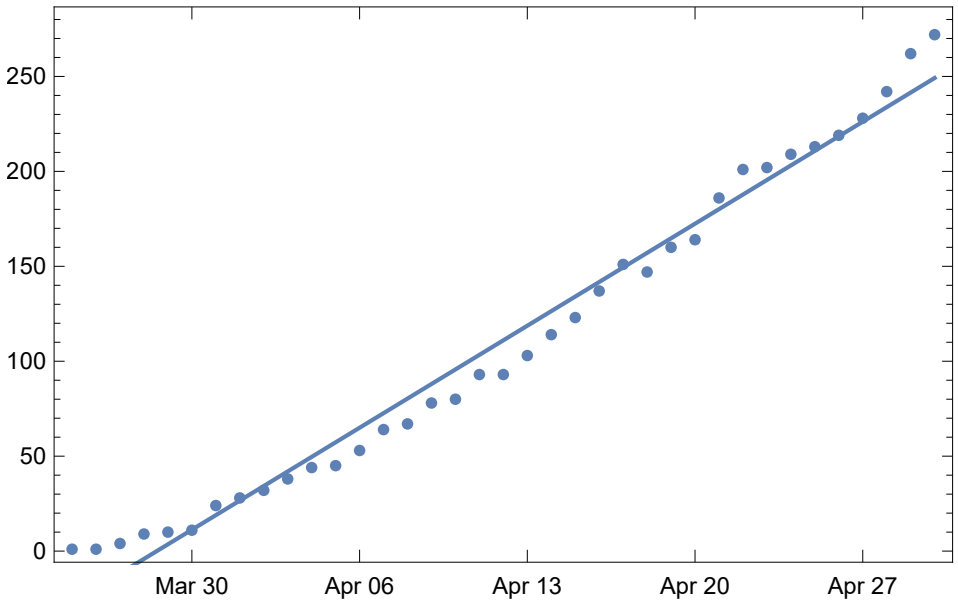
# LINEAR ALGEBRA

Lecture notes for MA 434/534

Rudi Weikard




Version of February 14, 2022

# Contents

# Preface

We all know how to solve two linear equations in two unknowns like

$$2x - 3y = 5 \quad \text{and} \quad x + 3y = -2.$$

Linear Algebra grew out of the need to solve simultaneously many such equations for perhaps many unknowns. For instance, the frontispiece of these notes shows a number of data points and an attempt to find the "best" straight line as an approximation. As we will see later this leads to 37 equations for 2 unknowns. How do we even know there is a solution (let alone "best" solution) and how do we find it?

From the practical point of view Linear Algebra is probably the most important subject in Mathematics. It is, for instance, indispensable for the numerical solution of differential equations and these, in turn, are ubiquitous in the natural sciences, engineering, the social sciences, and economics.

As a specific example of another application of Linear Algebra let me mention graphs and networks, themselves used in a wide variety of subjects; think World Wide Web, telecommunications, or gene regulatory networks to name just a few.

Linear Algebra may be described as the theory of finite-dimensional vector spaces. Many results, though, hold also in infinite-dimensional vector spaces, often with the same proofs. When this is the case we will formulate definitions and theorems in this more general situation but otherwise we will concentrate on finite-dimensional spaces. Another issue is the field underlying our vector spaces. Again many conclusions work for general fields and we will then state them that way. We would stick to the real number field only, if it were not the case that, particularly in the later chapters, the complex number field made many issues quite a bit simpler. Therefore we will present results often for a general field $K$ but the reader is encouraged to think of $K = \mathbb{R}$ or $K = \mathbb{C}$ if that is helpful.

Due to its importance there are hundreds of textbooks on Linear Algebra. I first learned the subject from Prof. H.-J. Kowalsky and am therefore familiar with his book [2]. Alas, it is in German and, at any rate, other books have influenced me, too. In particular, I recommend for further study Axler [1], Strang [3], and Trefethen and Bau [4].

If you come across a symbol or term about whose definition you are uncertain be sure to consult the list of special symbols or the index which show the page where the definition is (hopefully) to be found. There is also an appendix introducing some important notions from Set Theory and Algebra which we assume to be known.

CHAPTER 1

# Systems of linear equations

## 1.1. Introduction

**1.1.1 The simplest case.** The simplest case of a "system" of linear equations is when there is only one equation and one unknown, i.e., $Ax = b$ where $A$ and $b$ are real numbers. Investigation of existence and uniqueness of solutions leads to a trichotomy which will reappear in the general case. To see this determine the conditions on $A$ and $b$ for which one has existence or uniqueness or both.

**1.1.2 Two linear equations.** There are several ways to find the solution of two linear equations in two unknowns like

$$2x - 3y = 5 \quad \text{and} \quad x + 3y = -2.$$

Find some of them. One idea one will be particularly useful in the general case.

**1.1.3 Systems of linear equations.** Now suppose we have $m$ linear equations in $n$ unknowns. It is time to define the term *linear equation* precisely. The unknowns, which we will seek (for now) among the real numbers, are denoted by $x_1, ..., x_n$. An equation in these $n$ unknowns is called linear, if it is of the form

$$a_1x_1 + ... + a_nx_n = b$$

where $a_1, ..., a_n$ and $b$, called coefficients, are themselves real numbers. Note that there occur neither products nor powers of the unknowns.

However, we are interested in a system of such equations, i.e., we ask that, say, $m$ such equations hold simultaneously. Specifically, a *system* of $m$ linear equation in $n$ unknowns is of the form

$$\begin{aligned} A_{1,1}x_1 + ... + A_{1,n}x_n &= b_1 \\ A_{2,1}x_1 + ... + A_{2,n}x_n &= b_2 \\ &\vdots \\ A_{m,1}x_1 + ... + A_{m,n}x_n &= b_m \end{aligned}$$

where the $A_{j,k}$ and the $b_\ell$ are given numbers and the (perhaps impossible) task is to find the numbers $x_h$ rendering all equations true.

Note that, if $b_1 = ... = b_m = 0$, we always have the solution $x_1 = ... = x_n = 0$. The system is then called *homogeneous* and the given solution is called the *trivial solution*.

Exercise. Find the system of linear equations determining all cubic polynomials passing through the points $(-2, 3)$, $(1, 2)$, $(2, 3)$, and $(4, 7)$.

## 1.2. Solving systems of linear equations

**1.2.1 The idea of elimination.** Suppose we have the equations

$$A_1x_1 + ... + A_nx_n = b \tag{1}$$
$$A'_1x_1 + ... + A'_nx_n = b'. \tag{2}$$

If $x = (x_1, ..., x_n)$ is a solution for both equations and if $\alpha$ is a non-zero scalar, then $x$ is also a solution for

$$(A'_1 + \alpha A_1)x_1 + ... + (A'_n + \alpha A_n)x_n = b' + \alpha b. \tag{3}$$

Conversely, if $x$ is a solution of equations (1) and (3), then it is also a solution of equation (2).

In other words the system consisting of equations (1) and (2) has precisely the same solutions as the system consisting of equations (1) and (3). If $A_1 \neq 0$, we may choose $\alpha = -A'_1/A_1$ and thereby *eliminate* the occurrence of $x_1$ from equation (3).

**1.2.2 Repeated elimination.** We may use this idea to eliminate $x_1$ from all equations but one.[1] After this we might eliminate $x_2$ from all equations but one of those which are already free of $x_1$ so that in all but at most two equations neither $x_1$ nor $x_2$ occurs. In the end of this recursive process $x_n$ but only $x_n$ might appear in all equations.

Of course, we may also change the order of the equations without changing the set of possible solutions. We will list the equation containing $x_1$ first, then the one remaining equation containing $x_2$ (if any) second and so on. We will say that the system thus obtained is in *upper triangular* form.

Exercise. Put the the following system in upper triangular form:

$$\begin{aligned} x_3 - x_2 &= 2 \\ 4x_1 + 3x_2 + x_3 &= 6 \\ 2x_1 + 5x_2 + x_3 &= 0. \end{aligned}$$

What happens when the coefficient of $x_3$ in the last equation is replaced by $-3$? And what happens when additionally the number 0 on the right-hand side of the last equation is replaced by $-4$?

**1.2.3 Equivalent systems of equations.** Two systems of $m$ linear equations in $n$ unknowns are called equivalent if they have precisely the same solutions.

Consider the following two operations on systems of linear equations:

(1) Exchange any two of the equations.
(2) Add a multiple of one equation to another one.

Will applying any one of them change the set of solutions? Explain.

**1.2.4 Back-substitution.** Suppose we have a linear system which is in upper triangular form. It is then easy to determine whether a solution exists and, if so, relatively easy to obtain one.

Exercise. Do so, when possible, for the three cases discussed in Exercise 1.2.2.

[1] We are assuming here that $x_1$ was present to begin with. While it might appear pointless to consider a case where $x_1$ is listed among the unknowns without occurring in any of the equations, we do not want to rule this out.

**1.2.5 Linear equations in matrix form.** Instead of all the equations listed in 1.1.3 one writes simply $Ax = b$ where $A$ represents all the numbers $A_{j,k}$, respecting their rectangular arrangement, and $x$ and $b$ represent the numbers $x_1, ..., x_n$ and $b_1, ..., b_m$, again respecting their order. More precisely, a (horizontal) row of $A$ collects the coefficients of the unknowns coming from one of the equations. A (vertical) column, on the other hand, collects all the coefficients of the one of the unknowns.

$A$ is called a *matrix* and $b$ and $x$ are called *vectors*.

EXERCISE. Identify the matrix $A$ and the vector $b$ such that the system

$$\begin{aligned} x_1 - 2x_2 + 4x_3 &= -3 \\ 2x_1 + 2x_3 &= 3 \\ -2x_1 + 5x_2 - 3x_3 &= 0 \end{aligned}$$

is represented by the equation $Ax = b$.

## 1.3. Matrices and vectors

**1.3.1 Vectors.** An $n$-dimensional (real) *vector*[2] is an ordered list of $n$ (real) numbers. In such a list order is important, i.e., $(2, 4, -3)$ is different from $(4, 2, -3)$. There are two ways to represent vectors which we will have to distinguish. We can, as we did above, arrange the entries of the list horizontally (row vectors) or vertically (column vectors) as in $\begin{pmatrix} 7 \\ -3 \end{pmatrix}$. The row vector $(7, -3)$ and the column vector $\begin{pmatrix} 7 \\ -3 \end{pmatrix}$ are two different things! We will mostly think of vectors as columns but typesetting would of course favor the horizontal representation. We will therefore introduce the concept of a *transpose* which turns a row into a column (and vice versa). We indicate transposition by the symbol $\top$ as a superscript. For instance

$$(4, 2, -3)^\top = \begin{pmatrix} 4 \\ 2 \\ -3 \end{pmatrix}.$$

**1.3.2 Euclidean spaces.** The set of all real $n$-dimensional column vectors is denoted by $\mathbb{R}^n$. Of course, $\mathbb{R} = \mathbb{R}^1$ is represented by the familiar real line and we are also familiar with $\mathbb{R}^2$ and $\mathbb{R}^3$. The former is represented by a plane and the latter by ordinary 3-space in which coordinate axes have been chosen. The spaces $\mathbb{R}^n$ are called *euclidean spaces*.

**1.3.3 Vector addition.** Two vectors of the same euclidean space $\mathbb{R}^n$ are *added* entrywise, i.e.,

$$(a_1, ...., a_n)^\top + (b_1, ..., b_n)^\top = (a_1 + b_1, ..., a_n + b_n)^\top.$$

This operation is associative and commutative (find out what this means and prove it). The vector $(0, ..., 0)^\top \in \mathbb{R}^n$, the number 0 repeated $n$ times, is especially important. It is called the zero vector and denoted by 0 since, due to context, there is no danger that it could be confused with the number 0. Adding the zero vector to any element of $\mathbb{R}^n$ does not cause a change, i.e., for all $a$ in $\mathbb{R}^n$ we have

$$a + 0 = 0 + a = a.$$

No other vector has this property.

For every vector $a \in \mathbb{R}^n$ there is one and only one vector $b \in \mathbb{R}^n$ such that

$$a + b = b + a = 0.$$

[2]Later we will give a more general definition of the term vector.

The vector $b$ is called the *negative* of $a$. We will denote $b$ by $-a$ and we also use the notation $a-b$ as shorthand for $a+(-b)$. We mention in passing that a set for which an operation with these properties is defined is called a commutative group.

**1.3.4 Scalar multiplication.** The *scalar multiplication* is an operation combining real numbers (these are called *scalars*) with vectors. If $\alpha$ is a real number and $a \in \mathbb{R}^n$, then $\alpha a$ is the vector obtained by multiplying each entry of $a$ with $\alpha$, i.e,

$$\alpha(a_1, ...., a_n)^\top = (\alpha a_1, ..., \alpha a_n)^\top.$$

We have the following properties: if $\alpha$ and $\beta$ are scalars (real numbers) and $a$ and $b$ are vectors in $\mathbb{R}^n$, then the following statements hold:

(1) $(\alpha+\beta)a = \alpha a + \beta a$,
(2) $\alpha(a+b) = \alpha a + \alpha b$,
(3) $(\alpha\beta)a = \alpha(\beta a)$, and
(4) $1a = a$.

**1.3.5 Linear combinations.** Given vectors $a_1, ..., a_k \in \mathbb{R}^n$ and scalars $\alpha_1, ..., \alpha_k$ we may form the expression

$$\alpha_1 a_1 + ... + \alpha_k a_k$$

which is again a vector in $\mathbb{R}^n$. It is called a *linear combination* of the vectors $a_1, ..., a_k$.

For instance, if we collect the coefficients $A_{1,k}$, ..., $A_{m,k}$ in the system of linear equations discussed in 1.1.3 as a vector $a_k = (A_{1,k}, ..., A_{m,k})^\top$ and do so for every $k \in \{1, ..., n\}$ as well as setting $b = (b_1, ..., b_m)^\top$ we may write the system as

$$x_1 a_1 + ... + x_n a_n = b.$$

Solving the system of linear equations is therefore equivalent to finding scalars $x_1$, ..., $x_n$ such that the linear combination $x_1 a_1 + ... + x_n a_n$ equals the vector $b$.

Exercise. For the system given in 1.2.5 identify the vectors whose linear combination will give the vector $(-3, 3, 0)^\top$.

**1.3.6 Matrices.** Now we go one step further and collect the vectors $(A_{1,k}, ..., A_{m,k})^\top$ for $k = 1, ..., n$ in a rectangular field of numbers called a matrix as we did already in 1.2.5.

Thus a $m \times n$-*matrix* of real numbers is a rectangular array of real numbers with $m$ rows and $n$ columns.[3] The set of all real $m \times n$-matrices is denoted by $\mathbb{R}^{m\times n}$. Note that column vectors in $\mathbb{R}^m$ are special matrices, namely those where $n = 1$. Similar row vectors in $\mathbb{R}^n$ are matrices in $\mathbb{R}^{1\times n}$. We denote the rows and columns of $A$ by $A_{k,\cdot}$ for $k = 1, ..., m$ and $A_{\cdot,\ell}$ for $\ell = 1, ..., n$, respectively.

If $A \in \mathbb{R}^{m\times n}$ and $x \in \mathbb{R}^n$ we define the product $Ax$ (again refer back to 1.2.5) to be the linear combination $x_1 A_{\cdot,1} + ... + x_n A_{\cdot,n}$, i.e., the vector

$$\begin{pmatrix} A_{1,1}x_1 + ... + A_{1,n}x_n \\ \vdots \\ A_{m,1}x_1 + ... + A_{m,n}x_n \end{pmatrix} \in \mathbb{R}^m.$$

Note that $A$ transforms the vector $x \in \mathbb{R}^n$ into a vector in $\mathbb{R}^m$.

Later we will introduce a more general product of matrices with matrices.

[3] The entries of a matrix could also be other entities, e.g., elements of other fields but $\mathbb{R}$, functions, or matrices.

**1.3.7 Augmented matrices.** When we are trying to solve the system $Ax = b$ by elimination (and back-substitution) we leave the unknowns unaffected. Indeed, instead of adding a multiple of one equation to another, we can perform the corresponding operation on the matrix $A$ and the vector $b$ only. To do so in one swoop, we define the augmented matrix $(A, b)$ whose first $n$ columns are those of $A$ (in the given order) and whose last column is $b$.

EXERCISE. For the system given in 1.2.5 find the corresponding augmented matrix.

**1.3.8 Row-echelon matrices.** A row of a matrix is called a *zero row*, if all its entries are 0. Otherwise it is called a *non-zero row*. A matrix is said to be a *row-echelon matrix* if it satisfies the following two conditions:

(1) All zero rows occur below any other.
(2) The first non-zero entry of each non-zero row occurs to the right of the first non-zero entry of any previous row.

The first non-zero entry of a non-zero row in a row-echelon matrix is called a *pivot*. The number of pivots of a row-echelon matrix $R$ is called the *rank* of $R$.

EXERCISE. Which the following matrices are not row-echelon matrices? Explain. Identify the pivots in those matrices which are row-echelon matrices.

$$\begin{pmatrix}1&1&1\\2&2&2\\0&0&0\end{pmatrix} \quad \begin{pmatrix}0&1&2\\0&0&2\\0&0&0\end{pmatrix} \quad \begin{pmatrix}0&0&0\\1&1&1\\0&2&2\end{pmatrix} \quad \begin{pmatrix}1&2&3\\0&4&5\\0&0&6\end{pmatrix} \quad \begin{pmatrix}0&1&2\\0&0&3\\1&0&0\end{pmatrix} \quad \begin{pmatrix}1&1&2\\0&0&2\\0&0&0\end{pmatrix}$$

**1.3.9 Gaussian elimination.** To the operations among equations listed in 1.2.3 correspond operations on the rows of the augmented matrix. Hence, for given a matrix $M$, we define the *elementary row operations*:

(1) Exchange any two of the rows of $M$.
(2) Add a multiple of one row to another one.

Two matrices are called *row-equivalent*, if it is possible to transform one into the other by a finite sequence of elementary row operations.

It is now clear (why?) that the matrices $(A, b)$ and $(A', b')$ are row-equivalent if and only if the systems $Ax = b$ and $A'x = b'$ are equivalent.

EXERCISE. Use elementary row operations to turn the matrices in Exercise 1.3.8 into row-echelon form.

**1.3.10 Gaussian elimination is always successful.**

THEOREM. Every matrix $M$ is row-equivalent to a row-echelon matrix $R$.

SKETCH OF PROOF. The proof is simply an induction on the number of rows. □

## 1.4. Back to systems of linear equations

**1.4.1 Free unknowns.** If the augmented matrix $(A, b)$ is in row-echelon form so is $A$ itself. There may be columns of $A$ which do not contain a pivot. If column $j$ does not contain a pivot, then the $j$-th unknown is called *free*.

**1.4.2 Solving systems of linear equations.** We can now describe an algorithm to solve $Ax = b$, a linear system of $m$ equations in $n$ unknowns. First, using elementary row operations, transform the augmented matrix $(A, b)$ into a row-equivalent one in row-echelon form, say $(A', b')$. If $A'$ has a zero row where the entry of $b'$ in the same row is not 0, i.e.,

$b'$ contains a pivot, then there is no solution of the system. Otherwise one may choose the free unknowns freely and determine the others by back substitution. In particular, if there are no free unknowns, then there is a unique solution of the system.

In summary we have the following trichotomy (compare with 1.1.1):

(1) If $b'$ contains a pivot, then there is no solution at all.
(2) if $b'$ contains no pivot and $A'$ contains $n$ pivots, then there is a unique solution.
(3) if $b'$ contains no pivot and $A'$ contains less than $n$ pivots, then there are infinitely many solutions.

The situation just described can also be expressed by the following table.

| | $Ax = b = 0$ | $Ax = b \neq 0$ |
|---|---|---|
| $\operatorname{rank}(A', b') > \operatorname{rank} A'$ | does not happen | system is unsolvable |
| $\operatorname{rank}(A', b') = \operatorname{rank} A' = n$ | $x = 0$ is the unique solution | system is uniquely solvable |
| $\operatorname{rank}(A', b') = \operatorname{rank} A' < n$ | non-trivial solutions exist | many solutions exist |

Note that the only operations on the matrix entries are addition, multiplication, and division (by the pivots). These operations are possible in any field and therefore our conclusions hold for linear systems where the coefficients are taken from an arbitrary field.

CHAPTER 2

# Vector spaces

## 2.1. Spaces and subspaces

**2.1.1 Vector spaces.** Let $V$ be a set and let $K$ be a field[1]. Suppose there is a binary operation on $V$ (denoted by $+$) and a function $\sigma$ from $K \times V$ to $V$ (denoted by juxtaposition) such that the following properties are satisfied:
(a) $x + y \in V$ and $rx \in V$ for all $r \in K$ and all $x, y \in V$.
(b) $(x + y) + z = x + (y + z)$ for all $x, y, z \in V$ (the associative law).
(c) $x + y = y + x$ for all $x, y \in V$ (the commutative law).
(d) There is a vector 0 such that $x + 0 = x$ for all $x \in V$ (existence of the zero vector).
(e) For each $x \in V$ there is a vector $y$ such that $x + y = 0$ (existence of the negative).
(f) $(r + s)x = rx + sx$ for all $r, s \in K$ and all $x \in V$.
(g) $r(x + y) = rx + ry$ for all $r \in K$ and all $x, y \in V$.
(h) $(rs)x = r(sx)$ for all $r, s \in K$ and all $x \in V$.
(i) $1x = x$ for all $x \in V$.
Then $(V, K, +, \sigma)$ (or just $V$ to save space) is called a *vector space* over $K$. If $K = \mathbb{R}$ we call $V$ a real vector space and if $K = \mathbb{C}$ we call $V$ a complex vector space. The elements of $V$ are called *vectors* and the elements of $K$ are called *scalars*. The binary operation $+$ is called *(vector) addition*. The map $(r, x) \mapsto rx$ is called *scalar multiplication*. We use the same symbol for the vector 0 and the scalar 0. It is always clear from the context which one is meant.

We have already seen that the euclidean spaces $\mathbb{R}^n$ in 1.3.2 satisfy all the axioms listed above. Therefore euclidean spaces are vector spaces. In the same way one sees that $\mathbb{C}^n$ (whose elements are ordered lists of $n$ complex numbers) is a vector space for every natural number $n$. We emphasize, however, that there are other vector spaces, too, as we see next.

**2.1.2 Spaces of functions.** Suppose $X$ is a set, $K$ is a field, and consider the set of all functions defined on $X$ with values in $K$. To refer to this set we use the symbol $K^X$. If $f$ and $g$ are two functions in $K^X$ we add them as usual, i.e., $f + g$ is defined by $(f + g)(x) = f(x) + g(x)$ where $x$ varies in the set $X$. We also define a scalar multiplication: if $\alpha \in K$ we define the function $\alpha f$ by setting $(\alpha f)(x) = \alpha f(x)$ for all $x \in X$. With these two operations $K^X$ becomes a vector space.

We could, for example, have $X = (0, 1)$ and $K = \mathbb{R}$. Then $K^X$ is the set of all real-valued functions on the interval $(0, 1)$.

**2.1.3 The trivial vector space.** The set $\{0\}$ becomes a vector space, if we define $0+0 = 0$ and, for all $r \in K$, $r0 = 0$. It is then called the *trivial vector space*.

[1] We will use only $\mathbb{R}$ or $\mathbb{C}$ for $K$ but the definition is more general.

**2.1.4 Some basic facts.** Only one vector has the properties of the 0 vector and every vector has precisely one negative. The negative of $x$ and is denoted by $-x$. As a consequence, we also have that $-(-x) = x$.

For all $x \in V$ and all $r \in K$ we have $rx = 0$ if and only if $r = 0$ or $x = 0$. Moreover, $-x = (-1)x$.

Sketch of proof. To show the uniqueness of the zero vector assume there were at least two, say 0 and $e$. Then, using the vector space axioms (and only those), show that $e = 0$. The proof of uniqueness of the negative of a given vector $x$ follows a similar line of reasoning. To prove that $rx = 0$ if $r = 0$ or $x = 0$ one uses the fact that $0 + 0 = 0$ (which is true for the scalar 0 as well as the vector 0) and the existence of negatives. For the converse assume $rx = 0$. If $r \neq 0$ use that $r$ has a reciprocal. The last claim follows since $1 - 1 = 0$. □

**2.1.5 Subspaces.** A subset of a vector space $V$ which is itself a vector space (with respect to the operations in $V$) is called a *subspace* of $V$.

A nonempty subset $S$ of a vector space $V$ is a subspace of $V$ if and only if $\alpha x + \beta y \in S$ whenever $x, y \in S$ and $\alpha, \beta \in K$, the scalar field.

The intersection of a nonempty collection of subspaces of $V$ is again a subspace of $V$.

Exercise. Show the following claims:

(1) The set $\{(x_1, x_2)^\top \in \mathbb{C}^2 : x_1 = 2x_2\}$ is a subspace of $\mathbb{C}^2$.
(2) The set of real-valued differentiable functions defined on an interval $(a, b)$ is a subspace of the set of all real-valued functions on $(a, b)$.
(3) The set of real polynomial functions is a subspace of the set of all real-valued functions on $\mathbb{R}$.
(4) The set of polynomial functions on $\mathbb{R}$ (or $\mathbb{C}$) of degree at most $n$ is a subspace of the set of all polynomial functions on $\mathbb{R}$ (or $\mathbb{C}$).

## 2.2. Linear independence and spans

**2.2.1 Linear combinations.** If $x_1, ..., x_n$ are elements of a vector space $V$ and if $\alpha_1, ..., \alpha_n$ are scalars, then the vector

$$\alpha_1 x_1 + ... + \alpha_n x_n$$

is called a *linear combination* of $x_1, ..., x_n$.

If the vectors $x_1$, ..., $x_n$ are in a subspace $U$ of $V$, then so is any linear combination of these vectors.

**2.2.2 Linearly independent vectors.** Let $V$ be a vector space. The vectors $x_1, ..., x_n \in V$ are called *linearly independent* if $\alpha_1 x_1 + ... + \alpha_n x_n = 0$ implies that $\alpha_1 = ... = \alpha_n = 0$. Otherwise they are called *linearly dependent*. A set $M \subset V$ is called linearly independent if any finite number of pairwise distinct elements of $M$ are linearly independent. Otherwise $M$ is called linearly dependent. In particular, the empty set is linearly independent and a set consisting of precisely one element is linearly independent if and only if that element is not the zero vector. Moreover, any set containing the zero vector is linearly dependent. If $A \subset B$ and $B$ is linearly independent then so is $A$.

The vectors $x_1, ..., x_n$ are linearly dependent if and only if one of them can be expressed as a linear combination of the others.

EXERCISE. Show that the vectors $(3,5)$ and $(0,-2)$ are linearly independent but that the vectors $(3,5)$, $(0,-2)$, and $(1,1)$ are linearly dependent. Also show that the polynomials $2x+1$ and $x^2$ are linearly independent.

**2.2.3 Spans.** Let $A$ be a subset of $V$. Let $\mathcal{C}$ be the collection of all subspaces of $V$ which include $A$. Then the set $\operatorname{span} A = \bigcap_{S\in\mathcal{C}} S$ is a subspace of $V$ called the *span* of $A$. We also say that a vector space $W$ is spanned by $A$ or that $A$ spans (or that the elements of $A$ span) $W$ if $W = \operatorname{span} A$.

THEOREM. If $A = \emptyset$ then $\operatorname{span} A = \{0\}$. Otherwise $\operatorname{span} A$ is the set of all linear combinations of elements of $A$.

SKETCH OF PROOF. First note that $\operatorname{span} A$ is a subspace and that $A \subset \operatorname{span} A$. Let $U$ be the set of all linear combinations of (finitely many) elements of $A$. From 2.2.1 we get $U \subset \operatorname{span} A$. But $U$ is itself a subspace of $V$ (using 2.1.5) and we have $A \subset U$, implying that $\operatorname{span} A \subset U$. □

**2.2.4 Dimension of a vector space.** To any vector space $V$ we assign a *dimension* denoted by $\dim V$. To the trivial vector space $\{0\}$ we assign dimension 0. If a vector space has a finite subset which spans it, it is called *finite-dimensional*. In this case its dimension is defined to be the number of elements of the smallest spanning set (ordering spanning sets by the number of their elements). In all other cases the vector space is called *infinite-dimensional* and we say it has dimension $\infty$.

EXERCISE. Find the dimension of $\mathbb{R}^2$ and the dimension of the space of polynomials of degree at most 4. What is the dimension of the space of all polynomials?

**2.2.5 Bases.** A set $B \subset V$ is called a *basis* of the non-trivial vector space $V$, if it is linearly independent and spans $V$. This is equivalent to the statement that every $x \in V$ can be expressed uniquely as a linear combination of the elements of $B$. The empty set is a basis of the trivial vector space.

**2.2.6 Ordered bases.** Sometimes we might want to think of the elements of a basis to be arranged in a certain order. Therefore we introduce the concept of an *ordered basis*: if $V$ is a finite-dimensional vector space we call $(v_1, ..., v_n) \in V^n$ an ordered basis, if $v_1, ..., v_n$ are pairwise distinct and form a basis of $V$.

**2.2.7 The canonical basis of $K^n$.** Let $\delta_k \in K^n$ be the vector whose entries are all 0 except for a 1 in position $k$, e.g. $\delta_1 = (1,0,...,0)^\top$, $\delta_3 = (0,0,1,0,...,0)^\top$, and $\delta_n = (0,...,0,1)^\top$. Then $\{\delta_1, ..., \delta_n\}$ is a linearly independent set spanning $K^n$ and hence a basis of $K^n$. It is called the *canonical basis* of $K^n$.

**2.2.8 Extending linearly independent sets.** Suppose the set $S$ spans the vector space $V$. If $L \subset S$ is a linearly independent set which does not span $V$, then there is a vector $x \in S$ such that $L \cup \{x\}$ is still linearly independent.

SKETCH OF PROOF. Since $L$ does not span $V$ there is a vector $v \in V$ which is not in the span of $L$. The vector $v$ is a linear combination (with non-zero coefficients) of finitely many elements of $S$. At least one of these, which we call $x$, cannot be in the span of $L$. It follows that $L \cup \{x\}$ is linearly independent. □

**2.2.9 Creating a basis from a spanning set.** Suppose $V$ is a vector space of dimension $n$ and $S$ is a finite spanning subset of $V$. Then $\#S \geq n$ and there is a basis $B$ of $V$ such that $B \subset S$.

SKETCH OF PROOF. If $n = 0$ (and hence $V = \{0\}$) we choose $B = \emptyset$ which finishes the proof in this case. Otherwise we now prove by induction that, for every $k \in \{1, ..., n\}$, the set $S$ contains a linearly independent set $S_k$ of $k$ elements: Since $S$ must contain a non-zero element $x_1$ we may choose $S_1 = \{x_1\}$. Now suppose we have already a linearly independent set $S_k \subset S$ such that $\#S_k = k$. If $S_k$ does not span $V$ we use 2.2.8 to join another element of $S$ to create $S_{k+1}$. Then $S_{k+1} = S_k \cup \{x_{k+1}\}$ is again a linearly independent set and we proceed to the next number. Since $S$ is a finite set the process must come to an end, i.e., for some $\ell$ the set $S_\ell$ spans $V$. Thus $\#S \geq \#S_\ell \geq n$. Choosing $B = S_\ell$ we have a basis of $V$. □

COROLLARY. Every finite-dimensional vector space has a basis.

**2.2.10 Creating a basis from a linearly independent set.** Let $V$ be a vector space of dimension $n$ and $L$ a linearly independent subset of $V$. Then $\#L \leq n$ and there is a basis $B$ of $V$ such that $L \subset B$.

SKETCH OF PROOF. If $L$ spans $V$ it is a basis. Otherwise let $S$ be a finite spanning set and note that $L \cup S$ is also a spanning set. The proof may now be completed with the help of 2.2.8. □

**2.2.11 The number of elements in a basis.** Every basis of an $n$-dimensional vector space has precisely $n$ elements.

SKETCH OF PROOF. Suppose $V$ is a vector space, $\dim V = n$, and $B$ is a basis of $V$. Since $B$ spans $V$ we get from 2.2.9 that $\#B \geq n$. Since $B$ is linearly independent we get from 2.2.10 that $\#B \leq n$. □

Moreover, if $V$ is an $n$-dimensional vector space and $A \subset V$ has $n$ elements, the following statements hold.

(1) If $A$ spans $V$, it is linearly independent and hence a basis of $V$.
(2) If $A$ is a linearly independent, then it spans $V$ and hence is a basis of $V$.

## 2.3. Direct sums

**2.3.1 External direct sums of vector spaces.** Let $V$ and $W$ be two vector spaces over the field $K$ and consider the cartesian product $V \times W$, i.e., the set $\{(v, w) : v \in V, w \in W\}$. For $V \times W$ we define an addition and a scalar multiplication by setting $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$ and, for $r \in K$, $r(v, w) = (rv, rw)$. With these operations $V \times W$ becomes a vector space. It is called the *(external) direct sum* of $V$ and $W$ and denoted by $V \uplus W$.

THEOREM. The dimension of a direct sum of two vector spaces $V$ and $W$ satisfies $\dim(V \uplus W) = \dim V + \dim W$.

SKETCH OF PROOF. Let $B_1$ be a linearly independent subset of $V$ and $B_2$ a a linearly independent subset of $W$. Define $A_1 = \{(v, 0) : v \in B_1\}$, $A_2 = \{(0, w) : w \in B_2\}$ and $B = A_1 \cup A_2$. Then $B$ is a linearly independent subset of $V \uplus W$. This proves the claim when one of $V$ and $W$ is infinite-dimensional. Otherwise, choose $B_1$ and $B_2$ as bases to obtain a basis $B$ of $V \uplus W$. □

**2.3.2 Internal sums of subspaces.** Let $X$ and $Y$ be two subspaces of a vector space $V$. The union of $X$ and $Y$ is not necessarily a subspace of $V$. We define the *(internal) sum* of $X$ and $Y$ to be the subspace generated by their union, i.e., $X + Y = \text{span}(X \cup Y)$. It turns

out that $X + Y = \{x + y : x \in X, y \in Y\}$ and hence $X + Y = Y + X$. The dimension of $X + Y$ is infinite if at least one of $X$ and $Y$ has infinite dimension. Otherwise it is given by

$$\dim(X + Y) = \dim X + \dim Y - \dim(X \cap Y).$$

**2.3.3 Internal direct sums od subspaces.** Let $X$ and $Y$ be two subspaces of a vector space $V$. The internal sum $X + Y$ is called *direct*, if $X \cap Y = \{0\}$. To emphasize this we write $X \uplus Y$ instead of $X + Y$.[2]

THEOREM. Let $X$ be a subspace of a finite-dimensional vector space $V$. Then there exists a subspace $Y$ such that $X \cap Y = \{0\}$ and $X \uplus Y = V$.

SKETCH OF PROOF. Let $A$ be a basis of $X$. By Theorem 2.2.10 there is a basis $C$ of $V$ such that $A \subset C$. Define $B = C \setminus A$ and $Y = \operatorname{span} B$. Then $Y$ is a subspace of $V$ and $X \cap Y = \{0\}$. Also, since $C = A \cup B$ spans $V$ we get that $X + Y = V$. □

[2]The internal direct sum of $X$ and $Y$ is isomorphic (see 3.1.1) to their (external) direct sum. This justifies using the same notation.

CHAPTER 3

# Linear transformations

## 3.1. Basics

**3.1.1 Linear transformations.** Let $V$ and $W$ be two vector spaces over the same field $K$. The function $F : V \to W$ is called a *linear transformation*, if

$$F(\alpha x + \beta y) = \alpha F(x) + \beta F(y)$$

for all $\alpha, \beta \in K$ and all $x, y \in V$. In particular, $F(0) = 0$ and $F(-x) = -F(x)$.

Since $F$ distributes over sums like multiplication, it is customary to write $Fx$ in place of $F(x)$. We will also do so frequently.

**3.1.2 Examples.** We have the following simple examples:

(1) The multiplication of a $A \in \mathbb{R}^{m\times n}$ by a column vector $x \in \mathbb{R}^n$ as defined in 1.3.6 gives rise to a linear transformation from $\mathbb{R}^n$ to $\mathbb{R}^m$. Here we may, of course, replace $\mathbb{R}$ by any field $K$.
(2) The derivative is a linear transformation from the vector space of continuously differentiable functions on the real interval $(a, b)$ to the vector space of continuous functions on $(a, b)$.
(3) Multiplication with $x \mapsto x^2 + 1$ is a linear transformation from the space of polynomial functions, to itself.

**3.1.3 Kernel and range.** The *kernel* of a linear transformation $F : V \to W$ is the set $\{x \in V : F(x) = 0\}$, i.e., the set of all elements of the domain which are mapped to 0.

The *range* of a linear transformation $F : V \to W$ is the set $\{F(x) : x \in V\}$ of all images of $F$.

Kernel and range of $F$ are subspaces of $V$ and $W$, respectively. The former is denoted by $\ker F$ and the latter by $\operatorname{ran} F$ or by $F(V)$. The dimension of $\ker F$ is called the *nullity* of $F$ while the dimension of $\operatorname{ran} F$ is called the *rank* of $F$.

Exercise. Find kernel and range of the following linear transformations: (1) the matrix $\left(\begin{smallmatrix} 2 & -2 \\ 3 & -3 \end{smallmatrix}\right)$ and (2) the derivative as described in 3.1.2.

**3.1.4 Inverse transformations.** A linear transformation $F$ is injective if and only if $\ker F = \{0\}$.

If $F : V \to W$ is a bijective linear transformation, then it has a unique *inverse* $F^{-1} : W \to V$. $F^{-1}$ is again a linear transformation.

Sketch of proof. Denote the inverse function of $F$ by $G$. Suppose $a, b \in W$ and $\alpha, \beta \in K$. Let $x = G(a)$ and $y = G(b)$. Then we have

$$G(\alpha a + \beta b) = G(\alpha F(x) + \beta F(y)) = G(F(\alpha x + \beta y)) = \alpha x + \beta y = \alpha G(a) + \beta G(b)$$

since $a = F(x)$ and $b = F(y)$. □

**3.1.5 Projections.** A linear transformation $P : V \to V$ is called *idempotent* or a *projection*, if $P^2 = P$. $P$ is a projection if and only if $\mathbb{1} - P$ is one.

Note that $x \in \operatorname{ran} P$ if and only if $Px = x$ and that $\operatorname{ran} P \cap \ker P = \{0\}$.

**3.1.6 Isomorphisms.** A *bijective* linear transformation from $V$ to $W$ is called a (vector space) *isomorphism*. Two vector spaces $V$ and $W$ are called *isomorphic* if there exists an isomorphism from $V$ to $W$.

EXERCISE 1. Show that the spaces $\mathbb{R}^X$ for $X = \{1, 2\}$ and $X = \{5, 7\}$ (recall Exercise 2.1.2) are isomorphic.

EXERCISE 2. Let $X$ and $Y$ be two subspaces of a finite-dimensional vector space $V$ such that $X \cap Y = \{0\}$. Show that their internal direct sum and their external direct sum are isomorphic.

## 3.2. The fundamental theorem of linear algebra

**3.2.1 Linear transformations and bases.** Suppose $V$ and $W$ are vector spaces and $B$ is a basis of $V$. Then any function from $B$ to $W$ extends uniquely to a linear transformation from $V$ to $W$. In particular, any linear transformation is uniquely determined by the images of a basis of the domain of the transformation.

SKETCH OF PROOF. Denote the given function from $B$ to $W$ by $f$. Define $g$ on $V$ by $g(\alpha_1 x_1 + ... + \alpha_n x_n) = \alpha_1 f(x_1) + ... + \alpha_n f(x_n)$ where $\{x_1, ..., x_n\} \subset B$. Then $g$ is a linear transformation from $V$ to $W$. It is the only linear transformation whose restriction to $B$ is equal to $f$. □

**3.2.2 The fundamental theorem of linear algebra.** The dimensions of the kernel and the image of a linear transformation are not independent as the following theorem shows. This theorem is sometimes called the *fundamental theorem of linear algebra* or the *rank-nullity theorem*.

THEOREM. Suppose $V$ is a finite-dimensional vector space. Let $F : V \to W$ be a linear transformation. Then $\dim \operatorname{ran} F + \dim \ker F = \dim V$.

SKETCH OF PROOF. Since $\ker F \subset V$ we have $\dim \ker F \leq \dim V = n < \infty$. Assume that $\dim \ker F = k$ and that $B = \{b_1, ..., b_k\}$ is a basis of $\ker F$. By Theorem 2.3.3 there exists a subspace $Y$ of $V$ such that $\ker F \uplus Y = V$. Let $C$ be a basis of $Y$. We show below that $F(C)$ is a basis of $F(V)$ and that it has $n - k$ elements. Hence $\dim F(V) = n - k$ proving the theorem, provided $F(C)$ is, as claimed, a basis of $F(V)$.

If $C = \{c_1, ..., c_{n-k}\}$ let $w_k = F(c_k)$. Consider the equation $\alpha_1 w_1 + ... + \alpha_{n-k} w_{n-k} = 0$. Then $x = \alpha_1 c_1 + ... + \alpha_{n-k} c_{n-k} \in \ker F$, i.e., $x \in Y \cap \ker F$ and hence $x = 0$. This shows that all coefficients $\alpha_j$ are 0 and hence that $\{w_1, ..., w_{n-k}\}$ is a linearly independent set.

Let $w \in F(V)$. Then $w = F(v)$ for some $v \in V$. Hence $v = x + y$ where $x \in \ker F$ and $y \in Y$. But this shows that $F(v) = F(y)$ since $F(x) = 0$. Hence $F(C)$ spans $F(Y) = F(V)$. □

**3.2.3 Consequences.** Let $F$ be a linear transformation between finite-dimensional vector spaces $V$ and $W$ and suppose $B$ is a basis of $V$. Then the following statements are true.

(1) $\dim F(V) \leq \dim V$ and $\dim F(V) \leq \dim W$.
(2) $F$ is injective if and only if $F|_B$ is injective and $F(B)$ is linearly independent.
(3) $F$ is surjective if and only if $F(B)$ spans $W$.
(4) $F$ is injective if and only if $\dim F(V) = \dim V$.

(5) $F$ is surjective if and only if $\dim F(V) = \dim W$.
(6) If $V$ is finite-dimensional and $P$ is a projection, then $\operatorname{ran} P \uplus \ker P = V$.

## 3.3. The algebra of linear transformation

**3.3.1 The vector space of linear transformations.** Suppose $V$ and $W$ are two vector spaces over $K$. We denote the set of all linear transformations from $V$ to $W$ by $\mathcal{L}(V, W)$. On $\mathcal{L}(V, W)$ we define an addition and a scalar multiplication as follows. If $F, G \in \mathcal{L}(V, W)$ and $\alpha \in K$ let $(F + G)(x) = F(x) + G(x)$ and $(\alpha F)(x) = \alpha F(x)$ for all $x \in V$. Then $F + G$ and $\alpha F$ are again in $\mathcal{L}(V, W)$. In fact, $\mathcal{L}(V, W)$ becomes a vector space when doing so.

**3.3.2 Compositions of linear transformations.** Suppose $U$, $V$, and $W$ are vector spaces over $K$. If $F : U \to V$ and $G : V \to W$ are linear transformations we define

$$(G \circ F)(x) = G(F(x))$$

for all $x \in U$. Then $G \circ F$, the composition of $G$ and $F$, is a linear transformation from $U$ to $W$. Note that it makes no sense to define $F \circ G$ unless $W \subset U$.

For simplicity one often writes $GF$ in place of $G \circ F$ and $F^2$ in place of $F \circ F$. Analogous conventions are used, of course, for other powers.

## 3.4. Linear transformations and matrices

**3.4.1 Coordinates.** Let $V$ be a vector space over $K$ of dimension $n$ and $a = (a_1, ..., a_n)$ an ordered basis of $V$. If $x$ is an element of $V$, the (uniquely determined) coefficients $\alpha_1$, ..., $\alpha_n$ in the representation $x = \alpha_1 a_1 + ... + \alpha_n a_n$ are called the *coordinates* of $x$ with respect to the ordered basis $a$. The vector $(\alpha_1, ..., \alpha_n)^\top \in K^n$ of coordinates is denoted by $x_a$.

If $V = K^n$ we have to distinguish between an element $x$ of $V$ which is denoted by $(x_1, ..., x_n)^\top$ and the list $x_a$ of coordinates of $x$ with respect to some ordered basis $a$ of $K^n$. However, if $a$ is the canonical basis, then $x = x_a$.

Exercise. Show that the vectors $(1, 2, 1)^\top$, $(1, 2, 2)^\top$, and $(0, 2, 2)^\top$ form a basis of $\mathbb{R}^3$. Then find the list of coordinates of the vector $(2, 0, 2)^\top$ with respect to that basis.

**3.4.2 Matrices and linear transformations between euclidean spaces.** Let $M$ be a matrix in $K^{m\times n}$. As mentioned in 3.1.2 (and, indeed, in 1.3.6) the multiplication of $M$ by a column vector $x \in K^n$ gives rise to a linear transformation $T$ from $K^n$ to $K^m$. Note that $T(\delta_k)$ is the $k$-th column of $M$. Conversely, assume that $T : K^n \to K^m$ is a linear transformation. Collect the vectors $T(\delta_1)$, ..., $T(\delta_n)$ in a matrix $M \in K^{m\times n}$ and note that $T(x) = Mx$ for all $x \in K^n$. This shows that matrices in $K^{m\times n}$ and linear transformations from $K^n$ to $K^m$ are in one-to-one correspondence and one frequently identifies matrices with their corresponding linear transformations.

**3.4.3 Matrices and general linear transformations.** Let $V$ and $W$ be finite-dimensional vector spaces of dimensions $n$ and $m$, respectively, and $F$ a linear transformation from $V$ to $W$. Choose an ordered basis $a = (a_1, ..., a_n)$ for $V$ and an ordered basis $b = (b_1, ..., b_m)$ for $W$ and define bijections $S : K^n \to V$ and $T : K^m \to W$ by setting $S\delta_k = a_k$ for $k = 1, ..., n$ and $T\delta_j = b_j$ for $j = 1, ..., m$.[1] Then $M = T^{-1}FS$ is a linear transformation from $K^n$ to $K^m$ which we identify, according to our discussion in 3.4.2, with a matrix in $K^{m\times n}$ also

[1] The vectors in the domains of $S$ and $T$ have different lengths if $m \neq n$, i.e., the symbol $\delta_\ell$ may denote different vectors. Instead of introducing more cumbersome notation we emphasize that the context makes the precise meaning of $\delta_\ell$ clear.

denoted by $M$. Thus every linear transformation between finite-dimensional vector spaces can be represented by a matrix after specifying bases in domain and range.

EXERCISE 1. Suppose $T : \mathbb{R}^2 \to \mathbb{R}^2$ maps the vectors $(1, 2)^\top$ and $(2, 3)^\top$ to the vectors $(-1, 1)^\top$ and $(-1, 2)^\top$, respectively. Find the matrix representing $T$ with respect to the canonical basis in $\mathbb{R}^2$.

EXERCISE 2. Identify a basis in the space $V$ of all polynomials of degree at most 3 and determine the matrix which represents taking a derivative viewed as a transformation from $V$ to $V$.

**3.4.4 Representations with respect to different bases.** Let $V$, $W$, and $F$ be as in 3.4.3. As we saw, ordered bases $(a_1, ..., a_n)$ and $(b_1, ..., b_m)$ chosen in $V$ and $W$ allow the representation of $F$ by a matrix $M = T^{-1}FS$. Using different bases $(\tilde{a}_1, ..., \tilde{a}_n)$ and $(\tilde{b}_1, ..., \tilde{b}_m)$ instead yields a different matrix $\tilde{M} = \tilde{T}^{-1}F\tilde{S}$. The connection between $M$ and $\tilde{M}$ is therefore given by

$$\tilde{M} = R^{-1}MQ$$

where $R = T^{-1}\tilde{T}$ and $Q = S^{-1}\tilde{S}$. Note that $Q$ and $R$ are linear transformations from $K^n \to K^n$ and $K^m \to K^m$, respectively.

The entries of $Q$ describe the change of bases in $V$ since $\tilde{a}_k = \sum_{\ell=1}^{n} Q_{\ell,k}a_\ell$. Similarly, the entries of $R$ describe the change of bases in $W$.

It might be mentioned here that, when $V = W$ one typically chooses the same basis in domain and range and, when changing bases, one uses the same transformation in domain and range. Hence, in this case, one has $R = Q$ and $\tilde{M} = Q^{-1}MQ$. In Chapter 5 we will be concerned with the question of how to choose a basis so that the matrix representing a linear transformation $T : V \to V$ is particularly simple.

## 3.5. Matrix algebra

**3.5.1 Vector spaces of matrices.** We saw in 3.3.1 that the linear transformations between two vector spaces (over the same field) form a vector space themselves. This fact is reflected in the associated matrices (assuming finite-dimensional spaces).

To be more precise suppose we have two vector spaces $V$ and $W$ of dimensions $n$ and $m$, respectively. Let $\alpha$ be a scalar and $F$ and $G$ linear transformations from $V$ to $W$ represented by matrices $M$ and $N$ (after having chosen ordered bases in $V$ and $W$). Then $\alpha F$ and $F + G$ are represented by the matrices $\alpha M$ and $M + N$, if we define scalar multiplication by multiplication of each matrix entry by $\alpha$ and matrix addition by adding corresponding entries of the matrices. Thus if

$$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,n} \\ \vdots & & \vdots \\ M_{m,1} & \cdots & M_{m,n} \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} N_{1,1} & \cdots & N_{1,n} \\ \vdots & & \vdots \\ N_{m,1} & \cdots & N_{m,n} \end{pmatrix}$$

then

$$\alpha M = \begin{pmatrix} \alpha M_{1,1} & \cdots & \alpha M_{1,n} \\ \vdots & & \vdots \\ \alpha M_{m,1} & \cdots & \alpha M_{m,n} \end{pmatrix} \quad \text{and} \quad M + N \begin{pmatrix} M_{1,1} + N_{1,1} & \cdots & M_{1,n} + N_{1,n} \\ \vdots & & \vdots \\ M_{m,1} + N_{m,1} & \cdots & M_{m,n} + N_{m,n} \end{pmatrix}.$$

With the operations of scalar multiplication and addition thus defined the set of $m \times n$-matrices forms a vector space. In particular, matrix addition is associative and commutative.

The zero matrix (all entries are 0) is the additive identity. Replacing all entries of a matrix by their negatives gives the negative of the given matrix.

**3.5.2 Matrix multiplication.** The composition of linear transformations turns into a multiplication of matrices as we will see now. Let $F : U \to V$ and $G : V \to W$ be linear transformations between finite-dimensional vector spaces, each equipped with its ordered basis. If $\dim U = \ell$, $\dim V = m$, and $\dim W = n$, then $G$ is represented by an $n \times m$-matrix $N$ while $F$ is represented by an $m \times \ell$-matrix $M$. The composition $G \circ F$ is represented by the matrix $NM$, if we define a matrix product by

$$(NM)_{j,k} = \sum_{s=1}^{m} N_{j,s} M_{s,k}.$$

Note that it is necessary that the number of columns of $N$ equals the number of rows of $M$ in order to form the product $NM$. Also if $n = 1$, i.e., if $M$ is a vector in $K^m$ this definition of the product is in agreement with the one made in 1.3.6.

Matrix multiplication is associative but not commutative. In fact $MN$ might not even be defined even if $NM$ is.

**3.5.3 Distributive laws in matrix algebra.** We have the following distributive laws for matrices $A, B, C$ whenever it makes sense to form the sums and products in question: $(A + B)C = AC + BC$, $A(B + C) = AB + AC$, and $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

**3.5.4 Kernel and range of a matrix.** Since an $m \times n$-matrix may be considered as a linear transformation from $K^n$ to $K^m$ we may speak about their kernel and range. Specifically, if $M$ is an $m \times n$-matrix we get $\ker M = \{x \in K^n : Mx = 0\}$ and $\operatorname{ran} M = \{Mx : x \in K^n\}$. As before, $\ker M$ is a subspace of $K^n$ and $\operatorname{ran} M$ is a subspace of $K^m$. The rank-nullity theorem states that $\dim \ker M + \dim \operatorname{ran} M = n$. It is also useful to note that the range of $M$ is the span of its columns. It is therefore often called the column space of $M$.

**3.5.5 Rank of a matrix.** Recall from 3.1.3 that the dimension of the range of a linear transformation is called its *rank*. Thus the rank of a matrix $M$ is the dimension of its column space and is equal to the number of linearly independent columns of $M$, It is therefore sometimes called *column rank* of the matrix.

We may of course also consider the span of the rows of $M$. Its dimension is called the *row rank* of $M$. However, we have been too careful here as the following theorem shows.

THEOREM. Let $M$ be a matrix and $R$ a row-echelon matrix which is row-equivalent[2] to $M$. The row rank and the column rank of $M$, the row rank and the column of $R$ and the number of pivots of $R$ are all identical.

SKETCH OF PROOF. The elementary row operations leave the number of linearly independent rows of a matrix invariant as they do not change the space spanned by these rows. Hence the row ranks of $M$ and $R$ coincide. Since the systems $Mx = 0$ and $Rx = 0$ are equivalent, we have $\ker M = \ker R$ so that by the rank-nullity theorem we find that the column ranks of $M$ and $R$ also coincide. The proof is completed by the observation that column rank and row rank of $R$ are equal to the number of pivots of $R$. □

**3.5.6 Square matrices.** A matrix is called a *square matrix* if it has as many columns as it has rows. The elements $M_{1,1}$, ..., $M_{n,n}$ of an $n \times n$-matrix are called *diagonal elements*

[2]The terms row-echelon matrix and row equivalence can easily be defined for matrices with complex entries (or entries in any field) and we also get the validity of Theorem 1.3.9.

and together they form the *main diagonal* of the matrix. A matrix is called a *diagonal matrix*, if its only non-zero entries are on the main diagonal. Such a matrix is denoted by $\operatorname{diag}(a_1, ..., a_n)$, when $a_1$, ..., $a_n$ are its entries along the diagonal (in that order).

The *identity transformation* $F(x) = x$ defined on an $n$-dimensional vector space is represented by the *identity matrix* $\mathbb{1}$ which is an $n \times n$-matrix all of whose entries are 0 save for the ones on the main diagonal which are 1.

**3.5.7 Inverse of a matrix.** Suppose $A$ is an $m \times n$ matrix. If $m < n$ the rank-nullity theorem shows that $\ker A$ cannot be trivial and hence $A$ cannot be injective If $m > n$ then $\dim \operatorname{ran} A \leq n < m$ and hence $A$ cannot be surjective. If $m = n$, we have the following theorem.

THEOREM. If $A$ is a square matrix such that $\ker A = \{0\}$, then it has a unique inverse denoted by $A^{-1}$ such that $AA^{-1} = A^{-1}A = \mathbb{1}$.

SKETCH OF PROOF. By 3.2.3 the transformation $A : K^n \to K^n$ is not only injective but also surjective. Hence, according to 3.1.4 $A : K^n \to K^n$ has a unique inverse transformation $B$ such that $BA = \mathbb{1}$. $B$ also has an inverse transformation $C$ such that $CB = \mathbb{1}$. These imply $C = C(BA) = (CB)A = A$. □

Note that, even though multiplication is, in general, not commutative, left and right inverse of an invertible matrix are the same.

The inverse of an $n \times n$-matrix may be computed by solving $n$ linear systems of $n$ equation. In fact, $\delta_k$ the $k$-th column of $\mathbb{1}$ is obtained by multiplying the matrix $A$ with the $k$-th column of $A^{-1}$. Hence the unique solution of $Ax = \delta_k$ is the $k$-th column of $A^{-1}$.

**3.5.8 Structure of the set of solutions of a system of linear equations.** In 1.4.2 we described how to find solutions of $Ax = b$, a linear system of equations where $A$ is an $m \times n$-matrix and $b$ a vector of length $m$. In particular, it showed when to expect existence and uniqueness.[3] We will now investigate the solution set in a little more detail.

First assume that the system is *homogeneous*, i.e., that $b = 0$. In this case the set of solutions is a subspace of $K^n$, namely $Ax = 0$ if and only if $x \in \ker A$. The rank-nullity theorem shows that $\dim \ker A = n - \dim \operatorname{ran} A$. Hence, if $\dim \operatorname{ran} A$, the rank of $A$, is equal to $n$, then $\ker A$ is trivial and we have a unique solution, namely the trivial solution. In particular, $m < n$ implies (not surprisingly, that there are non-trivial solutions.

If $b \neq 0$, the system is called *non-homogeneous*. Note that $Ax$ is a linear combination of the columns of $A$. Hence there will be a solution of $Ax = b$ only if $b$ is in the span of the columns of $A$. Now suppose $x_p$ is a (known) solution of $Ax = b$, i.e., we have $Ax_p = b$. Another solution $x$, if any, has to satisfy $Ax = b = Ax_p$ and hence $A(x - x_p) = 0$. Thus the set of solutions of $Ax = b$ is given by $\{x_h + x_p : x_h \in \ker A\}$. In particular, if the rank of $A$ is $n$ or, equivalently, the kernel of $A$ is trivial, then there is only one solution, namely $x_p$.

[3] While 1.4.2 was formulated for systems with real coefficients everything works just the same for complex coefficients and indeed for coefficients in any field.

CHAPTER 4

# Inner product spaces

## 4.1. Inner products

**4.1.1 Inner products.** Let $V$ be a vector space over either the real or the complex numbers. A function $\langle \cdot, \cdot \rangle : V \times V \to K$ is called an *inner product* or a *scalar product* if it has the following properties:

(1) $\langle x, x \rangle \geq 0$ for all $x \in V$.
(2) $\langle x, x \rangle = 0$ if and only if $x = 0$.
(3) $\langle x, y \rangle = \overline{\langle y, x \rangle}$ for all $x, y \in V$.
(4) $\langle z, \alpha x + \beta y \rangle = \alpha \langle z, x \rangle + \beta \langle z, y \rangle$ for all $\alpha, \beta \in K$ and all $x, y, z \in V$.

Note that $y = 0$ if and only if $\langle x, y \rangle = 0$ for all $x \in V$.

If $K = \mathbb{R}$ the inner product is *bilinear* (linear in both of its arguments). If $K = \mathbb{C}$ the inner product is linear in its second argument but *anti-linear* in its first: $\langle \alpha x + \beta y, z \rangle = \overline{\alpha} \langle x, z \rangle + \overline{\beta} \langle y, z \rangle$.

If there exists an inner product $\langle \cdot, \cdot \rangle$ on $V$ then $(V, \langle \cdot, \cdot \rangle)$ is called an *inner product space*.

**4.1.2 Examples.** One may define inner products for $\mathbb{R}^n$ and $\mathbb{C}^n$ by setting $\langle x, y \rangle = \sum_{k=1}^{n} \overline{x_k} y_k$. This is the standard inner product (*dot product*) in $\mathbb{R}^2$ and $\mathbb{R}^3$.

Also $C^0([a, b])$, the space of continuous functions defined on the closed interval $[a, b]$ can be turned into an inner product space: For $f, g \in C^0([a, b])$ define $\langle f, g \rangle = \int_a^b \overline{f} g dx$.

**4.1.3 The Cauchy-Schwarz inequality.** The most important property of an inner product is the Cauchy-Schwarz inequality

$$|\langle x, y \rangle| \leq \langle x, x \rangle^{1/2} \langle y, y \rangle^{1/2},$$

which holds for any two vectors $x$ and $y$ in the space.

SKETCH OF PROOF. We may assume that $\langle x, y \rangle \neq 0$ and then define $\alpha = 1/\langle x, y \rangle$. For any real $r$ we have $0 \leq \langle x - r\alpha y, x - r\alpha y \rangle$. This is a quadratic polynomial in $r$ with real coefficients and its lowest value gives the inequality. □

**4.1.4 Inner products and norms.** Let $V$ be an inner product space and define the function $x \mapsto \|x\| = \langle x, x \rangle^{1/2}$. This assigns to every vector in $V$ a non-negative number called its *norm*. The norm has the following properties:

(1) $\|x\| \geq 0$ for all $x \in V$,
(2) $\|x\| = 0$ if and only if $x = 0$,
(3) $\|\alpha x\| = |\alpha| \|x\|$ for all $\alpha \in K$ and all $x \in V$, and
(4) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in V$ (the *triangle inequality*).

## 4.2. Orthogonality

**4.2.1 Orthogonality.** Suppose $\langle \cdot, \cdot \rangle$ is an inner product on a vector space $V$. If $\langle x, y \rangle = 0$ we say that $x$ and $y$ are *orthogonal* and denote this by $x \perp y$.

With the standard scalar product in $\mathbb{R}^2$ and $\mathbb{R}^3$ this is the usual notion of orthogonality.

Let $M$ be a subset of $V$ and define $M^\perp = \{x \in V : \langle x, y \rangle = 0 \text{ for all } y \in M\}$. If $x_1, x_2 \in M^\perp$ then so is $\alpha x_1 + \beta x_2$, i.e., $M^\perp$ is a subspace of $V$.

**4.2.2 Orthogonality and linear independence.** Let $X$ be a subset of an inner product space. If the elements of $X$ are non-zero and pairwise orthogonal then $X$ is linearly independent. To see this take the inner product of a linear combination of the vectors with each of the vectors themselves.

**4.2.3 Orthonormal subsets.** A set $X$ whose elements have norm one and are pairwise orthogonal is called *orthonormal*.

**4.2.4 The Gram-Schmidt procedure.** Suppose $x_1$, ..., $x_n$ are linearly independent vectors in an inner product space $V$. Then we can construct an orthonormal set $Z$ such that $\operatorname{span} Z = \operatorname{span}\{x_1, ..., x_n\}$ with the following algorithm, called the *Gram-Schmidt procedure*.

Define $z_1 = x_1/\|x_1\|$. Then $z_1$ has norm 1 and has the same span as $x_1$. Next assume that, for some $k < n$, the set $\{z_1, ..., z_k\}$ is orthonormal and spans $\operatorname{span}\{x_1, ..., x_k\}$. Define

$$y_{k+1} = x_{k+1} - \sum_{j=1}^{k} \langle z_j, x_{k+1} \rangle z_j.$$

Then $y_{k+1}$ is different from 0 and orthogonal to each of the $z_j$, $j = 1, ..., k$. Now define $z_{k+1} = y_{k+1}/\|y_{k+1}\|$ to obtain an orthonormal set $\{z_1, ..., z_k, z_{k+1}\}$, which has the same span as $\{x_1, ..., x_{k+1}\}$. Induction completes the proof.

**4.2.5 Orthogonal direct sums.** If $M$ and $N$ are orthogonal subspaces of a vector space $V$ we denote their internal direct sum by $M \oplus N$.

**4.2.6 Orthogonal complements.** Let $M$ be a subspace of the finite-dimensional inner product space $V$. Then $M \cap M^\perp = \{0\}$ and $V = M \oplus M^\perp$. In particular, $\dim M^\perp = \dim V - \dim M$ and $(M^\perp)^\perp = M$.

Sketch of proof. If $x \in M \cap M^\perp$, then $\langle x, x \rangle = 0$ and hence $x = 0$. Let $B = (b_1, ..., b_k)$ be an ordered basis of $M$. Using 2.2.8 we may extend $B$ to a basis $(b_1, ..., b_n)$ of $V$. Because of the Gram-Schmidt procedure we may assume that $B$ is orthonormal. Hence $b_{k+1}$, ..., $b_n$ are all in $M^\perp$. This implies that $V = M \oplus M^\perp$. The last claim follows since $M \oplus M^\perp = V = (M^\perp)^\perp \oplus M^\perp$. □

When $M$ is a subspace of $V$ one calls $M^\perp$ the *orthogonal complement* of $M$.

**4.2.7 Orthogonal projections.** Suppose $V$ is an inner product space. A projection $P : V \to V$ is called an *orthogonal projection*, if $\ker P \perp \operatorname{ran} P$. Since $\operatorname{ran}(\mathbb{1} - P) = \ker P$ and $\ker(\mathbb{1} - P) = \operatorname{ran} P$, $P$ is an orthogonal projection if and only if $\mathbb{1} - P$ is one.

Suppose $M$ is a subspace of $V$. Recall that each $x \in V$ has a unique decomposition $x = m + n$ where $m \in M$ and $n \in M^\perp$. If we define $P : V \to V$ by $Px = m$, it follows that $P$ is an orthogonal projection with range $M$. Since there is only one orthogonal projection with range $M$ we say that $P$ is *the* orthogonal projection onto $M$.

**4.2.8 Pythagorean theorem.** Let $P$ and $Q = \mathbb{1} - P$ be orthogonal projections of a finite-dimensional vector space $V$ onto subspaces $M$ and $M^\perp$, respectively. Then

$$\|x\|^2 = \|Px\|^2 + \|Qx\|^2.$$

## 4.3. Linear functionals and adjoints

Throughout this section $U$, $V$, and $W$ are finite-dimensional inner product spaces.

**4.3.1 Linear functionals.** Let $L : V \to K$ be a linear transformation on the vector space $V$. Then $L$ is called a *linear functional*. The set $\mathcal{L}(V, K)$ of all such linear functionals is a vector space as we saw in 3.3.1. This space of functionals is called the *dual space* of $V$ and is denoted by $V^*$, i.e., $V^* = \mathcal{L}(V, K)$.

**4.3.2 Riesz's representation theorem.** The following theorem determines the dual space of any finite-dimensional inner product space.

THEOREM. Let $V$ be a finite-dimensional inner product space and $L$ a linear functional on $V$. Then there exists a unique $y \in V$ such that $Lx = \langle y, x\rangle$ for all $x \in V$. Conversely, for every $y \in V$ the function $x \mapsto \langle y, x\rangle$ is a linear functional on $V$. In particular, there exists a bijection from $V^*$ to $V$. This bijection is linear if the scalar field is $\mathbb{R}$ and anti-linear if the scalar field is $\mathbb{C}$.

SKETCH OF PROOF. If $L = 0$ we may choose $y = 0$. Hence assume now that $L \neq 0$, i.e., that there is an $x_0 \in (\ker L)^\perp$ with $\|x_0\| = 1$. Set $y = \overline{(Lx_0)}x_0$. Any $x \in V$ may be written as $x = \alpha x_0 + w$ with $w \in \ker L$ so that $w \perp y$. Hence,

$$Lx = L(\alpha x_0 + w) = L(\alpha x_0) = \alpha\langle y, x_0\rangle + \langle y, w\rangle = \langle y, \alpha x_0 + w\rangle = \langle y, x\rangle.$$

To prove uniqueness assume $\langle y_1, x\rangle = Lx = \langle y_2, x\rangle$ for all $x$ which implies that $y_1 - y_2 \in V^\perp = \{0\}$. □

**4.3.3 Example.** A $1 \times n$ matrix $a$, i.e., a row, with entries in $K$ gives rise to a linear functional on $K^n$. In fact these are all linear functionals on $K^n$. The space of all rows with $n$ entries in $K$ is in a one-to-one correspondence with the space of all columns with $n$ entries in $K$.

**4.3.4 Adjoints.** Suppose $T : V \to W$ is a linear transformation. Fix $z \in W$. Then $x \mapsto \langle z, Tx\rangle$ is a linear functional. Riesz' representation theorem 4.3.2 shows that there is a unique vector in $V$, which we denote by $T^*z$, such that $\langle z, Tx\rangle = \langle T^*z, x\rangle$ for all $x \in V$. Since we may do this for any $z \in W$, we find that $T^*$ is a function defined on $W$ with values in $V$.

$T^*$ is a linear transformation, called the *adjoint* of $T$. To see linearity let $\alpha, \beta \in K$ and $z_1, z_2 \in W$. Then

$$\begin{aligned}\langle T^*(\alpha z_1 + \beta z_2), x\rangle &= \langle \alpha z_1 + \beta z_2, Tx\rangle = \overline{\alpha}\langle z_1, Tx\rangle + \overline{\beta}\langle z_2, Tx\rangle \\ &= \overline{\alpha}\langle T^*z_1, x\rangle + \overline{\beta}\langle T^*z_2, x\rangle = \langle \alpha T^*z_1 + \beta T^*z_2, x\rangle.\end{aligned}$$

Since this is true for all $x \in V$ we get, as desired, the linearity of $T^*$.

**4.3.5 Basic properties of adjoints.** Suppose $S$ and $T$ are linear transformations from $V$ to $W$ and $R$ is a linear transformation from $U$ to $V$. Furthermore, let $\alpha$ be a scalar. Then the following are true:

(1) $(S + T)^* = S^* + T^*$.
(2) $(\alpha S)^* = \overline{\alpha}S^*$.

(3) $(SR)^* = R^*S^*$.
(4) $T^{**} = T$.
(5) $\ker T = (\operatorname{ran} T^*)^\perp$.

**4.3.6 The rank of the adjoint.** Let $T$ be a linear transformation from $V$ to $W$. Then $\dim \operatorname{ran} T^* = \dim V - \dim(\operatorname{ran} T^*)^\perp = \dim V - \dim \ker T = \dim \operatorname{ran} T$.

**4.3.7 Transpose and conjugate transpose of a matrix.** Given an $m \times n$-matrix $A$ we define its *transpose* $A^\top$ to be the $n \times m$-matrix satisfying $(A^\top)_{j,k} = A_{k,j}$. The *conjugate transpose* $A^*$ of $A$ is defined by $(A^*)_{j,k} = \overline{A_{k,j}}$. Of course, in real vector spaces these concepts are the same.

The rank of a matrix equals the rank of both its transpose and its conjugate transpose.

The adjoint of the matrix $A$, considered as a transformation from $K^n$ to $K^m$, is given by $A^*$ (otherwise using the symbol $*$ would have been a very bad idea). Therefore, the properties listed in 4.3.5 hold also for matrices.

A square matrix which equals its transpose is called *symmetric* while one which equals its conjugate transpose is called *hermitian*.

**4.3.8 Matrix representation of the adjoint.** Let $(x_1, ..., x_n)$ be an orthonormal basis of $V$ and $(z_1, ..., z_m)$ an orthonormal basis of $W$. Suppose that, with respect to these bases, $T$ is represented by the matrix $A$ while $T^*$ is represented by the matrix $B$. Since $Tx_j = \sum_{\ell=1}^m A_{\ell,j} z_\ell$ and $T^* z_k = \sum_{\ell=1}^n B_{\ell,k} x_\ell$ we find

$$B_{j,k} = \langle x_j, \sum_{\ell=1}^n B_{\ell,k} x_\ell \rangle = \langle x_j, T^* z_k \rangle = \overline{\langle T^* z_k, x_j \rangle} = \overline{\langle z_k, T x_j \rangle} = \overline{A_{k,j}}.$$

Hence $B = A^*$, i.e., the matrix representing $T^*$ is the conjugate transpose of the matrix representing $T$. If $K = \mathbb{R}$ we have, of course, simply $B = A^\top$. Be warned though, that this simple relationship may fail when one of the bases is not orthonormal.

## 4.4. Normal and self-adjoint transformations

Throughout this section $V$ is a finite-dimensional inner product space.

**4.4.1 Normal and self-adjoint linear transformations.** A linear transformation $T : V \to V$ is called *normal*, if it commutes with its adjoint, i.e., if $TT^* = T^*T$. The transformation $T$ is called *self-adjoint*, if $T = T^*$. Note that any self-adjoint transformation is normal.

Exercise. Find a normal transformation which is not self-adjoint.

**4.4.2 Basic properties of normal transformations.** The transformation $T$ is normal, if and only if $\langle Tx, Ty \rangle = \langle T^*x, T^*y \rangle$ holds for all $x, y \in V$.

It follows that $\ker T = \ker T^*$ for any normal linear transformation. Moreover, if $T$ is normal and $x \in \ker T^2$, then $Tx \in \ker T = \ker T^*$. Therefore $0 = \langle T^*Tx, x \rangle = \langle Tx, Tx \rangle$ and hence $\ker T = \ker T^2$.

**4.4.3 Orthogonal projections are self-adjoint.** With the concept of self-adjointness we have now the following characterization of orthogonal projections.

Theorem. The linear transformation $P : V \to V$ is an orthogonal projection, if and only if $P^2 = P^* = P$.

Sketch of proof. Suppose $P$ is an orthogonal projection. Since we have $\langle P^{*2}x, y \rangle = \langle x, P^2 y \rangle = \langle x, Py \rangle = \langle P^*x, y \rangle$ for all $x, y \in V$ we find that $P^*$ is idempotent. Moreover,

$\operatorname{ran} P \oplus \ker P = V$, i.e., $\operatorname{ran} P = (\ker P)^\perp = \operatorname{ran} P^*$ by definition and 4.3.5. It follows that $P^*$ is the orthogonal projection onto $\operatorname{ran} P$, i.e., it coincides with $P$.

Conversely, if $P^2 = P^* = P$, we have $\ker P = (\operatorname{ran} P^*)^\perp = (\operatorname{ran} P)^\perp$, i.e., $P$ is an orthogonal projection. □

## 4.5. Least squares approximation

Throughout this section $V$ is a finite-dimensional inner product space.

**4.5.1 The problem.** Suppose $Ax = b$ does not have a solution since $b$ is not in the range of $A$. We then might be interested in finding an approximation. The best approximation would make the distance between $b$ and $Ax$ as small as possible, i.e., we should be trying to find the minimum of $\{\|Ax - b\| : x \in \mathbb{R}^n\}$ if there is such a thing.

This problem occurs frequently in data fitting. If two variables are expected to behave proportionally one is interested in the proportionality constant. To find it one takes a number of measurements but, due to measuring errors, it is unreasonable to hope that they all lie exactly on a line. In this case one tries to find the line which best describes the data.

**4.5.2 The distance of a point to a subspace.** Let $M$ be a subspace of $V$ and $b$ an element of $V$. Then $\min\{\|m - b\| : m \in M\}$, if it exists, is called the *distance* from $b$ to $M$.

THEOREM. If $b$ is an element of $V$ and $M$ a subspace of $V$, then the distance from $b$ to $M$ is given by $\|b - Pb\|$ where $P$ is the orthogonal projection onto $M$.

SKETCH OF PROOF. Let $m$ be an arbitrary point of $M$. Then $b - m = b - Pb + Pb - m$ where $Pb - m \in M$ and $b - Pb = (\mathbb{1} - P)b \in M^\perp$. By the Pythagorean theorem we have $\|b - m\|^2 = \|b - Pb\|^2 + \|Pb - m\|^2$ which implies that $\|b - m\| \geq \|b - Pb\|$ for all $m \in M$. Since we have equality for $m = Pb$, we see that the lower bound $\|b - Pb\|$ is actually attained, i.e., we have a minimum. □

**4.5.3 Orthogonal projections in $K^n$.** Suppose $M$ is a subspace of $K^n$ and $A$ is a matrix whose columns are a basis of $M$. Hence, if $\dim M = \ell$, then $A$ is an $n \times \ell$-matrix where $\ell \leq n$. By the rank-nullity theorem 3.2.2 we have $\ker A = \{0\}$. It follows that the $\ell \times \ell$-matrix $A^*A$ is invertible, since $A^*Ax = 0$ implies $x^*A^*Ax = \|Ax\|^2 = 0$ and hence $x = 0$. Now define the $n \times n$-matrix

$$P = A(A^*A)^{-1}A^*.$$

Then $P$ is the orthogonal projection onto $M$.

**4.5.4 Least squares approximation.** Suppose $A$ is an $m \times n$ matrix with real entries where the rank of $A$ is $n$ and $m > n$. By 4.5.2 the vector $Ax$ is closest to $b$ if $Ax = Pb$ when $P$ denotes the orthogonal projection onto the column space of $A$. Hence we want to find a solution of the system $Ax = Pb$. Since $Pb$ is in the range of $A$ the rank of $A$ and the rank of the augmented matrix $(A, Pb)$ are the same, namely $n$. Hence we have a unique solution $x_0$. It is called the *least squares solution*.

Since, by 4.5.3, $P = A(A^*A)^{-1}A^*$ the equation $Ax = Pb$ implies $A^*Ax = A^*b$. The latter has a unique solution which is $x_0$.

Note that to find $P$ we would have to compute an inverse. This is avoided by solving instead of $Ax = Pb$ the equation $A^*Ax = A^*b$.

**4.5.5 Approximating points in a plane.** Suppose $m$ (pairwise distinct) points with coordinates $(x_1, y_1)$, ..., $(x_m, y_m)$ are given. If $m = 2$, then there is a unique line passing through these points. A straight line is, of course given by the equation $y = sx + c$ and we

want to find, ideally, numbers $s$ and $c$ such that $y_j = sx_j + c$ for $j = 1, ..., m$. In other words we want to solve the system

$$\begin{pmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_m & 1 \end{pmatrix} \begin{pmatrix} s \\ c \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Denoting the vectors $(x_1, ..., x_m)^\top$ and $(y_1, ..., y_m)^\top$ by $X$ and $Y$, respectively, and the vector all of whose components are 1 by $E$ we may write this as $Ax = b$ where $A = (X, E)$, $x = \binom{s}{c}$, and $b = Y$. The equation $A^*Ax = A^*b$ becomes

$$\begin{pmatrix} X^*X & X^*E \\ E^*X & E^*E \end{pmatrix} \begin{pmatrix} s \\ c \end{pmatrix} = \begin{pmatrix} X^*Y \\ E^*Y \end{pmatrix}$$

which is merely a $2 \times 2$ system.

The frontispiece of these lecture notes was created using this algorithm (with $m = 37$).

EXERCISE 1. Find the best straight line approximating the points $(1, 2)$, $(3, 3)$, and $(5, 3)$.

EXERCISE 2. Assuming that none of the $y_j$ are 0 devise a scheme to compute the best approximation of the data from Exercise 1 by an exponential function $y = ce^{rx}$.

CHAPTER 5

# Spectral theory

Throughout this chapter $V$ is going to be a non-trivial complex vector space of dimension $n < \infty$ and $T$ is a linear transformation from $V$ to $V$.

## 5.1. Eigenvalues and Eigenvectors

**5.1.1 The Fibonacci sequence.** After setting $f_0 = 0$ and $f_1 = 1$ define recursively the numbers $f_{n+1} = f_n + f_{n-1}$ for all $n \in \mathbb{N}$. These famous numbers are called *Fibonacci numbers*. The first few are 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144. While it is always easy to compute the next number in the sequence, it would be desirable to compute, say, $f_{100}$ without computing all previous ones. And, indeed, it is possible to do so with the aid of eigenvalues and eigenvectors (whatever these may be).

Let $F_n = \left(\begin{smallmatrix} f_{n-1} \\ f_n \end{smallmatrix}\right)$ for $n \in \mathbb{N}$. Then the recursion relation is $F_{n+1} = MF_n$ where $M$ is the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. We may find $f_{100}$ as the second entry of $F_{100} = M^{99}\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ and the problem has become one of finding powers of matrices.

Let $\lambda_{1,2} = (1 \pm \sqrt{5})/2$ and $S = \left(\begin{smallmatrix} -\lambda_2 & -\lambda_1 \\ 1 & 1 \end{smallmatrix}\right)$ (the number $\lambda_1 = (1 + \sqrt{5})/2$ is the famous *golden ratio*). One may then compute that $S^{-1}MS = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ and a simple induction proof show that $S^{-1}M^nS = \left(\begin{smallmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{smallmatrix}\right)$. Hence

$$M^n = \frac{1}{\sqrt{5}} \begin{pmatrix} -\lambda_2 & -\lambda_1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \begin{pmatrix} 1 & \lambda_1 \\ -1 & -\lambda_2 \end{pmatrix}$$

and this gives $f_n = (\lambda_1^n - \lambda_2^n)/\sqrt{5} \approx 0.4472\ \mathrm{e}^{0.48121n}$.

At a first glance this procedure may look a bit mysterious but a second look shows that the key is to find the matrix $S$ which "diagonalizes" the matrix $M$. This, in turn is done, as we will see, by studying the eigenvalues and eigenvectors of $M$. The diagonalization of matrices (and linear transformations) is extremely important for theoretical as well as numerical linear algebra.

**5.1.2 Eigenvalues and eigenvectors.** Let $T : V \to V$ be a linear transformation, and $\lambda$ a scalar. If there exists a non-trivial (non-zero) element $x \in V$ such that $Tx = \lambda x$, then $\lambda$ is called an *eigenvalue* of $T$ and $x$ is called an *eigenvector* of $T$ associated with $\lambda$. Thus $\lambda$ is an eigenvalue of $T$, if and only if $T - \lambda\mathbb{1}$ is not injective.

The set of all eigenvalues is called the *spectrum* of $T$ and is denoted by $\sigma(T)$ (this definition assumes that $V$ is finite-dimensional).

**5.1.3 Geometric eigenspaces.** The eigenvectors of $T$ associated with the eigenvalue $\lambda$ are precisely the non-trivial elements of $\ker(T - \lambda\mathbb{1})$. The subspace $\ker(T - \lambda\mathbb{1})$ (including the zero element) is called the *geometric eigenspace* of $\lambda$ and its dimension is called the *geometric multiplicity* of $\lambda$.

**5.1.4 Existence of an eigenvalue.** Any linear transformation $T : V \to V$ has at least one eigenvalue. To see this pick a non-trivial $v_0 \in V$ and consider the vectors $v_k = T^k v_0$ for $k = 1, ..., n$. These vectors must be linearly dependent. Hence there are scalars $\alpha_0, ..., \alpha_n$, not all 0, such that $\alpha_0 v_0 + ... + \alpha_n v_n = 0$. If $\ell$ is the largest index such that $\alpha_\ell \neq 0$, we must have $\ell \geq 1$ and we may as well assume that $\alpha_\ell = 1$. By A.2.7, the fundamental theorem of algebra, we have $\alpha_0 + \alpha_1 z + ... + \alpha_\ell z^\ell = (z - \lambda_1)...(z - \lambda_\ell)$ for appropriate numbers $\lambda_1, ..., \lambda_\ell$. Hence we also have

$$S = \alpha_0 \mathbb{1} + \alpha_1 T + ... + \alpha_\ell T^\ell = (T - \lambda_1 \mathbb{1}) \circ ... \circ (T - \lambda_\ell \mathbb{1}).$$

Now assume that each $T - \lambda_j \mathbb{1}$ is invertible. Then $S$ is also invertible which prevents that $Sv_0 = 0$ which we know to be the case. Hence for at least one $j$ the space $\ker(T - \lambda_j \mathbb{1})$ is non-trivial so that $\lambda_j$ is an eigenvalue.

**5.1.5 Eigenvectors corresponding to distinct eigenvalues are linearly independent.** This claim is proved as follows: Let $v_1, ..., v_m$ be eigenvectors of $T$ respectively associated with the pairwise distinct eigenvalues $\lambda_1$, ..., $\lambda_m$. Suppose that $\alpha_1 v_1 + ... + \alpha_m v_m = 0$. Apply the operator $S = (T - \lambda_2 \mathbb{1})...(T - \lambda_m \mathbb{1})$ to both sides of the equation. Then $0 = \alpha_1(\lambda_1 - \lambda_2)...(\lambda_1 - \lambda_m)v_1$. Hence $\alpha_1 = 0$. Similarly, $\alpha_2 = ... = \alpha_m = 0$.

As a corollary we obtain also that $T$ can have at most $n = \dim V$ distinct eigenvalues.

**5.1.6 Diagonalizable transformations.** Suppose the eigenvalues of $T$ are $\lambda_1$, ..., $\lambda_m$ and that their respective geometric multiplicities are $\mu_1$, ..., $\mu_m$. If $\sum_{k=1}^m \mu_k = n$, the dimension of $V$, then $V$ has a basis of eigenvectors $e_1$, ..., $e_n$. Let $S : K^n \to V$ be defined by $S\delta_k = e_k$ as in 3.4.3. Then $M = S^{-1}TS$ is a diagonal matrix, in fact $M = \operatorname{diag}(\lambda_1, ..., \lambda_1, ..., \lambda_m, ..., \lambda_m)$ when the eigenvalues are repeated according to their geometric multiplicity and the basis is properly ordered.

Consequently, we define a linear transformation to be *diagonalizable*, if $V$ has a basis of eigenvectors or, equivalently, if $\sum_{k=1}^m \mu_k = n$.

**5.1.7 The functional calculus for diagonalizable matrices.** Let $T : V \to V$ be a diagonalizable linear transformation with eigenvalues $\lambda_1$, ..., $\lambda_n$ (repeated according to their geometric multiplicity). Define $S$ and $M$ as in 5.1.6 so that $M = S^{-1}TS = \operatorname{diag}(\lambda_1, ..., \lambda_n)$.

If $f$ a function from $\sigma(T) = \{\lambda_1, ..., \lambda_n\}$ to $\mathbb{C}$, define

$$f(T) = S \operatorname{diag}(f(\lambda_1), ..., f(\lambda_n))S^{-1}$$

which is a linear transformation from $V$ to $V$. When $f, g$ are both functions from $\sigma(T)$ to $\mathbb{C}$ and $\alpha \in \mathbb{C}$ we have the following properties:

(1) $(f + g)(T) = f(T) + g(T)$.
(2) $(\alpha f)(T) = \alpha f(T)$.
(3) $(fg)(T) = f(T)g(T) = g(T)f(T)$.

We emphasize that this definition is compatible with the previous definitions when $f$ is a polynomial and when $f(s) = 1/s$ (assuming that $0 \notin \sigma(T)$ and identifying $1/T$ with $T^{-1}$).

We can therefore define, for instance, roots and exponentials (in addition to powers) of diagonalizable linear transformations.

## 5.2. Spectral theory for general linear transformations

**5.2.1 Invariant subspaces.** A subspace $W$ of $V$ is called an invariant subspace of $T$ if $T(W) \subset W$. For instance, for any $k \in \mathbb{N}$ and $\lambda \in \mathbb{C}$ the spaces $\operatorname{ran}(T - \lambda \mathbb{1})^k$ and $\ker(T - \lambda \mathbb{1})^k$ are invariant subspaces of $T$.

If $W$ is an invariant subspace of $T$, then the restriction $T|_W$ of $T$ to $W$ is a linear transformation from $W$ to $W$.

**5.2.2 Kernels of powers of $T$.** We begin with an instructive example.

EXERCISE. Determine the eigenspaces of $A$, $A^2$, and $A^3$ when $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

Clearly we have in general

$$\{0\} = \ker T^0 \subset \ker T \subset \ker T^2 \subset \dots$$

and the exercise shows that some of the inclusions could be strict. However, we have the following two facts:

(1) If $\ker T^k = \ker T^{k+1}$ for some $k \in \mathbb{N}_0$, then $\ker T^{k+m} = \ker T^k$ for all $m \in \mathbb{N}$.
(2) $\ker T^n = \ker T^{n+1}$ where $n = \dim V$.

**5.2.3 Kernel and range of $T^n$.** Suppose $x \in \operatorname{ran} T^n \cap \ker T^n$, i.e., $x = T^n y$ for some $y$ and $T^n x = 0$. Then $y \in \ker T^{2n} = \ker T^n$ so that $x = 0$. Hence $\operatorname{ran} T^n$ and $\ker T^n$ intersect only trivially. By the rank-nullity theorem their union spans $V$. Thus we have shown that

$$V = \operatorname{ran} T^n \uplus \ker T^n$$

for any linear transformation $T : V \to V$.

**5.2.4 Algebraic eigenspaces.** If $\lambda$ is an eigenvalue of $T$ we call the space $\ker(T - \lambda\mathbb{1})^n$ the *algebraic eigenspace* of $\lambda$. The geometric eigenspace $\ker(T-\lambda\mathbb{1})$ is, of course, a subspace of the algebraic eigenspace. The algebraic eigenspaces of $T$ are invariant subspaces of $T$.

The nontrivial elements of the algebraic eigenspace are called *generalized eigenvectors* and its dimension is called the *algebraic multiplicity* of $\lambda$.

**5.2.5 The algebraic eigenspaces span $V$.** Let $\lambda_1$, ..., $\lambda_m$ be the pairwise distinct eigenvalues of $T$. Then

$$V = \ker(T - \lambda_1\mathbb{1})^n \uplus \dots \uplus \ker(T - \lambda_m\mathbb{1})^n$$

and, in particular, the sum of the algebraic multiplicities of the $\lambda_j$ equals $n = \dim V$.

SKETCH OF PROOF. Since $\operatorname{ran}(T-\lambda_1\mathbb{1})^n$ is an invariant subspace of $T$ this follows from 5.2.3 and induction. □

## 5.3. Spectral theory for normal transformations

**5.3.1 Eigenvectors of $T$ and $T^*$ coincide.** If $T$ is normal so is $T - \lambda\mathbb{1}$ and we have, by 4.4.2, that $\|(T - \lambda\mathbb{1})x\| = \|(T^* - \overline{\lambda}\mathbb{1})x\|$. Hence, if $x$ is an eigenvector of $T$ associated with $\lambda$, then it is also an eigenvector of $T^*$ associated with $\overline{\lambda}$.

If $x_1$ and $x_2$ are eigenvectors of $T$ associated with different eigenvalues $\lambda_1$ and $\lambda_2$, respectively, then they are orthogonal, since

$$(\lambda_1 - \lambda_2)\langle x_1, x_2\rangle = \langle\overline{\lambda_1}x_1, x_2\rangle - \langle x_1, \lambda_2 x_2\rangle = \langle T^* x_1, x_2\rangle - \langle x_1, Tx_2\rangle = 0.$$

**5.3.2 Normal linear transformations are diagonalizable.** Suppose $T : V \to V$ is a normal linear transformation. For normal transformations 4.4.2 shows that algebraic and geometric eigenspaces coincide. Hence $V$ has a basis of eigenvectors which proves that $T$ is diagonalizable. Indeed, using the previous result 5.3.1, we obtain that we may find an orthonormal basis of $V$ consisting of eigenvectors of $T$.

**5.3.3 Functions of $T$ and $T^*$.** If $T$ is normal and $f$ is a complex-valued function defined on $\sigma(T)$, then $f(T)^* = \overline{f}(T)$. This is true since $S$ satisfies $S^* = S^{-1}$ when the vectors $S\delta_k$ form an orthonormal basis.

**5.3.4 Self-adjoint transformations.** A normal linear transformation is self-adjoint if and only if all its eigenvalues are real.

**5.3.5 Positive linear transformations.** The linear transformation $T$ is called positive semi-definite if $\langle x, Tx\rangle \geq 0$ and positive definite if $\langle x, Tx\rangle > 0$ unless $x = 0$. Every positive semi-definite transformation is self-adjoint. To see this let $F = T - T^*$ and note that $\langle x, Fx\rangle = 0$ for all $x \in V$. Hence $0 = \langle x + y, F(x + y)\rangle + i\langle x + iy, F(x + iy)\rangle = 2\langle y, Fx\rangle$ for all $x, y \in V$. This implies $F = 0$.

The eigenvalues of a positive (semi)-definite linear transformation are all positive (non-negative).

**5.3.6 Roots.** Suppose $k \in \mathbb{N}$. If $R : V \to V$ is a linear transformation such that $R^k = T$, we call $R$ a $k$-th *root* of $T$. Since, by A.2.8, every non-zero complex number has exactly $k$ $k$-th roots (0 is the only $k$-th root of 0), the functional calculus shows that diagonalizable linear transformations have (in general) infinitely many $k$-th roots.

However, a positive semi-definite transformation has exactly one positive semi-definite $k$-th root.

Sketch of proof. Let $R$ be a positive semi-definite $k$-th root of $T$. By 3.2.1 it is enough to determine how $R$ acts on the eigenvectors of $T$. Let $v$ be one such eigenvector of $T$ associated with the eigenvalue $\lambda$ and let $e_1, ..., e_n$ be linearly independent eigenvectors of $R$ associated with the eigenvalues $\gamma_1$, ..., $\gamma_n$, respectively. Then $v = \alpha_1 e_1 + ... + \alpha_n e_n$ and $\lambda v = Tv = R^k v = \alpha_1\gamma_1^k e_1 + ...\alpha_n\gamma_n^k e_n$. This implies that $\alpha_j = 0$ unless $\gamma_j^k = \lambda$. Hence $Rv = \sqrt[k]{\lambda}\, v$. □

## 5.4. The functional calculus for general linear transformations

**5.4.1 Nilpotent transformations.** The linear transformation $T$ is called *nilpotent* if there exists a natural number $m$ such that $T^m = 0$. If $T$ is nilpotent, then $T^n = 0$ (recall that $n = \dim V$).

A nilpotent transformation $T : V \to V$ has only one eigenvalue, namely zero. Its algebraic multiplicity is $n$.

If $\lambda$ is an eigenvalue of $T$ and $W = \ker(T - \lambda\mathbb{1})^n$ then $T|_W : W \to W$ is nilpotent.

**5.4.2 Jordan chains and Jordan blocks.** Suppose that the vectors $x$, $(T - \lambda\mathbb{1})x$, ..., $(T - \lambda\mathbb{1})^{m-1}x$ are non-trivial and that $(T - \lambda\mathbb{1})^m x = 0$. Then these vectors are linearly independent generalized eigenvectors of $T$ associated with the eigenvalue $\lambda$. They span a subspace $W$ and the restriction $(T - \lambda\mathbb{1})|_W$ of $T - \lambda\mathbb{1}$ is a nilpotent transformation from $W$ to itself. The list $((T - \lambda\mathbb{1})^{m-1}x, ..., x)$ is an ordered basis of $W$ called the *Jordan chain* generated by $x$. With respect to this basis $T|_W$ is represented by the $m \times m$-matrix

$$N_m = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

Such a matrix is called a *Jordan block* of size $m$ with eigenvalue $\lambda$.

**5.4.3 The structure of nilpotent transformations.** Suppose $\lambda$ is the only eigenvalue of the linear transformation $T : V \to V$. Then $T - \lambda \mathbb{1}$ is nilpotent. Moreover, $V = \biguplus_{j=1}^{r} W(x_j)$ where each $W(x_j)$ is the span of a Jordan chains generated by a vector $x_j$. With respect to the basis (properly ordered) given by the union of these Jordan chains $T$ is represented by the matrix

$$\begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_r \end{pmatrix}$$

where each matrix $J_\ell$, $\ell = 1, ...r$, is a Jordan block with eigenvalue $\lambda$.

Sketch of proof. The proof is by induction on the dimension of $V$. We assume, without loss of generality, that $\lambda = 0$. Let $M$ be the set of all natural numbers for which the theorem is true. Then, clearly, $1 \in M$.

Next assume that $n-1 \in M$ and that $\dim V = n > 1$. Since $T$ is nilpotent $\dim T(V) \leq n-1$. Therefore there is a subspace $F$ of $V$ of dimension $n-1$ such that $T(V) \subset F$. Since $T|_F : F \to F$ is also nilpotent, we have that $F = \biguplus_{j=1}^{k} W(x_j)$ where the $W(x_j)$ are spaces spanned by Jordan chains generated by the vectors $x_1$, ..., $x_k$. We denote the lengths of these chains by $m_1$, ..., $m_k$ and arrange the labels so that $m_1 \leq m_2 \leq ... \leq m_k$. Now choose $g \in V \setminus F$. Since $Tg \in F$ there is an $h \in F$ and numbers $\alpha_1$, ..., $\alpha_k$ such that $Tg = Th + \sum_{j=1}^{k} \alpha_j x_j$.

We now distinguish two cases. In the first case all of the numbers $\alpha_j$ are zero and we define $x_{k+1} = g - h$. Then $(x_{k+1})$ is a Jordan chain of length 1 and $V = F \uplus \operatorname{span}\{x_{k+1}\}$.

In the second case there is a number $p$ such that $\alpha_p \neq 0$ but $\alpha_j = 0$ whenever $j > p$. In this case we define $\tilde{x}_p = (g-h)/\alpha_p$. Then $(T^{m_p}\tilde{x}_p, ..., \tilde{x}_p)$ is a Jordan chain of length $m_p + 1$. Set $F' = \biguplus_{j \neq p} W(x_j)$. Then $F' \cap W(\tilde{x}_p) = \{0\}$ and $V = F' \uplus W(\tilde{x}_p)$. This shows that $n \in M$ and the claim follows now from the induction principle. □

**5.4.4 The Jordan normal form of a linear transformation.** Let $T : V \to V$ be a linear transformation and $\lambda_1, ..., \lambda_m$ its pairwise distinct eigenvalues. Each algebraic eigenspace is a direct sum of subspaces spanned by Jordan chains, i.e.,

$$\ker(T - \lambda_k \mathbb{1})^n = \biguplus_{j=1}^{r_k} \operatorname{span} W(x_{k,j}).$$

Thus, in view of 5.2.5, we have

$$V = \biguplus_{k=1}^{m} \biguplus_{j=1}^{r_k} \operatorname{span} W(x_{k,j}).$$

The union of all these Jordan chains form a basis of $V$. With respect to this basis (properly ordered) the matrix associated with $T$ is of the form

$$J = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_r \end{pmatrix}$$

where each of the $A_j$ is a Jordan block and where $r = \sum_{k=1}^{m} r_k$ is the total number of Jordan chains involved. This matrix $J$ is called a *Jordan normal form* of the linear transformation

$T$. We have, of course, $J = S^{-1}TS$ where $S : K^n \to V$ is the transformation which assigns to $\delta_k$ the $k$-the vector in the basis described above.

**5.4.5 The functional calculus.** Given $k \in \mathbb{N}$ and a $k-1$ times differentiable function $f$ we define the $k \times k$-matrix

$$f_k^{\#}(\lambda) = \begin{pmatrix} f(\lambda) & f'(\lambda) & \frac{1}{2}f''(\lambda) & \dots & \frac{f^{(k-1)}(\lambda)}{(k-1)!} \\ 0 & f(\lambda) & f'(\lambda) & \dots & \frac{f^{(k-2)}(\lambda)}{(k-2)!} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & f(\lambda) & f'(\lambda) \\ 0 & 0 & \dots & 0 & f(\lambda) \end{pmatrix}.$$

Let $T : V \to V$ be a linear transformation and $J = S^{-1}TS$ its Jordan normal form. In $J$ replace every $k \times k$ Jordan block with eigenvalue $\lambda$ by $f_k\#(\lambda)$ to obtain a new matrix which we call $f(J)$. Then define $f(T) = Sf(J)S^{-1}$. This definition is compatible with the one in 5.1.7 since $k$ is there always equal to 1.

We have again the following properties:

(1) $(f+g)(T) = f(T) + g(T)$.
(2) $(\alpha f)(T) = \alpha f(T)$.
(3) $(fg)(T) = f(T)g(T) = g(T)f(T)$.

As before, this implies that the definition of $f(T)$ is compatible with the previous definitions when $f$ is a polynomial and when $f(s) = 1/s$.

**5.4.6 Projections onto spectral subspaces.** We call an algebraic eigenspace or a direct sum of such a *spectral subspace*. Let $f$ be a function which takes the value 1 near some of the eigenvalues and the value 0 near the others. Note that the function $f$ is then "idempotent", i.e., $f^2 = f$. Then the $f_k^{\#}(\lambda)$ is either a zero matrix or an identity matrix. It follows now that $f(T)$ is also idempotent, i.e., $f(T)$ is a projection. Its range is the direct sum of the algebraic subspaces of those $\lambda$ for which we have $f(\lambda) = 1$.

**5.4.7 Linear first order systems of ordinary differential equations.** Suppose $A$ is an $n \times n$-matrix and $(a, b)$ an interval in the real line. With the help of the functional calculus we can define $\exp(Ax)$ for $x \in (a, b)$ and hence $u(x) = \exp(Ax)u_0$ where $u_0$ is a fixed vector in $\mathbb{R}^n$. Then $u$ is a solution of the differential equation $u' = Au$ and, in fact, any solution of that equation can be obtained this way by choosing the vector $u_0$ appropriately.

Exercise. Compute $\exp(Ax)$ when $A = \left(\begin{smallmatrix} 1 & -4 \\ 1 & 5 \end{smallmatrix}\right)$. Then check that either column of this matrix solves $u' = Au$.

APPENDIX A

# Appendix

## A.1. Set Theory

**A.1.1 Relations.** A relation from a set $A$ to a set $B$ is a subset of $A \times B$, i.e., a collection of ordered pairs $(a, b)$ where $a \in A$ and $b \in B$. If $A = B$ we speak of a relation on $A$.

Let $R$ be a relation from $A$ to $B$. The set of all elements $a \in A$ for which there is a $b \in B$ such that $(a, b) \in R$ is called the domain of $R$ and denoted by $\operatorname{dom} R$. Similarly, the set of all elements $b \in B$ for which there is an $a \in A$ such that $(a, b) \in R$ is called the range of $R$ and denoted by $\operatorname{ran} R$.

**A.1.2 Reflexivity, symmetry, and transitivity.** A relation $R$ on $A$ is called reflexive, if $(a, a) \in R$ for all $a \in A$. It is called symmetric, if $(a, b) \in R$ implies that $(b, a) \in R$. Finally, it is called transitive, if $(a, b) \in R$ and $(b, c) \in R$ imply that $(a, c) \in R$.

**A.1.3 Equivalence relations.** A relation is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

An equivalence relation on $A$ partitions $A$ into so called equivalence classes, i.e., pairwise disjoint subsets of $A$ whose union is equal to $A$.

**A.1.4 Functions.** A function from a set $A$ to a set $B$ is a relation $f$ from $A$ to $B$ (written as $f : A \to B$) with the following properties: (1) $\operatorname{dom} f = A$ and (2) if $(a, b) \in f$ and $(a, b') \in f$ then $b = b'$, i.e., $b$ is uniquely determined by $a$. Customarily one writes $b = f(a)$, if $f$ is a function and $(a, b) \in f$. When $A$ and $B$ are real intervals you should think of $f$ as its graph.

A function $f : A \to B$ is called *surjective*, if every $b \in B$ is in the range of $f$. It is called *injective*, if $f(a_1) = f(a_2)$ implies $a_1 = a_2$. A function which is both injective and surjective is called *bijective*.

**A.1.5 The induction principle.** A most important tool for proving facts about the natural numbers is the induction principle:

THEOREM. Let $S$ be a subset of the set $\mathbb{N}$ of natural numbers. If $1 \in S$ and if $n+1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

An equivalent formulation is as follows:

COROLLARY. Let $S$ be a subset of the set $\mathbb{N}$ of natural numbers. If $1 \in S$ and if $n+1 \in S$ whenever $\{1, ..., n\} \subset S$, then $S = \mathbb{N}$.

## A.2. Algebra

**A.2.1 Binary operations.** Let $S$ be a set. A function which assigns an element of $S$ to any pair of elements of $S$ is called a *binary relation* on $S$. Frequently one denotes the image of $(a, b)$ under the binary operation by $a + b$, $a \cdot b$, or $ab$.

**A.2.2 Groups.** Suppose $G$ is a set and $\cdot$ a binary operation on $G$. Then $(G, \cdot)$ is called a *group*, if the following conditions are satisfied:

(1) For all $a, b, c \in G$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*associative law*).
(2) There is an element $e$ (called a left *identity*) such that $e \cdot a = a$ for all $a \in G$.
(3) For every $a \in G$ there is an element (called a left *inverse*) $b \in G$ such that $b \cdot a = e$.

It follows that a left identity is also a right identity (then just called an identity), i.e., $a \cdot e = a$ for all $a$, and that a left inverse is also a right inverse (then just called an inverse). In fact, the identity and the inverse of a given element are unique. The identity is often denoted by 1 and the inverse of $a$ by $a^{-1}$.

If $a \cdot b = b \cdot a$ for all $a, b \in G$, the group is called *abelian* or *commutative*. For abelian groups one often uses $+$ to symbolize the binary operation. The identity element is then denoted by 0 and the inverse of $a$ by $-a$. The sum $a + (-b)$ is abbreviated by $a - b$.

**A.2.3 Fields.** Suppose $F$ is a set and $+$ and $\cdot$ are two binary operations of $F$. Then $(F, +, \cdot)$ is called a *field*, if the following conditions are satisfied:

(1) $(F, +)$ is a commutative group with identity element 0.
(2) $(F \setminus \{0\}, \cdot)$ is a commutative group with identity element 1.
(3) For all $a, b, c \in F$ we have $a \cdot (b + c) = ab + ac$ (*distributive law*).

Recall that $\mathbb{Q}$ and $\mathbb{R}$ (with the usual addition and multiplication) are fields. Another important number field, the field of complex numbers, is described below.

**A.2.4 Polynomial functions.** Suppose $K$ is a field. A polynomial function $p$ on $K$ is a function $p : K \to K$ defined by $x \mapsto p(x) = \sum_{k=0}^{n} a_k x^k$ where $n \in \mathbb{N}_0$ and the $a_k$ are elements of $K$. We speak of real or complex polynomial functions when $K$ equals $\mathbb{R}$ or $\mathbb{C}$, respectively.

The largest index $k$ for which $a_k \neq 0$ is called the degree of $p$. Constant non-zero functions have thus degree 0. The zero function is also a polynomial but no degree is assigned to it.

An element $x$ of $K$ is called a root of the polynomial $p$, if $p(x) = 0$.

**A.2.5 The field of complex numbers.** Denote ordered pairs of real numbers $(a, b)$ by $a + ib$ allowing for the simplifications $a + i0 = a$ and $0 + ib = ib$, in particular, $0 + i1 = i$. Define two binary operations $+$ and $\cdot$ as follows: if $(a, b)$ and $(c, d)$ are pairs of real numbers, then

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

and

$$(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc).$$

Note that $i \cdot i = -1$.

The numbers $a + ib$ so defined are called complex numbers and the set of all *complex numbers* is a field denoted by $\mathbb{C}$.

Let $x$, $y$, and $z$ be complex numbers. Then we have the following conventions: One writes $x - y$ in place of $x + (-y)$, and $\frac{x}{y}$ or $x/y$ for $x \cdot y^{-1}$. It is also common to write $xy$ instead of $x \cdot y$ and to let multiplication take precedence over addition, i.e., $x + yz$ is short for $x + (yz)$.

**A.2.6 Real and imaginary parts of a complex number, absolute value.** If $a, b \in \mathbb{R}$ and $z = a + ib$ is a complex number, then $a$ is called the *real part* of $z$ (denoted by $\mathrm{Re}(z)$) and $b$ is called the *imaginary part* of $z$ (denoted by $\mathrm{Im}(z)$). The number $\overline{z} = a - ib$ is called

the *complex conjugate* of $z$. Finally, $|z| = \sqrt{z\overline{z}} = \sqrt{a^2+b^2} \in [0,\infty)$ is called the *absolute value* or *modulus* of $z$.

If $z \in \mathbb{C}$, then $z + \overline{z} = 2\operatorname{Re}(z)$, $z - \overline{z} = 2i\operatorname{Im}(z)$, $|\operatorname{Re}(z)| \leq |z|$, and $|\operatorname{Im}(z)| \leq |z|$. If $z, w \in \mathbb{C}$, then $\overline{z+w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$, and $|zw| = |z|\,|w|$. If $z \neq 0$, then $1/z = \overline{z}/|z|^2$.

**A.2.7 The fundamental theorem of algebra.** Suppose $p$ is a complex polynomial of degree $n \geq 1$ with complex coefficients. Then there exist complex numbers $a$ and $z_1$, ..., $z_n$ (not necessarily distinct) such that

$$p(z) = a\prod_{k=1}^{n}(z - z_k).$$

**A.2.8 Roots of complex numbers.** Let $k$ be a natural number. A complex number $a$ is called a $k$-th *root* of a complex number $b$, if $a^k = b$.

Every non-zero complex number as precisely $k$ pairwise distinct $k$-th roots. The number 0 has only one $k$-th root, namely 0.

# List of special symbols

$|z|$: the absolute value or modulus of the complex number $z$, 33
$T^*$: the adjoint of the linear transformation $T$, 21

$\overline{z}$: the complex conjugate of the complex number $z$, 32
$\delta_k$: the $k$-th member of the canonical basis of $K^n$, 9
$\mathbb{C}^n$: the complex euclidean space of dimension $n$, 7
$A^*$: the conjugate transpose of the matrix $A$, 22

$\operatorname{diag}(a_1, ..., a_n)$: the diagonal $n \times n$-matrix with diagonal elements $a_1$, ..., $a_n$, 18
$\dim V$: the dimension of the vector space $V$, 9
$\uplus$: external direct sum, 10
$\uplus$: internal direct sum, 11

$\operatorname{Im}(z)$: the imaginary part of the complex number $z$, 32
$\mathbb{1}$: the identity transformation or identity matrix, 18

$\ker F$: the kernel of $F$, 13

$\#S$: the number of elements of the finite set $S$, 9

$\oplus$: orthogonal direct sum, 20

$\operatorname{Re}(z)$: the real part of the complex number $z$, 32
$\operatorname{ran} F$: the range of $F$, 13
$\mathbb{R}^n$: the real euclidean space of dimension $n$, 7
$T|_W$: the restriction of a function $T$ to a subset $W$ of its domain, 27

$A \setminus B$: the set consisting of all those elements in $A$ which are not in $B$, 29
$K^X$: the set of all functions defined on $X$ with values in $K$, 7
span, 9

$A^\top$: the transpose of a matrix $A$, 22

# Index

# Bibliography


[1] Sheldon Axler. *Linear algebra done right*. Undergraduate Texts in Mathematics. Springer, Cham, third edition, 2015.

[2] Hans-Joachim Kowalsky. *Lineare Algebra*. Walter de Gruyter, Berlin-New York, 1977. Achte Auflage, de Gruyter Lehrbuch.

[3] Gilbert Strang. *Introduction to Linear Algebra*. Wellesley-Cambridge Press, 2016.

[4] Lloyd N. Trefethen and David Bau, III. *Numerical linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1997.