) = \frac{f(x+) + f(x-)}{2},$$

where $f(x+)$ and $f(x-)$ are the one-sided limits of f at x. Thus if moreover f is continuous, we do have

$$\lim_{n\to\infty} S_n(f)(x) = f(x),$$

which we can write as

$$f(x) = \sum_{k \in \mathbf{Z}} c_k(f) e^{ikx} = \frac{a_0(f)}{2} + \sum_{k=1}^{\infty} \left(a_k(f)\cos(kx) + b_k(f)\sin(kx)\right).$$

Orthogonal bases are extremely useful in practice, as we can easily compute orthogonal projections and distances once we have at our disposal an orthogonal basis of the space we are interested in. More precisely, we have the following very useful

Theorem 10.58. *Let V be a vector space over $\mathbf{R}$ endowed with an inner product $\langle\,,\,\rangle$ and let W be a finite dimensional subspace of V. Let $v_1, \ldots, v_n$ be an orthogonal basis of W. Then for all $v \in V$ we have*

$$p_W(v) = \sum_{i=1}^{n} \frac{\langle v, v_i\rangle}{||v_i||^2} v_i.$$

Proof. Let us write $v = p_W(v) + u$, with $u \in W^{\perp}$, that is $\langle u, v_i\rangle = 0$ for all $i \in [1, n]$. Letting $p_W(v) = \alpha_1 v_1 + \ldots + \alpha_n v_n$ and using the fact that $v_1, \ldots, v_n$ is an orthogonal family, we obtain

$$0 = \langle u, v_i\rangle = \langle v, v_i\rangle - \langle p_W(v), v_i\rangle$$

$$= \langle v, v_i\rangle - \sum_{j=1}^{n} \alpha_j \langle v_j, v_i\rangle = \langle v, v_i\rangle - \alpha_i ||v_i||^2.$$

It follows that

$$\alpha_i = \frac{\langle v, v_i\rangle}{||v_i||^2}$$

and the theorem is proved. □

We can say quite a bit more. The inequality in the theorem below is called **Bessel's inequality**.

Theorem 10.59. *Let V be a vector space over $\mathbf{R}$ endowed with an inner product $\langle\,,\,\rangle$, and let W be a finite dimensional subspace of V. If $v_1, \ldots, v_n$ is an orthonormal basis of W, then for all $v \in V$ we have*

$$p_W(v) = \sum_{i=1}^{n} \langle v, v_i\rangle \cdot v_i$$

and

$$d(v,W)^2 = ||v - \sum_{i=1}^{n} \langle v, v_i \rangle \cdot v_i||^2 = ||v||^2 - \sum_{i=1}^{n} \langle v, v_i \rangle^2.$$

In particular we have

$$\sum_{i=1}^{n} \langle v, v_i \rangle^2 \leq ||v||^2.$$

Proof. The formula for $p_W(v)$ is a direct consequence of the previous theorem. Next, using the Pythagorean theorem

$$||v||^2 = ||v - p_W(v)||^2 + ||p_W(v)||^2.$$

On the other hand, since $v_1, \ldots, v_n$ is an orthonormal basis, we have

$$||p_W(v)||^2 = ||\sum_{i=1}^{n} \langle v, v_i \rangle \cdot v_i||^2 =$$

$$\sum_{i,j=1}^{n} \langle \langle v, v_i \rangle v_i, \langle v, v_j \rangle v_j \rangle = \sum_{i,j=1}^{n} \langle v, v_i \rangle \cdot \langle v, v_j \rangle \cdot \langle v_i, v_j \rangle =$$

$$\sum_{i,j=1}^{n} \delta_{i,j} \langle v, v_i \rangle \cdot \langle v, v_j \rangle = \sum_{i=1}^{n} \langle v, v_i \rangle^2.$$

Combining these equalities yields

$$d(v,W)^2 = ||v - \sum_{i=1}^{n} \langle v, v_i \rangle \cdot v_i||^2 = ||v||^2 - \sum_{i=1}^{n} \langle v, v_i \rangle^2.$$

Finally, since $d(v,W)^2 \geq 0$, the last inequality is a direct consequence of the previous formula. □

Remark 10.60. Let V be a vector space over $\mathbf{R}$ endowed with an inner product and let $(v_i)_{i \in I}$ be an orthogonal family. If $(a_i)_{i \in I}$ are real numbers, all but finitely many being equal to 0, then

$$||\sum_{i \in I} a_i v_i||^2 = \sum_{i \in I} a_i^2 ||v_i||^2.$$

In particular, if $(v_i)_{i\in I}$ is an orthonormal family, then

$$||\sum_{i\in I} a_i v_i||^2 = \sum_{i\in I} a_i^2.$$

This can be proved in the same way as the previous theorem: we have

$$||\sum_{i\in I} a_i v_i||^2 = \langle \sum_{i\in I} a_i v_i, \sum_{j\in I} a_j v_j\rangle =$$

$$\sum_{i,j\in I} a_i a_j \langle v_i, v_j\rangle = \sum_{i\in I} a_i^2 \langle v_i, v_i\rangle = \sum_{i\in I} a_i^2 ||v_i||^2,$$

since the family is orthogonal. Note that the algebraic operations are allowed since we assumed that all but finitely many of the a_i's are zero, thus we never manipulate infinite sums.

Remark 10.61. Let us come back to the discussion preceding the previous theorem. If $f : \mathbf{R} \to \mathbf{R}$ is a continuous 2π-periodic map, we deduce from that discussion and the previous theorem that $S_n(f)$ (the nth partial Fourier series of f) is the orthogonal projection of f on the space $\mathcal{T}_n$ of trigonometric polynomials of degree at most n and that

$$\sum_{g\in\mathcal{F}_n} \langle f, g\rangle^2 \leq ||f||^2 = \int_{-\pi}^{\pi} f(x)^2 dx.$$

This can be rewritten in terms of the Fourier coefficients $a_m(f), b_m(f)$ of f as

$$\frac{a_0(f)^2}{2} + \sum_{k=1}^{n} (a_k(f)^2 + b_k(f)^2) \leq \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)^2 dx.$$

Since this holds for all n, we deduce that the series

$$\sum_{k\geq 1} (a_k(f)^2 + b_k(f)^2)$$

converges and

$$\frac{a_0(f)^2}{2} + \sum_{k=1}^{\infty} (a_k(f)^2 + b_k(f)^2) \leq \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)^2 dx.$$

The convergence of the previous series yields

$$\lim_{n\to\infty} a_n(f) = \lim_{n\to\infty} b_n(f) = 0,$$

a nontrivial result known as the **Riemann–Lebesgue theorem**. On the other hand, one can prove (this is the famous **Plancherel theorem**) that the previous inequality is actually an equality, that is for all continuous 2π-periodic maps f we have

$$\frac{a_0(f)^2}{2} + \sum_{k=1}^{\infty}(a_k(f)^2 + b_k(f)^2) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)^2 dx.$$

The proof is beyond the scope of this book. A good exercise for the reader is to convince himself that Plancherel's theorem can be rewritten as

$$\sum_{k\in\mathbf{Z}} |c_k(f)|^2 = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)^2 dx,$$

where we recall that

$$c_k(f) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-ikx} dx.$$

Plancherel's theorem also holds for functions $f : \mathbf{R} \to \mathbf{R}$ which are piecewise continuous and 2π-periodic.

Problem 10.62. a) Determine an orthogonal basis of $\mathbf{R}^3$ containing the vector $w = (1, 2, -1)$.

b) Let W be the subspace of $\mathbf{R}^3$ spanned by w. Find the projection of $v = (1, 2, 1)$ onto the orthogonal complement of W.

Solution. a) We look for an orthogonal basis w, v_1, v_2 of $\mathbf{R}^3$. In particular v_1, v_2 should be an orthogonal basis of $(\mathbf{R}w)^\perp$. A vector $v = (x, y, z)$ belongs to $(\mathbf{R}w)^\perp$ if and only if

$$0 = \langle v, w\rangle = x + 2y - z.$$

Thus we must have

$$v_1 = (x_1, y_1, x_1 + 2y_1), \quad v_2 = (x_2, y_2, x_2 + 2y_2)$$

for some real numbers x_1, x_2, y_1, y_2. Moreover, we should have $\langle v_1, v_2\rangle = 0$ and v_1, v_2 should be nonzero: this automatically implies that v_1, v_2 are linearly independent (because $\langle v_1, v_2\rangle = 0$) and so they form a basis of $(\mathbf{R}w)^\perp$. The condition $\langle v_1, v_2\rangle = 0$ is equivalent to

$$x_1x_2 + y_1y_2 + (x_1 + 2y_1)(x_2 + 2y_2) = 0.$$

We see that we have lots of choices: to keep things simple we choose $x_1 + 2y_1 = 0$, for instance $y_1 = 1$ and $x_1 = -2$. Then the condition becomes $-2x_2 + y_2 = 0$, so we choose $x_2 = 1$ and $y_2 = 2$. This gives

$$v_1 = (-2, 1, 0), \quad v_2 = (1, 2, 5).$$

We insist that this is only one of the many possible answers of the problem.

b) As we have already seen in part a), the orthogonal complement of W is exactly $\mathrm{Span}(v_1, v_2)$ and an orthogonal basis of $W^\perp$ is given by v_1, v_2. Applying the previous theorem yields

$$p_{W^\perp}(v) = \frac{\langle v, v_1\rangle}{||v_1||^2} v_1 + \frac{\langle v, v_2\rangle}{||v_2||^2} v_2$$

$$= \frac{1}{3} v_2 = (\frac{1}{3}, \frac{2}{3}, \frac{5}{3}).$$

We could have done this in a much easier way as follows: instead of computing $p_{W^\perp}(v)$ we compute first $p_W(v)$. Now an orthogonal basis of W is given by w, thus

$$p_W(v) = \frac{\langle v, w\rangle}{||w||^2} w = \frac{4}{6} w = (\frac{2}{3}, \frac{4}{3}, -\frac{2}{3}).$$

Next, we have

$$p_{W^\perp}(v) = v - p_W(v) = (\frac{1}{3}, \frac{2}{3}, \frac{5}{3}).$$ □

The previous results concerning orthonormal bases show rather clearly the crucial role played by these objects. Yet, we avoided a natural and very important question: can we always find an orthonormal basis? The answer is given by the following fundamental theorem. We do not give its proof right now since we will prove a much stronger result in just a few moments.

Theorem 10.63. *Any Euclidean space has an orthonormal basis.*

The following theorem refines Theorem 10.63 and gives an **algorithmic** construction of an orthonormal basis of an Euclidean space starting with an arbitrary basis of the corresponding vector space. It is absolutely fundamental:

Theorem 10.64 (Gram–Schmidt). *Let $v_1, \ldots, v_d$ be linearly independent vectors in a vector space V over $\mathbf{R}$ (not necessarily finite dimensional), endowed with an inner product $\langle\ ,\ \rangle$. Then there is a unique orthonormal family $e_1, \ldots, e_d$ in V with the property that for all $k \in [1, d]$ we have*

$$\mathrm{Span}(e_1, \ldots, e_k) = \mathrm{Span}(v_1, \ldots, v_k) \quad \textit{and} \quad \langle e_k, v_k\rangle > 0.$$

Proof. We will prove the theorem by induction on d. Let us start with the case $d = 1$. Suppose that e_1 is a vector satisfying the conditions imposed by the theorem. Since $e_1 \in \mathbf{R}v_1$, we can write $e_1 = \lambda v_1$ for some real number λ. Then $\langle e_1, v_1\rangle = \lambda||v_1||^2$ is positive, thus $\lambda > 0$. Next, $||e_1|| = 1$, thus $|\lambda| = \frac{1}{||v_1||}$ and so necessarily $\lambda = \frac{1}{||v_1||}$ and $e_1 = \frac{1}{||v_1||}v_1$. Conversely, this vector satisfies the desired properties, which proves the theorem when $d = 1$.

Assume now that $d \geq 2$ and that the theorem holds for $d - 1$. Let $v_1, \ldots, v_d$ be linearly independent vectors in V. By the inductive hypothesis we know that there is a unique orthonormal family $e_1, \ldots, e_{d-1}$ satisfying the conditions of the theorem with respect to the family $v_1, \ldots, v_{d-1}$. It suffices therefore to prove that there is a unique vector e_d such that $e_1, \ldots, e_d$ satisfies the conditions of the theorem with respect to $v_1, \ldots, v_d$, that is such that

$$||e_d|| = 1, \quad \langle e_d, e_i\rangle = 0 \quad \forall 1 \leq i \leq d-1,$$

and

$$\mathrm{Span}(e_1, \ldots, e_d) = \mathrm{Span}(v_1, \ldots, v_d).$$

Assume first that e_d is such a vector. Then

$$e_d \in \quad \mathrm{Span}(e_1, \ldots, e_d) = \mathrm{Span}(v_1, \ldots, v_d) = \mathbf{R}v_d + \mathrm{Span}(v_1, \ldots, v_{d-1})$$

$$= \mathbf{R}v_d + \mathrm{Span}(e_1, \ldots, e_{d-1}).$$

Thus we can write

$$e_d = \lambda v_d + \sum_{i=1}^{d-1} a_i e_i$$

for some real numbers $\lambda, a_1, \ldots, a_{d-1}$. Then for all $i \in [1, d-1]$ we have (since $e_1, \ldots, e_{d-1}$ is an orthonormal family)

$$0 = \langle e_d, e_i\rangle = \lambda\langle v_d, e_i\rangle + \sum_{j=1}^{d-1} a_j \langle e_j, e_i\rangle = \lambda\langle v_d, e_i\rangle + a_i,$$

thus $a_i = -\lambda\langle v_d, e_i\rangle$ are uniquely determined if λ is so. Next, we have

$$e_d = \lambda(v_d - \sum_{i=1}^{d-1}\langle v_d, e_i\rangle e_i).$$

Note that $z := v_d - \sum_{i=1}^{d-1}\langle v_d, e_i\rangle e_i$ is nonzero, since otherwise $v_d \in \mathrm{Span}(e_1, \ldots, e_{d-1}) = \mathrm{Span}(v_1, \ldots, v_{d-1})$, contradicting the hypothesis that $v_1, \ldots, v_d$ are linearly independent. Now $||e_d|| = 1$ forces $|\lambda| = \frac{1}{||z||}$, and the condition $\langle e_d, v_d\rangle > 0$ shows that the sign of λ is uniquely determined and is actually positive:

$$\langle e_d, v_d\rangle = \langle e_d, \frac{e_d}{\lambda} + \sum_{i=1}^{d-1}\langle v_d, e_i\rangle e_i\rangle = \frac{1}{\lambda}.$$

We deduce that λ is uniquely determined by

$$\lambda = \frac{1}{||z||}$$

and the uniqueness follows.

Conversely, we can define $\lambda = \frac{1}{||z||}$ and $e_d = \lambda z$. The previous computations show that e_d satisfies all required properties and this proves the existence part and finishes the proof of the inductive step. □

Remark 10.65. a) Let us try to understand the proof geometrically (i.e., let us give a less computational and more conceptual proof of the theorem). Assuming that we constructed $e_1, \ldots, e_{d-1}$, we would like to understand how to construct e_d. This vector e_d must be orthogonal to $e_1, \ldots, e_{d-1}$ and it must belong to $W = \mathrm{Span}(v_1, \ldots, v_d)$. It follows that e_d must be in the orthogonal of $\mathrm{Span}(e_1, \ldots, e_{d-1}) = \mathrm{Span}(v_1, \ldots, v_{d-1})$. However

$$\dim \mathrm{Span}(v_1, \ldots, v_{d-1})^{\perp} = \dim \mathrm{Span}(v_1, \ldots, v_d) - \dim \mathrm{Span}(v_1, \ldots, v_{d-1})$$

$$= d - (d-1) = 1,$$

thus e_d is uniquely determined up to a scalar. Since we further want e_d to be of norm 1, this pins down e_d up to a sign. Finally, the condition that $\langle e_d, v_d\rangle > 0$ determines uniquely the sign and so determines uniquely e_d.

b) Part a) (and the proof of the theorem also) gives the following algorithm, known as the **Gram–Schmidt process**, which constructs $e_1, \ldots, e_d$ starting from $v_1, \ldots, v_d$. Set $f_1 = v_1$ and $e_1 = \frac{f_1}{||f_1||}$, then assuming that we constructed $f_1, \ldots, f_{k-1}$ and $e_1, \ldots, e_{k-1}$, let

$$f_k = v_k - \sum_{i=1}^{k-1}\langle v_k, e_i\rangle e_i, \quad \text{and} \quad e_k = \frac{f_k}{||f_k||}.$$

That is, **at each step we subtract from v_k its orthogonal projection $\sum_{i=1}^{k-1}\langle v_k, e_i\rangle e_i$ onto $\mathrm{Span}(e_1, \ldots, e_{k-1})$ and obtain in this way f_k. Then**

we normalize f_k to get e_k. Note that in practice it can be very useful to observe that we can compute $||f_k||$ via

$$||f_k||^2 = \langle f_k, v_k \rangle.$$

This formula follows from the fact that $v_k = f_k + \sum_{i=1}^{k-1} \langle v_k, e_i \rangle e_i$ and e_i is orthogonal to f_k for $1 \leq i \leq k-1$.

Example 10.66. Let us consider the vectors

$$v_1 = (1,1,1), \quad v_2 = (0,2,1), \quad v_3 = (3,1,3) \in \mathbf{R}^3.$$

An easy computation shows that the determinant of the matrix whose columns are v_1, v_2, v_3 is nonzero, thus v_1, v_2, v_3 are linearly independent. Let us follow the Gram–Schmidt process and find the corresponding orthonormal basis of $\mathbf{R}^3$. We set

$$f_1 = v_1, \quad e_1 = \frac{v_1}{||v_1||} = \frac{v_1}{\sqrt{3}} = (\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}).$$

Next, set

$$f_2 = v_2 - \langle v_2, e_1 \rangle e_1 = v_2 - \sqrt{3} e_1 = v_2 - (1,1,1) = (-1,1,0)$$

and

$$e_2 = \frac{f_2}{||f_2||} = \frac{f_2}{\sqrt{2}} = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0).$$

Finally, set

$$f_3 = v_3 - \langle v_3, e_1 \rangle e_1 - \langle v_3, e_2 \rangle e_2 =$$

$$v_3 - \frac{7}{\sqrt{3}} e_1 + \sqrt{2} e_2 = (3,1,3) - (\frac{7}{3}, \frac{7}{3}, \frac{7}{3}) + (-1,1,0)$$

$$= (-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3})$$

and

$$e_3 = \frac{f_3}{||f_3||} = \frac{1}{\sqrt{6}}(-1,-1,2).$$

Problem 10.67. Let V be the space of polynomials with real coefficients whose degree does not exceed 2, endowed with the inner product defined by

$$\langle P, Q\rangle = \int_{-1}^{1} P(x)Q(x)dx.$$

Find the orthonormal basis of V obtained by applying the Gram–Schmidt process to the basis $1, X, X^2$ of V.

Solution. We start with $v_1 = 1, v_2 = X$ and $v_3 = X^2$ and apply the Gram–Schmidt process. We obtain

$$||v_1|| = \sqrt{2}, \quad e_1 = \frac{1}{\sqrt{2}},$$

then

$$f_2 = v_2 - \langle v_2, \frac{1}{\sqrt{2}}\rangle \frac{1}{\sqrt{2}} = X - \frac{1}{2}\int_{-1}^{1} x dx = X$$

and

$$||f_2||^2 = \langle f_2, v_2\rangle = \int_{-1}^{1} x^2 dx = \frac{2}{3},$$

thus

$$e_2 = \frac{f_2}{||f_2||} = \sqrt{\frac{3}{2}}X.$$

Finally,

$$f_3 = v_3 - \langle v_3, \frac{1}{\sqrt{2}}\rangle \frac{1}{\sqrt{2}} - \langle v_3, \sqrt{\frac{3}{2}}X\rangle \sqrt{\frac{3}{2}}X$$

$$= X^2 - \frac{1}{2}\int_{-1}^{1} x^2 dx - \frac{3}{2}(\int_{-1}^{1} x^3 dx)X = X^2 - \frac{1}{3}$$

and

$$||f_3||^2 = \langle f_3, v_3\rangle = \int_{-1}^{1} x^2(x^2 - \frac{1}{3})dx = \frac{8}{45}.$$

Hence

$$e_3 = \frac{f_3}{||f_3||} = \frac{3X^2 - 1}{2}\sqrt{\frac{5}{2}}.$$

Hence the answer is

$$\frac{1}{\sqrt{2}}, \quad \sqrt{\frac{3}{2}}X, \quad \frac{3X^2-1}{2}\sqrt{\frac{5}{2}}. \qquad \square$$

The following problem is a generalization of the previous one. It is much more challenging and represents an introduction to the beautiful theory of orthogonal polynomials.

Problem 10.68 (Legendre's Polynomials). Let $n \geq 1$ and let V be the space of polynomials with real coefficients whose degree does not exceed n, endowed with the inner product

$$\langle P, Q \rangle = \int_{-1}^{1} P(x)Q(x)dx.$$

Let L_n be the nth derivative of $(X^2-1)^n$.

a) Prove that $L_0, \ldots, L_n$ is an orthogonal basis of V.
b) Compute $||L_k||$.
c) What is the orthonormal basis of V obtained by applying the Gram–Schmidt process to the canonical basis $1, X, \ldots, X^n$ of V?

Solution. For $j \in [0, n]$ let $P_j = (X^2-1)^j$ and note that -1 and 1 are roots with multiplicity j of P_j. It follows that for $k \in [0, j]$, -1 and 1 and roots with multiplicity $j-k$ of $P_j^{(k)}$ (kth derivative of P_j). If $P \in V$, we deduce from this observation and integration by parts that for $j \geq 1$

$$\langle L_j, P \rangle = \int_{-1}^{1} P_j^{(j)}(x)P(x)dx = P_j^{(j-1)}(x)P(x)|_{-1}^{1} -$$

$$\int_{-1}^{1} P_j^{(j-1)}(x)P'(x)dx = -\int_{-1}^{1} P_j^{(j-1)}(x)P'(x)dx$$

and repeating this argument gives

$$\langle L_j, P \rangle = (-1)^k \int_{-1}^{1} P_j^{(j-k)}(x)P^{(k)}(x)dx$$

for $k \in [0, j]$ and $P \in V$. Taking $j = k$ yields the fundamental relation

$$\langle L_k, P \rangle = (-1)^k \int_{-1}^{1} (x^2-1)^k P^{(k)}(x)dx = \int_{-1}^{1} (1-x^2)^k P^{(k)}(x)dx \qquad (10.5)$$

for $k \in [0, n]$ and $P \in V$.

It is now rather easy to deal with the problem.

a) For $j < k$ we have by relation (10.5)

$$\langle L_k, L_j \rangle = \int_{-1}^{1} (1-x^2)^k L_j^{(k)}(x) dx.$$

Since $\deg L_j = j$, we have $L_j^{(k)} = 0$ and so $\langle L_k, L_j \rangle = 0$, proving that $L_0, \ldots, L_n$ is an orthogonal family.

b) By definition L_n has degree n and

$$L_n^{(n)}(X) = ((X^2-1)^n)^{(2n)} = (X^{2n})^{(2n)} = 2n(2n-1)\ldots 1 = (2n)!.$$

We deduce from relation (10.5) that

$$\langle L_n, L_n \rangle = (2n)! \int_{-1}^{1} (1-x^2)^n dx = 2(2n)! \int_{0}^{1} (1-x^2)^n dx.$$

Let

$$I_n = \int_0^1 (1-x^2)^n dx$$

and observe that an integration by parts yields

$$I_n = x(1-x^2)^n|_0^1 - \int_0^1 x(1-x^2)^{n-1}(-2x) = 2n \int_0^1 x^2(1-x^2)^{n-1} dx$$

$$= 2n \int_0^1 (1-(1-x^2))(1-x^2)^{n-1} dx = 2n(I_{n-1} - I_n),$$

thus

$$(2n+1)I_n = 2nI_{n-1}.$$

Taking into account that $I_0 = 1$ we obtain

$$I_n = \prod_{i=1}^{n} \frac{I_i}{I_{i-1}} = \prod_{i=1}^{n} \frac{2i}{2i+1} = \frac{2^n n!}{1 \cdot 3 \cdot \ldots \cdot (2n+1)} = \frac{4^n n!^2}{(2n+1)!}.$$

Finally

$$||L_n||^2 = \langle L_n, L_n \rangle = 2(2n)! I_n = \frac{2^{2n+1} n!^2}{2n+1}$$

and

$$||L_n|| = \sqrt{\frac{2}{2n+1}} 2^n n!.$$

c) Let $Q_k = \frac{L_k}{||L_k||}$. Then by part a) the family $Q_0, \ldots, Q_n$ is orthonormal in V and since $\dim V = n+1$, it follows that $Q_0, \ldots, Q_n$ is an orthonormal basis of V. Moreover, we have $\deg Q_k = \deg L_k = k$ for $k \in [0, n]$, which easily implies that

$$\text{Span}(Q_0, \ldots, Q_k) = \text{Span}(X^0, \ldots, X^k)$$

for $k \in [0, n]$. Finally,

$$\langle X^k, Q_k \rangle = \frac{\langle X^k, L_k \rangle}{||L_k||} = \frac{\int_0^1 L_k^{(k)} (1-x^2)^k dx}{||L_k||} > 0,$$

since we have already seen that $L_k^{(k)}$ is a positive real number. We conclude that $Q_0, \ldots, Q_n$ is obtained from $1, X, \ldots, X^n$ by applying the Gram–Schmidt process. □

10.5.1 Problems for Practice

1. Apply the Gram–Schmidt algorithm to the vectors

$$v_1 = (1, 2, -2), \quad v_2 = (0, -1, 2), \quad v_3 = (-1, 3, 1).$$

2. Consider the vector space V of polynomials with real coefficients and degree not exceeding 2, endowed with the inner product defined by

$$\langle P, Q \rangle = \int_0^1 xP(x)Q(x)dx.$$

Apply the Gram–Schmidt algorithm to the vectors $1, X, X^2$.

3. Consider the map $\langle\ ,\ \rangle : \mathbf{R}^3 \times \mathbf{R}^3 \to \mathbf{R}$ defined by

$$\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = (x_1 + x_2 + x_3)(y_1 + y_2 + y_3) +$$

$$(x_2 + x_3)(y_2 + y_3) + x_3 y_3.$$

a) Check that this defines an inner product on $\mathbf{R}^3$.
b) Applying the Gram–Schmidt algorithm to the canonical basis of $\mathbf{R}^3$, give an orthonormal basis for $\mathbf{R}^3$ endowed with this inner product.

4. Find an orthogonal basis of $\mathbf{R}^4$ containing the vector $(1, 2, -1, -2)$.
5. (The QR factorization) Let $A \in M_{m,n}(\mathbf{R})$ be a matrix with linearly independent columns $C_1, \ldots, C_n$. Let W be the span of $C_1, \ldots, C_n$, a subspace of $\mathbf{R}^m$.

   a) Prove that there is a matrix $Q \in M_{m,n}(\mathbf{R})$ whose columns are an orthonormal basis of W, and there is an upper-triangular matrix $R \in M_n(\mathbf{R})$ with positive diagonal entries such that

   $$A = QR.$$

   Hint: the columns of Q are the result of applying the Gram–Schmidt process to the columns of A.

   b) Prove that the factorization $A = QR$ with Q, R matrices as in part a) is unique.

6. Using the Gram–Schmidt process, find the QR factorization of the matrix

   $$A = \begin{bmatrix} 2 & 3 & 5 \\ 0 & 4 & 6 \\ 0 & 0 & 7 \end{bmatrix}.$$

7. Find the QR factorization of the matrix

   $$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 3 \end{bmatrix}.$$

8. Describe the QR factorization of an upper-triangular matrix $A \in M_n(\mathbf{R})$.
9. If $f : \mathbf{R} \to \mathbf{R}$ is a continuous 2π-periodic function, we denote

   $$c_n(f) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) e^{-inx} dx.$$

   a) Prove that if f is continuously differentiable, then for all $n \in \mathbf{Z}$ we have

   $$c_n(f') = in \cdot c_n(f).$$

   b) Deduce that under the assumptions of a) we have

   $$\lim_{n \to \infty} n c_n(f) = 0$$

and

$$\sum_{n\in\mathbf{Z}} n^2|c_n(f)|^2 < \infty.$$

Hint: use the Riemann–Lebesgue theorem and Bessel's inequality, as well as part a).

c) Prove that if $f, g : \mathbf{R} \to \mathbf{R}$ are continuous 2π-periodic maps such that $c_n(f) = c_n(g)$ for all $n \in \mathbf{Z}$, then $f = g$. Hint: use Plancherel's theorem for the function $f - g$.

10. Consider the 2π-periodic function $f : \mathbf{R} \to \mathbf{R}$ such that $f(0) = f(\pi) = 0$, $f(t) = 0$ for $t \in (0, \pi)$ and f is odd, i.e., $f(-x) = -f(x)$ for all x.

a) Explain why such a map exists, plot its graph and show that it is piecewise continuous.
b) Compute its Fourier coefficients $a_m(f)$ and $b_m(f)$ for all $m \geq 0$.
c) Using Plancherel's theorem, deduce Euler's famous identity

$$\sum_{n\geq 0} \frac{1}{(2n+1)^2} = \frac{\pi^2}{8}.$$

d) Deduce from part c) the even more famous Euler's identity

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

11. Consider the 2π-periodic function $f : \mathbf{R} \to \mathbf{R}$ such that $f(t) = t^2$ for $t \in [-\pi, \pi]$.

a) Compute the Fourier coefficients of f.
b) Using Plancherel's theorem, prove the following identity

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}.$$

12. Let E be an Euclidean space, let $e_1, \ldots, e_n$ be an orthonormal basis of E and let T be a linear transformation on E. Prove that

$$\mathrm{Tr}(T) = \sum_{i=1}^{n} \langle T(e_i), e_i \rangle.$$

13. Let V be an Euclidean space and let T be a linear transformation on V such that $\mathrm{Tr}(T) = 0$. Let $e_1, \ldots, e_n$ be an orthonormal basis of V.

a) Prove that one can find $i, j \in \{1, 2, \ldots, n\}$ such that $\langle T(e_i), e_i \rangle$ and $\langle T(e_j), e_j \rangle$ have opposite signs. Hint: use Problem 12.
b) Check that the map $f : [0, 1] \to \mathbf{R}$ defined by

$$f(t) = \langle T(te_i + (1-t)e_j), te_i + (1-t)e_j \rangle$$

is continuous and that $f(0)f(1) \leq 0$.
c) Conclude that there is a nonzero vector $x \in E$ such that

$$\langle T(x), x \rangle = 0.$$

d) Finally, prove by induction on n that there is an orthogonal basis of V in which the diagonal entries of the matrix of T are all equal to 0.

14. Let V be an Euclidean space of dimension n, let $e_1, \ldots, e_n$ be an orthonormal basis of V and let $T : V \to V$ be an orthogonal projection. Show that

$$\text{rank}(T) = \sum_{i=1}^{n} ||T(e_i)||^2.$$

15. Let V be an Euclidean space of dimension n and let $e_1, \ldots, e_n$ be nonzero vectors in V such that for all $x \in V$ we have

$$\sum_{k=1}^{n} \langle e_k, x \rangle^2 = ||x||^2.$$

a) Compute the orthogonal of $\text{Span}(e_1, \ldots, e_n)$ and deduce that $e_1, \ldots, e_n$ is a basis of V.
b) By choosing $x = e_i$, prove that $||e_i|| \leq 1$ for all $1 \leq i \leq n$.
c) By choosing $x \in \text{Span}(e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n)^{\perp}$, prove that $||e_i|| = 1$ for all $1 \leq i \leq n$.
d) Conclude that $e_1, \ldots, e_n$ is an orthonormal basis of V.

16. (Hermite's polynomials) Let n be a positive integer and let V be the space of polynomials with real coefficients whose degree does not exceed n, endowed with

$$\langle P, Q \rangle = \int_0^{\infty} P(t)Q(t)e^{-t}dt.$$

a) Explain why $\langle\ ,\ \rangle$ is well defined and an inner product on V.
b) Define $h_k = (X^k e^{-X})^{(k)} e^X$ for $k \geq 0$. What are the coefficients of h_k?
c) Prove that for all $k \in [0, n]$ and all $P \in V$ we have

$$\langle P, h_k \rangle = (-1)^k \int_0^{\infty} P^{(k)}(t)t^k e^{-t}dt.$$

d) Prove that $h_0, \ldots, h_n$ is an orthogonal basis of V.
e) Prove that $||h_k|| = k!$ for $k \in [0, n]$.

17. (Chebyshev's polynomials) Let n be a positive integer and let V be the space of real polynomials with degree not exceeding n, endowed with

$$\langle P, Q \rangle = \int_{-1}^{1} \frac{P(t)Q(t)}{\sqrt{1-t^2}} dt.$$

a) Explain why $\langle\ ,\ \rangle$ makes sense and defines an inner product on V.
b) Prove that for each $k \geq 0$ there is a unique polynomial T_k (the kth Chebyshev polynomial) such that $T_k(\cos x) = \cos kx$ for all $x \in \mathbf{R}$.
c) Prove that $T_0, \ldots, T_n$ is an orthogonal basis of V.
d) Find $||T_k||$ for $k \in [0, n]$.

18. (Cross-product) Let V be an Euclidean space of dimension $n \geq 3$ and let $(e_1, \ldots, e_n)$ be a fixed orthonormal basis. If $v_1, \ldots, v_n \in V$, write $\det(v_1, \ldots, v_n)$ instead of $\det_{(e_1,\ldots,e_n)}(v_1, \ldots, v_n)$.

a) Let $v_1, \ldots, v_{n-1} \in V$. Prove the existence of a unique vector $v_1 \wedge \ldots \wedge v_{n-1} \in V$ such that for all $v \in V$

$$\det(v_1, \ldots, v_{n-1}, v) = \langle v, v_1 \wedge \ldots \wedge v_{n-1} \rangle \tag{10.6}$$

We call this vector $v_1 \wedge \ldots \wedge v_{n-1}$ the **cross-product** of $v_1, \ldots, v_{n-1}$.
b) Prove that $v_1 \wedge \ldots \wedge v_{n-1}$ is orthogonal to $v_1, \ldots, v_{n-1}$.
c) Prove that $v_1, \ldots, v_{n-1}$ are linearly dependent if and only if

$$v_1 \wedge \ldots \wedge v_{n-1} = 0.$$

d) Let $v_j = \sum_{i=1}^{n} a_{ij} e_i$. By choosing $v = e_i$ in (10.6) prove that

$$v_1 \wedge \ldots \wedge v_{n-1} = \sum_{i=1}^{n} (-1)^{n-i} \Delta_i \cdot e_i,$$

where Δ_i is the determinant of the $(n-1) \times (n-1)$ matrix obtained from $[a_{ij}]$ (i.e., the matrix whose columns are $v_1, \ldots, v_{n-1}$) by deleting the ith row. In particular, if $n = 3$ check that

$$\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \wedge \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{bmatrix}.$$

e) Prove that if $f_1, \ldots, f_n$ is an orthonormal basis of V, then $\det(f_1, \ldots, f_n) \in \{-1, 1\}$. We say that $f_1, \ldots, f_n$ is **positive** or **positively oriented** (with respect to $(e_1, \ldots, e_n)$) if $\det(f_1, \ldots, f_n) = 1$.

f) Prove that if $v_1, \ldots, v_{n-1}$ is an orthonormal family, then $v_1, \ldots, v_{n-1}, v_1 \wedge \ldots \wedge v_{n-1}$ is a positive orthonormal basis.

19. Let $v_1, \ldots, v_{n-1}$ be linearly independent vectors in a Euclidean space V of dimension $n \geq 3$. Let H be the hyperplane spanned by $v_1, \ldots, v_{n-1}$.

a) Prove that for all $v \in V$ we have

$$p_H(v) = v - \frac{\langle v_1 \wedge \ldots \wedge v_{n-1}, v\rangle}{||v_1 \wedge \ldots \wedge v_{n-1}||^2}(v_1 \wedge \ldots \wedge v_{n-1})$$

and

$$d(v, H) = \frac{|\langle v, v_1 \wedge \ldots \wedge v_{n-1}\rangle|}{||v_1 \wedge \ldots \wedge v_{n-1}||}.$$

b) Prove that

$$H = \{v \in V \,|\, \langle v, v_1 \wedge \ldots \wedge v_{n-1}\rangle = 0\}.$$

20. In this problem V is an Euclidean space of dimension 3.

a) (Lagrange's formula) Prove that for all $x, y \in V$ we have

$$\langle x, y\rangle^2 + ||x \wedge y||^2 = ||x||^2 \cdot ||y||^2.$$

b) Prove that if θ is the angle between x and y, then

$$||x \wedge y|| = ||x|| \cdot ||y|| \cdot |\sin\theta|.$$

21. This exercise develops the theory of orthogonal bases over the complex numbers. Let V be a finite dimensional vector space over $\mathbf{C}$, endowed with a hermitian inner product $\langle\ ,\ \rangle$, i.e., a hermitian sesquilinear form $\langle\ ,\ \rangle : V \times V \to \mathbf{C}$ such that $\langle x, x\rangle > 0$ for all nonzero vectors $x \in V$. Such a space is called a **hermitian space**. Two vectors $x, y \in V$ are orthogonal if $\langle x, y\rangle = 0$. Starting with this definition, one defines the notion of orthogonal/orthonormal family and orthogonal/orthonormal basis as in the case of vector spaces over $\mathbf{R}$.

a) Prove that an orthogonal family consisting of nonzero vectors is linearly independent, and deduce that if $\dim V = n$, then an orthonormal family consisting of n vectors is an orthonormal basis of V.

b) Let $e_1, \ldots, e_n$ be an orthonormal basis of V and let $x = x_1e_1 + \ldots + x_ne_n$ and $y = y_1e_1 + \ldots + y_ne_n$ be two vectors in V. Prove that

$$\langle x, y\rangle = \overline{x_1}y_1 + \ldots + \overline{x_n}y_n$$

and

$$||x||^2 = |x_1|^2 + \ldots + |x_n|^2.$$

c) State and prove a version of the Gram–Schmidt process in this context.
d) Prove that there is an orthonormal basis of V.
e) Prove that any orthonormal family in V can be completed to an orthonormal basis of V.
f) Let W be a subspace of V and let $w_1, \ldots, w_k$ be an orthonormal basis of W.

i) Prove that $W \oplus W^\perp = V$ and $(W^\perp)^\perp = W$.
ii) The orthogonal projection p_W of V onto W is the projection of V onto W along $W^\perp$. Prove that for all $v \in V$

$$p_W(v) = \sum_{i=1}^{k} \langle w_i, v\rangle w_i$$

and

$$||v - p_W(v)|| = \min_{w\in W} ||v - w||.$$

10.6 The Adjoint of a Linear Transformation

Let $(V, \langle\ ,\ \rangle)$ be an Euclidean space (the condition that V is finite dimensional will be crucial in this section, so we insist on it). Let $T : V \to V$ be a linear transformation. For all $y \in V$, the map $x \mapsto \langle T(x), y\rangle$ is a linear form on V. It follows from Theorem 10.37 that there is a unique vector $T^*(y) \in V$ such that

$$\langle T(x), y\rangle = \langle T^*(y), x\rangle = \langle x, T^*(y)\rangle$$

for all $x \in V$. We obtain in this way a map $T^* : V \to V$, uniquely characterized by the condition

$$\langle T(x), y\rangle = \langle x, T^*(y)\rangle$$

for all $x, y \in V$. It is easy to see that T^* is itself linear and we call T^* **the adjoint of** T. All in all, we obtain the following

Theorem 10.69. *Let $(V, \langle\ ,\ \rangle)$ be an Euclidean space. For each linear transformation $T : V \to V$ there is a unique linear transformation $T^* : V \to V$, called the adjoint of T, such that for all $x, y \in V$*

$$\langle T(x), y\rangle = \langle x, T^*(y)\rangle.$$

As the following problem shows, the previous result fails rather badly if we don't assume that V is finite dimensional:

Problem 10.70. Let V be the space of continuous real-valued maps on $[0, 1]$, endowed with the inner product

$$\langle f, g\rangle = \int_0^1 f(t)g(t)dt.$$

Prove that the linear transformation T sending f to the constant map equal to $f(0)$ has no adjoint.

Solution. Suppose that T has some adjoint T^*. Let $W = \ker T$, that is the subspace of maps f with $f(0) = 0$. Fix $g \in V$. Since

$$\langle T(f), g\rangle = \langle f, T^*(g)\rangle$$

for all $f, g \in V$, we deduce that $\langle T^*(g), f\rangle = 0$ for all $f \in W$. Applying this to the function f given by $x \mapsto xT^*(g)(x)$ which is in W, we conclude that

$$\langle T^*(g), f\rangle = \int_0^1 x(T^*(g)(x))^2 dx = 0.$$

Since $x \mapsto x(T^*(g)(x))^2$ is continuous, nonnegative, and with average equal to 0, it is the zero map, thus $T^*(g)$ vanishes on $(0, 1]$ and then on $[0, 1]$ by continuity. We conclude that $T^*(g) = 0$ for all $g \in V$, thus $\langle T(f), g\rangle = 0$ for all $f, g \in V$ and finally $T(f) = 0$ for all $f \in V$. Since this is clearly absurd, the problem is solved. □

Note that for all $x, y \in V$ we have

$$\langle y, T(x)\rangle = \langle T(x), y\rangle = \langle x, T^*(y)\rangle = \langle T^*(y), x\rangle = \langle y, (T^*)^*(x)\rangle$$

It follows that $T(x) - (T^*)^*(x) = 0$ and so

$$(T^*)^* = T,$$

which we write as

$$T^{**} = T.$$

Thus the map $T \to T^*$ is an involution of the space of linear transformations on V. The fixed points of this involution are called **symmetric or self-adjoint linear transformations**. They will play a fundamental role in this chapter. More precisely, we introduce the following definitions:

Definition 10.71. Let $(V, \langle\ ,\ \rangle)$ be an Euclidean space. A linear transformation $T : V \to V$ is called **symmetric or self-adjoint** if $T^* = T$ and **alternating or skew-symmetric** if $T^* = -T$.

In the next problems the reader will have the opportunity to find quite a few different characterizations and/or properties of self-adjoint and alternating linear transformations.

Problem 10.72. Let $(V, \langle\ ,\ \rangle)$ be an Euclidean space and let $T : V \to V$ be a linear transformation. Let $e_1, \ldots, e_n$ be an **orthonormal basis** and let A be the matrix of T with respect to $e_1, \ldots, e_n$. Prove that the matrix of T^* with respect to $e_1, \ldots, e_n$ is ${}^tA$. Thus T **is symmetric if and only if** A **is symmetric, and** T **is alternating if and only if** A **is skew-symmetric (be careful to the hypothesis that** $e_1, \ldots, e_n$ **is an orthonormal basis, nor just any basis!).**

Solution. Let $B = [b_{ij}]$ be the matrix of T^* with respect to $e_1, \ldots, e_n$, thus for all $i \in [1, n]$ we have

$$T^*(e_i) = \sum_{k=1}^{n} b_{ki} e_k.$$

Since

$$\langle T(e_i), e_j \rangle = \langle e_i, T^*(e_j) \rangle$$

and $T(e_i) = \sum_{k=1}^{n} a_{ki} e_k$, and since the basis is orthonormal we obtain

$$\langle T(e_i), e_j \rangle = \sum_{k=1}^{n} a_{ki} \langle e_k, e_j \rangle = a_{ji}$$

and

$$\langle e_i, T^*(e_j) \rangle = \sum_{k=1}^{n} b_{kj} \langle e_i, e_k \rangle = b_{ij}.$$

We conclude that $b_{ij} = a_{ji}$ for all $i, j \in [1, n]$, and the result follows. □

Problem 10.73. Prove that any two distinct eigenspaces of a symmetric linear transformation are orthogonal.

Solution. Let λ_1, λ_2 be different eigenvalues of T and let x, y be nonzero vectors in V such that $T(x) = \lambda_1 x$ and $T(y) = \lambda_2 y$. Since T is symmetric we have

$$\langle T(x), y\rangle = \langle x, T(y)\rangle.$$

The left-hand side equals $\lambda_1\langle x, y\rangle$, while the right-hand side equals $\lambda_2\langle x, y\rangle$. Since $\lambda_1 \neq \lambda_2$, it follows that $\langle x, y\rangle = 0$ and the result follows. □

Problem 10.74. Let n be a positive integer and let V be the space of polynomials with real coefficients whose degree does not exceed n, endowed with the inner product defined by

$$\langle P, Q\rangle = \int_{-1}^{1} P(x)Q(x)dx.$$

Prove that the linear transformation $T{:}V \to V$ sending P to $2XP'(X)+(X^2-1)$ $P''(X)$ is symmetric.

Solution. Since the maps $P \mapsto P'$ and $P \mapsto P''$ are linear, it follows that T is a linear transformation (note that $T(P)$ belongs to V since $\deg XP' \leq \deg P \leq n$ and $\deg(X^2-1)P'' \leq \deg P \leq n$). In order to prove that T is symmetric, we need to prove that

$$\langle T(P), Q\rangle = \langle P, T(Q)\rangle$$

for all polynomials $P, Q \in V$. Note that using the product rule for derivatives, we can write

$$T(P) = ((X^2-1)P')'.$$

Hence integration by parts gives

$$\langle T(P), Q\rangle = \int_{-1}^{1} ((x^2-1)P'(x))'Q(x)\,dx = \int_{-1}^{1} (1-x^2)P'(x)Q'(x)\,dx.$$

Note that this last expression is symmetric in P and Q, so it also equals $\langle T(Q), P\rangle = \langle P, T(Q)\rangle$. Thus T is symmetric. □

Problem 10.75. Let V be an Euclidean space and let $T : V \to V$ be a linear transformation.

a) Prove that T is alternating if and only if $\langle T(x), x\rangle = 0$ for all $x \in V$.
b) Prove that if this is the case, then the only possible real root of the characteristic polynomial of T is 0.

Solution. a) Suppose that T is alternating, thus $T + T^* = 0$. Then for all $x \in V$ we have

$$\langle T(x), x\rangle = \langle x, T^*(x)\rangle = \langle x, -T(x)\rangle = -\langle T(x), x\rangle,$$

thus $\langle T(x), x\rangle = 0$.

Conversely, suppose that $\langle T(x), x\rangle = 0$ for all $x \in V$. Thus for all $x, y \in V$ we have

$$0 = \langle T(x+y), x+y\rangle = \langle T(x) + T(y), x+y\rangle =$$

$$\langle T(x), x\rangle + \langle T(x), y\rangle + \langle x, T(y)\rangle + \langle T(y), y\rangle =$$

$$\langle T(x), y\rangle + \langle T^*(x), y\rangle = \langle (T + T^*)(x), y\rangle.$$

Thus $(T + T^*)(x)$ is orthogonal to V and thus it equals 0, and this holds for all $x \in V$. It follows that T is alternating.

b) Suppose that λ is a real root of the characteristic polynomial of T. Thus there is a nonzero vector $x \in V$ such that $T(x) = \lambda x$. Then

$$\lambda ||x||^2 = \langle \lambda x, x\rangle = \langle T(x), x\rangle = 0,$$

and so $\lambda = 0$. □

Problem 10.76. Let V be an Euclidean space and let $e_1, \ldots, e_n$ be a basis of V. Prove that the map $T : V \to V$ defined by

$$T(x) = \sum_{k=1}^{n} \langle e_k, x\rangle e_k$$

is a symmetric linear transformation on V. Is T positive? Is it positive definite?

Solution. Note that $x \mapsto \langle e_k, x\rangle$ is a linear map for all $1 \leq k \leq n$ (by definition of an inner product). It follows that T itself is a linear transformation of V. In order to check that T is symmetric, we need to prove that

$$\langle T(x), y\rangle = \langle x, T(y)\rangle$$

for all $x, y \in V$. Using the bilinearity of $\langle\ ,\ \rangle$, we obtain

$$\langle T(x), y\rangle = \langle \sum_{k=1}^{n} \langle e_k, x\rangle e_k, y\rangle = \sum_{k=1}^{n} \langle e_k, x\rangle \cdot \langle e_k, y\rangle.$$

A similar computation yields

$$\langle x, T(y)\rangle = \langle x, \sum_{k=1}^{n} \langle e_k, y\rangle e_k\rangle = \sum_{k=1}^{n} \langle e_k, x\rangle \cdot \langle e_k, y\rangle,$$

establishing therefore the desired equality and proving that T is symmetric.

Notice that the previous computations also give

$$\langle T(x), x\rangle = \sum_{k=1}^{n} \langle e_k, x\rangle^2.$$

The last sum is nonnegative since it is a sum of squares of real numbers. It follows that T is positive. Moreover, if $\langle T(x), x\rangle = 0$, then the previous argument yields $\langle e_k, x\rangle = 0$ for all $1 \leq k \leq n$. Thus x is orthogonal to $\text{Span}(e_1, \ldots, e_n) = V$ and so $x = 0$. It follows that T is positive definite. □

Problem 10.77. Let T be a linear transformation on an Euclidean space V. Prove that the following statements are equivalent:

a) For all $x \in V$ we have $||T(x)|| = ||T^*(x)||$.
b) For all $x, y \in V$ we have $\langle T(x), T(y)\rangle = \langle T^*(x), T^*(y)\rangle$.
c) T^* and T commute.

Such a linear transformation T is called **normal**. Note that symmetric as well as alternating linear transformations are normal.

Solution. Suppose that a) holds. Using the polarization identity twice and the linearity of T and T^*, we obtain

$$\langle T(x), T(y)\rangle = \frac{||T(x+y)||^2 - ||T(x)||^2 - ||T(y)||^2}{2} =$$

$$\frac{||T^*(x+y)||^2 - ||T^*(x)||^2 - ||T^*(y)||^2}{2} = \langle T^*(x), T^*(y)\rangle.$$

Thus b) holds.

Suppose now that b) holds. For all $x, y \in V$ we have

$$\langle (T \circ T^* - T^* \circ T)(x), y\rangle = \langle T(T^*(x)), y\rangle - \langle T^*(T(x)), y\rangle$$

$$= \langle T^*(x), T^*(y)\rangle - \langle y, T^*(T(x))\rangle = \langle T(x), T(y)\rangle - \langle T(y), T(x)\rangle = 0.$$

Thus $(T \circ T^* - T^* \circ T)(x) = 0$ for all $x \in V$, that is T and T^* commute and so c) holds.

Finally, suppose that c) holds. Then

$$||T(x)||^2 = \langle T(x), T(x)\rangle = \langle x, T^*(T(x))\rangle =$$

$$\langle x, T(T^*(x))\rangle = \langle T(T^*(x)), x\rangle = \langle T^*(x), T^*(x)\rangle = ||T^*(x)||^2,$$

thus $||T(x)|| = ||T^*(x)||$ for all $x \in V$ and so a) holds. The problem is solved. □

Problem 10.78. Let T be a normal linear transformation on an Euclidean space V. Prove that if V_1 is a subspace of V which is stable under T, then $V_1^{\perp}$ is also stable under T.

Solution. The result is clear if $V_1 = 0$ or $V_1 = V$, so assume that this is not the case. Choose an orthonormal basis $e_1, \ldots, e_n$ of V obtained by patching an orthonormal basis of V_1 and an orthonormal basis of $V_1^{\perp}$. Since V_1 is stable under T, the matrix of T with respect to $e_1, \ldots, e_n$ is of the form $M = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$ for some matrices A, B, C. Since T and T^* commute, we have

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \cdot \begin{bmatrix} {}^tA & 0 \\ {}^tB & {}^tC \end{bmatrix} = \begin{bmatrix} {}^tA & 0 \\ {}^tB & {}^tC \end{bmatrix} \cdot \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

In particular, we must have $C\,{}^tC = {}^tBB + {}^tCC$. Thus

$$\operatorname{Tr}({}^tBB) = \operatorname{Tr}(C\,{}^tC) - \operatorname{Tr}({}^tCC) = 0,$$

which can be written as $\sum_{i,j} b_{ij}^2 = 0$, where $B = [b_{ij}]$. We deduce that $b_{ij} = 0$ for all i, j, that is $B = 0$. But then it is clear that $V_1^{\perp}$ is stable under T. □

10.6.1 Problems for Practice

1. Let V be an Euclidean space and let T be a linear transformation on V. Prove that $\ker T^* \circ T = \ker T$. Hint: if $x \in \ker T^* \circ T$, compute $||T(x)||^2$.
2. Let T be a symmetric linear transformation of an Euclidean space V. Prove that $V = \operatorname{Im}(T) \oplus \ker T$ and that $\operatorname{Im}(T)$ and $\ker T$ are orthogonal.
3. Prove that if T is a normal endomorphism of an Euclidean space V, then
$$\ker T = \ker T^*.$$
4. Prove that if T is a linear transformation on an Euclidean space V, then
$$\det T = \det T^*.$$
5. Prove that if T is a linear transformation on an Euclidean space V, then
$$\ker(T^*) = \operatorname{Im}(T)^{\perp}, \quad \operatorname{Im}(T^*) = (\ker T)^{\perp}.$$
6. Let V be an Euclidean space and let $v \in V$ be a vector with $||v|| = 1$. Prove that if k is a real number, then the map
$$T : V \to V, \quad T(x) = x + k\langle x, v\rangle v$$
is a symmetric linear transformation on V.

7. Let V be the space of polynomials with real coefficients whose degree does not exceed n and consider the map $\langle\ ,\ \rangle : V \times V \to \mathbf{R}$ defined by

$$\langle P, Q\rangle = \int_{-1}^{1} \sqrt{\frac{1-x}{1+x}} P(x)Q(x)dx.$$

   a) Explain why $\langle\ ,\ \rangle$ is well defined and an inner product on V.
   b) Prove that the map $T : V \to V$ defined by

$$T(P(X)) = (X^2 - 1)P''(X) + (2X + 1)P'(X)$$

   is a self-adjoint linear transformation on V.

8. Prove that if a, b are real numbers, then the linear transformation

$$T : \mathbf{R}^2 \to \mathbf{R}^2, \quad T(x, y) = (ax + by, -bx + ay)$$

   is normal.
9. Let V be an Euclidean space of dimension 2 and let $T : V \to V$ be a normal linear transformation. Let A be the matrix of T with respect to an orthonormal basis of V. Prove that either T is symmetric or

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

   for some real numbers a, b.
10. Let $P \in \mathrm{GL}_n(\mathbf{R})$ be an invertible matrix and let $E = M_n(\mathbf{R})$ endowed with the inner product given by

$$\langle A, B\rangle = \mathrm{Tr}(A^t B).$$

    Find the adjoint of the linear transformation $T : E \to E$ sending A to PAP^{-1}.
11. Let V be an Euclidean space and let T be a linear transformation on V such that $||T(x)|| \leq ||x||$ for all $x \in V$.

    a) Prove that $||T^*(x)|| \leq ||x||$ for all $x \in V$.
    b) Prove that $\ker(T - \mathrm{id}) = \ker(T^* - \mathrm{id})$.
    c) Deduce that V is the orthogonal direct sum of $\ker(T - \mathrm{id})$ and $\mathrm{Im}(T - \mathrm{id})$.

12. Let V be a hermitian space, that is a finite dimensional vector space over $\mathbf{C}$ endowed with a hermitian inner product $\langle\ ,\ \rangle : V \times V \to \mathbf{C}$.

    a) Prove that for any linear transformation $T : V \to V$ there is a unique linear transformation $T^* : V \to V$ (called the **adjoint of** T) such that for all $x, y \in V$

$$\langle x, T(y)\rangle = \langle T^*(x), y\rangle.$$

Be careful that the left-hand side is no longer equal to $\langle T(y), x\rangle$, but rather $\overline{\langle T(y), x\rangle}$.

b) Prove that the map $T \mapsto T^*$ is a linear involution on the space of linear transformations on V, such that for all S, T

$$(S \circ T)^* = T^* \circ S^*.$$

c) Prove that T is invertible if and only if T^* is invertible, and then

$$(T^*)^{-1} = (T^{-1})^*.$$

d) If $e_1, \ldots, e_n$ is an orthonormal basis of V and if A is the matrix of T with respect to this basis, prove that the matrix of T^* is $A^* := {}^t\overline{A}$. We say that T **is self-adjoint or hermitian if** $T = T^*$**.**

e) Prove that any orthogonal projection is a hermitian linear transformation.

f) Prove that $\ker T^* = (\mathrm{Im}(T))^\perp$ and $\mathrm{Im}(T^*) = (\ker T)^\perp$.

g) Prove that if T is hermitian, then the orthogonal of a subspace stable under T is also stable under T.

10.7 The Orthogonal Group

Let V_1, V_2 be Euclidean spaces with inner products $\langle\ ,\ \rangle_1$ and $\langle\ ,\ \rangle_2$, and with corresponding norms $||\cdot||_1$ and $||\cdot||_2$.

Definition 10.79. An **isometry** (or **isomorphism of Euclidean spaces**) between V_1 and V_2 is an isomorphism of $\mathbf{R}$-vector spaces $T : V_1 \to V_2$ such that for all $x, y \in V_1$

$$\langle T(x), T(y)\rangle_2 = \langle x, y\rangle_1.$$

Thus **an isometry is a bijective linear map which is compatible with the inner products on** V_1 **and** V_2. The following exercise gives an equivalent formulation of this compatibility:

Problem 10.80. Let V_1 and V_2 be as above and let $T : V_1 \to V_2$ be a linear transformation. Prove that the following statements are equivalent:

a) For all $x, y \in V_1$ we have

$$\langle T(x), T(y)\rangle_2 = \langle x, y\rangle_1.$$

b) For all $x \in V_1$ we have $||T(x)||_2 = ||x||_1$.

Solution. If a) holds, then taking $y = x$ we obtain

$$||T(x)||_2^2 = ||x||_1^2$$

and so $||T(x)||_2 = ||x||_1$, showing that b) holds.

If b) holds, then the polarization identity and the linearity of T yield

$$\langle T(x), T(y)\rangle_2 = \frac{||T(x)+T(y)||_2^2 - ||T(x)||_2^2 - ||T(y)||_2^2}{2} =$$

$$\frac{||T(x+y)||_2^2 - ||T(x)||_2^2 - ||T(y)||_2^2}{2} = \frac{||x+y||_1^2 - ||x||_1^2 - ||y||_1^2}{2} = \langle x, y\rangle_1,$$

finishing the solution. □

Remark 10.81. If T is a linear transformation as in the previous problem, then T is automatically injective: if $T(x) = 0$, then $||T(x)||_2 = 0$, thus $||x||_1 = 0$ and then $x = 0$.

Definition 10.82. a) Let V be an Euclidean space. A linear transformation $T : V \to V$ is called **orthogonal** if T is an isometry between V and V. In other words, T is orthogonal if T is bijective and for all $x, y \in V$

$$\langle T(x), T(y)\rangle = \langle x, y\rangle.$$

Note that the bijectivity of T is a consequence of the last relation, thanks to the previous remark. Thus T is orthogonal if and only if T preserves the inner product.

b) A matrix $A \in M_n(\mathbf{R})$ is called orthogonal if

$$A\,{}^tA = I_n.$$

The equivalence between the first and last point in the following problem implies the following compatibility of the previous definitions: let $A \in M_n(\mathbf{R})$ and endow $\mathbf{R}^n$ with its canonical inner product. Then A is orthogonal if and only if the linear transformation $X \mapsto AX$ on $\mathbf{R}^n$ is orthogonal. Also, by the previous problem a linear map T on V is orthogonal if and only if $||T(x)|| = ||x||$ for all $x \in V$. Hence A is orthogonal if and only if

$$||AX|| = ||X||$$

for all $X \in \mathbf{R}^n$, where $||\cdot||$ is the norm associated with the canonical inner product on $\mathbf{R}^n$, that is

$$||(x_1, \ldots, x_n)|| = \sqrt{x_1^2 + \ldots + x_n^2}.$$

Example 10.83. A very important class of orthogonal transformations/matrices is given by **orthogonal symmetries**. Namely, consider an Euclidean space V and a subspace W. Then $V = W \oplus W^{\perp}$, so we can define the symmetry s_W with respect to W along $W^{\perp}$. Recall that if $v \in V$ is written as $v = w + w^{\perp}$ with $w \in W$ and $w^{\perp} \in W^{\perp}$, then

$$s_W(v) = w - w^{\perp},$$

so that s_W fixes pointwise W_1, and $-s_W$ fixes pointwise $W^{\perp}$.

In order to see that s_W is an orthogonal transformation, it suffices to check that $||s_W(v)|| = ||v||$ for all $v \in V$, or equivalently

$$||w - w^{\perp}|| = ||w + w^{\perp}||$$

for all $(w, w^{\perp}) \in W \times W^{\perp}$. But by the Pythagorean theorem the squares of both sides are equal to $||w||^2 + ||w^{\perp}||^2$, whence the result.

Orthogonal symmetries can be easily recognized among orthogonal maps: they are precisely the self-adjoint orthogonal transformations, that is their matrices in an orthonormal basis of the space are simultaneously symmetric and orthogonal. The point is that an orthogonal matrix A is symmetric if and only if $A^2 = I_n$, since $A \cdot {}^tA = I_n$.

Let us come back to the general context of an orthogonal matrix $A \in M_n(\mathbf{R})$ and analyze a little bit the relation

$$A\,{}^tA = I_n.$$

Using the product rule and denoting $R_1, \ldots, R_n$ the rows of A, we see that the previous equality is equivalent to

$$\langle R_i, R_j \rangle = 0 \quad \text{if} \quad i \neq j, \quad ||R_i||^2 = 1, \quad 1 \leq i \leq n,$$

in other words A is orthogonal if and only if its rows $R_1, \ldots, R_n$ form an orthonormal basis of $\mathbf{R}^n$. Also, notice that A is orthogonal if and only if ${}^tA$ is orthogonal, thus we have just proved the following:

Theorem 10.84. *Let $A \in M_n(\mathbf{R})$ be a matrix and endow $\mathbf{R}^n$ with the canonical inner product, with associated norm $||\cdot||$. The following statements are equivalent:*

a) A is orthogonal.
b) The rows of A form an orthonormal basis of $\mathbf{R}^n$.
c) The columns of A form an orthonormal basis of $\mathbf{R}^n$.
d) For all $X \in \mathbf{R}^n$ we have

$$||AX|| = ||X||.$$

Problem 10.85. Let V be an Euclidean space and let $T : V \to V$ be a linear transformation. Prove that the following assertions are equivalent:

a) T is orthogonal.
b) We have $\langle T(x), T(y)\rangle = \langle x, y\rangle$ for all $x, y \in V$.
c) For all $x \in V$ we have $||T(x)|| = ||x||$.
d) $T^* \circ T = \mathrm{Id}$.

Solution. By definition a) implies b), which is equivalent to c) by Problem 10.80. If b) holds, then

$$\langle T^* \circ T(x) - x, y\rangle = \langle y, T^*(T(x))\rangle - \langle x, y\rangle = \langle T(x), T(y)\rangle - \langle x, y\rangle = 0$$

for all $x, y \in V$, thus $T^*(T(x)) = x$ for all $x \in V$ and d) follows. It remains to see that d) implies a). It already implies that T is bijective, with inverse T^*, so it suffices to see that b) holds. Since b) is equivalent to c) by Problem 10.80, it suffices to check that c) holds. Or

$$||T(x)||^2 = \langle T(x), T(x)\rangle = \langle x, T^*(T(x))\rangle = \langle x, x\rangle = ||x||^2$$

for all $x \in V$, which yields c). □

We can also characterize orthogonal linear transformations in terms of their effect on orthonormal bases, as the following problem shows:

Problem 10.86. Let V be an Euclidean space and let $T : V \to V$ be a linear transformation. Then the following statements are equivalent:

a) T is orthogonal.
b) For any orthonormal basis $e_1, \ldots, e_n$ of V, the vectors $T(e_1), \ldots, T(e_n)$ form an orthonormal basis of V.
c) There is an orthonormal basis $e_1, \ldots, e_n$ of V such that $T(e_1), \ldots, T(e_n)$ is an orthonormal basis of V.

Solution. Suppose that a) holds and let $e_1, \ldots, e_n$ be an orthonormal basis of V. Then for all $i, j \in [1, n]$ we have

$$\langle T(e_i), T(e_j)\rangle = \langle e_i, e_j\rangle = 1_{i=j}.$$

It follows that $T(e_1), \ldots, T(e_n)$ is an orthonormal family, and since it has $n = \dim V$ elements, we deduce that it is an orthonormal basis of V. Thus a) implies b), which clearly implies c).

Suppose that c) holds. Let $x \in V$ and write $x = x_1 e_1 + \ldots + x_n e_n$. Since $T(e_1), \ldots, T(e_n)$ and $e_1, \ldots, e_n$ are orthonormal bases of V, we have

$$||T(x)||^2 = ||x_1 T(e_1) + \ldots + x_n T(e_n)||^2 = x_1^2 + \ldots + x_n^2 = ||x||^2.$$

Thus $||T(x)|| = ||x||$ for all $x \in V$, and T is orthogonal (by the previous problem). □

Remark 10.87. The previous problem has the following very useful consequence: let $e_1, \ldots, e_n$ be an orthonormal basis of V and let $e'_1, \ldots, e'_n$ be another basis of V. Let P be the change of basis matrix from $e_1, \ldots, e_n$ to $e'_1, \ldots, e'_n$. Then $e'_1, \ldots, e'_n$ is orthonormal if and only if P is orthogonal. We leave the details of the proof to the reader.

Theorem 10.88. *The set of orthogonal linear transformations on an Euclidean space V forms a group under composition. In more concrete terms, the composition of two orthogonal transformations is an orthogonal transformation, and the inverse of an orthogonal transformation is an orthogonal transformation.*

Proof. If T_1, T_2 are orthogonal linear transformations, then $T_1 \circ T_2$ is a linear transformation and

$$||T_1 \circ T_2(x)|| = ||T_1(T_2(x))|| = ||T_2(x)|| = ||x||$$

for all $x \in V$ thus $T_1 \circ T_2$ is an orthogonal linear transformation on V by Problem 10.85. Similarly, we prove that the inverse of an orthogonal transformation is an orthogonal transformation. The result follows. □

The group $O(V)$ of orthogonal transformations (or isometries) of V is called the **orthogonal group of** V. It is the group of automorphisms of the Euclidean space V and plays a crucial role in understanding the space V.

Problem 10.89. Let V be an Euclidean space and let T be an orthogonal linear transformation on V. Let W be a subspace of V which is stable under T.

a) Prove that $T(W) = W$ and $T(W^\perp) = W^\perp$.
b) Prove that the restriction of T to W (respectively $W^\perp$) is an orthogonal linear transformation on W (respectively $W^\perp$).

Solution. a) This follows easily from Problems 10.85 and 10.78, but for the reader's convenience we give a direct argument. Since T maps W into W by assumption and since $T|_W$ is injective (because T is injective on V), it follows that $T|_W : W \to W$ is surjective, thus $T(W) = W$. The same argument reduces the proof of the equality $T(W^\perp) = W^\perp$ to that of the inclusion $T(W^\perp) \subset W^\perp$. Let $x \in W^\perp$ and $y \in W$. We want to prove that $\langle T(x), y\rangle = 0$. But T is orthogonal, so $T^* = T^{-1}$ (Problem 10.85) and so

$$\langle T(x), y\rangle = \langle x, T^{-1}(y)\rangle.$$

Since W is stable under T^{-1}, we obtain $T^{-1}(y) \in W$, and since $x \in W^\perp$, we must have $\langle x, T^{-1}(y)\rangle = 0$. Thus $\langle T(x), y\rangle = 0$ and we are done.

b) Let T_1 be the restriction of T to W. Using Problem 10.85 we obtain for all $x \in W$

$$||T_1(x)|| = ||T(x)|| = ||x||,$$

thus using Problem 10.85 again we obtain that T_1 is an orthogonal linear map on W. The argument for $W^\perp$ being identical, the problem is solved. □

We will now classify the orthogonal transformations of an Euclidean space in terms of simple transformations. The proof requires two preliminary results, which are themselves of independent interest.

Lemma 10.90. *Let V be an Euclidean space and let T be a linear transformation on V. Then there is a line or a plane in V which is stable under T.*

Proof. The minimal polynomial of T is a polynomial P with real coefficients. If it has a real root, it follows that T has an eigenvalue and so the line spanned by an eigenvector for that eigenvalue is stable under T. Suppose that P has no real root. Let z be a complex root of P. Then since P has real coefficients, $\overline{z}$ is also a root of P and so $Q = (X - z)(X - \overline{z})$ divides P. Moreover, $Q(T)$ is not invertible, otherwise $\frac{P}{Q}$ would be a polynomial of smaller degree killing T. Thus there is a nonzero vector $x \in V$ such that $Q(T)(x) = 0$. This can be written as $T^2(x) + aT(x) + bx = 0$ for some real numbers a, b. It follows that the space generated by x and $T(x)$ is a plane which is stable under T, and the lemma is proved. □

Lemma 10.91. *Let V be a two-dimensional Euclidean space and let T be an orthogonal transformation on V with no real eigenvalue. Then there is an orthonormal basis of V with respect to which the matrix of T is of the form*

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Proof. Let e_1, e_2 be an arbitrary orthonormal basis of V and write $T(e_1) = ae_1 + be_2$ for some real numbers a, b. Since

$$a^2 + b^2 = ||T(e_1)||^2 = ||e_1||^2 = 1,$$

we can find a real number θ such that $a = \cos\theta$ and $b = \sin\theta$. The orthogonal of $T(e_1)$ is given by the line $\mathbf{R}(-\sin\theta e_1 + \cos\theta e_2)$. Since $\langle T(e_1), T(e_2)\rangle = \langle e_1, e_2\rangle = 0$, we deduce that $T(e_2) \in \mathbf{R}(-\sin\theta e_1 + \cos\theta e_2)$ and so

$$T(e_2) = c(-\sin\theta e_1 + \cos\theta e_2)$$

for some real number c. Since

$$||T(e_2)|| = ||e_2|| = 1,$$

we deduce that $|c| = 1$ and so $c \in \{-1, 1\}$. It remains to exclude the case $c = -1$. But if $c = -1$, then the matrix of T with respect to e_1, e_2 is

$$A = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

and one can easily check that its characteristic polynomial is $X^2 - 1$, which has real roots. It follows that if $c = -1$, then T has a real eigenvalue, contradiction. The result follows. □

We are now ready for the proof of the fundamental theorem classifying orthogonal linear transformations on an Euclidean space:

Theorem 10.92. *Let V be an Euclidean space and let T be an orthogonal transformation on V. Then we can find an orthonormal basis of V with respect to which the matrix of T is of the form*

$$A = \begin{bmatrix} I_p & 0 & \dots & 0 & 0 \\ 0 & -I_q & \dots & 0 & 0 \\ 0 & 0 & R_{\theta_1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \\ 0 & 0 & \dots & 0 & R_{\theta_k} \end{bmatrix}$$

where $\theta_1, \dots, \theta_k$ are real numbers and

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Proof. We will prove the result by induction on $\dim V$. If $\dim V = 1$, then everything is clear, since we must have $T = \pm\mathrm{id}$. Assume now that $\dim V = n \geq 2$ and that the result is known in dimension at most $n - 1$.

Suppose that T has a real eigenvalue λ and let e_1 be an eigenvector. Then

$$|\lambda|||e_1|| = ||\lambda e_1|| = ||T(e_1)|| = ||e_1||,$$

thus $\lambda \in \{-1, 1\}$. Let $W = \mathbf{R}e_1$, then W is stable under T, hence $W^\perp$ is stable under T (because T is orthogonal). Moreover, the restriction of T to $W^\perp$ is still an orthogonal transformation, since we have $||T(x)|| = ||x||$ for all $x \in V$, thus also for all $x \in W^\perp$. By the inductive hypothesis, $W^\perp$ has an orthonormal basis $e_2, \dots, e_n$ with respect to which the matrix of T restricted to $W^\perp$ is of the right shape (i.e., as in the statement of the theorem). Adding the vector $\frac{e_1}{||e_1||}$ and possibly permuting the resulting orthonormal basis $\frac{e_1}{||e_1||}, e_2, \dots, e_n$ of V yields an orthonormal basis with respect to which the matrix of T has the desired shape.

Assume now that T has no real eigenvalue. By Lemma 10.90 we can find two dimensional subspace V of T stable under T. Since T is orthogonal, the space $W^\perp$ is also stable under T, and the restrictions of T to W and $W^\perp$ are orthogonal transformations on these spaces. By the inductive hypothesis $W^\perp$ has an orthonormal basis $e_3, \dots, e_n$ with respect to which the matrix of $T|_{W^\perp}$ is block-diagonal, with blocks of the form R_{θ_i}. By Lemma 10.91 the space W has an

orthonormal basis e_1, e_2 with respect to which the matrix of $T|_W$ is of the form R_θ. Then the matrix of T with respect to $e_1, \ldots, e_n$ has the desired shape. The theorem is proved. □

We can also rewrite the previous theorem purely in terms of matrices:

Corollary 10.93. *Let $A \in M_n(\mathbf{R})$ be an orthogonal matrix. There is an orthogonal matrix $P \in M_n(\mathbf{R})$, integers p, q, k such that $p + q + 2k = n$ and real numbers $\theta_1, \ldots, \theta_k$ such that*

$$A = P^{-1} \begin{bmatrix} I_p & 0 & \ldots & 0 & 0 \\ 0 & -I_q & \ldots & 0 & 0 \\ 0 & 0 & R_{\theta_1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \\ 0 & 0 & \ldots & 0 & R_{\theta_k} \end{bmatrix} P.$$

Remark 10.94. a) The determinant of the matrix

$$\begin{bmatrix} I_p & 0 & \ldots & 0 & 0 \\ 0 & -I_q & \ldots & 0 & 0 \\ 0 & 0 & R_{\theta_1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \\ 0 & 0 & \ldots & 0 & R_{\theta_k} \end{bmatrix}$$

is $(-1)^q \in \{-1, 1\}$, since $\det R_{\theta_i} = 1$ for $1 \leq i \leq k$. It follows that

$$\det T \in \{-1, 1\}$$

for any orthogonal transformation T on V. Equivalently, $\det A \in \{-1, 1\}$ for any orthogonal matrix $A \in M_n(\mathbf{R})$. Of course, we can prove this directly, without using the previous difficult theorem: since $A \cdot {}^tA = I_n$ and $\det({}^tA) = \det A$, we deduce that

$$1 = \det(A \cdot {}^tA) = \det(A)^2,$$

thus $\det A \in \{-1, 1\}$.

An isometry T with $\det T = 1$ is called a **positive isometry**, while an isometry T with $\det T = -1$ is called a **negative isometry**. Geometrically, positive isometries preserve the orientation of the space, while negative ones reverse the orientation.

We can use the previous remark to define the notion of **oriented orthonormal basis of** V. Fix an orthonormal basis $\mathcal{B} = (e_1, \ldots, e_n)$ of V. If $\mathcal{B}' = (f_1, \ldots, f_n)$ is another orthonormal basis of V, then the change of basis matrix P from $\mathcal{B}$ to $\mathcal{B}'$ is orthogonal, thus $\det P \in \{-1, 1\}$. We say that $\mathcal{B}'$ is **positive or positively oriented (with respect to $\mathcal{B}$)** if $\det P = 1$, and **negative or negatively oriented (with respect to $\mathcal{B}$)** if $\det P = -1$. If $V = \mathbf{R}^n$ is endowed with the canonical

inner product, then we always take for $\mathcal{B}$ the canonical basis, so we simply say that an orthonormal basis is positive or negative if it is positive or negative with respect to the canonical basis of $\mathbf{R}^n$.

b) The characteristic polynomial of the matrix

$$\begin{bmatrix} I_p & 0 & \dots & 0 & 0 \\ 0 & -I_q & \dots & 0 & 0 \\ 0 & 0 & R_{\theta_1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \\ 0 & 0 & \dots & 0 & R_{\theta_k} \end{bmatrix}$$

is

$$(X-1)^p \cdot (X+1)^q \cdot \prod_{i=1}^{k} (X^2 - 2\cos\theta_i X + 1).$$

Notice that the complex roots of the polynomial $X^2 - 2\cos\theta X + 1$ are $e^{i\theta}$ and $e^{-i\theta}$, and they have absolute value 1. We deduce from the previous theorem that if λ is a complex root of the characteristic polynomial of an orthogonal matrix, then $|\lambda| = 1$. In other words, **all complex eigenvalues of an orthogonal matrix have absolute value** 1. This can also be proved directly, but the proof is trickier than the one that $\det A \in \{-1, 1\}$ for an orthogonal matrix A.

Let us try to study the orthogonal group in small dimension, by starting in dimension 2. We could use the previous theorem, but we prefer to give direct arguments in this case, since everything can be done by hand in a fairly simple and explicit way. So, let us try to understand orthogonal matrices $A \in M_2(\mathbf{R})$. Consider a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

satisfying $A \cdot {}^tA = I_2$. We know by the previous discussion that $\det A \in \{-1, 1\}$ (recall that this is immediate from the relation $A \cdot {}^tA = I_2$). Therefore, it is natural to consider two cases:

- $\det A = 1$. In this case the inverse of A is simply

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

and since A is orthogonal we have $A^{-1} = {}^tA$, giving $a = d$ and $b = -c$, that is

$$A = \begin{bmatrix} a & -c \\ c & a \end{bmatrix}.$$

Moreover, we have $a^2 + c^2 = 1$, thus there is a unique real number $\theta \in (-\pi, \pi]$ such that $a = \cos\theta$ and $c = \sin\theta$. Therefore

$$A = R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

The corresponding linear transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$ (sending X to AX) is given by

$$T(x, y) = (\cos\theta x - \sin\theta y, \sin\theta x + \cos\theta y)$$

and geometrically this is the **rotation of angle** θ. A simple computation shows that

$$R_{\theta_1} \cdot R_{\theta_2} = R_{\theta_1+\theta_2} = R_{\theta_2} \cdot R_{\theta_1} \tag{10.7}$$

for all real numbers. In particular, **all rotations commute with each other**. An important consequence of this observation is that the matrix of T with respect to **any** positive orthonormal basis of $\mathbf{R}^2$ is still R_θ (since the change of basis matrix from the canonical basis to this new positive orthonormal basis is still a rotation, thus it commutes with R_θ). Similarly, one checks that the matrix of T with respect to **any** negative orthonormal basis of $\mathbf{R}^2$ is $R_{-\theta}$. The formula (10.7) also shows that it is very easy to find the angle of the composite of two rotations: simply add their angles and subtract a suitable multiple of 2π to bring this angle in the interval $(-\pi, \pi]$.

- $\det A = -1$. Now the inverse of A is $\begin{bmatrix} -d & b \\ c & -a \end{bmatrix}$, thus the condition $A^{-1} = {}^tA$ yields $d = -a$ and $b = c$. Also, we have $a^2 + b^2 = 1$, thus there is a unique real number $\theta \in (-\pi, \pi]$ such that $a = \cos\theta$ and $b = \sin\theta$. Then

$$A = S_\theta := \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}.$$

Note that S_θ is symmetric and orthogonal, thus $S_\theta^2 = I_2$ and the corresponding transformation $T : \mathbf{R}^2 \to \mathbf{R}^2$

$$T(x, y) = (\cos\theta x + \sin\theta y, \sin\theta x - \cos\theta y)$$

is an orthogonal symmetry. In order to find the line with respect to which T is an orthogonal symmetry, it suffices to solve the system $AX = X$. An easy computation left to the reader shows that the system is equivalent to

$$\sin\left(\frac{\theta}{2}\right) \cdot x = \cos\left(\frac{\theta}{2}\right) \cdot y$$

and so the line $AX = X$ is spanned by the vector

$$e_1 = \left(\cos\left(\frac{\theta}{2}\right), \sin\left(\frac{\theta}{2}\right)\right).$$

Note that the orthogonal of this line is spanned by the vector

$$e_2 = \left(-\sin\left(\frac{\theta}{2}\right), \cos\left(\frac{\theta}{2}\right)\right),$$

and the vectors e_1, e_2 form a positive orthonormal basis of $\mathbf{R}^2$ in which the matrix of T is $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

One can easily check that

$$S_{\theta_1} \cdot S_{\theta_2} = R_{\theta_1 - \theta_2},$$

thus **the composite of two orthogonal symmetries is a rotation** (this was actually clear from the beginning, since the product of two matrices of determinant -1 is a matrix with determinant 1). Similarly, one checks that

$$S_{\theta_1} R_{\theta_2} = S_{\theta_1 - \theta_2}, \quad R_{\theta_1} S_{\theta_2} = S_{\theta_1 + \theta_2},$$

thus **the composite of a rotation and an orthogonal symmetry is an orthogonal symmetry** (this was also clear for determinant reasons).

All in all, the previous discussion gives

Theorem 10.95. *Let $A \in M_2(\mathbf{R})$ be an orthogonal matrix.*

a) If $\det A = 1$, *then*

$$A = R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

for a unique real number $\theta \in (-\pi, \pi]$, and the corresponding linear transformation T on $\mathbf{R}^2$ is the rotation of angle θ. Any two such matrices commute and ***the matrix of T in any positive orthonormal basis of $\mathbf{R}^2$ is R_θ.***

b) If $\det A = -1$, *then*

$$A = S_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

for a unique real number $\theta \in (-\pi, \pi]$. The matrix A is symmetric and the corresponding linear transformation on $\mathbf{R}^2$ is the orthogonal symmetry with respect to the line spanned by $\left(\cos\left(\frac{\theta}{2}\right), \sin\left(\frac{\theta}{2}\right)\right)$.

Let us consider now the more complicated case $\dim V = 3$. Here it is no longer easy to do explicit computations, so we will use Theorem 10.92 and our understanding of the case $\dim V = 2$ in order to understand the case $\dim V = 3$.

Recall the integers p, q, k from Theorem 10.92. Since

$$p + q + 2k = 3,$$

we see that necessarily $p \neq 0$ or $q \neq 0$. We can also prove this directly, observing that the characteristic polynomial of T has degree 3, thus it has a real root and so T has a real eigenvalue, which is necessarily equal to -1 or 1 since it has absolute value 1.

Replacing T with $-T$, we exchange the roles of p and q. For simplicity, let us assume that $p \geq 1$, i.e., T has at least one fixed point v. Then T fixes the line D spanned by v, and induces an isometry on the plane P orthogonal to D. This isometry is classified by Theorem 10.95, which deals with isometries of a plane. Thus we reduced the case $\dim V = 3$ to the case $\dim V = 2$. We can be a little bit more explicit, by discussing the following cases:

- **Either T or $-T$ is the identity map**. This case is not very interesting.
- **We have $\dim \ker(T - \mathrm{id}) = 2$.** If e_2, e_3 is an orthonormal basis of the plane $\ker(T - \mathrm{id})$, completed to an orthonormal basis e_1, e_2, e_3 of V, then T fixes pointwise $\mathrm{Span}(e_2, e_3)$ and leaves invariant the line spanned by e_1. Thus the matrix of T with respect to e_1, e_2, e_3 is of the form $\begin{bmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ for some real number λ, which is necessarily -1 (it must be -1 or 1 since the matrix must be orthogonal, and it cannot be 1 as otherwise $T = \mathrm{id}$). **We deduce that T is the orthogonal symmetry with respect to the plane** $\ker(T - \mathrm{id})$. Notice that $\det T = -1$ in this case (i.e., T is a **negative isometry**).
- **We have** $\dim \ker(T - \mathrm{id}) = 1$, thus $\ker(T - \mathrm{id})$ is the line spanned by some vector e_1 of norm 1. Complete e_1 to a positive orthonormal basis e_1, e_2, e_3 of $V = \mathbf{R}^3$. For instance, one can simply find a vector e_2 of norm 1 orthogonal for e_1, and if

$$e_1 = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \quad \text{and} \quad e_2 = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix},$$

set

$$e_3 = e_1 \wedge e_2 := \begin{bmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{bmatrix}.$$

The isometry that T induces on $\mathrm{Span}(e_2, e_3)$ has no fixed point (since all fixed points of T are on the line spanned by e_1), thus it is a rotation of angle θ for a unique real number $\theta \in (-\pi, \pi]$. The matrix of T with respect to e_1, e_2, e_3 is

$$R_\theta := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}.$$

We say that T is the **rotation of angle θ around the axis $\mathbf{R}e_1$**. Note that $\det T = 1$, that is T is a **positive isometry**. Also, note that the angle θ satisfies

$$1 + 2\cos\theta = \mathrm{Tr}(A),$$

but **this relation does not uniquely characterize the angle** θ (since $-\theta$ is also a solution of that equation). In order to find θ, it remains to find $\sin\theta$. In order to do that, one checks that

$$\det_{(e_1,e_2,e_3)}(e_1, e_2, T(e_2)) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & \cos\theta \\ 0 & 0 & \sin\theta \end{vmatrix} = \sin\theta.$$

- Finally, assume that $\ker(T - \mathrm{id}) = \{0\}$. One possibility is that $T = -\mathrm{id}$. Assume that $T \neq -\mathrm{id}$. Since either T or $-T$ have a fixed point (this follows from the fact that p or q is nonzero, i.e., that T has a real eigenvalue, which must be ± 1) and since T has no fixed point, it follows that $-T$ has a fixed point. Let e_1 be a vector of norm 1 which is fixed by $-T$, thus $T(e_1) = -e_1$. Complete e_1 to a positive orthonormal basis e_1, e_2, e_3 of V, then arguing as in the previous case we deduce that the matrix of T with respect to e_1, e_2, e_3 is

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix} = R_\theta \cdot \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for some $\theta \in (-\pi, \pi]$. Thus T **is the composite of a rotation of angle θ and of an orthogonal symmetry with respect to the orthogonal of the axis of the rotation**. Also, notice that $\det T = -1$, thus T is a **negative isometry**.

We can also **slightly change the point of view and discuss the situation in terms of matrices**. Consider an orthogonal matrix $A \in M_3(\mathbf{R})$ and the associated linear transformation $T : V \to V$ sending X to AX, where $V = \mathbf{R}^3$ is endowed with the canonical inner product. **We exclude the trivial cases $A = \pm I_3$.** In order to study the isometry T, **we first check whether T is a positive or negative isometry by computing** $\det T = \det A$.

Assume first that T is positive, i.e., $\det A = 1$**. We then check whether A is symmetric, i.e., $A = {}^tA$.** Let us consider two cases:

- **If A is symmetric**, then $A^2 = I_3$ (since A is orthogonal and symmetric) and so T **is an orthogonal symmetry**. **We claim that T is the orthogonal symmetry with respect to a line**. Indeed, since $A^2 = I_3$, all eigenvalues of A are -1 or 1. Moreover, they are not all equal since we excluded the cases $A = \pm I_3$, and their product is 1, since $\det A = 1$. Thus one eigenvalue is 1 and the other 2 are equal to -1. It follows that the matrix of T with respect to some orthonormal basis e_1, e_2, e_3 of $\mathbf{R}^3$ is $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ and T is the orthogonal symmetry with respect to the line spanned by e_1. **To find this line, we compute** $\ker(A - I_3)$ **by solving the system** $AX = X$. A basis v of the space of solutions of this system will span the line we are looking for.
- **If A is not symmetric, then A is a rotation of angle θ for a unique $\theta \in (-\pi, \pi]$. We find the axis of the rotation by solving the system $AX = X$: if $Ae_1 = e_1$ for some unit vector e_1, then the axis of the rotation is spanned by e_1. To find the angle of the rotation, we start by using the relation**

$$1 + 2\cos\theta = \mathrm{Tr}(A), \qquad (\star)$$

which pins down θ up to a sign. Next, we choose any vector e_2 of norm 1 orthogonal to e_1 and we set $e_3 = e_1 \wedge e_2$. Then e_1, e_2, e_3 is a positive orthonormal basis of $\mathbf{R}^3$ and $\det_{(e_1,e_2,e_3)}(e_1, e_2, Ae_2)$ **gives** $\sin\theta$**, which then determines θ uniquely**. Notice that **in practice it suffices to find the sign of the determinant of the vectors e_1, e_2, Ae_2 with respect to the canonical basis of $\mathbf{R}^3$, as this sign gives the sign of** $\sin\theta$**, which in turn determines θ uniquely thanks to relation** ($\star$).

Assume now that T is negative, i.e., $\det A = -1$**.** Then $-T$ is positive, thus the previous discussion applies to $-T$.

Let us see two concrete examples:

Problem 10.96. a) Prove that

$$A = \frac{1}{3}\begin{bmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{bmatrix}$$

is an orthogonal matrix.

b) Describe the isometry of $\mathbf{R}^3$ defined by A, i.e., the map $T : \mathbf{R}^3 \to \mathbf{R}^3$ given by $T(X) = AX$.

Solution. a) Using the product rule, one easily checks that $A \cdot {}^tA = I_3$, thus A is orthogonal. Alternatively, one checks that the columns (or rows) of A form an orthonormal family.

b) First, we check whether T is a positive or negative isometry by computing $\det A$. An easy computation shows that $\det A = 1$, so T is a positive isometry. Since

A is symmetric, we deduce from the above discussion that A is the orthogonal symmetry with respect to a line. To find this line, we solve the system $AX = X$. If x, y, z are the coordinates of X, the system is equivalent to

$$\begin{cases} -x + 2y + 2z = 3x \\ 2x - y + 2z = 3y \\ 2x + 2y - z = 3z \end{cases}$$

and has the solution $x = y = z$. Thus T is the orthogonal symmetry with respect to the line spanned by $(1, 1, 1)$. □

Problem 10.97. Prove that the matrix

$$A = \frac{1}{3}\begin{bmatrix} 2 & 2 & 1 \\ -2 & 1 & 2 \\ 1 & -2 & 2 \end{bmatrix}$$

is orthogonal and study the associated isometry of $\mathbf{R}^3$.

Solution. One easily checks either that $A \cdot {}^tA = I_3$ or that the rows of A form an orthonormal family. Next, one computes $\det A = 1$, thus the associated isometry T is positive. Since A is not symmetric, it follows that T is a rotation. To find its axis, we solve the system $AX = X$, which is equivalent to

$$\begin{cases} 2x + 2y + z = 3x \\ -2x + y + 2z = 3y \\ x - 2y + 2z = 3z \end{cases}$$

and then to

$$x = z, \quad y = 0.$$

Thus the axis of the rotation is spanned by the vector $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$. We normalize it to make it have norm 1, thus we consider instead the vector

$$e_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix},$$

which spans the axis of T.

Let θ be the angle of the rotation, so that

$$1 + 2\cos\theta = \mathrm{Tr}(A) = \frac{5}{3},$$

thus

$$\cos\theta = \frac{1}{3}.$$

It remains to find the sign of $\sin\theta$. For that, we choose a unit vector orthogonal to e_1, say

$$e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

and compute the sign of

$$\det(e_1, e_2, Ae_2) = \frac{1}{3\sqrt{2}} \begin{vmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 1 & 0 & -2 \end{vmatrix} = -\frac{4}{3\sqrt{2}} < 0,$$

thus $\sin\theta < 0$ and finally

$$\theta = -\arccos\frac{1}{3}.$$ □

10.7.1 Problems for Practice

1. Prove the result stated in Remark 10.87.
2. a) Prove that the matrix

$$A = \begin{bmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{bmatrix}$$

   is orthogonal.
   b) Describe the isometry $T : \mathbf{R}^2 \to \mathbf{R}^2$ sending X to AX: is it positive or negative? If it is a rotation, describe the angle, if it is a symmetry describe the line with respect to which T is the orthogonal symmetry.
3. a) Prove that each of the following matrices is orthogonal

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \frac{1}{3}\begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}.$$

   b) If A is one of these matrices, describe the isometry $T : \mathbf{R}^3 \to \mathbf{R}^3$ sending X to AX (for instance, if T is a rotation then you will need to find the axis and the angle of the corresponding rotation).

4. Prove that the matrix

$$A = \frac{1}{7}\begin{bmatrix} 2 & -6 & 3 \\ -6 & -3 & -2 \\ 3 & -2 & -6 \end{bmatrix}$$

is orthogonal and study the associated isometry of $\mathbf{R}^3$.

5. Find the matrix of the rotation of angle $\frac{\pi}{3}$ around the line spanned by $(1, 1, 1)$.
6. Let V be an Euclidean space and let $T : V \to V$ be a linear map. Prove that T is orthogonal if and only if $||T(x)|| = 1$ whenever $||x|| = 1$.
7. a) Describe all orthogonal matrices $A \in M_n(\mathbf{R})$ having integer entries.
   b) How many such matrices are there?
8. a) Describe the matrices in $M_n(\mathbf{R})$ which are simultaneously diagonal and orthogonal.
   b) Describe the matrices in $M_n(\mathbf{R})$ which are simultaneously upper-triangular and orthogonal.
9. Let V be an Euclidean space. Recall that if W is a subspace of V, then s_W denotes the orthogonal symmetry with respect to W, that is the symmetry with respect to W along $W^\perp$.

   a) Let v be a vector in V with $||v|| = 1$ and let $H = (\mathbf{R}v)^\perp$ be its orthogonal. Prove that for all $x \in V$ we have

$$s_H(x) = x - 2\langle v, x\rangle v.$$

   b) Let $v_1, v_2 \in V$ be vectors in V with the same norm. Prove that there is a hyperplane H of V such that $s_H(v_1) = v_2$.

10. Find the matrix (in the canonical basis of $\mathbf{R}^3$) of the orthogonal symmetry of $\mathbf{R}^3$ with respect to the line spanned by $(1, 2, 3)$.
11. Find the matrix (in the canonical basis of $\mathbf{R}^3$) of the orthogonal symmetry of $\mathbf{R}^3$ with respect to the plane spanned by $(1, 1, 1)$ and $(0, 1, 0)$.
12. Let V be a three-dimensional Euclidean space and let r be a rotation on V and s an orthogonal symmetry. Prove that $s \circ r \circ s$ is a rotation and describe its axis and its angle in terms of those of r.
13. Let V be a three-dimensional Euclidean space. When does a rotation of V commute with an orthogonal symmetry of V?
14. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be an orthogonal matrix. Prove that

$$n \leq \sum_{i,j=1}^{n} |a_{ij}| \leq n\sqrt{n}.$$

Hint: the sum of squares of the elements in each row is 1. For the inequality on the right use the Cauchy–Schwarz inequality.

15. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be an orthogonal matrix.

    a) Let X be the vector in $\mathbf{R}^n$ all of whose coordinates are equal to 1. Compute $\langle X, AX \rangle$, where $\langle\ ,\ \rangle$ is the standard inner product on $\mathbf{R}^n$.
    b) Prove that

$$|\sum_{i,j=1}^{n} a_{ij}| \leq n.$$

16. Let $v \in \mathbf{R}^n$ be a nonzero vector. Find all real numbers k for which the linear map $T : \mathbf{R}^n \to \mathbf{R}^n$ defined by

$$T(x) = x + k\langle x, v \rangle v$$

    is an isometry.

17. Let V be an Euclidean space and let $T : V \to V$ be a linear transformation such that $\langle T(x), T(y) \rangle = 0$ whenever $\langle x, y \rangle = 0$.

    a) Let x, y be vectors of norm 1 in V. Compute $\langle x + y, x - y \rangle$.
    b) Prove that there is a nonnegative real number k such that for all $x \in V$

$$||T(x)|| = k||x||.$$

    Hint: if $||x|| = ||y|| = 1$, show that $||T(x)|| = ||T(y)||$ using part a) and the hypothesis.
    c) Prove that there is an orthogonal transformation S on V such that $T = kS$.

18. Let $V = M_n(\mathbf{R})$ be endowed with the inner product

$$\langle A, B \rangle = \mathrm{Tr}({}^t AB).$$

    Let $A \in V$. Prove that the following statements are equivalent:

    a) A is orthogonal
    b) The linear transformation $T : V \to V$ sending B to AB is orthogonal.

19. (Cayley transform)

    a) Let $A \in M_n(\mathbf{R})$ be a skew-symmetric matrix. Prove that $I_n + A$ is invertible. Hint: if $AX = -X$, compute $\langle AX, X \rangle$ in two different ways.
    b) Prove that if $A \in M_n(\mathbf{R})$ is skew-symmetric, then $(I_n - A)(I_n + A)^{-1}$ is an orthogonal matrix which does not have -1 as eigenvalue.
    c) Conversely, prove that if B is an orthogonal matrix not having -1 as eigenvalue, then we can find a skew-symmetric matrix A such that $B = (I_n - A)(I_n + A)^{-1}$.
    d) Prove that the map $A \mapsto (I_n - A)(I_n + A)^{-1}$ induces a bijection between the skew-symmetric matrices in $M_n(\mathbf{R})$ and the orthogonal matrices in $M_n(\mathbf{R})$ for which -1 is not an eigenvalue.

20. (Compactness of the orthogonal group) Let $(A_k)_{k\geq 1}$ be a sequence of orthogonal matrices in $M_n(\mathbf{R})$. Let $a_{i,j}^{(k)}$ be the (i,j)-entry of A_k. Prove that there exists a sequence of integers $k_1 < k_2 < \ldots$ such that for all $i, j \in \{1, 2, \ldots, n\}$ the sequence $(a_{i,j}^{(k_l)})_{l\geq 1}$ converges to some real number x_{ij} and such that the matrix $X = [x_{ij}]$ is an orthogonal matrix. Hint: use the classical fact from real analysis that each sequence in $[-1, 1]$ has a convergent subsequence.
21. Let $A \in M_n(\mathbf{R})$ be a skew-symmetric matrix and let $T : \mathbf{R}^n \to \mathbf{R}^n$ be the map $X \to AX$. Prove that there is an orthonormal basis of $\mathbf{R}^n$ with respect to which the matrix of T is a block-diagonal matrix, in which each block is either the zero matrix or a matrix of the form $\begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}$ for some real number a. Hint: use induction on n and Lemma 10.90, and argue as in the proof of Theorem 10.92.
22. Prove that if $A \in M_n(\mathbf{R})$ is a skew-symmetric matrix, then $\det A \geq 0$ and the rank of A is even.

    In the following problems we consider a finite dimensional vector space V over $\mathbf{C}$ endowed with a positive definite hermitian product $\langle\ ,\ \rangle$ and associated norm $||\ ||$. A linear map $T : V \to V$ is called **unitary** or **an isometry** if

$$\langle T(x), T(y)\rangle = \langle x, y\rangle$$

    for all $x, y \in V$. A matrix $A \in M_n(\mathbf{C})$ is called **unitary** if the associated linear map $\mathbf{C}^n \to \mathbf{C}^n$ sending X to AX is unitary (where $\mathbf{C}^n$ is endowed with its standard hermitian product).
23. Prove that for a linear map $T : V \to V$ the following assertions are equivalent:

    a) T is unitary.
    b) We have $||T(x)|| = ||x||$ for all $x \in V$.
    c) T maps unit vectors (i.e., vectors of norm 1) to unit vectors.

24. Prove that a matrix $A \in M_n(\mathbf{C})$ is unitary if and only if $A \cdot A^* = I_n$, where $A^* = {}^t\overline{A}$ is the conjugate transpose of A (thus if $A = [a_{ij}]$ then $A^* = [\overline{a_{ji}}]$).
25. Prove that the inverse of a unitary matrix is a unitary matrix, and that the product of two unitary matrices is a unitary matrix.
26. Prove that if A is a unitary matrix, then $|\det A| = 1$.
27. Describe the diagonal and unitary matrices in $M_n(\mathbf{C})$.
28. Prove that for a matrix $A \in M_n(\mathbf{C})$ the following assertions are equivalent:

    a) A is unitary.
    b) There is an orthonormal basis $X_1, \ldots, X_n$ of $\mathbf{C}^n$ (endowed with its standard hermitian product) such that $AX_1, \ldots, AX_n$ is an orthonormal basis of $\mathbf{C}^n$.
    c) For any orthonormal basis $X_1, \ldots, X_n$ of $\mathbf{C}^n$ the vectors $AX_1, \ldots, AX_n$ form an orthonormal basis of $\mathbf{C}^n$.

29. Let $T : V \to V$ be a unitary linear transformation on V. Prove that there is an orthogonal basis of V consisting of eigenvectors of T.

10.8 The Spectral Theorem for Symmetric Linear Transformations and Matrices

In this section we will prove the fundamental theorem concerning real symmetric matrices or linear transformations. This classifies the symmetric linear transformations on an Euclidean space in the same way as Theorem 10.92 classifies orthogonal transformations. We will then use this theorem to prove the rather amazing result that any matrix $A \in M_n(\mathbf{R})$ is the product of a symmetric positive matrix and of an orthogonal matrix. This result, called the **polar decomposition**, is the matrix analogue of the classical result saying that any complex number can be written as the product of a nonnegative real number and of a complex number of magnitude 1.

We start by establishing a **first fundamental property of real symmetric matrices: their complex eigenvalues are actually real.**

Theorem 10.98. *Let $A \in M_n(\mathbf{R})$ be a symmetric matrix. Then all roots of the characteristic polynomial of A are real.*

Proof. Let λ be a root of the characteristic polynomial of A. Let us see A as a matrix in $M_n(\mathbf{C})$. Since $\det(\lambda I_n - A) = 0$, there exists $X \in \mathbf{C}^n$ nonzero such that $AX = \lambda X$. Write $X = Y + iZ$ for two vectors $Y, Z \in \mathbf{R}^n$ and write $\lambda = a + ib$ for some real numbers a, b. The equality $AX = \lambda X$ becomes

$$AY + iAZ = (a + ib)(Y + iZ) = aY - bZ + i(aZ + bY)$$

and taking real and imaginary parts yields

$$AY = aY - bZ, \quad AZ = aZ + bY \tag{10.8}$$

Since A is symmetric, we have

$$\langle AY, Z\rangle = \langle Y, AZ\rangle \tag{10.9}$$

By relation (10.8), the left-hand side of relation (10.9) is equal to $a\langle Y, Z\rangle - b||Z||^2$, while the right-hand side is equal to $a\langle Y, Z\rangle + b||Y||^2$. We deduce that

$$b(||Y||^2 + ||Z||^2) = 0$$

and since at least one of Y, Z is nonzero (otherwise $X = 0$, a contradiction), we deduce that $b = 0$ and λ is real. □

We need one further preliminary remark before proving the fundamental theorem:

Lemma 10.99. *Let V be an euclidian space and let $T : V \to V$ be a symmetric linear transformation on V. Let W be a subspace of V which is stable under T. Then*

a) $W^\perp$ is also stable under T.
b) The restrictions of T to W and $W^\perp$ are symmetric linear transformations on these spaces.

Proof. This follows fairly easily from Problem 10.78, but we prefer to give a straightforward argument.

a) Let $x \in W^\perp$ and $y \in W$. Then

$$\langle T(x), y\rangle = \langle x, T(y)\rangle.$$

Now $x \in W^\perp$ and $T(y) \in T(W) \subset W$, thus $\langle x, T(y)\rangle = 0$ and so $T(W^\perp) \subset W^\perp$, which yields the desired result.

b) Let T_1 be the restriction of T to W. For $x, y \in W$ we have

$$\langle T_1(x), y\rangle = \langle T(x), y\rangle = \langle x, T(y)\rangle = \langle x, T_1(y)\rangle,$$

thus T_1 is symmetric as linear map on W. The argument being identical for $W^\perp$, the lemma is proved. □

We are finally in good shape for the fundamental theorem of the theory of symmetric linear transformations (or matrices), which shows that all such transformations are diagonalizable in an orthonormal basis:

Theorem 10.100 (Spectral Theorem). *Let V be an Euclidean space and let $T : V \to V$ be a symmetric linear transformation. Then there is an orthonormal basis of V consisting of eigenvectors for T.*

Proof. We will prove the theorem by strong induction on $n = \dim V$. Everything being clear when $n = 1$, suppose that the statement holds up to $n - 1$ and let us prove it for n. So let V be Euclidean with $\dim V = n$ and let T be a symmetric linear transformation on V. Let $e_1, \ldots, e_n$ be an orthonormal basis of V. The matrix A of T in this basis is symmetric, hence it has a real eigenvalue λ by Theorem 10.98 (and the fact that any matrix with real-or complex-entries has a complex eigenvalue).

Let $W = \ker(\lambda \mathrm{id} - T)$ be the λ-eigenspace of T. If $W = V$, then $T = \lambda \mathrm{id}$ and so $e_1, \ldots, e_n$ is an orthonormal basis consisting of eigenvectors for T. So assume that $\dim W < n$. We have $V = W \oplus W^\perp$ and T leaves stable $W^\perp$, inducing a symmetric linear transformation on this subspace (Lemma 10.99). Applying the inductive hypothesis to the restriction of T to $W^\perp$ we find an orthonormal basis $f_1^\perp, \ldots, f_k^\perp$ of $W^\perp$ consisting of eigenvectors for T. Choosing any orthonormal basis $f_1, \ldots, f_s$ of W (consisting automatically of eigenvectors for T), we obtain an orthonormal basis $f_1, \ldots, f_s, f_1^\perp, \ldots, f_k^\perp$ of $V = W \oplus W^\perp$ consisting of eigenvectors for T. This finishes the proof of the theorem. □

If $A \in M_n(\mathbf{R})$ is a symmetric matrix, then the linear transformation $T : X \mapsto AX$ on $V = \mathbf{R}^n$ is symmetric. Applying the previous theorem, we can find an orthonormal basis of V with respect to which the matrix of T is diagonal. Since the

canonical basis of V is orthonormal and since the change of basis matrix between two orthonormal bases is orthogonal (Remark 10.87), we obtain the following all-important result:

Theorem 10.101. *Let $A \in M_n(\mathbf{R})$ be a symmetric matrix. There exists an **orthogonal** matrix $P \in M_n(\mathbf{R})$ such that PAP^{-1} is diagonal (in particular A is diagonalizable). In other words, there is an **orthonormal** basis of $\mathbf{R}^n$ consisting in eigenvectors of A.*

The next result gives a very useful characterization of positive (respectively positive definite) symmetric matrices:

Theorem 10.102. *Let $A \in M_n(\mathbf{R})$ be a symmetric matrix. Then the following statements are equivalent:*

a) A is positive
b) All eigenvalues of A are nonnegative.
c) $A = B^2$ for some symmetric matrix $B \in M_n(\mathbf{R})$.
d) $A = {}^tB \cdot B$ for some matrix $B \in M_n(\mathbf{R})$.

Proof. Suppose that A is positive and that λ is an eigenvalue of A, with eigenvector v. Since $Av = \lambda v$, we obtain

$$\lambda ||v||^2 = \langle v, Av \rangle = {}^tvAv \geq 0,$$

thus $\lambda \geq 0$. It follows that a) implies b).

Assume that b) holds and let $\lambda_1, \ldots, \lambda_n$ be all eigenvalues of A, counted with multiplicities. By assumption $\lambda_i \geq 0$ for all $i \in [1, n]$. Moreover, by the spectral theorem we can find an orthogonal matrix P such that $PAP^{-1} = D$, where D is the diagonal matrix with entries $\lambda_1, \ldots, \lambda_n$. Let D_1 be the diagonal matrix with entries $\mu_i = \sqrt{\lambda_i}$ and let $B = P^{-1}D_1P$. Then B is symmetric, since P is orthogonal and D_1 is symmetric:

$${}^tB = {}^tP{}^tD_1{}^tP^{-1} = P^{-1}D_1P.$$

Moreover, by construction $B^2 = P^{-1}D_1^2P = P^{-1}DP = A$. Thus c) holds.

It is clear that c) implies d). Finally, if d) holds, then for all $X \in \mathbf{R}^n$ we have

$${}^tXAX = ||BX||^2 \geq 0$$

and so A is positive. □

The reader is invited to state and prove the corresponding theorem for positive definite matrices.

After this hard work, we will take a break and see some nice applications of the above theorems. The result established in the next problem is very important.

Problem 10.103. a) Let T be a symmetric positive definite linear transformation on an Euclidean space V. Prove that for all $d \geq 2$ there is a unique symmetric positive definite linear transformation T_d such that $T_d^d = T$. Moreover, prove that there is a polynomial $P_d \in \mathbf{R}[X]$ such that $T_d = P_d(T)$.

b) Let $A \in M_n(\mathbf{R})$ be a symmetric positive definite matrix. Prove that for all $d \geq 2$ there is a unique symmetric positive definite matrix A_d such that $A_d^d = A$. Moreover, there is a polynomial $P_d \in \mathbf{R}[X]$ such that $A_d = P_d(A)$.

Solution. Clearly part b) is a consequence of part a), so we focus on part a) only. Let us establish the existence part first. Since T is symmetric and positive definite, there are positive real numbers $\lambda_1, \ldots, \lambda_n$ and an orthonormal basis $e_1, \ldots, e_n$ of V such that $T(e_i) = \lambda_i e_i$ for $1 \leq i \leq n$. Define $T_d : V \to V$ by $T_d(e_i) = \sqrt[d]{\lambda_i} e_i$ for $1 \leq i \leq n$ and extend it by linearity. Then $T_d^d(e_i) = \sqrt[d]{\lambda_i}^d e_i = \lambda_i e_i = T(e_i)$ for $1 \leq i \leq n$. Thus $T_d^d = T$. Moreover, T_d is symmetric and positive definite: indeed, in the orthonormal basis $e_1, \ldots, e_d$ the matrix of T_d is diagonal with positive entries.

Next, we prove that T_d is a polynomial in T. It suffices to prove that there is a polynomial P such that $P(\lambda_i) = \sqrt[d]{\lambda_i}$ for $1 \leq i \leq n$, as then

$$P(T)(e_i) = P(\lambda_i)e_i = \sqrt[d]{\lambda_i} e_i = T_d(e_i),$$

thus $P(T) = T_d$. In order to prove the existence of P, let us assume without loss of generality that the different numbers appearing in the list $\lambda_1, \ldots, \lambda_n$ are $\lambda_1, \ldots, \lambda_k$ for some $1 \leq k \leq n$. It is enough to construct a polynomial P such that $P(\lambda_i) = \sqrt[d]{\lambda_i}$ for $1 \leq i \leq k$. Simply take the Lagrange interpolation polynomial associated with the data $(\lambda_1, \ldots, \lambda_k)$ and $\sqrt[d]{\lambda_1}, \ldots, \sqrt[d]{\lambda_k}$.

Let us prove now that T_d is unique. Let S be a symmetric positive definite linear transformation such that $S^d = T$. Then S commutes with $T = S^d$, thus it also commutes with any polynomial in T. It follows from the previous paragraph that S commutes with T_d. Since S and T_d are diagonalizable and since they commute, it follows that there is a basis $f_1, \ldots, f_n$ of V in which the matrices of S and T_d are both diagonal, say D_1 and D_2. Note that the entries $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ of D_1, respectively D_2 are positive (since they are the eigenvalues of S and T_d) and they satisfy $a_i^d = b_i^d$ for $1 \leq i \leq n$ (since $S^d = T_d^d = T$). It follows that $a_i = b_i$ for $1 \leq i \leq n$ and then $D_1 = D_2$ and $S = T_d$. Thus T_d is unique. The problem is solved. □

Remark 10.104. a) As the proof shows, the same result applies to symmetric positive (but not necessarily positive definite) linear transformations and matrices (of course, the resulting transformation T_d, respectively matrix A_d will also be symmetric positive, but not necessarily positive definite).

b) We will simply write $\sqrt[d]{T}$, respectively $\sqrt[d]{A}$ for the linear transformation T_d, respectively matrix A_d in the previous problem.

Consider now a matrix $A \in M_n(\mathbf{R})$. The matrix ${}^tA \cdot A$ is then symmetric and positive. By the previous problem (and the remark following it), there is a unique

symmetric positive matrix $S = \sqrt{{}^tA \cdot A}$ such that $S^2 = {}^tA \cdot A$. **Suppose now that A is invertible**, then S is invertible (because ${}^tA \cdot A = S^2$ is invertible) and so we can define

$$U = AS^{-1}.$$

Then, taking into account that S is symmetric, we obtain

$${}^tU \cdot U = {}^tS^{-1}\,{}^tAAS^{-1} = S^{-1}S^2S^{-1} = I_n,$$

that is U is orthogonal. We have just obtained half of the following important

Theorem 10.105 (Polar Decomposition, Invertible Case). *Let $A \in M_n(\mathbf{R})$ be an **invertible** matrix. There is a unique pair (S, U) with S a symmetric positive definite matrix and U an orthogonal matrix such that $A = US$.*

Proof. The existence part follows from the previous discussion, it remains to establish the uniqueness of U and S. Suppose that $A = US$ with U orthogonal and S symmetric positive definite. Then

$${}^tA \cdot A = S\,{}^tU \cdot US = S^2$$

and by the uniqueness part in Problem 10.103 we deduce that $S = \sqrt{{}^tA \cdot A}$ and then $U = AS^{-1}$. Hence U and S are unique. □

One may wonder what is happening when $A = [a_{ij}]$ is no longer invertible. We will prove that we still have a decomposition $A = US$ with U orthogonal and S symmetric positive (not positive definite). The pair (S, U) is however no longer unique (if $A = O_n$, then $A = UO_n$ for any orthogonal matrix U). The existence of the decomposition in the case when A is no longer invertible is rather tricky. We will consider the matrices $A_k = A + \frac{1}{k}I_n$. There exists k_0 such that for all $k > k_0$ the matrix A_k is invertible (because A has only finitely many eigenvalues). By the previous theorem applied to A_k we can find an orthogonal matrix U_k and a symmetric positive definite matrix S_k such that

$$A_k = U_kS_k.$$

Write $U_k = [u_{ij}^{(k)}]$ and $S_k = [s_{ij}^{(k)}]$. Since U_k is orthogonal, the sum of squares of the elements in each column of U_k equals 1, thus $u_{ij}^{(k)} \in [-1, 1]$ for all $i, j \in \{1, \ldots, n\}$ and all $k > k_0$. By a classical result in real analysis, any sequence of numbers between -1 and 1 has a convergent subsequence (this is saying that the interval $[-1, 1]$ is compact). Applying this result n^2 times (for each pair $i, j \in \{1, 2, \ldots n\}$) we deduce the existence of a sequence $k_0 < k_1 < k_2 < \ldots$ such that

$$u_{ij} := \lim_{l\to\infty} u_{ij}^{(k_l)}$$

exists for all $i, j \in \{1, 2, \ldots, n\}$. We claim that the matrix $U = [u_{ij}]$ is orthogonal. Indeed, passing to the limit in each entry of the equality ${}^tU_{k_l} \cdot U_{k_l} = I_n$ yields ${}^tU \cdot U = I_n$. Moreover, since

$$S_{k_l} = U_{k_l}^{-1} A_{k_l} = {}^tU_{k_l} A_{k_l},$$

and since each (i, j)-entry of ${}^tU_{k_l}$ converges (when $l \to \infty$) to u_{ji} and each (i, j)-entry of A_{k_l} converges (when $l \to \infty$) to a_{ij}, we deduce that for all $i, j \in \{1, 2, \ldots, n\}$ the sequence $(s_{ij}^{(k_l)})_l$ converges to some s_{ij}, the matrix $S = [s_{ij}]$ is symmetric and

$$S = {}^tU \cdot A,$$

that is $A = US$. It remains to check that S is positive, but if $X \in \mathbf{R}^n$, then passing to the limit in the inequality ${}^tXS_{k_l}X \geq 0$ yields ${}^tXSX \geq 0$, thus S is positive. All in all, we have just proved the following:

Theorem 10.106 (Polar Decomposition, The General Case). *Any matrix $A \in M_n(\mathbf{R})$ can be written as the product of an orthogonal matrix and of a symmetric positive matrix.*

Note that if $A = US$, then necessarily

$${}^tA \cdot A = S^2$$

and so $S = \sqrt{{}^tA \cdot A}$ is uniquely determined. We call the eigenvalues of S the **singular values of** A. For more information about these, see the problems section.

We end this section with a few other applications of the results seen so far.

Problem 10.107. Let V be an Euclidean space and let T be a symmetric linear transformation on V. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of T. Prove that

$$\sup_{x \in V - \{0\}} \frac{||T(x)||}{||x||} = \max_{1 \leq i \leq n} |\lambda_i|.$$

Solution. By renumbering the eigenvalues, we may assume that $\max_i |\lambda_i| = |\lambda_n|$. Let $e_1, \ldots, e_n$ be an orthonormal basis of V in which $T(e_i) = \lambda_i e_i$ for $1 \leq i \leq n$. If $x \in V - \{0\}$, we can write $x = x_1 e_1 + \ldots + x_n e_n$ for some real numbers x_i, and we have

$$T(x) = \sum_{i=1}^{n} \lambda_i x_i e_i.$$

Thus

$$\frac{||T(x)||}{||x||} = \sqrt{\frac{\sum_{i=1}^{n} \lambda_i^2 x_i^2}{\sum_{i=1}^{n} x_i^2}} \leq |\lambda_n|$$

since $\lambda_i^2 x_i^2 \leq \lambda_n^2 x_i^2$ for $1 \leq i \leq n$. We conclude that

$$\sup_{x \in V - \{0\}} \frac{||T(x)||}{||x||} \leq |\lambda_n|.$$

Since

$$\frac{||T(e_n)||}{||e_n||} = |\lambda_n|,$$

we deduce that the previous inequality is actually an equality, which yields the desired result. □

Problem 10.108. Find all nilpotent symmetric matrices $A \in M_n(\mathbf{R})$.

Solution. If A is nilpotent, then all eigenvalues of A are 0. If A is moreover symmetric, then it is diagonalizable and so it must be O_n. Thus only the zero matrix is simultaneously symmetric and nilpotent. □

Problem 10.109. Let A be a symmetric matrix with real entries and suppose that $A^k = I_n$ for some positive integer k. Prove that $A^2 = I_n$.

Solution. Since A is symmetric and has real entries, its complex eigenvalues are actually real. Since they are moreover kth roots of unity, they must be ± 1. Thus all eigenvalues of A^2 are equal to 1. Since A^2 is symmetric, it is diagonalizable, and since all of its eigenvalues are 1, we must have $A^2 = I_n$. □

Problem 10.110. Let $A \in M_n(\mathbf{R})$ be a symmetric positive matrix. Prove that

$$\sqrt[n]{\det A} \leq \frac{1}{n} \mathrm{Tr}(A).$$

Solution. $\det A$ and $\mathrm{Tr}(A)$ do not change if we replace A with any matrix similar to it. Using the spectral theorem, we may therefore assume that A is diagonal. Since A is positive, its diagonal entries $a_i := a_{ii}$ are nonnegative numbers. It suffices therefore to prove that

$$\sqrt[n]{a_1 a_2 \ldots a_n} \leq \frac{a_1 + a_2 + \ldots + a_n}{n}$$

for all nonnegative real numbers $a_1, \ldots, a_n$. This is the AM-GM inequality. Let us recall the proof: the inequality is clear if one of the a_i's is 0. If all a_i are positive, the inequality is a consequence of the convexity of $x \mapsto e^x$ (more precisely of Jensen's inequality applied to $\ln a_1, \ldots, \ln a_n$). □

Problem 10.111. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a symmetric positive matrix with eigenvalues $\lambda_1, \ldots, \lambda_n$. Prove that if $f : [0, \infty) \to \mathbf{R}$ is a convex function, then

$$f(a_{11}) + f(a_{22}) + \ldots + f(a_{nn}) \leq f(\lambda_1) + \ldots + f(\lambda_n).$$

Solution. Since A is symmetric and positive, there is an orthogonal matrix P such that $A = PDP^{-1}$, where D is the diagonal matrix with diagonal entries $\lambda_1, \ldots, \lambda_n$. Let $P = [p_{ij}]$, then the equality $A = PD^tP$ yields

$$a_{ij} = \sum_{k=1}^{n} p_{ik}\lambda_k p_{jk}.$$

Since P is orthogonal, we have $\sum_{k=1}^{n} p_{ik}^2 = 1$ for all i, and since f is convex, we deduce that

$$f(a_{ii}) = f\left(\sum_{k=1}^{n} p_{ik}^2 \lambda_k\right) \leq \sum_{k=1}^{n} p_{ik}^2 f(\lambda_k).$$

Adding up these inequalities yields

$$\sum_{i=1}^{n} f(a_{ii}) \leq \sum_{i=1}^{n}\sum_{k=1}^{n} p_{ik}^2 f(\lambda_k) =$$

$$\sum_{k=1}^{n} f(\lambda_k) \sum_{i=1}^{n} p_{ik}^2 = \sum_{k=1}^{n} f(\lambda_k),$$

the last equality being again a consequence of the fact that P is orthogonal. The result follows. □

Problem 10.112. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a symmetric positive matrix. Prove that

$$\det A \leq a_{11}a_{22}\ldots a_{nn}.$$

Solution. If $\det A = 0$, then everything is clear, since $a_{ii} = {}^t e_i A e_i \geq 0$ for all i, where $e_1, \ldots, e_n$ is the canonical basis of $\mathbf{R}^n$. So suppose that $\det A > 0$, thus A is positive definite. Then $a_{ii} > 0$, since $e_i \neq 0$. If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of A, then $\det A = \lambda_1 \ldots \lambda_n$, thus the inequality is equivalent to

$$\sum_{k=1}^{n} \log \lambda_k \leq \sum_{k=1}^{n} \log a_{kk}.$$

This follows from Problem 10.111 applied to the convex function $f(x) = -\log x$. □

Problem 10.113 (Hadamard's Inequality). Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be an arbitrary matrix. Prove that

$$|\det A|^2 \leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij}^2 \right).$$

Solution. We will apply Problem 10.112 to the matrix $B = A^t A$, which is symmetric and positive. Note that $\det B = (\det A)^2$ and $b_{ii} = \sum_{j=1}^{n} a_{ij}^2$ for all i. The result follows therefore from Problem 10.112. □

10.8.1 Problems for Practice

1. Give an example of a symmetric matrix with complex coefficients which is not diagonalizable.
2. Let T be a linear transformation on an Euclidean space V, and suppose that V has an orthonormal basis consisting of eigenvectors of T. Prove that T is symmetric (thus the converse of the spectral theorem holds).
3. Consider the matrix

$$A = \begin{bmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{bmatrix}.$$

   a) Explain why A is diagonalizable in $M_3(\mathbf{R})$.
   b) Find an orthogonal matrix P such that $P^{-1}AP$ is diagonal.

4. Find an orthogonal basis consisting of eigenvectors for the matrix

$$A = \frac{1}{7} \begin{bmatrix} -2 & 6 & -3 \\ 6 & 3 & 2 \\ -3 & 2 & 6 \end{bmatrix}.$$

5. Let $A \in M_n(\mathbf{R})$ be a nilpotent matrix such that $A\,{}^tA = {}^tAA$. Prove that $A = O_n$. Hint: prove that $B = A\,{}^tA$ is nilpotent.
6. Let $A \in M_n(\mathbf{R})$ be a matrix. Prove that A^tA and ${}^tAA$ are similar (in fact A and ${}^tA$ are always similar matrices, but the proof of this innocent-looking statement is much harder and requires Jordan's classification theorem). Hint: both these matrices are symmetric, hence diagonalizable.
7. Let $A \in M_n(\mathbf{R})$ be a symmetric matrix. Prove that

$$\operatorname{rank}(A) \geq \frac{(\operatorname{Tr}(A))^2}{\operatorname{Tr}(A^2)}.$$

   Hint: consider an orthonormal basis of eigenvectors for A.

8. The entries of a matrix $A \in M_n(\mathbf{R})$ are between -1 and 1. Prove that

$$|\det A| \leq n^{n/2}.$$

Hint: use Hadamard's inequality.

9. Let $A, B \in M_n(\mathbf{R})$ be matrices such that ${}^tAA = {}^tBB$. Prove that there is an orthogonal matrix $U \in M_n(\mathbf{R})$ such that $B = UA$. Hint: use the polar decomposition.

10. (The Courant–Fischer theorem) Let E be an Euclidean space of dimension n and let $p \in [1, n]$ be an integer. Let T be a symmetric linear transformation on E and let $\lambda_1 \leq \ldots \leq \lambda_n$ be its eigenvalues.

    a) Let $e_1, \ldots, e_n$ be an orthonormal basis of E such that $T(e_i) = \lambda_i e_i$ for all $1 \leq i \leq n$ and let $F = \text{Span}(e_1, \ldots, e_p)$. Prove that

$$\max_{\substack{x \in F \\ ||x||=1}} \langle T(x), x \rangle \leq \lambda_p.$$

    b) Let F be a subspace of E of dimension p. Prove that $F \cap \text{Span}(e_p, \ldots, e_n)$ is nonzero and deduce that

$$\max_{\substack{x \in F \\ ||x||=1}} \langle T(x), x \rangle \geq \lambda_p.$$

    c) Prove the Courant–Fischer theorem:

$$\lambda_p = \min_{\substack{F \subset E \\ \dim F = p}} \max_{\substack{x \in F \\ ||x||=1}} \langle T(x), x \rangle,$$

    the minimum being taken over all subspaces F of E of dimension p.

11. Find all matrices $A \in M_n(\mathbf{R})$ satisfying $A^t AA = I_n$. Hint: start by proving that any solution of the problem is a symmetric matrix.

12. Find all symmetric matrices $A \in M_n(\mathbf{R})$ such that

$$A + A^3 + A^5 = 3I_n.$$

13. Let $A, B \in M_n(\mathbf{R})$ be symmetric positive matrices.

    a) Let $e_1, \ldots, e_n$ be an orthonormal basis of $\mathbf{R}^n$ consisting of eigenvectors of B, say $Be_i = \lambda_i e_i$. Let $\mu_i = \langle Ae_i, e_i \rangle$. Explain why $\lambda_i, \mu_i \geq 0$ for all i and why

$$\text{Tr}(A) = \sum_{i=1}^{n} \mu_i \quad \text{and} \quad \text{Tr}(AB) = \sum_{i=1}^{n} \lambda_i \mu_i.$$

b) Prove that

$$\mathrm{Tr}(AB) \leq \mathrm{Tr}(A) \cdot \mathrm{Tr}(B).$$

14. Let $A = [a_{ij}] \in M_n(\mathbf{R})$ be a symmetric matrix and let $\lambda_1, \ldots, \lambda_n$ be its eigenvalues (counted with multiplicities). Prove that

$$\sum_{i,j=1}^{n} a_{ij}^2 = \sum_{i=1}^{n} \lambda_i^2.$$

15. (Cholesky's decomposition) Let A be a symmetric positive definite matrix in $M_n(\mathbf{R})$. Prove that there is a unique upper-triangular matrix $T \in M_n(\mathbf{R})$ with positive diagonal entries such that

$$A = {}^tT \cdot T.$$

Hint: for the existence part, consider the inner product $\langle x, y\rangle_1 = \langle Ax, y\rangle$ on $\mathbf{R}^n$ (with $\langle\ ,\ \rangle$ the canonical inner product on $\mathbf{R}^n$), apply the Gram–Schmidt process to the canonical basis $\mathcal{B}$ of $\mathbf{R}^n$ and to the inner product $\langle\ ,\rangle_1$, and consider the change of basis matrix from $\mathcal{B}$ to the basis given by the Gram–Schmidt process.

16. a) Let V be an Euclidean space and let T be a linear transformation on V. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $T^* \circ T$. Prove that

$$\sup_{x \in V - \{0\}} \frac{||T(x)||}{||x||} = \max_{1 \leq i \leq n} \sqrt{\lambda_i}.$$

b) Let V be an Euclidean space and let T be a symmetric linear transformation on V. Let $\lambda_1 \leq \ldots \leq \lambda_n$ be the eigenvalues of T. Prove that

$$\sup_{x \in V - \{0\}} \frac{\langle T(x), x\rangle}{||x||^2} = \lambda_n.$$

17. Let $A, B \in M_n(\mathbf{R})$ be symmetric matrices. Define a map $f : \mathbf{R} \to \mathbf{R}$ by: $f(t)$ is the largest eigenvalue of $A + tB$. Prove that f is a convex function. Hint: use Problem 16.
18. Let T be a diagonalizable linear transformation on an Euclidean space V. Prove that if T and T^* commute, then T is symmetric.
19. Let V be the vector space of polynomials with real coefficients whose degree does not exceed n, endowed with the inner product

$$\langle P, Q\rangle = \int_0^1 P(x)Q(x)dx.$$

Consider the map $T : V \to V$ defined by

$$T(P)(X) = \int_0^1 (X + t)^n P(t)dt.$$

a) Give a precise meaning to $T(P)(X)$ and prove that T is a symmetric linear transformation on V.
b) Let $P_0, \ldots, P_n$ be an orthonormal basis of V consisting of eigenvectors for T, with corresponding eigenvalues $\lambda_0, \ldots, \lambda_n$. Prove that for all $x, y \in \mathbf{R}$ we have

$$(x + y)^n = \sum_{k=0}^{n} \lambda_k P_k(x) P_k(y).$$

20. Prove that if A, B are symmetric positive matrices in $M_n(\mathbf{R})$, then

$$\det(A + B) \geq \det A + \det B.$$

21. a) Prove that if $x_1, \ldots, x_n$ are real numbers and $\lambda_1, \ldots, \lambda_n$ are positive real numbers, then

$$\left(\sum_{i=1}^{n} \lambda_i x_i^2\right) \cdot \left(\sum_{i=1}^{n} \lambda_i^{-1} x_i^2\right) \geq \left(\sum_{i=1}^{n} x_i^2\right)^2.$$

b) Prove that if T is a symmetric and positive definite linear transformation on an Euclidean space V, then for all $x \in V$ we have

$$\langle T(x), x\rangle \cdot \langle T^{-1}(x), x\rangle \geq ||x||^4.$$

22. a) Prove that if $\lambda_1, \ldots, \lambda_n$ are nonnegative real numbers, then

$$\sqrt[n]{(1 + \lambda_1) \ldots (1 + \lambda_n)} \geq 1 + \sqrt[n]{\lambda_1 \ldots \lambda_n}.$$

Hint: check that the map $f(x) = \ln(1 + e^x)$ is convex on $[0, \infty)$ and use Jensen's inequality.
b) Let $A \in M_n(\mathbf{R})$ be a symmetric positive definite matrix. Prove that

$$\sqrt[n]{\det(I_n + A)} \geq 1 + \sqrt[n]{\det A}.$$

23. (Singular value decomposition) Let $\lambda_1, \ldots, \lambda_n$ be the singular values of $A \in M_n(\mathbf{R})$, counted with multiplicities (algebraic or geometric, it does not matter since S is diagonalizable).

a) Prove the existence of orthonormal bases $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ of $\mathbf{R}^n$ such that $Ae_i = \lambda_i f_i$ for $1 \leq i \leq n$. Hint: let $A = US$ be the polar decomposition of A. Pick an orthonormal basis $e_1, \ldots, e_n$ of $\mathbf{R}^n$ such that $Se_i = \lambda_i e_i$ and set $f_i = Ue_i$.

b) Prove that if $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ are bases as in a), then for all $X \in \mathbf{R}^n$ we have

$$AX = \sum_{i=1}^{n} \lambda_i \langle X, e_i \rangle f_i.$$

We call this the singular value decomposition of A.

c) Let $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ be orthonormal bases of $\mathbf{R}^n$ giving a singular value decomposition of A. Prove that the singular value decomposition of A^{-1} is given by

$$A^{-1}X = \sum_{j=1}^{n} \frac{1}{\lambda_j} \langle X, f_j \rangle e_j.$$

d) Prove that two matrices $A_1, A_2 \in M_n(\mathbf{R})$ have the same singular values if and only if there are orthogonal matrices U_1, U_2 such that

$$A_2 = U_1 A_1 U_2.$$

e) Prove that A is invertible if and only if 0 is not a singular value of A.

f) Compute the rank of A in terms of the singular values of A.

g) Prove that A is an orthogonal matrix if and only if all of its singular values are equal to 1.

24. The goal of this long exercise is to establish the analogues of the main results of this section for hermitian spaces.

Let V be a hermitian space, that is a finite dimensional $\mathbf{C}$-vector space endowed with a hermitian inner product $\langle\ ,\ \rangle$. A linear transformation $T: V \to V$ is called hermitian if $\langle T(x), y \rangle = \langle x, T(y) \rangle$ for all $x, y \in V$.

a) Let $e_1, \ldots, e_n$ be an **orthonormal** basis of V. Prove that T is hermitian if and only if the matrix A of T with respect to $e_1, \ldots, e_n$ is hermitian, that is $A = A^*$ (recall that $A^* = {}^t\overline{A}$).

From now on, until part e), we let T be a hermitian linear transformation on V.

b) Prove that the eigenvalues of T are real numbers.

c) Prove that if W is a subspace of V stable under T, then $W^\perp$ is also stable under T, and the restrictions of T to W and $W^\perp$ are hermitian linear transformations on these subspaces.

d) Prove that there is an orthonormal basis of V consisting of eigenvectors of T.

e) Conversely, prove that if V has an orthonormal basis consisting of eigenvectors of T **with real eigenvalues**, then T is hermitian.
f) Prove that for any hermitian matrix $A \in M_n(\mathbf{C})$ we can find a unitary matrix P and a diagonal matrix D with real entries such that $A = P^{-1}DP$.
g) Let $T : V \to V$ be any invertible linear transformation. Prove that there is a unique pair (S, U) of linear transformations on V such that H is hermitian positive (i.e., H is hermitian and its eigenvalues are positive), U is unitary and $T = U \circ H$.

Chapter 11
Appendix: Algebraic Prerequisites

Abstract This appendix recalls the basic algebraic structures that are needed in the study of linear algebra, with special emphasis on permutations and polynomials.

Even though the main objects of this book are vector spaces and linear maps between them, groups and polynomials naturally appear at several key moments in the development of linear algebra. In this brief chapter we define these objects and state the main properties that will be needed in the sequel. The reader is advised to skip reading this chapter and return to it whenever reference to this chapter is made.

11.1 Groups

Morally, a group is just a set in which one can multiply objects of the set (staying in that set) according to some rather natural rules. Formally, we have the following definition.

Definition 11.1. A group is a nonempty set G endowed with a map $\cdot : G \times G \to G$ satisfying the following properties:

a) (associativity) For all $a, b, c \in G$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
b) (identity) There is an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$.
c) (existence of inverses) For all $a \in G$ there is $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If moreover $a \cdot b = b \cdot a$ for all $a, b \in G$, we say that the group G is commutative or abelian.

Note that the element e of G is unique. Indeed, if e' is another element with the same properties, then $e' = e' \cdot e = e \cdot e' = e$. We call e the identity element of G. Secondly, the element a^{-1} is also unique, for if x is another element with the same properties, then

$$x = x \cdot e = x \cdot (a \cdot a^{-1}) = (x \cdot a) \cdot a^{-1} = e \cdot a^{-1} = a^{-1}.$$

We call a^{-1} the inverse of a.

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3_11

We will usually write ab instead of $a \cdot b$. Moreover, if the group G is abelian, we will usually prefer the additive notation $a + b$ instead of ab and write 0 instead of e, and $-a$ instead of a^{-1}.

Since the definition of a group is not restrictive, there is a huge amount of interesting groups. For instance, all vector spaces (which we haven't properly defined yet, but which are the main actors of this book) are examples of commutative groups. There are many other groups, which we will see in action further on: groups of permutations of a set, groups of invertible linear transformations of a vector space, the group of positive real numbers or the group of integers, etc.

11.2 Permutations

11.2.1 The Symmetric Group S_n

A bijective map $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is called a **permutation** of degree n. We usually describe a permutation by a table

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

where the second line represents the images of $1, 2, \ldots, n$ by σ.

The set of all permutations of degree n is denoted by S_n. It is not difficult to see that S_n has $n!$ elements: we have n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$ (as it can be any element different from $\sigma(1)$),..., one choice for $\sigma(n)$, thus $n \cdot (n-1) \cdot \ldots \cdot 1 = n!$ choices in total.

We denote by e the identity map sending k to k for $1 \leq k \leq n$, thus

$$e = \begin{pmatrix} 1\ 2 \ldots n \\ 1\ 2 \ldots n \end{pmatrix}.$$

The product $\sigma\tau$ of two permutations $\sigma, \tau \in S_n$ is defined as the composition $\sigma \circ \tau$. Thus for all $1 \leq k \leq n$

$$(\sigma\tau)(k) = \sigma(\tau(k)).$$

Example 11.2. Let $\sigma, \tau \in S_4$ be the permutations given by

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 3\ 4\ 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{pmatrix}.$$

Then

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

and

$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Since σ and τ are bijections, so is their composition and so $\sigma\tau \in S_n$. The easy proof of the following theorem is left to the reader.

Theorem 11.3. *Endowed with the previously defined multiplication, S_n is a group with $n!$ elements.*

Note that the inverse of a permutation with respect to multiplication is simply its inverse as a bijective map (i.e., σ^{-1} is the unique map such that $\sigma^{-1}(x) = y$ whenever $\sigma(y) = x$). For example, the inverse of permutation

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

is the permutation

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

The previous Example 11.2 shows that we generally have $\sigma \cdot \tau \neq \tau \cdot \sigma$, thus S_n is a non commutative group in general (actually for all $n \geq 3$, the groups S_1 and S_2 being commutative). The group S_n is called the **symmetric group** of degree n or the **group of permutations** of degree n.

Problem 11.4. Let $\sigma \in S_n$, where $n \geq 3$. Prove that if $\sigma \cdot \alpha = \alpha \cdot \sigma$ for all permutations $\alpha \in S_n$, then $\sigma = e$.

Solution. Fix $i \in \{1, 2, \ldots, n\}$ and choose a permutation α having i as unique fixed point, for instance

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & i-1 & i & i+1 & \ldots & n \\ 2 & 3 & \ldots & i+1 & i & i+2 & \ldots & 1 \end{pmatrix}.$$

Since

$$\sigma(i) = \sigma(\alpha(i)) = \alpha(\sigma(i))$$

and i is the unique fixed point of α, we must have $\sigma(i) = i$. As i was arbitrary, the result follows.

11.2.2 Transpositions as Generators of S_n

The group S_n has a special class of elements which have a rather simple structure and which determine the whole group S_n, in the sense that any element of S_n is a product of some of these elements. They are called **transpositions** and are defined as follows.

Definition 11.5. Let $i, j \in \{1, 2, \ldots, n\}$ be distinct. The transposition (ij) is the permutation σ sending k to k for all $k \neq i, j$ and for which $\sigma(i) = j$ and $\sigma(j) = i$. Thus (ij) exchanges i and j, while keeping all the other elements fixed.

It follows straight from the definition that a transposition τ satisfies $\tau^2 = e$ and so $\tau^{-1} = \tau$. Note also that the set $\{i, j\}$ is uniquely determined by the transposition (ij), since it is exactly the set of those $k \in \{1, 2, \ldots, n\}$ for which $(ij)(k) \neq k$. Since there are

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

subsets with two elements of $\{1, 2, \ldots, n\}$, it follows that there are $\binom{n}{2}$ transpositions. Let us prove now that the group S_n is generated by transpositions.

Theorem 11.6. *Let $n \geq 2$. Any permutation $\sigma \in S_n$ is a product of transpositions.*

Proof. For $\sigma \in S_n$ we let m_σ be the number of elements $k \in \{1, 2, \ldots, n\}$ for which $\sigma(k) \neq k$. We prove the theorem by induction on m_σ. If $m_\sigma = 0$, then $\sigma = e = (12)^2$ and we are done.

Assume that $m_\sigma > 0$ and that the statement holds for all permutations $\alpha \in S_n$ with $m_\alpha < m_\sigma$. Since $m_\sigma > 0$, there is $i \in \{1, 2, \ldots, n\}$ such that $\sigma(i) \neq i$. Let $j = \sigma(i)$, $\tau = (ij)$ and $\alpha = \sigma\tau$. Let $A = \{k, \alpha(k) \neq k\}$ and $B = \{k, \sigma(k) \neq k\}$. Note that if $\sigma(k) = k$, then $k \neq i$ and $k \neq j$, hence

$$\alpha(k) = (\sigma\tau)(k) = \sigma(\tau(k)) = \sigma(k) = k.$$

This shows that $A \subset B$. Moreover, we have $A \neq B$ since j belongs to B but not to A. It follows that $m_\alpha < m_\sigma$.

Using the induction hypothesis, we can write α as a product of transpositions. Since $\sigma = \alpha\tau^{-1} = \alpha\tau$, σ itself is a product of transpositions and we are done.

Note that the proof of the theorem also gives an algorithm allowing to express a given permutation as a product of transpositions. Let us see a concrete example. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}.$$

Since $\sigma(1) = 2$, we compute $\sigma \cdot (12)$ in order to create a fixed point

$$\sigma_1 = \sigma \cdot (12) = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 2\ 5\ 4\ 1\ 3 \end{pmatrix} \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 2\ 1\ 3\ 4\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 5\ 2\ 4\ 1\ 3 \end{pmatrix}.$$

Because $\sigma_1(1) = 5$, we compute $\sigma_1 \cdot (15)$ to create a new fixed point

$$\sigma_2 = \sigma_1 \cdot (15) = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 5\ 2\ 4\ 1\ 3 \end{pmatrix} \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 5\ 2\ 3\ 4\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 2\ 4\ 1\ 5 \end{pmatrix}.$$

Computing $\sigma_2(13)$ we obtain a new fixed point in the permutation

$$\sigma_3 = \sigma_2(13) = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 2\ 3\ 1\ 5 \end{pmatrix}.$$

Now, observe that $\sigma_3 = (14)$, thus $\sigma_3 \cdot (14) = e$. We deduce that $\sigma \cdot (12) \cdot (15) \cdot (13) \cdot (14) = e$ and so

$$\sigma = (14)(13)(15)(12).$$

11.2.3 The Signature Homomorphism

An **inversion** of a permutation $\sigma \in S_n$ is a pair (i, j) with $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. Let $\mathrm{Inv}(\sigma)$ be the number of inversions of σ. Note that

$$0 \leq \mathrm{Inv}(\sigma) \leq \frac{n(n-1)}{2}, \quad \sigma \in S_n,$$

and these inequalities are optimal: $\mathrm{Inv}(e) = 0$ and $\mathrm{Inv}(\sigma) = \frac{n(n-1)}{2}$ for

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}.$$

Example 11.7. The permutation

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 5\,6\,2\,1\,4\,3 \end{pmatrix}$$

has $\mathrm{Inv}(\sigma) = 4 + 4 + 1 + 1 = 10$ inversions, since $\sigma(1) > \sigma(3)$, $\sigma(1) > \sigma(4)$, $\sigma(1) > \sigma(5)$, $\sigma(1) > \sigma(6)$, $\sigma(2) > \sigma(3)$, $\sigma(2) > \sigma(4)$, $\sigma(2) > \sigma(5)$, $\sigma(2) > \sigma(6)$, $\sigma(3) > \sigma(4)$, $\sigma(5) > \sigma(6)$.

We introduce now a fundamental map $\varepsilon : S_n \to \{-1, 1\}$, the **signature**.

Definition 11.8. The **sign** of a permutation $\sigma \in S_n$ is defined by

$$\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}.$$

If $\varepsilon(\sigma) = 1$, then we say that σ is an **even** permutation and if $\varepsilon(\sigma) = -1$, then we say that σ is an **odd** permutation. Note that a transposition $\tau = (ij)$ with $i < j$ is an odd permutation, as the number of inversions of τ is $j - i + j - i - 1 = 2(j - i) - 1$.

Here is the fundamental property of the signature map:

Theorem 11.9. *The signature map $\varepsilon : S_n \to \{-1, 1\}$ is a homomorphism of groups, i.e., $\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$ for all $\sigma_1, \sigma_2 \in S_n$.*

Without giving the formal proof of this theorem, let us mention that the key point is the equality

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

for any $\sigma \in S_n$. This follows rather easily from the definition of $\varepsilon(\sigma)$ and can be used to prove the multiplicative character of σ.

Remark 11.10. a) The signature is the **unique nontrivial homomorphism** $S_n \to \{-1, 1\}$. Indeed, let $\varphi : S_n \to \{-1, 1\}$ be a surjective homomorphism of groups. If $\tau_1 = (i, j)$ and $\tau_2 = (k, l)$ are two transpositions, then we can find $\sigma \in S_n$ such that $\tau_2 = \sigma\tau_1\sigma^{-1}$ (indeed, it suffices to impose $\sigma(i) = k$ and $\sigma(j) = l$). Then $\varphi(\tau_2) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma)^{-1} = \varphi(\tau_1)$. Thus all transpositions of S_n are sent to the same element of $\{-1, 1\}$, which must be -1, as the transpositions generate S_n and φ is not the trivial homomorphism. Thus $\varphi(\tau) = -1 = \varepsilon(\tau)$ for all transpositions and using again that the transpositions generate S_n, it follows that $\varphi = \varepsilon$.

b) Let $\sigma \in S_n$ be a permutation, and write $\sigma = \tau_1\tau_2 \ldots \tau_k$, where $\tau_1, \tau_2, \ldots, \tau_k$ are transpositions. This decomposition is definitely not unique, but the parity of k is the same in all decompositions. This is definitely not an obvious statement, but it follows easily from the previous theorem: for any such decomposition we must have $\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\tau_i) = (-1)^k$, thus the parity of k is independent of the decomposition.

11.3 Polynomials

Let F be a field, for instance $\mathbf{R}$ or $\mathbf{C}$. The set $F[X]$ of polynomials with coefficients in X will play a key role in this chapter. In this section we recall, without proof, a few basic facts about polynomials.

Any element P of $F[X]$ can be uniquely written as a formal expression

$$P = a_0 + a_1 X + \ldots + a_n X^n$$

with $a_0, \ldots, a_n \in F$. If $P \neq 0$, then at least one of the coefficients $a_0, \ldots, a_n$ is nonzero, and we may assume that $a_n \neq 0$. **We then say that P has degree n (and write $\deg P = n$) and leading coefficient a_n.** By convention, the degree of the zero polynomial is $-\infty$. A fundamental property of polynomials with coefficients in a field is the equality

$$\deg(PQ) = \deg P + \deg Q$$

for all polynomials $P, Q \in F[X]$. We say that P is **unitary** or **monic** if its leading coefficient is 1. Polynomials of degree 0 or $-\infty$ are also called **constant polynomials**.

Remark 11.11. Sometimes we will write $P(X)$ instead of P for an element of $F[X]$, in order to emphasize that the variable is X.

The first fundamental result is the **division algorithm**:

Theorem 11.12. *Let $A, B \in F[X]$ with $B \neq 0$. There is a unique pair (Q, R) of elements of $F[X]$ such that $A = BQ + R$ and $\deg R < \deg B$.*

The polynomials Q and R are called the **quotient**, respectively **remainder** of A when divided by B. We say that B **divides** A if $R = 0$. We say that a polynomial $P \in F[X]$ is **irreducible** if P is not constant, but cannot be written as the product of two nonconstant polynomials. Thus all divisors of an irreducible polynomial are either constant polynomials or constant times the given polynomial. For instance, all polynomials of degree 1 are irreducible. For some special fields, these are the only irreducible polynomials:

Definition 11.13. A field F is called **algebraically closed** if any irreducible polynomial $P \in F[X]$ has degree 1.

An element $a \in F$ is called a **root** of a polynomial $P \in F[X]$ if $P(a) = 0$. In this case, the division algorithm implies the existence of a factorization

$$P = (X - a)Q$$

for some polynomial $Q \in F[X]$. Repeating this argument, we deduce that if $a_1, a_2, \ldots, a_k \in F$ are **pairwise distinct** roots of P, then we can write

$$P = (X - a_1)(X - a_2) \ldots (X - a_k)Q$$

for some polynomial $Q \in F[X]$. Taking degrees, we obtain the following

Theorem 11.14. *A nonzero polynomial $P \in F[X]$ of degree n has at most n pairwise distinct roots in F.*

Stated otherwise, if a polynomial of degree at most n vanishes at $n + 1$ distinct points of F, then it must be the zero polynomial. The notion of irreducible polynomial can also be expressed in terms of roots:

Theorem 11.15. *A field F is algebraically closed if and only if any nonconstant polynomial $P \in F[X]$ has a root in F. If this is the case, then any nonconstant polynomial $P \in F[X]$ can be written as*

$$P = c(X - a_1)^{n_1} \ldots (X - a_k)^{n_k}$$

for some nonzero constant $c \in F$, some pairwise distinct elements $a_1, .., a_k$ of F and some positive integers $n_1, \ldots, n_k$.

We call n_i the **multiplicity** of the root a_i of P. It is the largest positive integer m for which $(X - a_i)^m$ divides P.

Finally, we state the fundamental theorem of algebra:

Theorem 11.16 (Gauss). *The field* $\mathbf{C}$ *of complex numbers is algebraically closed.*

References

1. Axler, S.: Linear Algebra Done Right, 2nd edn. Springer, New York (1997)
2. Halmos, P.: Finite Dimensional Vector Spaces, 2nd edn. Van Nostrand, New York (1958)
3. Hoffman, K., Kunze, R.: Linear Algebra, 2nd edn. Prentice Hall, Englewood Cliffs (1971)
4. Lang, S.: Linear Algebra, 3rd edn. Undergraduate Texts in Mathematics. Springer, New York (1987)
5. Lax, P.D.: Linear Algebra and Its Applications, 2nd edn. Wiley Interscience, New York (2007)
6. Munkres, J.: Elementary Linear Algebra. Addison-Wesley, Reading (1964)
7. Strang, G.: Linear Algebra and Its Applications, 4th edn. Brooks cole, Stamford (2005)

T. Andreescu, *Essential Linear Algebra with Applications: A Problem-Solving Approach*, DOI 10.1007/978-0-8176-4636-3