

# LINEAR ALGEBRA

by

Alexander Givental



Sumizdat



**Published by Sumizdat**

5426 Hillside Avenue, El Cerrito, California 94530, USA

<http://www.sumizdat.org>

## University of California, Berkeley Cataloging-in-Publication Data

Givental, Alexander

Linear Algebra / by Alexander Givental ;

El Cerrito, Calif. : Sumizdat, 2009.

iv, 200 p. : ill. ; 23 cm.

Includes bibliographical references and index.

ISBN 978-0-9779852-4-1

1. Linear algebra. I. Givental, Alexander.

## Library of Congress Control Number:

## ©2009 by Alexander Givental

All rights reserved. Copies or derivative products of the whole work or any part of it may not be produced without the written permission from Alexander Givental ([givental@math.berkeley.edu](mailto:givental@math.berkeley.edu)), except for brief excerpts in connection with reviews or scholarly analysis.

## Credits

Editing: Alisa Givental.

Art advising: Irina Mukhacheva, <http://irinartstudio.com>

Cataloging-in-publication: Catherine Moreno,  
Technical Services Department, Library, UC Berkeley.

Layout, typesetting and graphics: using  $L^A T_E X$  and *Xfig*.

Printing and binding: *Thomson-Shore, Inc.*, <http://www.tshore.com>  
Member of the Green Press Initiative.

7300 West Joy Road, Dexter, Michigan 48130-9701, USA.

Offset printing on 30% recycled paper; cover: by 4-color process on Kivar-7.

**ISBN 978-0-9779852-4-1**

# Contents

<b>1</b>	<b>A Crash Course</b>	<b>1</b>
1	Vectors . . . . .	1
2	Quadratic Curves . . . . .	9
3	Complex Numbers . . . . .	17
4	Problems of Linear Algebra . . . . .	23
<b>2</b>	<b>Dramatis Personae</b>	<b>31</b>
1	Matrices . . . . .	31
2	Determinants . . . . .	41
3	Vector Spaces . . . . .	59
<b>3</b>	<b>Simple Problems</b>	<b>71</b>
1	Dimension and Rank . . . . .	71
2	Gaussian Elimination . . . . .	83
3	The Inertia Theorem . . . . .	97
<b>4</b>	<b>Eigenvalues</b>	<b>117</b>
1	The Spectral Theorem . . . . .	117
2	Jordan Canonical Forms . . . . .	137
	Hints . . . . .	149
	Answers . . . . .	153
	Bibliography . . . . .	157
	Index . . . . .	158



# Foreword

“Mathematics is a form of culture. Mathematical ignorance is a form of national culture.”

“In antiquity, they knew few ways to learn, but modern pedagogy discovered 1001 ways to fail.”

August Dumbel<sup>1</sup>

---

<sup>1</sup>From his eye-opening address to NCVM, the National Council of Visionaries of Mathematics.



# Chapter 1

## A Crash Course

### 1 Vectors

#### Operations and their properties

The following definition of vectors can be found in elementary geometry textbooks, see for instance [4].

A **directed segment**  $\overrightarrow{AB}$  on the plane or in space is specified by an ordered pair of points: the **tail**  $A$  and the **head**  $B$ . Two directed segments  $\overrightarrow{AB}$  and  $\overrightarrow{CD}$  are said to **represent the same vector** if they are obtained from one another by translation. In other words, the lines  $AB$  and  $CD$  must be parallel, the lengths  $|AB|$  and  $|CD|$  must be equal, and the segments must point toward the same of the two possible directions (Figure 1).

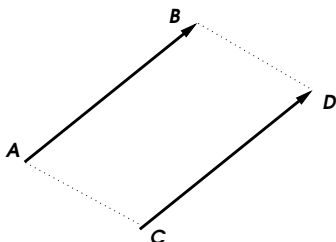


Figure 1

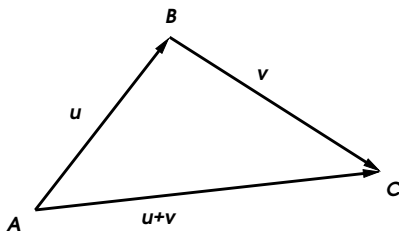


Figure 2

A trip from  $A$  to  $B$  followed by a trip from  $B$  to  $C$  results in a trip from  $A$  to  $C$ . This observation motivates the definition of the

**vector sum**  $\mathbf{w} = \mathbf{v} + \mathbf{u}$  of two vectors  $\mathbf{v}$  and  $\mathbf{u}$ : if  $\overrightarrow{AB}$  represents  $\mathbf{v}$  and  $\overrightarrow{BC}$  represents  $\mathbf{u}$  then  $\overrightarrow{AC}$  represents their sum  $\mathbf{w}$  (Figure 2).

The vector  $3\mathbf{v} = \mathbf{v} + \mathbf{v} + \mathbf{v}$  has the same direction as  $\mathbf{v}$  but is 3 times longer. Generalizing this example one arrives at the definition of the **multiplication of a vector by a scalar**: given a vector  $\mathbf{v}$  and a real number  $\alpha$ , the result of their multiplication is a vector, denoted  $\alpha\mathbf{v}$ , which has the same direction as  $\mathbf{v}$  but is  $\alpha$  times longer. The last phrase calls for comments since it is literally true only for  $\alpha > 1$ . If  $0 < \alpha < 1$ , being “ $\alpha$  times longer” actually means “shorter.” If  $\alpha < 0$ , the direction of  $\alpha\mathbf{v}$  is in fact opposite to the direction of  $\mathbf{v}$ . Finally,  $0\mathbf{v} = \mathbf{0}$  is the **zero vector** represented by directed segments  $\overrightarrow{AA}$  of zero length.

Combining the operations of vector addition and multiplication by scalars we can form expressions  $\alpha\mathbf{u} + \beta\mathbf{v} + \dots + \gamma\mathbf{w}$ . They are called **linear combinations** of the vectors  $\mathbf{u}, \mathbf{v}, \dots, \mathbf{w}$  with the coefficients  $\alpha, \beta, \dots, \gamma$ .

The pictures of a parallelogram and parallelepiped (Figures 3 and 4) prove that the addition of vectors is **commutative** and **associative**: for all vectors  $\mathbf{u}, \mathbf{v}, \mathbf{w}$ ,

$$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u} \quad \text{and} \quad (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}).$$

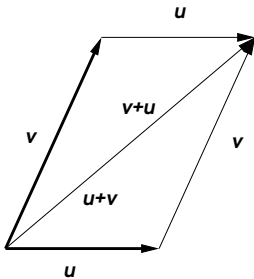


Figure 3

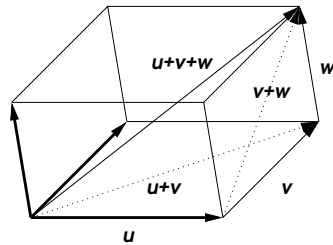


Figure 4

From properties of proportional segments and similar triangles, the reader will easily derive the following two **distributive laws**: for all vectors  $\mathbf{u}, \mathbf{v}$  and scalars  $\alpha, \beta$ ,

$$(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u} \quad \text{and} \quad \alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}.$$



## Coordinates

From a point  $O$  in space, draw three directed segments  $\overrightarrow{OA}$ ,  $\overrightarrow{OB}$ , and  $\overrightarrow{OC}$  not lying in the same plane and denote by  $\mathbf{i}$ ,  $\mathbf{j}$ , and  $\mathbf{k}$  the vectors they represent. Then every vector  $\mathbf{u} = \overrightarrow{OU}$  can be uniquely written as a linear combination of  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  (Figure 5):

$$\mathbf{u} = \alpha\mathbf{i} + \beta\mathbf{j} + \gamma\mathbf{k}.$$

The coefficients form the array  $(\alpha, \beta, \gamma)$  of **coordinates** of the vector  $\mathbf{u}$  (and of the point  $U$ ) with respect to the **basis**  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  (or the **coordinate system**  $OABC$ ).

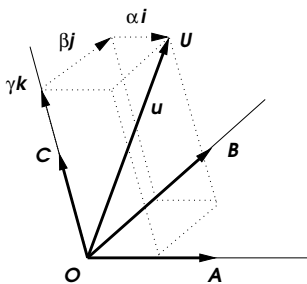


Figure 5

Multiplying  $\mathbf{u}$  by a scalar  $\lambda$  or adding another vector  $\mathbf{u}' = \alpha'\mathbf{i} + \beta'\mathbf{j} + \gamma'\mathbf{k}$ , and using the above algebraic properties of the operations with vectors, we find:

$$\lambda\mathbf{u} = \lambda\alpha\mathbf{i} + \lambda\beta\mathbf{j} + \lambda\gamma\mathbf{k}, \quad \text{and} \quad \mathbf{u} + \mathbf{u}' = (\alpha + \alpha')\mathbf{i} + (\beta + \beta')\mathbf{j} + (\gamma + \gamma')\mathbf{k}.$$

Thus, the geometric operations with vectors are expressed by componentwise operations with the arrays of their coordinates:

$$\begin{aligned} \lambda(\alpha, \beta, \gamma) &= (\lambda\alpha, \lambda\beta, \lambda\gamma), \\ (\alpha, \beta, \gamma) + (\alpha', \beta', \gamma') &= (\alpha + \alpha', \beta + \beta', \gamma + \gamma'). \end{aligned}$$

## What is a vector?

No doubt, the idea of vectors is not new to the reader. However, some subtleties of the above introduction do not easily meet the eye, and we would like to say here a few words about them.

As many other mathematical notions, vectors come from physics, where they represent quantities, such as velocities and forces, which are characterized by their magnitude and direction. Yet, the popular slogan “Vectors *are* magnitude and direction” does not qualify for a mathematical definition of vectors, e.g. because it does not tell us how to operate with them.

The computer science definition of vectors as *arrays* of numbers, to be added “apples with apples, oranges with oranges,” will meet the following objection by physicists. When a coordinate system rotates, the coordinates of the *same* force or velocity will change, but the numbers of apples and oranges won’t. Thus forces and velocities *are not* arrays of numbers.

The geometric notion of a directed segment resolves this problem. Note however, that calling directed segments *vectors* would constitute abuse of terminology. Indeed, strictly speaking, directed segments can be added only when the head of one of them coincides with the tail of the other.

So, what is a vector? In our formulations, we actually avoided answering this question directly, and said instead that *two directed segments represent the same vector if...* Such wording is due to pedagogical wisdom of the authors of elementary geometry textbooks, because a direct answer sounds quite abstract: *A vector is the class of all directed segments obtained from each other by translation in space.* Such a class is shown in Figure 6.

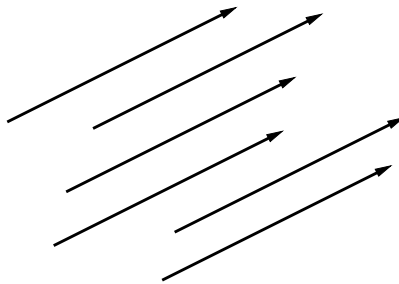


Figure 6

This picture has another interpretation: For every point in space (the tail of an arrow), it indicates a new position (the head). The geometric transformation in space defined this way is translation. This leads to another attractive point of view: a vector *is* a translation. Then the sum of two vectors is the *composition* of the translations.

## The dot product

This operation encodes *metric* concepts of elementary Euclidean geometry, such as lengths and angles. Given two vectors  $\mathbf{u}$  and  $\mathbf{v}$  of lengths  $|\mathbf{u}|$  and  $|\mathbf{v}|$  and making the angle  $\theta$  to each other, their dot product (also called **inner product** or **scalar product**) is a *number* defined by the formula:

$$\langle \mathbf{u}, \mathbf{v} \rangle = |\mathbf{u}| |\mathbf{v}| \cos \theta.$$

Of the following properties, the first three are easy (check them!):

- (a)  $\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle$  (**symmetricity**);
- (b)  $\langle \mathbf{u}, \mathbf{u} \rangle = |\mathbf{u}|^2 > 0$  unless  $\mathbf{u} = \mathbf{0}$  (**positivity**);
- (c)  $\langle \lambda \mathbf{u}, \mathbf{v} \rangle = \lambda \langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{u}, \lambda \mathbf{v} \rangle$  (**homogeneity**);

(d)  $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$  (**additivity** with respect to the first factor).

To prove the last property, note that due to homogeneity, it suffices to check it assuming that  $\mathbf{w}$  is a **unit vector**, i.e.  $|\mathbf{w}| = 1$ . In this case, consider (Figure 7) a triangle  $ABC$  such that  $\overrightarrow{AB} = \mathbf{u}$ ,  $\overrightarrow{BC} = \mathbf{v}$ , and therefore  $\overrightarrow{AC} = \mathbf{u} + \mathbf{v}$ , and let  $\overrightarrow{OW} = \mathbf{w}$ . We can consider the line  $OW$  as the number line, with the points  $O$  and  $W$  representing the numbers 0 and 1 respectively, and denote by  $\alpha, \beta, \gamma$  the *numbers* representing perpendicular projections to this line of the vertices  $A, B, C$  of the triangle. Then

$$\langle \overrightarrow{AB}, \mathbf{w} \rangle = \beta - \alpha, \quad \langle \overrightarrow{BC}, \mathbf{w} \rangle = \gamma - \beta, \quad \text{and} \quad \langle \overrightarrow{AC}, \mathbf{w} \rangle = \gamma - \alpha.$$

The required identity follows, because  $\gamma - \alpha = (\gamma - \beta) + (\beta - \alpha)$ .

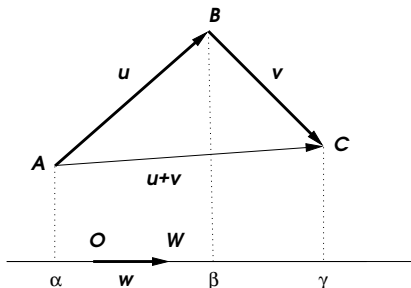


Figure 7

Combining the properties (c) and (d) with (a), we obtain the following identities, expressing **bilinearity** of the dot product (i.e.

linearity with respect to each factor):

$$\langle \alpha \mathbf{u} + \beta \mathbf{v}, \mathbf{w} \rangle = \alpha \langle \mathbf{u}, \mathbf{w} \rangle + \beta \langle \mathbf{v}, \mathbf{w} \rangle$$

$$\langle \mathbf{w}, \alpha \mathbf{u} + \beta \mathbf{v} \rangle = \alpha \langle \mathbf{w}, \mathbf{u} \rangle + \beta \langle \mathbf{w}, \mathbf{v} \rangle.$$

The following example illustrates the use of nice algebraic properties of dot product in elementary geometry.

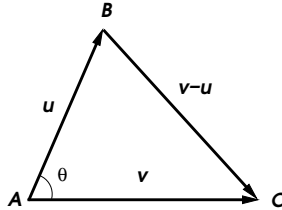


Figure 8

**Example.** Given a triangle  $ABC$ , let us denote by  $\mathbf{u}$  and  $\mathbf{v}$  the vectors represented by the directed segments  $\overrightarrow{AB}$  and  $\overrightarrow{AC}$  and use properties of the inner product in order to compute the length  $|BC|$ . Notice that the segment  $\overrightarrow{BC}$  represents  $\mathbf{v} - \mathbf{u}$ . We have:

$$\begin{aligned} |BC|^2 &= \langle \mathbf{v} - \mathbf{u}, \mathbf{v} - \mathbf{u} \rangle = \langle \mathbf{v}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{u} \rangle - 2\langle \mathbf{u}, \mathbf{v} \rangle \\ &= |AC|^2 + |AB|^2 - 2|AB| |AC| \cos \theta. \end{aligned}$$

This is the famous **Law of Cosines** in trigonometry.

When the vectors  $\mathbf{u}$  and  $\mathbf{v}$  are **orthogonal**, i.e.  $\langle \mathbf{u}, \mathbf{v} \rangle = 0$ , then the formula turns into the **Pythagorean theorem**:

$$|\mathbf{u} \pm \mathbf{v}|^2 = |\mathbf{u}|^2 + |\mathbf{v}|^2.$$

When basis vectors  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  are pairwise orthogonal and *unit*, the coordinate system is called **Cartesian**.<sup>1</sup> We have:

$$\langle \mathbf{i}, \mathbf{i} \rangle = \langle \mathbf{j}, \mathbf{j} \rangle = \langle \mathbf{k}, \mathbf{k} \rangle = 1, \text{ and } \langle \mathbf{i}, \mathbf{j} \rangle = \langle \mathbf{j}, \mathbf{k} \rangle = \langle \mathbf{k}, \mathbf{i} \rangle = 0.$$

Thus, in Cartesian coordinates, the inner squares and the dot products of vectors  $\mathbf{r} = x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$  and  $\mathbf{r}' = x'\mathbf{i} + y'\mathbf{j} + z'\mathbf{k}$  are given by the formulas:

$$|\mathbf{r}|^2 = x^2 + y^2 + z^2, \quad \langle \mathbf{r}, \mathbf{r}' \rangle = xx' + yy' + zz'.$$

<sup>1</sup>After René **Descartes** (1596–1650).

**EXERCISES**

1. A mass  $m$  rests on an inclined plane making  $30^\circ$  with the horizontal plane. Find the forces of friction and reaction acting on the mass. ✓

2. A ferry, capable of making  $5\text{ mph}$ , shuttles across a river of width  $0.6\text{ mi}$  with a strong current of  $3\text{ mph}$ . How long does each round trip take? ✓

3. Prove that for every closed broken line  $ABC\dots DE$ ,

$$\overrightarrow{AB} + \overrightarrow{BC} + \dots + \overrightarrow{DE} + \overrightarrow{EA} = \mathbf{0}.$$

4. Three medians of a triangle  $ABC$  intersect at one point  $M$  called the **barycenter** of the triangle. Let  $O$  be any point on the plane. Prove that

$$\overrightarrow{OM} = \frac{1}{3}(\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}).$$

5. Prove that  $\overrightarrow{MA} + \overrightarrow{MB} + \overrightarrow{MC} = \mathbf{0}$  if and only if  $M$  is the barycenter of the triangle  $ABC$ .

6.\* Along three circles lying in the same plane, vertices of a triangle are moving clockwise with the equal constant angular velocities. Find how the barycenter of the triangle is moving. ✓

7. Prove that if  $AA'$  is a median in a triangle  $ABC$ , then

$$\overrightarrow{AA'} = \frac{1}{2}(\overrightarrow{AB} + \overrightarrow{AC}).$$

8. Prove that from medians of a triangle, another triangle can be formed. ✎

9. Sides of one triangle are parallel to the medians of another. Prove that the medians of the latter triangle are parallel to the sides of the former one.

10. From medians of a given triangle, a new triangle is formed, and from its medians, yet another triangle is formed. Prove that the third triangle is similar to the first one, and find the coefficient of similarity. ✓

11. Midpoints of  $AB$  and  $CD$ , and of  $BC$  and  $DE$  are connected by two segments, whose midpoints are also connected. Prove that the resulting segment is parallel to  $AE$  and congruent to  $AE/4$ .

12. Prove that a point  $X$  lies on the segment  $AB$  if and only if for any origin  $O$  and some scalar  $0 \leq \lambda \leq 1$  the radius-vector  $\overrightarrow{OX}$  has the form:

$$\overrightarrow{OX} = \lambda\overrightarrow{OA} + (1 - \lambda)\overrightarrow{OB}.$$

13.\* Given a triangle  $ABC$ , we construct a new triangle  $A'B'C'$  in such a way that  $A'$  is centrally symmetric to  $A$  with respect to the center  $B$ ,  $B'$  centrally symmetric to  $B$  with respect to  $C$ , and  $C'$  centrally symmetric to  $C$  with respect to  $A$ , and then erase the original triangle. Reconstruct  $ABC$  from  $A'B'C'$  by straightedge and compass. ✓

**14.** Prove the **Cauchy – Schwarz inequality**:  $\langle \mathbf{u}, \mathbf{v} \rangle^2 \leq \langle \mathbf{u}, \mathbf{u} \rangle \langle \mathbf{v}, \mathbf{v} \rangle$ . In which cases does the inequality turn into equality? Deduce the **triangle inequality**:  $|\mathbf{u} + \mathbf{v}| \leq |\mathbf{u}| + |\mathbf{v}|$ . ♪

**15.** Compute the inner product  $\langle \overrightarrow{AB}, \overrightarrow{BC} \rangle$  if  $ABC$  is a regular triangle inscribed into a unit circle. ✓

**16.** Prove that if the sum of three unit vectors is equal to  $\mathbf{0}$ , then the angle between each pair of these vectors is equal to  $120^\circ$ .

**17.** Express the inner product  $\langle \mathbf{u}, \mathbf{v} \rangle$  in terms of the lengths  $|\mathbf{u}|, |\mathbf{v}|, |\mathbf{u} + \mathbf{v}|$  of the two vectors and of their sum. ✓

**18.** (a) Prove that if four unit vectors lying in the same plane add up to  $\mathbf{0}$ , then they form two pairs of opposite vectors. (b) Does this remain true if the vectors do not have to lie in the same plane? ✓

**19.\*** Let  $AB \dots E$  be a regular polygon with the center  $O$ . Prove that

$$\overrightarrow{OA} + \overrightarrow{OB} + \dots + \overrightarrow{OE} = \mathbf{0}. \quad \spadesuit$$

**20.** Prove that if  $\mathbf{u} + \mathbf{v}$  and  $\mathbf{u} - \mathbf{v}$  are perpendicular, then  $|\mathbf{u}| = |\mathbf{v}|$ .

**21.** For arbitrary vectors  $\mathbf{u}$  and  $\mathbf{v}$ , verify the equality:

$$|\mathbf{u} + \mathbf{v}|^2 + |\mathbf{u} - \mathbf{v}|^2 = 2|\mathbf{u}|^2 + 2|\mathbf{v}|^2,$$

and derive the theorem: The sum of the squares of the diagonals of a parallelogram is equal to the sum of the squares of the sides.

**22.** Prove that for every triangle  $ABC$  and every point  $X$  in space,

$$\overrightarrow{XA} \cdot \overrightarrow{BC} + \overrightarrow{XB} \cdot \overrightarrow{CA} + \overrightarrow{XC} \cdot \overrightarrow{AB} = \mathbf{0}. \quad \spadesuit$$

**23.\*** For four arbitrary points  $A, B, C$ , and  $D$  in space, prove that if the lines  $AC$  and  $BD$  are perpendicular, then  $AB^2 + CD^2 = BC^2 + DA^2$ , and *vice versa*. ♪

**24.\*** Given a quadrilateral with perpendicular diagonals. Show that every quadrilateral, whose sides are respectively congruent to the sides of the given one, has perpendicular diagonals. ♪

**25.\*** A regular triangle  $ABC$  is inscribed into a circle of radius  $R$ . Prove that for every point  $X$  of this circle,  $XA^2 + XB^2 + XC^2 = 6R^2$ . ♪

**26.\*** Let  $A_1B_1A_2B_2 \dots A_nB_n$  be a  $2n$ -gon inscribed into a circle. Prove that the length of the vector  $\overrightarrow{A_1B_1} + \overrightarrow{A_2B_2} + \dots + \overrightarrow{A_nB_n}$  does not exceed the diameter. ♪

**27.\*** A polyhedron is filled with air under pressure. The pressure force to each face is the vector perpendicular to the face, proportional to the area of the face, and directed to the exterior of the polyhedron. Prove that the sum of these vectors is equal to  $\mathbf{0}$ . ♪

## 2 Quadratic Curves

### Conic Sections

On the coordinate plane, consider points  $(x, y)$ , satisfying an equation of the form

$$ax^2 + 2bxy + cy^2 + dx + ey + f = 0.$$

Generally speaking, such points form a curve. The set of solutions is called a **quadratic curve**, provided that not all of the coefficients  $a, b, c$  vanish.

Being a quadratic curve is a geometric property. Indeed, if the coordinate system is changed (say, rotated, stretched, or translated), the same curve will be described by a different equation, but the L.H.S. of the equation will remain a polynomial of degree 2.

Our goal in this section is to describe all possible quadratic curves geometrically (i.e. disregarding their positions with respect to coordinate systems); or, in other words, to *classify* quadratic equations in two variables up to suitable changes of the variables.

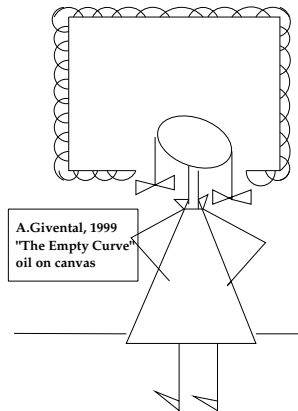


Figure 9

**Example: Dandelin's spheres.** The equation  $x^2 + y^2 = z^2$  describes in a Cartesian coordinate system a cone (a half of which is shown on Figure 10). Intersecting the cone by planes, we obtain examples of quadratic curves. Indeed, substituting the equation  $z = \alpha x + \beta y$  of a secting plane into the equation of the cone, we get a quadratic equation  $x^2 + y^2 = (\alpha x + \beta y)^2$  (which actually describes the projection of the conic section to the horizontal plane).

The conic section on the picture is an **ellipse**. According to one of many equivalent definitions,<sup>2</sup> an ellipse consists of all points on the plane with a fixed sum of the distances to two given points (called **foci** of the ellipse). Our picture illustrates an elegant way<sup>3</sup> to locate foci of a conic section. Place into the conic cup two balls (a small and a large one), and inflate the former and deflate the latter until they touch the plane (one from inside, the other from outside). Then the points  $F$  and  $G$  of tangency are the foci. Indeed, let  $A$  be an arbitrary point on the conic section. The segments  $AF$  and  $AG$  lie in the cutting plane and are therefore tangent to the balls at the points  $F$  and  $G$  respectively. On the generatrix  $OA$ , mark the points  $B$  and  $C$  where it crosses the circles of tangency of the cone with the balls. Then  $AB$  and  $AC$  are tangent at these points to the respective balls. Since all tangent segments from a given point to a given ball have the same length, we find that  $|AF| = |AB|$ , and  $|AG| = |AC|$ . Therefore  $|AF| + |AG| = |BC|$ . But  $|BC|$  is the distance along the generatrix between two parallel horizontal circles on the cone, and is the same for all generatrices. Therefore the sum  $|AF| + |AG|$  stays fixed when the point  $A$  moves along our conic section.

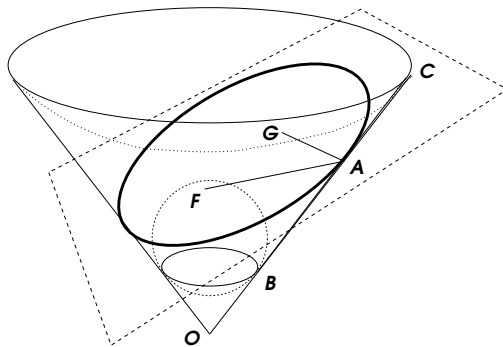


Figure 10

Beside ellipses, we find among conic sections: **hyperbolas** (when a plane cuts through both halves of the cone), parabolas (cut by planes parallel to generatrices), and their degenerations (obtained when the cutting plane is replaced with the parallel one passing through the vertex  $O$  of the cone): just one point  $O$ , pairs of intersecting lines, and “double-lines.” We will see that this list exhausts all possible quadratic curves, except two degenerate cases: pairs of parallel lines and (yes!) empty curves.

<sup>2</sup>According to a mock definition, “an ellipse is a circle inscribed into a square with unequal sides.”

<sup>3</sup>Due to Germinal Pierre **Dandelin** (1794–1847).



## Orthogonal Diagonalization (Toy Version)

Let  $(x, y)$  be Cartesian coordinates on a Euclidean plane, and let  $Q$  be a **quadratic form** on the plane, i.e. a *homogeneous* degree-2 polynomial:

$$Q(x, y) = ax^2 + 2bxy + cy^2.$$

**Theorem.** *Every quadratic form in a suitably rotated coordinate system assumes the form:*

$$Q = AX^2 + CY^2.$$

**Proof.** Rotating the basis vectors  $\mathbf{i}$  and  $\mathbf{j}$  counter-clockwise through

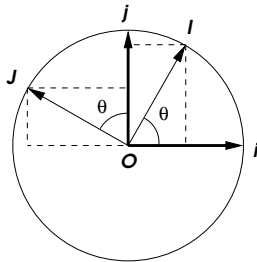


Figure 11

the angle  $\theta$  we obtain (Figure 11):

$$\mathbf{I} = (\cos \theta)\mathbf{i} + (\sin \theta)\mathbf{j} \quad \text{and} \quad \mathbf{J} = -(\sin \theta)\mathbf{i} + (\cos \theta)\mathbf{j}.$$

Therefore

$$x\mathbf{i} + y\mathbf{j} = X\mathbf{I} + Y\mathbf{J} = (X \cos \theta - Y \sin \theta)\mathbf{i} + (X \sin \theta + Y \cos \theta).$$

This shows that the old coordinates  $(x, y)$  are expressed in terms of the new coordinates  $(X, Y)$  by the formulas

$$x = X \cos \theta - Y \sin \theta, \quad y = X \sin \theta + Y \cos \theta. \quad (*)$$

Substituting into  $ax^2 + 2bxy + cy^2$ , we rewrite the quadratic form in the new coordinates as  $AX^2 + 2BXY + CY^2$ , where  $A, B, C$  are certain expressions of  $a, b, c$  and  $\theta$ . We want to show that choosing the rotation angle  $\theta$  appropriately, we can make  $2B = 0$ . Indeed, making the substitution explicitly and ignoring  $X^2$ - and  $Y^2$ -terms, we find  $Q$  in the form

$$\dots + XY(-2a \sin \theta \cos \theta + 2b(\cos^2 \theta - \sin^2 \theta) + 2c \sin \theta \cos \theta) + \dots$$

Thus  $2B = (c - a) \sin 2\theta + 2b \cos 2\theta$ . When  $b = 0$ , our task is trivial, as we can take  $\theta = 0$ . When  $b \neq 0$ , we can divide by  $2b$  to obtain

$$\cot 2\theta = \frac{a - c}{2b}.$$

Since  $\cot$  assumes arbitrary real values, the theorem follows.

**Example.** For  $Q = x^2 + xy + y^2$ , we have  $\cot 2\theta = 0$ , and find  $2\theta = \pi/2 + \pi k$  ( $k = 0, \pm 1, \pm 2, \dots$ ), i.e. up to multiples of  $2\pi$ ,  $\theta = \pm\pi/4$  or  $\pm 3\pi/4$ . (This is a general rule: together with a solution  $\theta$ , the angle  $\theta + \pi$  as well as  $\theta \pm \pi/2$ , also work. Could you give an *a priori* explanation?) Taking  $\theta = \pi/4$ , we compute  $x = (X - Y)/\sqrt{2}$ ,  $y = (X + Y)/\sqrt{2}$ , and finally find:

$$x^2 + y^2 + xy = X^2 + Y^2 + \frac{1}{2}(X^2 - Y^2) = \frac{3}{2}X^2 + \frac{1}{2}Y^2.$$

## Completing the Squares

In our study of quadratic curves, the plan is to simplify the equation of the curve as much as possible by changing the coordinate system. In doing so we may assume that the coordinate system has already been rotated to make the coefficient at  $xy$ -term vanish. Therefore the equation at hands assumes the form

$$ax^2 + cy^2 + dx + ey + f = 0,$$

where  $a$  and  $c$  cannot both be zero. Our next step is based on **completing squares**: whenever one of these coefficients (say,  $a$ ) is non-zero, we can remove the corresponding linear term ( $dx$ ) this way:

$$ax^2 + dx = a\left(x^2 + \frac{d}{a}x\right) = a\left(\left(x + \frac{d}{2a}\right)^2 - \frac{d^2}{4a^2}\right) = aX^2 - \frac{d^2}{4a}.$$

Here  $X = x + d/2a$ , and this change represents translation of the origin of the coordinate system from the point  $(x, y) = (0, 0)$  to  $(x, y) = (-d/2a, 0)$ .

**Example.** The equation  $x^2 + y^2 = 2ry$  can be rewritten by completing the square in  $y$  as  $x^2 + (y - r)^2 = r^2$ . Therefore, it describes the circle of radius  $r$  centered at the point  $(0, r)$  on the  $y$ -axis.

With the operations of completing the squares in one or both variables, renaming the variables if necessary, and dividing the whole equation by a non-zero number (which does not change the quadratic curve), we are well-armed to obtain the classification.

## Classification of Quadratic Curves

**Case I:**  $a \neq 0 \neq c$ . The equation is reduced to  $aX^2 + cY^2 = F$  by completing squares in each of the variables.

**Sub-case (i):**  $F \neq 0$ . Dividing the whole equation by  $F$ , we obtain the equation  $(a/F)X^2 + (c/F)Y^2 = 1$ . When both  $a/F$  and  $c/F$  are positive, the equation can be re-written as

$$\frac{X^2}{\alpha^2} + \frac{Y^2}{\beta^2} = 1.$$

This is the equation of an ellipse with **semiaxes**  $\alpha$  and  $\beta$  (Figure 12). When one  $a/F$  and  $c/F$  have opposite signs, we get (possibly renaming the variables) the equation of a hyperbola (Figure 13)

$$\frac{X^2}{\alpha^2} - \frac{Y^2}{\beta^2} = 1.$$

When  $a/F$  and  $c/F$  are both negative, the equation has no real solutions, so that the quadratic curve is *empty* (Figure 9).

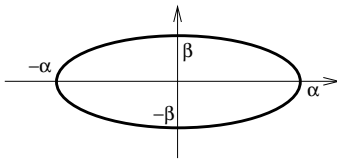


Figure 12

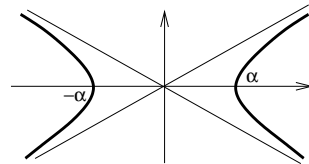


Figure 13

**Sub-case (ii):**  $F = 0$ . Then, when  $a$  and  $c$  have opposite signs (say,  $a = \alpha^2 > 0$ , and  $c = -\gamma^2 < 0$ ), the equation  $\alpha^2 X^2 = \gamma^2 Y^2$  describes a pair of intersecting lines  $Y = \pm kX$ , where  $k = \alpha/\gamma$  (Figure 14). When  $a$  and  $c$  are of the same sign, the equation  $aX^2 + cY^2 = 0$  has only one real solution:  $(X, Y) = (0, 0)$ . The quadratic curve is a “thick” point.<sup>4</sup>

**Case II: One of  $a, c$  is 0.** We may assume without loss of generality that  $c = 0$ . Since  $a \neq 0$ , we can still complete the square in  $x$  to obtain an equation of the form  $aX^2 + eY + F = 0$ .

**Sub-case (i):**  $e \neq 0$ . Divide the whole equation by  $e$  and put  $Y = y - F/e$  to arrive at the equation  $Y = -aX^2/e$ . This curve is a **parabola**  $Y = kX^2$ , where  $k = -a/e \neq 0$  (Figure 15).

---

<sup>4</sup>In fact this is the point of intersection of a pair of “imaginary” lines consisting of non-real solutions.

**Sub-case (ii):**  $e = 0$ . The equation  $X^2 = -F/a$  describes: a pair of parallel lines  $X = \pm k$  (where  $k = \sqrt{-F/e}$ ), or the empty set (when  $F/e > 0$ ), or a “double-line”  $X = 0$  (when  $F = 0$ ).

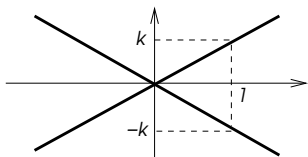


Figure 14

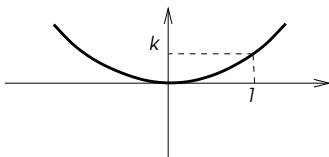


Figure 15

We have proved the following:

**Theorem.** *Every quadratic curve on a Euclidean plane is one of the following: an ellipse, hyperbola, parabola, a pair of intersecting, parallel, or coinciding lines, a “thick” point or the empty set. In a suitable Cartesian coordinate system, the curve is described by one of the standard equations:*

$$\frac{X^2}{\alpha^2} \pm \frac{Y^2}{\beta^2} = 1, -1, \text{ or } 0; \quad Y = kX^2; \quad X^2 = k.$$

### EXERCISES

**28.** Prove that with the exception of parabolas, each conic section has a center of symmetry. ♣

**29.** Prove that a hyperbolic conic section consists of all points on the section plane with a fixed *difference* of the distances to two points (called **foci**). Locate the foci by adjusting the construction of Dandelin’s spheres.

**30.** Locate foci of (a) ellipses and (b) hyperbolas given by the standard equations  $x^2/\alpha^2 \pm y^2/\beta^2 = 1$ , where  $\alpha > \beta > 0$ . ✓

**31.** A line is called an **axis of symmetry** of a given function  $Q(x, y)$  if the function takes on the same values at every pair of points symmetric about this line. Prove that every quadratic form has two perpendicular axes of symmetry. (They are called **principal axes**.) ♣

**32.** Prove that if a line passing through the origin is an axis of symmetry of a quadratic form  $Q = ax^2 + 2bxy + cy^2$ , then the perpendicular line is also its axis of symmetry. ♣

**33.** Can a quadratic form on the plane have  $> 2$  axes of symmetry? ✓

**34.** Find axes of symmetry of the following quadratic forms  $Q$ :

$$(a) x^2 + xy + y^2, \quad (b) x^2 + 2xy + y^2, \quad (c) x^2 + 4xy + y^2.$$

Which of them have level curves  $Q = \text{const}$  ellipses? hyperbolas? ✓

**35.** Transform the equation  $23x^2 + 72xy + 2y^2 = 25$  to one of the standard forms by rotating the coordinate system explicitly.  $\zeta \checkmark$

**36.** Prove that ellipses are obtained by stretching (or shrinking) the unit circle in two perpendicular directions with two different coefficients.

**37.** Prove that every quadratic form on the plane in a suitable (but non necessarily Cartesian) coordinate system assumes one of the forms:

$$X^2 + Y^2, X^2 - Y^2, -X^2 - Y^2, X^2, -Y^2, 0.$$

Sketch graphs of these functions.

**38.** Complete squares to find out which of the following curves are ellipses and which are hyperbolas:  $\checkmark$

$$x^2 + 4xy = 1, x^2 + 2xy + 4y^2 = 1, x^2 + 4xy + 4y^2 = 1, x^2 + 6xy + 4y^2 = 1.$$

**39.** Find the place of the quadratic curve  $x^2 - 4y^2 = 2x - 4y$  in the classification of quadratic curves.  $\checkmark$

**40.\*** Prove that  $ax^2 + 2bxy + cy^2 = 1$  is a hyperbola if and only if  $ac < b^2$ .

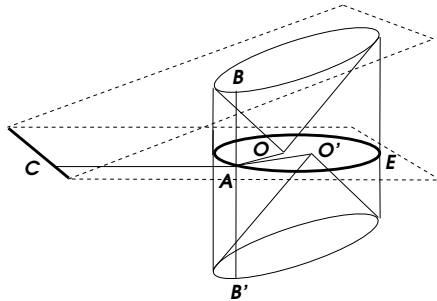


Figure 16

**41.** Examine Figure 16 (showing two cones centrally symmetric to each other about the center of the ellipse  $E$ ), and prove that  $|AO| + |AO'| = |BB'|$ . Derive that the vertex  $O$  of the cone is a focus of the *projection* of a conic section along the axis of the cone to the perpendicular plane passing through its vertex.<sup>5</sup>

**42.\*** Prove that ellipses, parabolas and hyperbolas can be characterized as plane curves formed by all points with a fixed ratio  $e$  (called **eccentricity**) between the distances to a fixed point (a **focus**) and a fixed line (called the **directrix**), and that  $e > 1$  for ellipses,  $e = 1$  for parabolas, and  $1 > e > 0$  for hyperbolas (e.g.  $e = |AO|/|AC'|$  in Figure 16).  $\zeta$

**43.\*** Prove that light rays emitted from one focus of an ellipse and reflected in it as in a mirror will focus at the other focus. Formulate and prove similar optical properties of hyperbolas and parabolas.  $\zeta$

<sup>5</sup>The proof based on Figure 16 is due to Anil **Hirani**.



## 3 Complex Numbers

### Law and Order

Life is unfair: The quadratic equation  $x^2 - 1 = 0$  has two solutions  $x = \pm 1$ , but a similar equation  $x^2 + 1 = 0$  has no solutions at all. To restore justice one introduces new number  $i$ , the **imaginary unit**, such that  $i^2 = -1$ , and thus  $x = \pm i$  become two solutions to the equation. This is how complex numbers could have been invented.

More formally, complex numbers are introduced as ordered pairs  $(a, b)$  of real numbers, written in the form  $z = a + bi$ . The real numbers  $a$  and  $b$  are called respectively the **real part** and **imaginary part** of the complex number  $z$ , and are denoted  $a = \operatorname{Re} z$  and  $b = \operatorname{Im} z$ .

The sum of  $z = a + bi$  and  $w = c + di$  is defined as

$$z + w = (a + c) + (b + d)i.$$

The product is defined so as to comply with the relation  $i^2 = -1$ :

$$zw = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

The operations of addition and multiplication of complex numbers enjoy the same properties as those of real numbers do. In particular, the product is commutative and associative.

The complex number  $\bar{z} = a - bi$  is called **complex conjugate** to  $z = a + bi$ . The operation of complex conjugation *respects* sums and products:

$$\overline{z + w} = \bar{z} + \bar{w} \quad \text{and} \quad \overline{zw} = \bar{z}\bar{w}.$$

This can be easily checked from definitions, but there is a more profound explanation. The equation  $x^2 + 1 = 0$  has two roots,  $i$  and  $-i$ , and the choice of the one to be called  $i$  is totally ambiguous. The complex conjugation consists in systematic renaming  $i$  by  $-i$  and *vice versa*, and such renaming cannot affect properties of complex numbers.

Complex numbers satisfying  $\bar{z} = z$  are exactly the real numbers  $a + 0i$ . We will see that this point of view on real numbers as complex numbers *invariant* under complex conjugation is quite fruitful.

The product  $z\bar{z} = a^2 + b^2$  (check this formula!) is real, and is positive unless  $z = 0 + 0i = 0$ . This shows that

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Hence the division by  $z$  is well-defined for any non-zero complex number  $z$ . In terminology of Abstract Algebra, complex numbers form therefore a **field**<sup>6</sup> (just as real or rational numbers do).

The field of complex numbers is denoted by  $\mathbb{C}$  (while  $\mathbb{R}$  stands for reals, and  $\mathbb{Q}$  for rationals).

The non-negative real number  $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$  is called the **absolute value** of  $z$ . The absolute value function is **multiplicative**:

$$|zw| = \sqrt{zw\bar{z}\bar{w}} = \sqrt{z\bar{z}w\bar{w}} = |z| \cdot |w|.$$

It actually coincides with the absolute value of real numbers when applied to complex numbers with zero imaginary part:  $|a + 0i| = |a|$ .

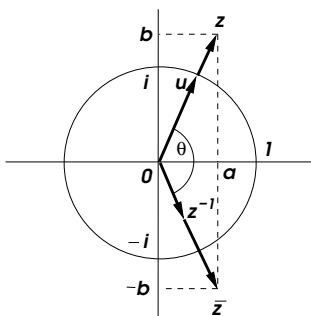


Figure 17

## Geometry

We can identify complex numbers  $z = a + bi$  with points  $(a, b)$  on the real coordinate plane (Figure 17). This way, the number 0 is identified with the origin, and 1 and  $i$  become the unit basis vectors  $(1, 0)$  and  $(0, 1)$ . The coordinate axes are called respectively the real and imaginary axes. Addition of complex numbers coincides with the operation of vector sum (Figure 18).

The absolute value function has the geometrical meaning of the distance from the origin:  $|z| = \langle z, z \rangle^{1/2}$ . In particular, the triangle inequality  $|z + w| \leq |z| + |w|$  holds true. Complex numbers of unit absolute value  $|z| = 1$  form the unit circle centered at the origin.

The operation of complex conjugation acts on the radius-vectors  $z$  as the reflection about the real axis.

<sup>6</sup>This requires that a set be equipped with commutative and associative operations (called addition and multiplication) satisfying the **distributive law**  $z(v + w) = zv + zw$ , possessing the zero and unit elements 0 and 1, additive opposites  $-z$  for every  $z$ , and multiplicative inverses  $1/z$  for every  $z \neq 0$ .



In order to describe a geometric meaning of complex multiplication, let us study the way multiplication by a given complex number  $z$  acts on all complex numbers  $w$ , i.e. consider the function  $w \mapsto zw$ . For this, write the vector representing a non-zero complex number  $z$  in the **polar** (or trigonometric) form  $z = ru$  where  $r = |z|$  is a positive real number, and  $u = z/|z| = \cos \theta + i \sin \theta$  has absolute value 1 (see Figure 19). Here  $\theta = \mathbf{arg} z$ , called the **argument** of the complex number  $z$ , is the angle that  $z$  as a vector makes with the positive direction of the real axis.

Clearly, multiplication by  $r$  acts on all vectors  $w$  by stretching them  $r$  times. Multiplication by  $u$  applied to  $w = x + yi$  yields a new complex number  $uw = X + Yi$  according to the rule:

$$\begin{aligned} X &= \operatorname{Re} [(\cos \theta + i \sin \theta)(x + yi)] = x \cos \theta - y \sin \theta \\ Y &= \operatorname{Im} [(\cos \theta + i \sin \theta)(x + yi)] = x \sin \theta + y \cos \theta. \end{aligned}$$

Comparing with the formula (\*) in Section 2, we conclude that the transformation  $w \mapsto uw$  is the counter-clockwise rotation through the angle  $\theta$ .

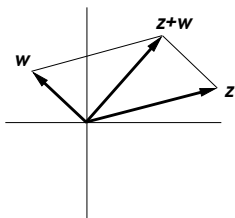


Figure 18

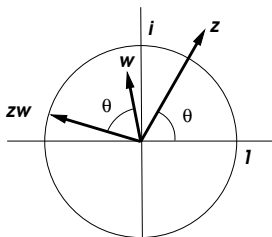


Figure 19

Notice a difference though: In Section 2, we rotated the coordinate system, and the formulas (\*) expressed old coordinates of a vector via new coordinates of the *same* vector. This time, we transform vectors, while the coordinate system remains unchanged. The same formulas now express coordinates  $(X, Y)$  of a new vector in terms of the coordinates  $(x, y)$  of a the old one.

Anyway, the conclusion is that multiplication by  $z$  is the composition of two operations: stretching  $|z|$  times, and rotating through the angle  $\mathbf{arg} z$ .

In other words, the product operation of two complex numbers sums their arguments and multiplies absolute values:

$$|zw| = |z| \cdot |w|, \quad \mathbf{arg} zw = \mathbf{arg} z + \mathbf{arg} w \text{ modulo } 2\pi.$$

For example, if  $z = r(\cos \theta + i \sin \theta)$ , then  $z^n = r^n(\cos n\theta + i \sin n\theta)$ .

## The Fundamental Theorem of Algebra

A degree 2 polynomial  $z^2 + pz + q$  has two roots

$$z_{\pm} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

This **quadratic formula** works regardless of the sign of the **discriminant**  $p^2 - 4q$ , provided that we allow the roots to be complex, and take in account **multiplicity**. Namely, if  $p^2 - 4q = 0$ ,  $z^2 + pz + q = (z + p/2)^2$  and therefore the single root  $z = -p/2$  has multiplicity two. If  $p^2 - 4q < 0$  the roots are complex conjugate with  $\operatorname{Re} z_{\pm} = -p/2$ ,  $\operatorname{Im} z_{\pm} = \pm\sqrt{|p^2 - 4q|}/2$ . The Fundamental Theorem of Algebra shows that not only justice has been restored, but that any degree  $n$  polynomial has  $n$  complex roots, possibly — multiple.

**Theorem. A degree  $n$  polynomial**

$$P(z) = z^n + a_1 z^{n-1} + \dots + a_{n-1} z + a_n$$

**with complex coefficients  $a_1, \dots, a_n$  factors as**

$$P(z) = (z - z_1)^{m_1} \dots (z - z_r)^{m_r}.$$

**Here  $z_1, \dots, z_r$  are complex roots of  $P$ , and  $m_1, \dots, m_r$  their multiplicities,  $m_1 + \dots + m_r = n$ .**

A proof of this theorem deserves a separate chapter (if not a book). Many proofs are known, based on various ideas of Algebra, Analysis or Topology. We refer to [6] for an exposition of the classical proof due to Euler, Lagrange and de Foncenex, which is almost entirely algebraic. Here we merely illustrate the theorem with several examples.

**Examples.** (a) To solve the quadratic equation  $z^2 = w$ , equate the absolute value  $r$  and argument  $\theta$  of the given complex number  $w$  with those of  $z^2$ :

$$|z|^2 = \rho, \quad 2 \operatorname{arg} z = \phi + 2\pi k, \quad k = 0, \pm 1, \pm 2, \dots$$

We find:  $|z| = \sqrt{\rho}$ , and  $\operatorname{arg} z = \phi/2 + \pi k$ . Increasing  $\operatorname{arg} z$  by even multiples  $\pi$  does not change  $z$ , and by odd changes  $z$  to  $-z$ . Thus the equation has two solutions:

$$z = \pm \sqrt{\rho} \left( \cos \frac{\phi}{2} + i \sin \frac{\phi}{2} \right).$$

(b) The equation  $z^2 + pz + q = 0$  with coefficients  $p, q \in \mathbb{C}$  has two complex solutions given by the quadratic formula (see above), because according to Example (a), the **square root** of a complex number takes on two opposite values (distinct, unless both are equal to 0).

(c) The complex numbers  $1, i, -1, -i$  are the roots of the polynomial  $z^4 - 1 = (z^2 - 1)(z^2 + 1) = (z - 1)(z + 1)(z - i)(z + i)$ .

(d) There are  $n$  complex  **$n$ th roots of unity** (see Figure 20, where  $n = 5$ ). Namely, if  $z = r(\cos \theta + i \sin \theta)$  satisfies  $z^n = 1$ , then  $r^n = 1$  (and hence  $r = 1$ ), and  $n\theta = 2\pi k$ ,  $k = 0, \pm 1, \pm 2, \dots$ . Therefore  $\theta = 2\pi k/n$ , where only the remainder of  $k$  modulo  $n$  is relevant. Thus the  $n$  roots are:

$$z = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k = 0, 1, 2, \dots, n - 1.$$

For instance, if  $n = 3$ , the roots are 1 and

$$\cos \frac{2\pi}{3} \pm i \sin \frac{2\pi}{3} = -\frac{1}{2} \pm i \frac{\sqrt{3}}{2}.$$

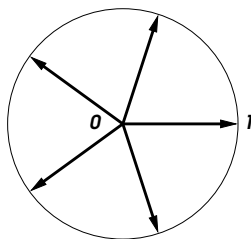


Figure 20

As illustrated by the previous two examples, even if all coefficients  $a_1, \dots, a_n$  of a polynomial  $P$  are real, its roots don't have to be real. But then the non-real roots come in pairs of complex conjugate ones. To verify this, we can use the fact that being real means stay *invariant* (i.e. unchanged) under complex conjugation. Namely,  $\bar{a}_i = a_i$  for all  $i$  means that

$$\overline{P(\bar{z})} = z^n + \bar{a}_1 z^{n-1} + \dots + \bar{a}_n = P(z).$$

Therefore we have two factorizations of the same polynomial:

$$\bar{P}(\bar{z}) = (z - \bar{z}_1)^{m_1} \dots (z - \bar{z}_r)^{m_r} = (z - z_1)^{m_1} \dots (z - z_r)^{m_r} = P(z).$$

They can differ only by orders of the factors. Thus, for each non-real root  $z_i$  of  $P$ , the complex conjugate  $\bar{z}_i$  must be also a root, and of the same multiplicity.

## Expanding the product

$$(z - z_1)\dots(z - z_n) = z^n - (z_1 + \dots + z_n)z^{n-1} + \dots + (-1)^n z_1\dots z_n$$

we can express coefficients  $a_1, \dots, a_n$  of the polynomial in terms of the roots  $z_1, \dots, z_n$  (here multiple roots are repeated according to their multiplicities). In particular, the sum and product of the roots are

$$z_1 + \dots + z_n = -a_1, \quad z_1\dots z_n = (-1)^n a_n.$$

These relations generalize **Vieta's theorem**  $z_+ + z_- = -p$ ,  $z_+ z_- = q$  about roots  $z_{\pm}$  of quadratic equations  $z^2 + pz + q = 0$ .

**EXERCISES**

44. Can complex numbers be: real? real *and* imaginary? neither? ✓

45. Compute: (a)  $(1 + i)/(3 - 2i)$ ; (b)  $(\cos \pi/3 + i \sin \pi/3)^{-1}$ . ✓

46. Verify the commutative and distributive laws for multiplication of complex numbers.

47. Show that  $z^{-1}$  is real proportional to  $\bar{z}$  and find the proportionality coefficient. ✓

48. Find all  $z$  satisfying the equations:  $|z - 1| = |z + 1| = 2$ . ✓

49. Sketch the solution set to the following system of inequalities:

$$|z - 1| \leq 1, \quad |z| \leq 1, \quad \operatorname{Re}(iz) \leq 0.$$

50. Compute absolute values and arguments of (a)  $1 - i$ , (b)  $1 - i\sqrt{3}$ . ✓

51. Compute  $\left(\frac{\sqrt{3}+i}{2}\right)^{100}$ . ✓

52. Express  $\cos 3\theta$  and  $\sin 3\theta$  in terms of  $\cos \theta$  and  $\sin \theta$ . ♣

53. Express  $\cos(\theta_1 + \theta_2)$  and  $\sin(\theta_1 + \theta_2)$  in terms of  $\cos \theta_i$  and  $\sin \theta_i$ .

54. Prove **Bézout's theorem**<sup>7</sup>: A number  $z_0$  is a root of a polynomial  $P$  in one variable  $z$  if and only if  $P$  is divisible by  $z - z_0$ . ♣

55. Find roots of degree 2 polynomials:

$$z^2 - 4z + 5, \quad z^2 - iz + 1, \quad z^2 - 2(1 + i)z + 2i, \quad z^2 - 2z + i\sqrt{3}. \quad \checkmark$$

56. Find all roots of polynomials:

$$z^3 + 8, \quad z^3 + i, \quad z^4 + 4z^2 + 4, \quad z^4 - 2z^2 + 4, \quad z^6 + 1. \quad \checkmark$$

57. Prove that every polynomial with real coefficients factors into the product of polynomials of degree 1 and 2 with real coefficients. ♣

58. Prove that the sum of all 5th roots of unity is equal to 0. ♣

59.\* Find general **Vieta's formulas**<sup>8</sup> expressing all coefficients of a polynomial in terms of its roots. ✓

<sup>7</sup>Named after Étienne **Bézout** (1730–1783).

<sup>8</sup>Named after François Viète (1540–1603) also known as Franciscus **Vieta**.

## 4 Problems of Linear Algebra

One of our goals in this book is to equip the reader with a unifying view of Linear Algebra, or at least of what is studied under this name in traditional university courses. Following this mission, we give here a *preview* of the subject and describe its main achievements in lay terms.

To begin with a few words of praise: Linear Algebra is a very simple and useful subject, underlying most of other areas of mathematics, as well as its applications to physics, engineering, and economics. What makes Linear Algebra useful and efficient is that it provides ultimate solutions to several important mathematical problems. Furthermore, as should be expected of a truly fruitful mathematical theory, the problems it solves can be formulated in a rather elementary language and make sense even before any advanced machinery is developed. Even better, the *answers* to these problems can also be described in elementary terms (in contrast with the *justification* of those answers, which better be postponed until adequate tools are developed). Finally, those several problems we are talking about are similar in their nature; namely, they all have the form of problems of *classification* of very basic mathematical objects. Before presenting explicitly the problems and the answers, we need to discuss the general idea of classification in mathematics.

### Classifications in Mathematics

Classifications are intended to bring order into seemingly complex or chaotic matters. Yet, there is a major difference between, say, our classification of quadratic curves and Carl **Linnaeus**' *Systema Naturae*.

For two quadratic curves to be in the same *class*, it is not enough that they share a number of features. What is required is a *transformation* of a prescribed type that would transform one of the curves into the other, and thus make them **equivalent** in this sense, i.e. *up to* such transformations.

What types of transformations are allowed (e.g., changes to *arbitrary* new coordinate systems, or only to *Cartesian* ones) may be a matter of choice. With every choice, the classification of objects of a certain kind (i.e. quadratic curves in our example) *up to* transformations of the selected type becomes a well-posed mathematical problem.

- A complete answer to a classification problem should consist of
- a list of **normal** (or **canonical**) **forms**, i.e. representatives of the classes of equivalence, and
  - a **classification theorem** establishing that each object of the kind (quadratic curve in our example) is equivalent to exactly one of the normal forms, i.e. in other words, that
    - (i) each object can be transformed into a normal form, and
    - (ii) no two normal forms can be transformed into each other.

Simply put, Linear Algebra deals with classifications of linear and/or quadratic equations, or systems of such equations. One might think that all that equations do is ask: *Solve us!* Unfortunately this attitude toward equations does not lead too far. It turns out that very few equations (and kinds of equations) can be explicitly *solved*, but all can be *studied* and many *classified*.

The idea is to replace a given “hard” (possibly unsolvable) equation with another one, the normal form, which should be chosen to be as “easy” as it is possible to find in the same equivalence class. Then the normal form should be studied (and hopefully “solved”) thus providing information about the original “hard” equation.

What sort of information? Well, *any* sort that remains *invariant* under the equivalence transformations in question.

For example, in classification of quadratic curves up to changes of Cartesian coordinate systems, all equivalent ellipses are indistinguishable from each other *geometrically* (in particular, they have the same semi-axes) and differ only by the choice of a Cartesian coordinate system. However, if arbitrary rescaling of coordinates is also allowed, then all ellipses become indistinguishable from circles (but still different from hyperbolas, parabolas, etc.)

Whether a classification theorem really simplifies the matters, depends on the kind of objects in question, the chosen type of equivalence transformations, and the applications in mind. In practice, the problem often reduces to finding sufficiently simple normal forms and studying them in great detail.

The subject of Linear Algebra fits well into the general philosophy just outlined. Below we formulate *four* classification problems and respective answers. Together with a number of variations and applications, which will be presented later in due course, they form what is usually considered the main course of Linear Algebra.

## The Rank Theorem

**Question.** Given  $m$  linear functions in  $n$  variables,

$$\begin{aligned} y_1 &= a_{11}x_1 + \dots + a_{1n}x_n \\ &\dots \\ y_m &= a_{m1}x_1 + \dots + a_{mn}x_n \end{aligned} ,$$

what is the simplest form to which they can be transformed by linear changes of the variables,

$$\begin{aligned} y_1 &= b_{11}Y_1 + \dots + b_{1m}Y_m & x_1 &= c_{11}X_1 + \dots + c_{1n}X_n \\ &\dots & &\dots \\ y_m &= b_{m1}Y_1 + \dots + b_{mm}Y_m & x_n &= c_{n1}X_1 + \dots + c_{nn}X_n \end{aligned} ?$$

**Theorem.** *Every system of  $m$  linear functions in  $n$  variables can be transformed by suitable linear changes of dependent and independent variables to exactly one of the normal forms:*

$$Y_1 = X_1, \quad \dots, \quad Y_r = X_r, \quad Y_{r+1} = 0, \quad \dots, \quad Y_m = 0,$$

where  $0 \leq r \leq m, n$ .

The number  $r$  featuring in the answer is called the **rank** of the given system of  $m$  linear functions.

## The Inertia Theorem

**Question.** Given a **quadratic form** (i.e. a homogeneous quadratic function) in  $n$  variables,

$$Q = q_{11}x_1^2 + 2q_{12}x_1x_2 + 2q_{13}x_1x_3 + \dots + q_{nn}x_n^2,$$

what is the simplest form to which it can be transformed by a linear change of the variables

$$\begin{aligned} x_1 &= c_{11}X_1 + \dots + c_{1n}X_n \\ &\dots \\ x_n &= c_{n1}X_1 + \dots + c_{nn}X_n \end{aligned} ?$$

**Theorem.** *Every quadratic form in  $n$  variables can be transformed by a suitable linear change of the variables to exactly one of the normal forms:*

$$X_1^2 + \dots + X_p^2 - X_{p+1}^2 - \dots - X_{p+q}^2 \quad \text{where } 0 \leq p + q \leq n.$$

The numbers  $p$  and  $q$  of positive and negative squares in the normal form are called **inertia indices** of the quadratic form in question. If the quadratic form  $Q$  is known to be positive everywhere outside the origin, the Inertia Theorem tells us that in a suitable coordinate system  $Q$  assumes the form  $X_1^2 + \dots + X_n^2$ , i.e. its inertia indices are  $p = n$ ,  $q = 0$ .

## The Orthogonal Diagonalization Theorem

**Question.** *Given two homogeneous quadratic forms in  $n$  variables,  $Q(x_1, \dots, x_n)$  and  $S(x_1, \dots, x_n)$ , of which the first one is known to be positive everywhere outside the origin, what is the simplest form to which they can be simultaneously transformed by a linear change of the variables?*

**Theorem.** *Every pair  $Q, S$  of quadratic forms in  $n$  variables, of which  $Q$  is positive everywhere outside the origin, can be transformed by a linear changes of the variables to exactly one of the normal forms*

$$Q = X_1^2 + \dots + X_n^2, \quad S = \lambda_1 X_1^2 + \dots + \lambda_n X_n^2, \quad \text{where } \lambda_1 \geq \dots \geq \lambda_n.$$

The real numbers  $\lambda_1, \dots, \lambda_n$  are called **eigenvalues** of the given pair of quadratic forms (and are often said to form their **spectrum**).

## The Jordan Canonical Form Theorem

The fourth question deals with a system of  $n$  linear functions in  $n$  variables. Such an object is the special case of systems of  $m$  functions in  $n$  variables when  $m = n$ . According to the Rank Theorem, such a system of rank  $r \leq n$  can be transformed to the form  $Y_1 = X_1, \dots, Y_r = X_r, Y_{r+1} = \dots = Y_n = 0$  by linear changes of dependent and independent variables. There are many cases however where relevant information about the system does not stay invariant when dependent and independent variables are changed *separately*. This happens whenever both groups of variables describe objects in the same space (rather than in two different ones).

An important class of examples comes from the theory of Ordinary Differential Equations (for short: ODE). Such equations (e.g.  $\dot{x} = ax$ ) relate values of quantities with the rates of their change in



time. Transforming the variables (e.g. by rescaling:  $x = cy$ ) would make little sense if not accompanied with the simultaneous change of the rates ( $\dot{x} = c\dot{y}$ ). We will describe the fourth classification problem in the context of the ODE theory.

**Question.** *Given a system of  $n$  linear homogeneous 1st order constant coefficient ODEs in  $n$  unknowns:*

$$\begin{aligned} \dot{x}_1 &= a_{11}x_1 + \dots + a_{1n}x_n \\ &\dots \\ \dot{x}_n &= a_{n1}x_1 + \dots + a_{nn}x_n \end{aligned} ,$$

*what is the simplest form to which it can be transformed by a linear change of the unknowns:*

$$\begin{aligned} x_1 &= c_{11}X_1 + \dots + c_{1n}X_n \\ &\dots \\ x_n &= c_{n1}X_1 + \dots + c_{nn}X_n \end{aligned} ?$$

Due to the Fundamental Theorem of Algebra, there is an advantage in answering this question *over complex numbers*, i.e. assuming that the coefficients  $c_{ij}$  in the change of variables, as well as the coefficients  $a_{ij}$  of the given ODE system are allowed to be complex numbers.

**Example.** Consider a single  $m$ th order linear ODE of the form:

$$\left(\frac{d}{dt} - \lambda\right)^m y = 0, \quad \text{where } \lambda \in \mathbb{C}.$$

By setting

$$y = x_1, \quad \frac{d}{dt}y - \lambda y = x_2, \quad \left(\frac{d}{dt} - \lambda\right)^2 y = x_3, \quad \dots, \quad \left(\frac{d}{dt} - \lambda\right)^{m-1} y = x_m,$$

the equation can be written as the following system of  $m$  ODEs of the 1st order:

$$\begin{aligned} \dot{x}_1 &= \lambda x_1 + x_2 \\ \dot{x}_2 &= \lambda x_2 + x_3 \\ &\dots \\ \dot{x}_{m-1} &= \lambda x_{m-1} + x_m \\ \dot{x}_m &= \lambda x_m \end{aligned} .$$

Let us call this system the **Jordan cell** of size  $m$  with the eigenvalue  $\lambda$ . Introduce a **Jordan system** of several Jordan cells of sizes

$m_1, \dots, m_r$  with the eigenvalues  $\lambda_1, \dots, \lambda_r$ . It can be similarly compressed into the system

$$\left(\frac{d}{dt} - \lambda_1\right)^{m_1} y_1 = 0, \quad \dots, \quad \left(\frac{d}{dt} - \lambda_r\right)^{m_r} y_r = 0$$

of  $r$  *unlinked* ODEs of the orders  $m_1, \dots, m_r$ .

**Theorem.** *Every constant coefficient system of  $n$  linear 1st order ODEs in  $n$  unknowns can be transformed by a complex linear change of the unknowns to exactly one (up to reordering of the cells) of the Jordan systems with  $m_1 + \dots + m_r = n$ .*

## Fools and Wizards

In the rest of the text we will undertake a more systematic study of the four basic problems and prove the classification theorems stated here. The reader should be prepared however to meet the following three challenges of Chapter 2.

Firstly, one will find there much more diverse material than what has just been described. This is because many mathematical objects and classification problems about them can be *reduced* (speaking roughly or literally) to the four problems discussed above. The challenge is to learn how to recognize situations where results of Linear Algebra can be helpful. Many of those objects will be introduced in the opening section of Chapter 2.

Secondly, we will encounter one more fundamental result of Linear Algebra, which is not a classification, but an important (and beautiful) formula. It answers the question *which substitutions of the form*

$$\begin{aligned} x_1 &= c_{11}X_1 + \dots + c_{1n}X_n \\ &\dots \\ x_n &= c_{n1}X_1 + \dots + c_{nn}X_n \end{aligned}$$

*are indeed changes of the variables and can therefore be inverted by expressing  $X_1, \dots, X_n$  linearly in terms of  $x_1, \dots, x_n$ , and how to describe such inversion explicitly.* The answer is given in terms of the **determinant**, a remarkable function of  $n^2$  variables  $c_{11}, \dots, c_{nn}$ , which will also be studied in Chapter 2.

Thirdly, Linear Algebra has developed an adequate language, based on the abstract notion of **vector space**. It allows one to represent relevant mathematical objects and results in ways much

less cumbersome and thus more efficient than those found in the previous discussion. This language is introduced at the end of Chapter 2. The challenge here is to get accustomed to the abstract way of thinking.

Let us describe now the principle by which our main four themes are grouped in Chapters 3 and 4.

Note that Jordan canonical forms and the normal forms in the Orthogonal Diagonalization Theorem do not form discrete lists, but instead depend on continuous parameters — the eigenvalues. Based on experience with many mathematical classifications, it is considered that the number of parameters on which equivalence classes in a given problem depend, is the right measure of complexity of the classification problem. Thus, Chapter 3 deals with **simple problems** of Linear Algebra, i.e. those classification problems where equivalence classes do not depend on continuous parameters. Respectively, the non-simple problems are studied in Chapter 4.

Finally, let us mention that the proverb: *Fools ask questions that wizards cannot answer*, fully applies in Linear Algebra. In addition to the four basic problems, there are many similarly looking questions that one can ask: for instance, to classify *triples* of quadratic forms in  $n$  variables up to linear changes of the variables. In fact, in this problem, the number of parameters, on which equivalence classes depend, grows with  $n$  at about the same rate as the number of parameters on which the three given quadratic forms depend. We will have a chance to touch upon such problems of Linear Algebra in the last section, in connection with *quivers*. The modern attitude toward such problems is that they are *unsolvable*.

### EXERCISES

**60.** Classify quadratic forms  $Q = ax^2$  in one variable with *complex* coefficients (i.e.  $a \in \mathbb{C}$  up to complex linear changes:  $x = cy$ ,  $c \in \mathbb{C}$ ,  $c \neq 0$ ). ✓

**61.** Using results of Section 2, derive the Inertia Theorem in dimension  $n = 2$ .

**62.** Show that classification of real quadratic curves up to arbitrary linear inhomogeneous changes of coordinates consists of 8 equivalence classes. Show that if the coordinate systems are required to remain Cartesian, then there are infinitely many equivalence classes, which depend on 2 continuous parameters.

**63.** Is there any difference between classification of quadratic equations in two variables  $F(x, y) = 0$  up to linear inhomogeneous changes of the variables and multiplications of the equations by non-zero constants, and the

classification of quadratic curves, i.e. sets  $\{(x, y) | F(x, y) = 0\}$  of solutions to such equations, up to the same type of coordinate transformations?  $\checkmark$

**64.** Prove the Rank Theorem on the line, i.e. show that every linear function  $y = ax$  can be transformed to exactly one of the normal forms:  $Y = X$  or  $Y = 0$ , by the changes:  $y = bY$ ,  $x = cX$ , where  $b \neq 0 \neq c$ .

**65.** For the pair of linear functions describing a rotation of the plane (see the formula (\*) in Section 2), find the normal form to which they can be transformed according to the Rank Theorem.  $\checkmark$

**66.** Show that  $X_1^2 + \dots + X_n^2$  is the only one of the normal forms of The Inertia Theorem which is positive everywhere outside the origin.

**67.\*** In the Inertia Theorem with  $n = 2$ , show that there are six normal forms, and prove that they are pairwise non-equivalent.  $\zeta$

**68.** Sketch the surfaces  $Q(X_1, X_2, X_3) = 0$  for all normal forms in the Inertia Theorem with  $n = 3$ .

**69.** How many equivalence classes are there in the Inertia Theorem for quadratic forms in  $n$  variables?  $\checkmark$

**70.\*** Prove the Orthogonal Diagonalization Theorem for  $n = 2$  using results of Section 2.  $\zeta$

**71.** Classify ODEs  $\dot{x} = ax$  up to the changes  $x = cy$ ,  $c \neq 0$ .  $\checkmark$

**72.** Verify that  $y(t) = e^{\lambda t} (c_0 + tc_1 + \dots + c_{m-1}t^{m-1})$ , where  $c_i \in \mathbb{C}$  are arbitrary constants, is the general solution to the ODE  $(\frac{d}{dt} - \lambda)^m y = 0$ .

**73.** Using the **binomial formula**  $(a+b)^m = \sum_{k=0}^m \binom{m}{k} a^k b^{m-k}$ , show that the Jordan cell of size  $m$  with the eigenvalue  $\lambda$  can be written as the  $m$ -th order ODE

$$y^{(m)} - \binom{m}{1} \lambda y^{(m-1)} + \dots + (-1)^{m-1} \binom{m}{m-1} \lambda^{m-1} y' + (-1)^m y = 0.$$

**74.\*** Prove that the **binomial coefficient**  $\binom{m}{k}$  “ $m$  choose  $k$ ” is equal to the number of  $k$ -element subsets in a set of  $m$  elements.  $\zeta$

**75.\*** Prove that  $\binom{m}{k} = \frac{m!}{k!(m-k)!}$ .

**76.** Rewrite the *pendulum* equation  $\ddot{x} = -x$  as a system.  $\zeta$

**77.\*** Identify the Jordan form of the system  $\dot{x}_1 = x_2$ ,  $\dot{x}_2 = -x_1$ .  $\checkmark$

**78.\*** Solve the following Jordan systems and show that they are not equivalent to each other:

$$\begin{array}{lcl} \dot{x}_1 & = & \lambda x_1 \\ \dot{x}_2 & = & \lambda x_2 \end{array} \quad \text{and} \quad \begin{array}{lcl} \dot{y}_1 & = & \lambda y_1 + y_2 \\ \dot{y}_2 & = & \lambda y_2 \end{array}. \quad \zeta$$

**79.** How many arbitrary coefficients are there in a quadratic form in  $n$  variables?  $\checkmark$

**80.\*** Show that equivalence classes of *triples* of quadratic forms in  $n$  variables must depend on at least  $n^2/2$  parameters.  $\zeta$

# Chapter 2

## Dramatis Personae

### 1 Matrices

**Matrices** are rectangular arrays of numbers. An  $m \times n$ -matrix

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & a_{ij} & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

has  $m$  rows and  $n$  columns. The **matrix entry**  $a_{ij}$  is positioned in row  $i$  and column  $j$ .

We usually assume that the matrix entries are taken from either of the fields  $\mathbb{R}$  or  $\mathbb{C}$  of real or complex numbers respectively. These two choices are sufficient for all our major goals. However all we use is basic properties of addition and multiplication of numbers. Thus everything we say in this section (and in the next section about determinants) works well when matrix entries are taken from *any* field (or even any commutative **ring** with unity, e.g. the ring  $\mathbb{Z}$  of all integers, where multiplication is commutative, but division by non-zero numbers is not always defined). Various choices of a field will be discussed at the beginning of Section 3 on vector spaces.

Matrices are found in Linear Algebra all over the place. Yet, the main point of this section is that matrices *per se* are not objects of Linear Algebra. Namely, the same matrix  $A$  can represent different mathematical objects, and will behave differently depending on what kind of object is meant by it.

## Vectors

The standard convention is that vectors are represented by *columns* of their coordinates. Thus,  $\lambda \mathbf{x}$  and  $\mathbf{x} + \mathbf{y}$  are expressed in coordinates by the following operations with  $3 \times 1$ -matrices:

$$\lambda \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \lambda x_2 \\ \lambda x_3 \end{bmatrix}, \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{bmatrix}.$$

More generally, one refers to  $n \times 1$ -matrices as **coordinate vectors**, which can be term-wise multiplied by scalars or added. Such vectors form the **coordinate space**  $\mathbb{R}^n$  (or  $\mathbb{C}^n$ , or  $\mathbb{Q}^n$ , if the matrix entries and the scalars are taken to be complex or rational numbers).

## Linear Functions

A **linear function** (or **linear form**) on the coordinate space has the form

$$\mathbf{a}(\mathbf{x}) = a_1x_1 + \cdots + a_nx_n$$

and is determined by the *row*  $[a_1, \dots, a_n]$  of its coefficients. Linear combinations  $\lambda \mathbf{a} + \mu \mathbf{b}$  of linear functions are linear functions. Their coefficients are expressed by linear combinations of  $1 \times n$ -matrices:

$$\lambda[a_1, \dots, a_n] + \mu[b_1, \dots, b_n] = [\lambda a_1 + \mu b_1, \dots, \lambda a_n + \mu b_n].$$

The operation of **evaluation**, i.e. taking the value  $\mathbf{a}(\mathbf{x})$  of a linear function on a vector, leads to the simplest instance of **matrix product**, namely the product of a  $1 \times n$  row with an  $n \times 1$  column:

$$\mathbf{a}(\mathbf{x}) = [a_1, \dots, a_n] \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} = a_1x_1 + \cdots + a_nx_n.$$

Note that

$$\mathbf{a}(\lambda \mathbf{x} + \mu \mathbf{y}) = \lambda \mathbf{a}(\mathbf{x}) + \mu \mathbf{a}(\mathbf{y}) \text{ for all vectors } \mathbf{x}, \mathbf{y} \text{ and scalars } \lambda, \mu.$$

This can be viewed as a manifestation of the **distributive law** for matrix product. As we will see later, it actually expresses the very property of **linearity**, namely, the property of linear functions to *respect* operations with vectors, i.e. to assign to linear combinations of vectors linear combinations of respective values with the same coefficients.

## Linear Maps

An  $m$ -tuple of linear functions  $\mathbf{a}_1, \dots, \mathbf{a}_m$  in  $n$  variables defines a **linear map**  $A : \mathbb{R}^n \rightarrow \mathbb{R}^m$ . Namely, to a vector  $\mathbf{x} \in \mathbb{R}^n$  it associates the vector  $\mathbf{y} = \mathbf{A}\mathbf{x} \in \mathbb{R}^m$  whose  $m$  components are computed as

$$y_i = \mathbf{a}_i(\mathbf{x}) = a_{i1}x_1 + \dots + a_{in}x_n, \quad i = 1, \dots, m.$$

Whereas each  $y_i$  is given by the product of a row with a column, the whole linear map can be described as the product of the  $m \times n$ -matrix  $A$  with the column:

$$\mathbf{y} = \begin{bmatrix} y_1 \\ \dots \\ y_m \end{bmatrix} = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} = \mathbf{A}\mathbf{x}.$$

The rows of the matrix  $A$  represent the  $m$  linear functions  $\mathbf{a}_1, \dots, \mathbf{a}_m$ . To interpret the columns, note that every vector  $\mathbf{x}$  can be uniquely written as a linear combination  $\mathbf{x} = x_1\mathbf{e}_1 + \dots + x_n\mathbf{e}_n$  of the **standard basis** vectors  $\mathbf{e}_1, \dots, \mathbf{e}_n$ :

$$\begin{bmatrix} x_1 \\ \dots \\ \dots \\ x_n \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \\ \dots \\ 0 \end{bmatrix} + \dots + x_n \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \end{bmatrix}.$$

Respectively,  $\mathbf{A}\mathbf{x} = x_1\mathbf{A}\mathbf{e}_1 + \dots + x_n\mathbf{A}\mathbf{e}_n$ . The  $n$  columns of the matrix  $A$  are exactly  $\mathbf{A}\mathbf{e}_j$ ,  $j = 1, \dots, n$ , i.e. the *images* in  $\mathbb{R}^m$  of the standard basis vectors from  $\mathbb{R}^n$  under the linear map  $A$ .

Given linear maps  $B : \mathbb{R}^n \rightarrow \mathbb{R}^m$  and  $A : \mathbb{R}^m \rightarrow \mathbb{R}^l$ , we can form their **composition**  $\mathbb{R}^n \rightarrow \mathbb{R}^l$  by substituting  $\mathbf{y} = \mathbf{B}\mathbf{x}$  into  $\mathbf{z} = \mathbf{A}\mathbf{y}$ . The corresponding operation with the matrices  $A$  and  $B$  leads to the general notion of **matrix product**  $C = \mathbf{A}\mathbf{B}$  defined whenever the number of columns of  $A$  coincides with the number of rows of  $B$ :

$$\begin{bmatrix} c_{11} & \dots & c_{1n} \\ \dots & c_{ij} & \dots \\ c_{l1} & \dots & c_{ln} \end{bmatrix} = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{l1} & \dots & a_{lm} \end{bmatrix} \begin{bmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{bmatrix}.$$

By definition of composition, the entry  $c_{ij}$  located at the intersection of the  $i$ th row and  $j$ th column of  $C$  is the value of the linear function  $\mathbf{a}_i$  on the image  $\mathbf{B}\mathbf{e}_j \in \mathbb{R}^m$  of the standard basis vector  $\mathbf{e}_j \in \mathbb{R}^n$ .

Since  $\mathbf{a}_i$  and  $B\mathbf{e}_j$  are represented by the  $i$ th row and  $j$ th column respectively of the matrices  $A$  and  $B$ , we find:

$$c_{ij} = [a_{i1}, \dots, a_{im}] \begin{bmatrix} b_{1j} \\ \dots \\ b_{mj} \end{bmatrix} = a_{i1}b_{1j} + \dots + a_{im}b_{mj}.$$

In other words,  $c_{ij}$  is the product of the  $i$ th row of  $A$  with the  $j$ th column of  $B$ .

Based on this formula, it is not hard to verify that the matrix product is **associative**, i.e.  $(AB)C = A(BC)$ , and satisfies the *left* and *right* distributive laws:  $P(\lambda Q + \mu R) = \lambda PQ + \mu PR$  and  $(\lambda X + \mu Y)Z = \lambda XZ + \mu YZ$ , whenever the sizes of the matrices are right. However, one of the key points in mathematics is that there is no point in making such verifications. The operations with matrices encode in the coordinate form meaningful operations with linear maps, and the properties of matrices simply reflect those of the maps. For instance, matrix product is associative because composition of *arbitrary* (and not only linear) maps is associative. We will have a chance to discuss properties of linear maps in the more general context of abstract vector spaces, where coordinate expressions may not even be available.

## Changes of Coordinates

Suppose that standard coordinates  $(x_1, \dots, x_n)$  in  $\mathbb{R}^n$  are expressed in terms of new variables  $(x'_1, \dots, x'_n)$  by means of  $n$  linear functions:

$$\begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} = \begin{bmatrix} c_{11} & \dots & c_{1n} \\ \dots & & \dots \\ c_{n1} & \dots & c_{nn} \end{bmatrix} \begin{bmatrix} x'_1 \\ \dots \\ x'_n \end{bmatrix}.$$

In matrix notation, this can be written as  $\mathbf{x} = C\mathbf{x}'$  where  $C$  is the **square matrix** of size  $n$ . We call this a linear **change of coordinates**, if conversely,  $\mathbf{x}'$  can be expressed by linear functions of  $\mathbf{x}$ . In other words, there must exist a square matrix  $D$  such that the substitutions  $\mathbf{x}' = D\mathbf{x}$  and  $\mathbf{x} = C\mathbf{x}'$  are inverse to each other, i.e.  $\mathbf{x} = CD\mathbf{x}$  and  $\mathbf{x}' = DC\mathbf{x}'$  for all  $\mathbf{x}$  and  $\mathbf{x}'$ . It is immediate to see that this happens exactly when the matrices  $C$  and  $D$  satisfy  $CD = I = DC$  where  $I$  is the **identity matrix** of size  $n$ :

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



When this happens, the square matrices  $C$  and  $D$  are called **inverse** to each other, and one writes:  $D = C^{-1}$ ,  $C = D^{-1}$ . The rows of  $C$  express old coordinates  $x_i$  as linear functions of new coordinates,  $x'_j$ . The columns of  $C$  represent, in the old coordinate system, the vectors which in the new coordinate system serve as standard basis vectors  $\mathbf{e}'_j$ . The matrix  $C$  is often called the **transition matrix** between the coordinate systems.

In spite of apparent simplicity of this notion, it is easy to get lost here. As we noticed in connection with rotations on the complex plane, a change of coordinates is easy to confuse with a linear map from the space  $\mathbb{R}^n$  to itself. We will reserve for such maps the term **linear transformation**. Thus, the formula  $\mathbf{x}' = C\mathbf{x}$  describes a linear transformation, that associates to a vector  $\mathbf{x} \in \mathbb{R}^n$  a new vector  $\mathbf{x}'$  written in the same coordinate system. The **inverse transformation**, when exists, is given by the formula  $\mathbf{x} = C^{-1}\mathbf{x}'$ .

Let us now return to changes of coordinates and examine how they affect linear functions and maps.

Making the change of variables  $\mathbf{x} = C\mathbf{x}'$  in a linear function  $\mathbf{a}$  results in the values  $\mathbf{a}(\mathbf{x})$  of this function being expressed as  $\mathbf{a}'(\mathbf{x}')$  in terms of new coordinates of the same vectors. Using the matrix product notation, we find:  $\mathbf{a}'\mathbf{x}' = \mathbf{a}\mathbf{x} = \mathbf{a}(C\mathbf{x}') = (\mathbf{a}C)\mathbf{x}'$ . Thus, coordinates of vectors and coefficients of linear functions are transformed differently:

$$\mathbf{x} = C\mathbf{x}', \text{ or } \mathbf{x}' = C^{-1}\mathbf{x}, \text{ but } \mathbf{a}' = \mathbf{a}C, \text{ or } \mathbf{a} = \mathbf{a}'C^{-1}.$$

Next, let  $\mathbf{y} = A\mathbf{x}$  be a linear map from  $\mathbb{R}^n$  to  $\mathbb{R}^m$ , and let  $\mathbf{x} = C\mathbf{x}'$  and  $\mathbf{y} = D\mathbf{y}'$  be changes of coordinates in  $\mathbb{R}^n$  and  $\mathbb{R}^m$  respectively. Then in new coordinates the same linear map is given by the new formula  $\mathbf{y}' = A'\mathbf{x}'$ . We compute  $A'$  in terms of  $A$ ,  $C$  and  $D$ :  $D\mathbf{y}' = \mathbf{y} = A\mathbf{x} = AC\mathbf{x}'$ , i.e.  $\mathbf{y}' = D^{-1}AC\mathbf{x}'$ , and hence

$$A' = D^{-1}AC.$$

In particular, if  $\mathbf{x} \mapsto A\mathbf{x}$  is a linear transformation on  $\mathbb{R}^n$  (i.e. — we remind — a linear map from  $\mathbb{R}^n$  to itself), and a change of coordinates  $\mathbf{x} = C\mathbf{x}'$  is made, then in new coordinates the same linear transformation is  $\mathbf{x}' \mapsto A'\mathbf{x}'$ , where

$$A' = C^{-1}AC,$$

i.e. in the the previous rule we need to take  $D = C$ . This is because the same change applies to both: the input vector  $\mathbf{x}$  and its image  $A\mathbf{x}$ . The operation  $A \mapsto C^{-1}AC$  over a square matrix  $A$  is often called the **similarity transformation** by the invertible matrix  $C$ .

## Bilinear Forms

The **dot product** of two coordinate vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$  is defined by the formula

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + \cdots + x_ny_n.$$

It is an example of a **bilinear form**, i.e. a function of an ordered pair  $(\mathbf{x}, \mathbf{y})$  of vector variables, which is a linear function of each of them. In general, the vectors may come from different spaces,  $\mathbf{x} \in \mathbb{R}^m$  and  $\mathbf{y} \in \mathbb{R}^n$ . We can write a bilinear form as a linear function of  $x_i$  whose coefficients are linear functions of  $y_j$ :

$$B(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m x_i \sum_{j=1}^n b_{ij}y_j = \sum_{i=1}^m \sum_{j=1}^n x_i b_{ij}y_j.$$

Thus the bilinear form  $B$  is determined by the  $m \times n$ -matrix of its coefficients  $b_{ij}$ . Slightly abusing notation, we will denote this matrix with the same letter  $B$  as the bilinear form. Here is the meaning of the matrix entries:  $b_{ij} = B(\mathbf{e}_i, \mathbf{f}_j)$ , the value of the form on the pair of standard basis vectors,  $\mathbf{e}_i \in \mathbb{R}^m$  and  $\mathbf{f}_j \in \mathbb{R}^n$ .

With a bilinear form  $B$  of  $\mathbf{x}$  and  $\mathbf{y}$ , one associates another bilinear form called **transposed** to  $B$ , which is a function of  $\mathbf{y}$  and  $\mathbf{x}$  (in this order!), denoted  $B^t$ , and defined by  $B^t(\mathbf{y}, \mathbf{x}) = B(\mathbf{x}, \mathbf{y})$ . Explicitly:

$$\sum_{i=1}^n \sum_{j=1}^m y_i b_{ij}^t x_j = B^t(\mathbf{y}, \mathbf{x}) = B(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^m \sum_{i=1}^n x_j b_{ji} y_i.$$

We conclude that  $b_{ij}^t = b_{ji}$ . In other words, the  $n \times m$ -matrix of coefficients of  $B^t$  is obtained from the  $m \times n$ -matrix  $B$  by the operation of **transposition**:

$$B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix}, \quad B^t = \begin{bmatrix} b_{11} & b_{n1} \\ \cdots & \cdots \\ b_{1m} & b_{nm} \end{bmatrix}.$$

Note that transposition transforms rows into columns, thus messing up our convention to represent vectors by columns and linear functions by rows. Taking advantage of this, we can compute values of bilinear forms using matrix product and transposition:

$$B(\mathbf{x}, \mathbf{y}) = \mathbf{x}^t B \mathbf{y}, \quad B^t(\mathbf{y}, \mathbf{x}) = \mathbf{y}^t B^t \mathbf{x}.$$

In particular, when  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ , we have:  $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^t \mathbf{y}$ .

To find out how changes of variables  $\mathbf{x} = D\mathbf{x}'$ ,  $\mathbf{y} = C\mathbf{y}'$  transform the matrix of a bilinear form, take  $B'(\mathbf{x}', \mathbf{y}') = B(D\mathbf{x}', C\mathbf{y}')$ , the value  $B(\mathbf{x}, \mathbf{y})$  written in new coordinates. We have:  $b'_{ij} = B'(\mathbf{e}_i, \mathbf{f}_j) = B(D\mathbf{e}_i, C\mathbf{f}_j) = (D\mathbf{e}_i)^t B(C\mathbf{f}_j)$ . Note that  $(D\mathbf{e}_i)^t$  is the transposed  $i$ th column of  $D$ , i.e. the  $i$ th row of  $D^t$ , and  $B(C\mathbf{f}_j)$  is the  $j$ th column of  $BC$ . Combining these results for all  $i$  and  $j$ , we find:

$$B' = D^t B C.$$

Were the same matrix  $B$  representing a linear map, the transformation law would've been different:  $B \mapsto D^{-1} B C$ .

Consider now the case when both vector inputs  $\mathbf{x}, \mathbf{y}$  of a bilinear form  $B$  lie in the same space  $\mathbb{R}^n$ . Then the transposed form  $B^t$  can be evaluated on the same pair of vectors  $(\mathbf{x}, \mathbf{y})$  (in this order!) and the result  $B(\mathbf{y}, \mathbf{x})$  compared with  $B(\mathbf{x}, \mathbf{y})$ . The form  $B$  is called **symmetric** if  $B^t = B$ , i.e.  $B(\mathbf{y}, \mathbf{x}) = B(\mathbf{x}, \mathbf{y})$  for all  $\mathbf{x}, \mathbf{y}$ . It is called **anti-symmetric** if  $B^t = -B$ , i.e.  $B(\mathbf{y}, \mathbf{x}) = -B(\mathbf{x}, \mathbf{y})$  for all  $\mathbf{x}, \mathbf{y}$ . Every bilinear form (of two vectors from the same space) can be uniquely written as the sum of a symmetric and an anti-symmetric bilinear forms:

$$B = \frac{B + B^t}{2} + \frac{B - B^t}{2}.$$

## Quadratic Forms

To a bilinear form  $B$  on  $\mathbb{R}^n$ , one associates a function on  $\mathbb{R}^n$  by substituting the same vector  $\mathbf{x} \in \mathbb{R}^n$  for both inputs:

$$B(\mathbf{x}, \mathbf{x}) = \sum_{i=1}^n \sum_{j=1}^n b_{ij} x_i x_j.$$

The result is a **quadratic form**, i.e. a degree-2 homogeneous polynomial in  $n$  variables  $(x_1, \dots, x_n)$ . Since  $b_{ij}$  can be arbitrary, all quadratic forms are obtained this way.

Moreover, if  $B$  is written as the sum  $S + A$  of symmetric and anti-symmetric forms, then  $A(\mathbf{x}, \mathbf{x}) = -A(\mathbf{x}, \mathbf{x}) = 0$ , and  $B(\mathbf{x}, \mathbf{x}) = S(\mathbf{x}, \mathbf{x})$ , i.e. the quadratic form depends only on the symmetric part of  $B$ . Further abusing our notation, we will write  $S(\mathbf{x})$  for the values  $S(\mathbf{x}, \mathbf{x})$  of the quadratic form corresponding to the bilinear form  $S$ .

The correspondence between symmetric bilinear forms and quadratic forms is not only “onto” but is also “one-to-one,” i.e. the values  $S(\mathbf{x}, \mathbf{y})$  of a symmetric bilinear form can be reconstructed from the values of the corresponding quadratic form. Explicitly:

$$S(\mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y}) = S(\mathbf{x}, \mathbf{x}) + S(\mathbf{x}, \mathbf{y}) + S(\mathbf{y}, \mathbf{x}) + S(\mathbf{y}, \mathbf{y}).$$

Due to the symmetry  $S(\mathbf{x}, \mathbf{y}) = S(\mathbf{y}, \mathbf{x})$ , we have:

$$2S(\mathbf{x}, \mathbf{y}) = S(\mathbf{x} + \mathbf{y}) - S(\mathbf{x}) - S(\mathbf{y}).$$

The transformation law for coefficients of a quadratic form under the changes of variables  $\mathbf{x} = C\mathbf{x}'$  is  $S \mapsto C^t S C$ . Here  $S = S^t$  denotes the **symmetric matrix** of coefficients of the quadratic form

$$S(\mathbf{x}) = \sum_{i=1}^n \sum_{j=1}^n s_{ij} x_i x_j, \quad s_{ij} = s_{ji} \quad \text{for all } i, j.$$

### EXERCISES

**81.** Are the functions  $3x$ ,  $x^3$ ,  $x+1$ ,  $0$ ,  $\sin x$ ,  $(1+x)^2 - (1-x)^2$ ,  $\tan \arctan x$ ,  $\arctan \tan x$  linear? ✓

**82.** Check the *linearity* property of functions  $\mathbf{a}(\mathbf{x}) = \sum a_i x_i$ , i.e. that  $\mathbf{a}(\lambda\mathbf{x} + \mu\mathbf{y}) = \lambda\mathbf{a}(\mathbf{x}) + \mu\mathbf{a}(\mathbf{y})$ .

**83.** Prove that every function on  $\mathbb{R}^n$  that possesses the linearity property has the form  $\sum a_i x_i$ . ✚

**84.** Let  $\mathbf{v} \in \mathbb{R}^m$ , and let  $\mathbf{a} : \mathbb{R}^n \rightarrow \mathbb{R}$  be a linear function. Define a linear map  $E : \mathbb{R}^n \rightarrow \mathbb{R}^m$  by  $E(\mathbf{x}) = \mathbf{a}(\mathbf{x})\mathbf{v}$ , and compute the matrix of  $E$ . ✓

**85.** Write down the matrix of rotation through the angle  $\theta$  in  $\mathbb{R}^2$ . ✓

**86.** Let

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

Compute those of the products  $ABC$ ,  $BAC$ ,  $BCA$ ,  $CBA$ ,  $CAB$ ,  $ACB$  which are defined. ✓

**87.** Let  $\sum_{j=1}^n a_{ij} x_j = b_i$ ,  $i = 1, \dots, m$ , be a system of  $m$  **linear equations** in  $n$  unknowns  $(x_1, \dots, x_n)$ . Show that it can be written in the matrix form  $A\mathbf{x} = \mathbf{b}$ , where  $A$  is a linear map from  $\mathbb{R}^n$  to  $\mathbb{R}^m$ .

**88.** A square matrix  $A$  is called **upper triangular** if  $a_{ij} = 0$  for all  $i < j$  and **lower triangular** if  $a_{ij} = 0$  for all  $i > j$ . Prove that products of upper triangular matrices are upper triangular and products of lower triangular matrices are lower triangular.

**89.** For an identity matrix  $I$ , prove  $AI = A$  and  $IB = B$  for all allowed sizes of  $A$  and  $B$ .

**90.** For a square matrix  $A$ , define its **powers**  $A^k$  for  $k > 0$  as  $A \cdots A$  ( $k$  times), for  $k = 0$  as  $I$ , and for  $k < 0$  as  $A^{-1} \cdots A^{-1}$  ( $k$  times), assuming  $A$  invertible. Prove that  $A$  that  $A^k A^l = A^{k+l}$  for all integer  $k, l$ .

**91.\*** Compute  $\begin{bmatrix} \cos 19^\circ & -\sin 19^\circ \\ \sin 19^\circ & \cos 19^\circ \end{bmatrix}^{19}$ . ✓

**92.** Compute powers  $A^k$ ,  $k = 0, 1, 2, \dots$ , of the square matrix  $A$  all of whose entries are zeroes, except that  $a_{i,i+1} = 1$  for all  $i$ . ✓

**93.** For which sizes of matrices  $A$  and  $B$ , both products  $AB$  and  $BA$ : (a) are defined, (b) have the same size? ✓

**94.\*** Give examples of matrices  $A$  and  $B$  which do not *commute*, i.e.  $AB \neq BA$ , even though both products are defined and have the same size. ✎

**95.** When does  $(A + B)^2 = A^2 + 2AB + B^2$ ? ✓

**96.** A square matrix  $A$  is called **diagonal** if  $a_{ij} = 0$  for all  $i \neq j$ . Which diagonal matrices are invertible? ✓

**97.** Prove that an inverse of a given matrix is unique when exists. ✎

**98.** Let  $A, B$  be invertible  $n \times n$ -matrices. Prove that  $AB$  is also invertible, and  $(AB)^{-1} = B^{-1}A^{-1}$ . ✎

**99.\*** If  $AB$  is invertible, does it imply that  $A$ ,  $B$ , and  $BA$  are invertible? ✎

**100.\*** Give an example of matrices  $A$  and  $B$  such that  $AB = I$ , but  $BA \neq I$ .

**101.** Let  $A : \mathbb{R}^n \rightarrow \mathbb{R}^m$  be an *invertible* linear map. (Thus,  $m = n$ , but we consider  $\mathbb{R}^n$  and  $\mathbb{R}^m$  as two different copies of the coordinate space.) Prove that after suitable changes of coordinates in  $\mathbb{R}^n$  and  $\mathbb{R}^m$ , the matrix of this transformation becomes the identity matrix  $I$ . ✎

**102.** Is the function  $xy$ : linear? bilinear? quadratic? ✓

**103.** Find the coefficient matrix of the dot product. ✓

**104.** Prove that all anti-symmetric bilinear forms in  $\mathbb{R}^2$  are proportional to each other. ✎

**105.** Represent the bilinear form  $B = 2x_1(y_1 + y_2)$  in  $\mathbb{R}^2$  as the sum  $S + A$  of symmetric and anti-symmetric ones. ✓

**106.** Find the symmetric bilinear forms corresponding to the quadratic forms  $(x_1 + \cdots + x_n)^2$  and  $\sum_{i < j} x_i x_j$ . ✓

**107.** Is  $AB$  necessarily symmetric if  $A$  and  $B$  are? ✓

**108.** Prove that for any matrix  $A$ , both  $A^t A$  and  $AA^t$  are symmetric.

**109.** Find a square matrix  $A$  such that  $A^t A \neq AA^t$ . ✎



## 2 Determinants

### Definition

Let  $A$  be a *square* matrix of size  $n$ :

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ & \dots & \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

Its **determinant** is a *scalar*  $\det A$  defined by the formula

$$\det A = \sum_{\sigma} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Here  $\sigma$  is a **permutation** of the indices  $1, 2, \dots, n$ . A permutation  $\sigma$  can be considered as an invertible function  $i \mapsto \sigma(i)$  from the set of  $n$  elements  $\{1, \dots, n\}$  to itself. We use the functional notation  $\sigma(i)$  in order to specify the  $i$ -th term in the permutation  $\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$ . Thus, each **elementary product** in the determinant formula contains exactly one matrix entry from each row, and these entries are chosen from  $n$  different columns. The sum is taken over all  $n!$  ways of making such choices. The coefficient  $\varepsilon(\sigma)$  in front of the elementary product equals 1 or  $-1$  and is called the **sign** of the permutation  $\sigma$ .

We will explain the general rule of the signs after a few examples. In these examples, we begin using one more conventional notation for determinants. According to it, a square array of matrix entries placed between two vertical bars denotes the *determinant* of the matrix. Thus,  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  denotes a *matrix*, but  $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$  denotes a *number* equal to the determinant of that matrix.

**Examples.** (1) For  $n = 1$ , the determinant  $|a_{11}| = a_{11}$ .

(2) For  $n = 2$ , we have:  $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$ .

(3) For  $n = 3$ , we have  $3! = 6$  summands

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32}$   
corresponding to permutations  $\begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}$ .

The rule of signs for  $n = 3$  is schematically shown on Figure 21.

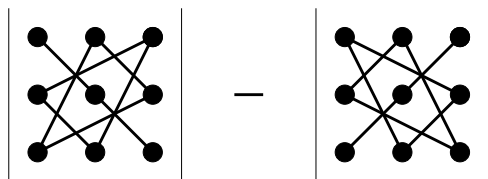


Figure 21

## Parity of Permutations

The general rule of signs depends on properties of permutations.

We say that  $\sigma$  **inverses** a pair of indices  $i < j$  if  $\sigma(i) > \sigma(j)$ . The total number  $l(\sigma)$  of pairs  $i < j$  that  $\sigma$  inverses is called the **length** of the permutation  $\sigma$ . Permutations are called **even** or **odd** depending on their lengths being respectively even or odd. We put  $\varepsilon(\sigma) := (-1)^{l(\sigma)}$  (i.e.  $\varepsilon(\sigma) = 1$  for even and  $-1$  for odd permutations).

**Examples.** (1) If  $l(\sigma) = 0$ , then  $\sigma(1) < \sigma(2) < \dots < \sigma(n)$ , and hence  $\sigma = \text{id}$ , the **identity permutation**. In particular,  $\varepsilon(\text{id}) = 1$ .

(2) Consider a **transposition**  $\tau$ , i.e. a permutation that swaps two indices, say  $i < j$ , leaving all other indices in their respective places. Then  $\tau(j) < \tau(i)$ , i.e.  $\tau$  inverses the pair of indices  $i < j$ . Besides, for every index  $k$  such that  $i < k < j$  we have:  $\tau(j) < \tau(k) < \tau(i)$ , i.e. both pairs  $i < k$  and  $k < j$  are inverted. Note that all other pairs of indices are not inverted by  $\tau$ , and hence  $l(\tau) = 2(j - i) + 1$ . In particular, *every transposition is odd*:  $\varepsilon(\tau) = -1$ .

(3) There are  $n - 1$  transpositions of length 1, namely  $\tau^{(i)}$ ,  $i = 1, \dots, n - 1$ , defined as transpositions of nearby indices  $i$  and  $i + 1$ .

**Lemma.** *Let  $\sigma' = \sigma\tau^{(i)}$  be the composition: a permutation  $\sigma$  preceded by  $\tau^{(i)}$ . Then*

$$l(\sigma') = \begin{cases} l(\sigma) + 1 & \text{if } \sigma(i) < \sigma(i+1) \\ l(\sigma) - 1 & \text{if } \sigma(i) > \sigma(i+1) \end{cases}.$$

*In particular,  $\sigma$  and  $\sigma'$  have opposite parities.*

**Proof.** Indeed,  $\sigma' = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$ , i.e.  $\sigma'$  is obtained from  $\sigma$  by the extra swap of  $\sigma(i)$  and  $\sigma(i + 1)$ . This swap does not affect monotonicity of any pairs of entries, except the monotonicity of  $\sigma(i), \sigma(i + 1)$ , which is reversed.  $\square$



Several corollaries follow immediately.

**Corollary 1.** *Every permutation  $\sigma$ , of length  $l > 0$ , can be represented as a composition  $\tau^{(i_1)} \dots \tau^{(i_l)}$  of  $l$  transpositions of length 1.*

Indeed, locating a pair of nearby indices  $i < i + 1$  inverted by  $\sigma$  and composing  $\sigma$  with  $\tau^{(i)}$  as in Lemma, we obtain a permutation  $\sigma'$  of length  $l - 1$ . Continuing the same way with  $\sigma'$ , we after  $l$  steps arrive at the permutation of length 0, which is the identity permutation (Example (1)). Reversing the order of transpositions, we obtain the required result.

**Corollary 2.** *If a permutation is represented as composition of transpositions of length 1, then the parity of the number of these transpositions coincides with the parity of the permutation.*

Indeed, according to the lemma, precomposing with each transposition of length 1 reverses the parity of the permutation. Since the identity permutation is even, the number of factors  $\tau^{(i)}$  in a composition must be even for even permutations and odd for odd.

**Corollary 3.** *The sign of permutations is multiplicative with respect to compositions:  $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ .*

Indeed, representing each  $\sigma$  and  $\sigma'$  as a composition of transpositions of length 1 and concatenating them, we obtain such a representation for the composition  $\sigma\sigma'$ . The result follows from Corollary 2, since the number (and hence parity) of factors behaves additively under concatenation.

**Corollary 2'.** *If a permutation is represented as a composition of arbitrary transpositions, then the parity of the number of these transpositions coincides with the parity of the permutation.*

Indeed, according to Example (2), every transposition is odd, and hence  $\varepsilon(\tau_1 \cdots \tau_N) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_N) = (-1)^N$ .

Here are some illustrations of the above properties in connection with the definition of determinants.

**Examples.** (4) The transposition (21) is odd. That is why the term  $a_{12}a_{21}$  occurs in  $2 \times 2$ -determinants with the negative sign.

(5) The permutations  $\begin{pmatrix} 123 \\ 123 \end{pmatrix}$ ,  $\begin{pmatrix} 123 \\ 213 \end{pmatrix}$ ,  $\begin{pmatrix} 123 \\ 231 \end{pmatrix}$ ,  $\begin{pmatrix} 123 \\ 321 \end{pmatrix}$ ,  $\begin{pmatrix} 123 \\ 312 \end{pmatrix}$ ,  $\begin{pmatrix} 123 \\ 132 \end{pmatrix}$  have lengths  $l = 0, 1, 2, 3, 2, 1$  and respectively signs  $\varepsilon = 1, -1, 1, -1, 1, -1$  (thus explaining Figure 21). Notice that each next permutation here is obtained from the previous one by an extra flip.

(6) The permutation  $\begin{pmatrix} 1234 \\ 4321 \end{pmatrix}$  inverses all the 6 pairs of indices and has therefore length  $l = 6$ . Thus the elementary product  $a_{14}a_{23}a_{32}a_{41}$  occurs with the sign  $\varepsilon = (-1)^6 = +1$  in the definition of  $4 \times 4$ -determinants.

(7) Permutations  $\sigma$  and  $\sigma^{-1}$  inverse to each other have the same parity since their composition  $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \text{id}$  is even. This shows that the definition of determinants can be rewritten “by columns:”

$$\det A = \sum_{\sigma} \varepsilon(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

Indeed, each summand in this formula is equal to the summand in the original definition corresponding to the permutation  $\sigma^{-1}$ , and *vice versa*. Namely, reordering the factors  $a_{\sigma(1)1} \dots a_{\sigma(n)n}$ , so that  $\sigma(1), \dots, \sigma(n)$  increase monotonically, yields  $a_{1\sigma^{-1}(1)} \dots a_{n\sigma^{-1}(n)}$ .

## Properties of determinants

(i) *Transposed matrices have equal determinants:*

$$\det A^t = \det A.$$

This follows from the last Example. Below, we will think of an  $n \times n$  matrix as an array  $A = [\mathbf{a}_1, \dots, \mathbf{a}_n]$  of its  $n$  columns of size  $n$  (vectors from  $\mathbb{C}^n$  if you wish) and formulate all further properties of determinants in terms of columns. The same properties hold true for rows, since the transposition of  $A$  changes columns into rows without changing the determinant.

(ii) *Interchanging any two columns changes the sign of the determinant:*

$$\det[\dots, \mathbf{a}_j, \dots, \mathbf{a}_i, \dots] = -\det[\dots, \mathbf{a}_i, \dots, \mathbf{a}_j, \dots].$$

Indeed, the operation replaces each permutation in the definition of determinants by its composition with the transposition of the indices  $i$  and  $j$ . Thus changes the parity of the permutation, and thus reverses the sign of each summand.

Rephrasing this property, one says that the determinant, considered as a function of  $n$  vectors  $\mathbf{a}_1, \dots, \mathbf{a}_n$  is **totally anti-symmetric**, i.e. changes the sign under every odd permutation of the vectors, and stays invariant under even. It implies that *a matrix with two equal columns has zero determinant*. It also allows one to formulate further

column properties of determinants referring to the 1st column only, since the properties of all columns are alike.

**(iii) *Multiplication of a column by a number multiplies the determinant by this number:***

$$\det[\lambda \mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n] = \lambda \det[\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n].$$

Indeed, this operation simply multiplies each of the  $n!$  elementary products by the factor of  $\lambda$ .

This property shows that *a matrix with a zero column has zero determinant.*

**(iv) *The determinant function is additive with respect to each column:***

$$\det[\mathbf{a}'_1 + \mathbf{a}''_1, \mathbf{a}_2, \dots, \mathbf{a}_n] = \det[\mathbf{a}'_1, \mathbf{a}_2, \dots, \mathbf{a}_n] + \det[\mathbf{a}''_1, \mathbf{a}_2, \dots, \mathbf{a}_n].$$

Indeed, each elementary product contains exactly one factor picked from the 1-st column and thus splits into the sum of two elementary products  $a'_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n}$  and  $a''_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n}$ . Summing up over all permutations yields the sum of two determinants on the right hand side of the formula.

The properties (iv) and (iii) together mean that *the determinant function is linear with respect to each column* separately. Together with the property (ii), they show that ***adding a multiple of one column to another one does not change the determinant of the matrix.*** Indeed,

$$|\mathbf{a}_1 + \lambda \mathbf{a}_2, \mathbf{a}_2, \dots| = |\mathbf{a}_1, \mathbf{a}_2, \dots| + \lambda |\mathbf{a}_2, \mathbf{a}_2, \dots| = |\mathbf{a}_1, \mathbf{a}_2, \dots|,$$

since the second summand has two equal columns.

The determinant function shears all the above properties with the identically zero function. The following property shows that these functions do not coincide.

$$\text{(v) } \det I = 1.$$

Indeed, since all off-diagonal entries of the identity matrix are zeroes, the only elementary product in the definition of  $\det A$  that survives is  $a_{11} \dots a_{nn} = 1$ .

The same argument shows that *the determinant of any diagonal matrix equals the product of the diagonal entries.* It is not hard to generalize the argument in order to see that the determinant of any

upper or lower triangular matrix is equal to the product of the diagonal entries. One can also deduce this from the following factorization property valid for block triangular matrices.

Consider an  $n \times n$ -matrix  $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$  subdivided into four **blocks**  $A, B, C, D$  of sizes  $m \times m$ ,  $m \times l$ ,  $l \times m$  and  $l \times l$  respectively (where of course  $m + l = n$ ). We will call such a matrix **block triangular** if  $C$  or  $B$  is the zero matrix  $0$ . We claim that

$$\det \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} = \det A \det D.$$

Indeed, consider a permutation  $\sigma$  of  $\{1, \dots, n\}$  which sends at least one of the indices  $\{1, \dots, m\}$  to the other part of the set,  $\{m+1, \dots, m+l\}$ . Then  $\sigma$  must send at least one of  $\{m+1, \dots, m+l\}$  back to  $\{1, \dots, m\}$ . This means that every elementary product in our  $n \times n$ -determinant which contains a factor from  $B$  must also contain a factor from  $C$ , and hence vanish, if  $C = 0$ . Thus only the permutations  $\sigma$  which permute  $\{1, \dots, m\}$  separately from  $\{m+1, \dots, m+l\}$  contribute to the determinant in question. Elementary products corresponding to such permutations factor into elementary products from  $\det A$  and  $\det D$  and eventually add up to the product  $\det A \det D$ .

Of course, the same holds true if  $B = 0$  instead of  $C = 0$ .

We will use the factorization formula in the 1st proof of the following fundamental property of determinants.

## Multiplicativity

**Theorem.** *The determinant is multiplicative with respect to matrix products: for arbitrary  $n \times n$ -matrices  $A$  and  $B$ ,*

$$\det(AB) = (\det A)(\det B).$$

We give two proofs: one *ad hoc*, the other more conceptual.

**Proof I.** Consider the auxiliary  $2n \times 2n$  matrix  $\begin{bmatrix} A & 0 \\ -I & B \end{bmatrix}$  with the determinant equal to the product  $(\det A)(\det B)$  according to the factorization formula. We begin to change the matrix by adding to the last  $n$  columns linear combinations of the first  $n$  columns with such coefficients that the submatrix  $B$  is eventually replaced by zero

submatrix. Thus, in order to kill the entry  $b_{kj}$  we must add the  $b_{kj}$ -multiple of the  $k$ -th column to the  $n + j$ -th column. According to the properties of determinants (see (iv)) these operations do not change the determinant but transform the matrix to the form

$$\begin{bmatrix} A & C \\ -I & 0 \end{bmatrix}.$$

We ask the reader to check that the entry  $c_{ij}$  of the submatrix  $C$  in the upper right corner equals  $a_{i1}b_{1j} + \dots + a_{in}b_{nj}$  so that  $C = AB$  is the matrix product! Now, interchanging the  $i$ -th and  $n + i$ -th columns,  $i = 1, \dots, n$ , we change the determinant by the factor of  $(-1)^n$  and transform the matrix to the form

$$\begin{bmatrix} C & A \\ 0 & -I \end{bmatrix}.$$

The factorization formula applies again and yields  $\det C \det(-I)$ . We conclude that  $\det C = \det A \det B$  since  $\det(-I) = (-1)^n$  compensates for the previous factor  $(-1)^n$ .  $\square$

**Proof II.** We will first show that the properties (i - v) completely characterize  $\det[\mathbf{v}_1, \dots, \mathbf{v}_n]$  as a function of  $n$  columns  $\mathbf{v}_i$  of size  $n$ .

Indeed, consider a function  $f$ , which to  $n$  columns  $\mathbf{v}_1, \dots, \mathbf{v}_n$ , associates a number  $f(\mathbf{v}_1, \dots, \mathbf{v}_n)$ . Suppose that  $f$  is *linear* with respect to each column. Let  $\mathbf{e}_i$  denotes the  $i$ th column of the identity matrix. Since  $\mathbf{v}_1 = \sum_{i=1}^n v_{i1}\mathbf{e}_i$ , we have:

$$f(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n) = \sum_{i=1}^n v_{i1}f(\mathbf{e}_i, \mathbf{v}_2, \dots, \mathbf{v}_n).$$

Using linearity with respect to the 2nd column  $\mathbf{v}_2 = \sum_{j=1}^n v_{j2}\mathbf{e}_j$ , we similarly obtain:

$$f(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n) = \sum_{i=1}^n \sum_{j=1}^n v_{i1}v_{j2}f(\mathbf{e}_i, \mathbf{e}_j, \mathbf{v}_3, \dots, \mathbf{v}_n).$$

Proceeding the same way with all columns, we get:

$$f(\mathbf{v}_1, \dots, \mathbf{v}_n) = \sum_{i_1, \dots, i_n} v_{i_1 1} \cdots v_{i_n n} f(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_n}).$$

Thus,  $f$  is determined by its values  $f(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_n})$  on strings of  $n$  basis vectors.

Let us assume now that  $f$  is *totally anti-symmetric*. Then, if any two of the indices  $i_1, \dots, i_n$  coincide, we have:  $f(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_n}) = 0$ .

All other coefficients correspond to *permutations*  $\sigma = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$  of the indices  $(1, \dots, n)$ , and hence satisfy:

$$f(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_n}) = \varepsilon(\sigma)f(\mathbf{e}_1, \dots, \mathbf{e}_n).$$

Therefore, we find:

$$\begin{aligned} f(\mathbf{v}_1, \dots, \mathbf{v}_n) &= \sum_{\sigma} v_{\sigma(1)1} \dots v_{\sigma(n)n} \varepsilon(\sigma) f(\mathbf{e}_1, \dots, \mathbf{e}_n), \\ &= f(\mathbf{e}_1, \dots, \mathbf{e}_n) \det[\mathbf{v}_1, \dots, \mathbf{v}_n]. \end{aligned}$$

Thus, we have established:

**Proposition 1.** *Every totally anti-symmetric function of  $n$  coordinate vectors of size  $n$  which is linear in each of them is proportional to the determinant function.*

Next, given an  $n \times n$  matrix  $C$ , put

$$f(\mathbf{v}_1, \dots, \mathbf{v}_n) := \det[C\mathbf{v}_1, \dots, C\mathbf{v}_n].$$

Obviously, the function  $f$  is a totally anti-symmetric in all  $\mathbf{v}_i$  (since det is). Multiplication by  $C$  is linear:

$$C(\lambda\mathbf{u} + \mu\mathbf{v}) = \lambda C\mathbf{u} + \mu C\mathbf{v} \quad \text{for all } \mathbf{u}, \mathbf{v} \text{ and } \lambda, \mu.$$

Therefore,  $f$  is linear with respect to each  $\mathbf{v}_i$  (as composition of two linear operations). By the previous result,  $f$  is proportional to det. Since  $C\mathbf{e}_i$  are columns of  $C$ , we conclude that the coefficient of proportionality  $f(\mathbf{e}_1, \dots, \mathbf{e}_n) = \det C$ . Thus, we have found the following interpretation of  $\det C$ .

**Proposition 2.**  *$\det C$  is the factor by which the determinant function of  $n$  vectors  $\mathbf{v}_i$  is multiplied when the vectors are replaced with  $C\mathbf{v}_i$ .*

Now our theorem follows from the fact that when  $C = AB$ , the substitution  $\mathbf{v} \mapsto C\mathbf{v}$  is the composition  $\mathbf{v} \mapsto A\mathbf{v} \mapsto AB\mathbf{v}$  of consecutive substitutions defined by  $A$  and  $B$ . Under the action of  $A$ , the function det is multiplied by the factor  $\det A$ , then under the action of  $B$  by another factor  $\det B$ . But the resulting factor  $(\det A)(\det B)$  must be equal to  $\det C$ .  $\square$

**Corollary.** *If  $A$  is invertible, then  $\det A$  is invertible.*

Indeed,  $(\det A)(\det A^{-1}) = \det I = 1$ , and hence  $\det A^{-1}$  is reciprocal to  $\det A$ . The converse statement: that matrices with invertible determinants are invertible, is also true due to the explicit formula for the inverse matrix, described in the next section.

**Remark.** Of course, a real or complex number  $\det A$  is invertible whenever  $\det A \neq 0$ . Yet over the integers  $\mathbb{Z}$  this is not the case: the only invertible integers are  $\pm 1$ . The above formulation, and several similar formulations that follow, which refer to invertibility of determinants, are preferable as they are more general.

## The Cofactor Theorem

In the determinant formula for an  $n \times n$ -matrix  $A$  each elementary product  $\pm a_{1\sigma(1)} \dots$  begins with one of the entries  $a_{11}, \dots, a_{1n}$  of the first row. The sum of all terms containing  $a_{11}$  in the 1-st place is the product of  $a_{11}$  with the determinant of the  $(n-1) \times (n-1)$ -matrix obtained from  $A$  by crossing out the 1-st row and the 1-st column. Similarly, the sum of all terms containing  $a_{12}$  in the 1-st place looks like the product of  $a_{12}$  with the determinant obtained by crossing out the 1-st row and the 2-nd column of  $A$ . In fact it differs by the factor of  $-1$  from this product, since switching the columns 1 and 2 changes signs of all terms in the determinant formula and interchanges the roles of  $a_{11}$  and  $a_{12}$ . Proceeding in this way with  $a_{13}, \dots, a_{1n}$  we arrive at the **cofactor expansion** formula for  $\det A$  which can be stated as follows.

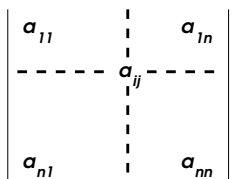


Figure 22

$i \setminus j$	1	2	3	4	5
1	+	-	+	-	+
2	-	+	-	+	-
3	+	-	+	-	+
4	-	+	-	+	-
5	+	-	+	-	+

Figure 23

The determinant of the  $(n-1) \times (n-1)$ -matrix obtained from  $A$  by crossing out the row  $i$  and column  $j$  is called the  $(ij)$ -**minor** of  $A$  (Figure 22). Denote it by  $M_{ij}$ . The  $(ij)$ -**cofactor**  $A_{ij}$  of the matrix  $A$  is the number that differs from the minor  $M_{ij}$  by a factor  $\pm 1$ :

$$A_{ij} = (-1)^{i+j} M_{ij}.$$

The chess-board of the signs  $(-1)^{i+j}$  is shown on Figure 23. With these notations, the cofactor expansion formula reads:

$$\det A = a_{11}A_{11} + a_{12}A_{12} + \dots + a_{1n}A_{1n}.$$

**Example.**

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}.$$

Using the properties (i) and (ii) of determinants we can adjust the cofactor expansion to the  $i$ -th row or  $j$ -th column:

$$\det A = a_{i1}A_{i1} + \dots + a_{in}A_{in} = a_{1j}A_{1j} + \dots + a_{nj}A_{nj}, \quad i, j = 1, \dots, n.$$

These formulas reduce evaluation of  $n \times n$ -determinants to that of  $(n-1) \times (n-1)$ -determinants and can be useful in recursive computations.

Furthermore, we claim that applying the cofactor formula to the entries of the  $i$ -th row but picking the cofactors of another row we get the zero sum:

$$a_{i1}A_{j1} + \dots + a_{in}A_{jn} = 0 \text{ if } i \neq j.$$

Indeed, construct a new matrix  $\tilde{A}$  replacing the  $j$ -th row by a copy of the  $i$ -th row. This forgery does not change the cofactors  $A_{j1}, \dots, A_{jn}$  (since the  $j$ -th row is crossed out anyway) and yields the cofactor expansion  $a_{i1}A_{j1} + \dots + a_{in}A_{jn}$  for  $\det \tilde{A}$ . But  $\tilde{A}$  has two identical rows and hence  $\det \tilde{A} = 0$ . The same arguments applied to the columns yield the dual statement:

$$a_{1i}A_{1j} + \dots + a_{ni}A_{nj} = 0 \text{ if } i \neq j.$$

All the above formulas can be summarized in a single matrix identity. Introduce the  $n \times n$ -matrix  $\text{adj}(A)$ , called **adjoint** to  $A$ , by placing the cofactor  $A_{ij}$  on the intersection of  $j$ -th row and  $i$ -th column. In other words, each  $a_{ij}$  is replaced with the corresponding cofactor  $A_{ij}$ , and then the resulting matrix is transposed:

$$\text{adj} \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & a_{ij} & \dots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} A_{11} & \dots & A_{n1} \\ \dots & A_{ji} & \dots \\ A_{1n} & \dots & A_{nn} \end{bmatrix}.$$

**Theorem.**  $A \text{ adj}(A) = (\det A) I = \text{adj}(A) A$ .

**Corollary.** *If  $\det A$  is invertible then  $A$  is invertible, and*

$$A^{-1} = \frac{1}{\det A} \text{adj}(A).$$

**Example.** If  $ad - bc \neq 0$ , then  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ .



## Cramer's Rule

This is an application of the Cofactor Theorem to systems of linear equations. Consider a system

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ &\dots \\ a_{n1}x_1 + \cdots + a_{nn}x_n &= b_n \end{aligned}$$

of  $n$  linear equations with  $n$  unknowns  $(x_1, \dots, x_n)$ . It can be written in the matrix form

$$A\mathbf{x} = \mathbf{b},$$

where  $A$  is the  $n \times n$ -matrix of the coefficients  $a_{ij}$ ,  $\mathbf{b} = [b_1, \dots, b_n]^t$  is the column of the right hand sides, and  $\mathbf{x}$  is the column of unknowns. In the following Corollary,  $\mathbf{a}_i$  denote columns of  $A$ .

**Corollary.** *If  $\det A$  is invertible then the system of linear equations  $A\mathbf{x} = \mathbf{b}$  has a unique solution given by the formulas:*

$$x_1 = \frac{\det[\mathbf{b}, \mathbf{a}_2, \dots, \mathbf{a}_n]}{\det[\mathbf{a}_1, \dots, \mathbf{a}_n]}, \dots, x_n = \frac{\det[\mathbf{a}_1, \dots, \mathbf{a}_{n-1}, \mathbf{b}]}{\det[\mathbf{a}_1, \dots, \mathbf{a}_n]}.$$

Indeed, when  $\det A \neq 0$ , the matrix  $A$  is invertible. Multiplying the matrix equation  $A\mathbf{x} = \mathbf{b}$  by  $A^{-1}$  on the left, we find:  $\mathbf{x} = A^{-1}\mathbf{b}$ . Thus the solution is unique, and  $x_i = (\det A)^{-1}(A_{1i}b_1 + \dots + A_{ni}b_n)$  according to the cofactor formula for the inverse matrix. But the sum  $b_1A_{1i} + \dots + b_nA_{ni}$  is the cofactor expansion for  $\det[\mathbf{a}_1, \dots, \mathbf{a}_{i-1}, \mathbf{b}, \mathbf{a}_{i+1}, \dots, \mathbf{a}_n]$  with respect to the  $i$ -th column.

**Example.** Suppose that  $a_{11}a_{22} \neq a_{12}a_{21}$ . Then the system

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1 \\ a_{21}x_1 + a_{22}x_2 &= b_2 \end{aligned}$$

has a unique solution

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \quad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}.$$

### Three Cool Formulas

We collect here some useful generalizations of previous results.

**A.** We don't know of any reasonable generalization of determinants to the situation when matrix entries do *not* commute. However the following generalization of the formula  $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc$  is instrumental in some non-commutative applications.<sup>1</sup>

*In the block matrix  $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ , assume that  $D^{-1}$  exists.*

*Then  $\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det(A - BD^{-1}C) \det D$ .*

*Proof:*  $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} I & 0 \\ -D^{-1}C & I \end{bmatrix} = \begin{bmatrix} A - BD^{-1}C & B \\ 0 & D \end{bmatrix}$ .

**B. Lagrange's formula**<sup>2</sup> below generalizes cofactor expansions.

By a **multi-index**  $I$  of length  $|I| = k$  we mean an increasing sequence  $i_1 < \dots < i_k$  of  $k$  indices from the set  $\{1, \dots, n\}$ . Given and  $n \times n$ -matrix  $A$  and two multi-indices  $I, J$  of the same length  $k$ , we define the  $(IJ)$ -**minor** of  $A$  as the determinant of the  $k \times k$ -matrix formed by the entries  $a_{i_\alpha j_\beta}$  of  $A$  located at the intersections of the rows  $i_1, \dots, i_k$  with columns  $j_1, \dots, j_k$  (see Figure 24). Also, denote by  $\bar{I}$  the multi-index **complementary** to  $I$ , i.e. formed by those  $n - k$  indices from  $\{1, \dots, n\}$  which are *not* contained in  $I$ .

*For each multi-index  $I = (i_1, \dots, i_k)$ , the following cofactor expansion with respect to rows  $i_1, \dots, i_k$  holds true:*

$$\det A = \sum_{J:|J|=k} (-1)^{i_1+\dots+i_k+j_1+\dots+j_k} M_{IJ} M_{\bar{I}\bar{J}},$$

*where the sum is taken over all multi-indices  $J = (j_1, \dots, j_k)$  of length  $k$ .*

Similarly, one can similarly write Lagrange's cofactor expansion formula with respect to given  $k$  columns.

**Example.** Let  $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4$  and  $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4$  be 8 vectors on the plane. Then  $\begin{vmatrix} \mathbf{a}_1 & \mathbf{a}_2 & \mathbf{a}_3 & \mathbf{a}_4 \\ \mathbf{b}_1 & \mathbf{b}_2 & \mathbf{b}_3 & \mathbf{b}_4 \end{vmatrix} = |\mathbf{a}_1 \ \mathbf{a}_2| |\mathbf{b}_3 \ \mathbf{b}_4| - |\mathbf{a}_1 \ \mathbf{a}_3| |\mathbf{b}_2 \ \mathbf{b}_4| + |\mathbf{a}_1 \ \mathbf{a}_4| |\mathbf{b}_2 \ \mathbf{b}_3| - |\mathbf{a}_2 \ \mathbf{a}_3| |\mathbf{b}_1 \ \mathbf{b}_4| + |\mathbf{a}_2 \ \mathbf{a}_4| |\mathbf{b}_1 \ \mathbf{b}_3| - |\mathbf{a}_3 \ \mathbf{a}_4| |\mathbf{b}_1 \ \mathbf{b}_2|$ .

<sup>1</sup>Notably in the definition of *Berezinian* in super-mathematics [7].

<sup>2</sup>After Joseph-Louis **Lagrange** (1736–1813).

In the proof of Lagrange's formula, it suffices to assume that it is written with respect to the *first*  $k$  rows, i.e. that  $I = (1, \dots, k)$ . Indeed, interchanging them with the rows  $i_1 < \dots < i_k$  takes  $(i_1 - 1) + (i_2 - 2) + \dots + (i_k - k)$  transpositions, which is accounted for by the sign  $(-1)^{i_1 + \dots + i_k}$  in the formula.

Next, multiplying out  $M_{IJ}M_{\bar{I}\bar{J}}$ , we find  $k!(n - k)!$  elementary products of the form:

$$\pm a_{1,j_{\alpha_1}} \cdots a_{k,j_{\alpha_k}} a_{k+1,\bar{j}_{\beta_1}} \cdots a_{n,\bar{j}_{\beta_{n-k}}},$$

where  $\alpha = \begin{pmatrix} 1 & \cdots & k \\ \alpha_1 & \cdots & \alpha_k \end{pmatrix}$  and  $\beta = \begin{pmatrix} 1 & \cdots & n - k \\ \beta_1 & \cdots & \beta_{n-k} \end{pmatrix}$  are permutations, and  $j_{\alpha_\mu} \in J$ ,  $\bar{j}_{\beta_\nu} \in \bar{J}$ . It is clear that the total sum over multi-indices  $I$  contains each elementary product from  $\det A$ , and does it exactly once. Thus, to finish the proof, we need to compare the signs.

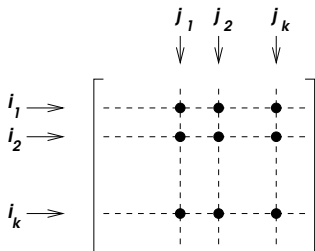


Figure 24

The sign  $\pm$  in the above formula is equal to  $\varepsilon(\alpha)\varepsilon(\beta)$ , the product of the signs of the permutations  $\alpha$  and  $\beta$ . The sign of this elementary product in the definition of  $\det A$  is equal to the sign of the permutation  $\begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ j_{\alpha_1} & \cdots & j_{\alpha_k} & \bar{j}_{\beta_1} & \cdots & \bar{j}_{\beta_{n-k}} \end{pmatrix}$  on the set  $J \cup \bar{J} = \{1, \dots, n\}$ . Reordering separately the first  $k$  and last  $n - k$  indices in the increasing order changes the sign of the permutation by  $\varepsilon(\alpha)\varepsilon(\beta)$ . Therefore the signs of all summands of  $\det A$  which occur in  $M_{IJ}M_{\bar{I}\bar{J}}$  are *coherent*. It remains to find the total sign with which  $M_{IJ}M_{\bar{I}\bar{J}}$  occurs in  $\det A$ , by computing the sign of the permutation  $\sigma := \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ j_1 & \cdots & j_k & \bar{j}_1 & \cdots & \bar{j}_{n-k} \end{pmatrix}$ , where  $j_1 < \dots < j_k$  and  $\bar{j}_1 < \dots < \bar{j}_{n-k}$ .

Starting with the identity permutation  $(1, 2, \dots, j_1, \dots, j_2, \dots, n)$ , it takes  $j_1 - 1$  transpositions of nearby indices to move  $j_1$  to the 1st place. Then it takes  $j_2 - 2$  such transpositions to move  $j_2$  to the 2nd

place. Continuing this way, we find that

$$\varepsilon(\sigma) = (-1)^{(j_1-1)+\dots+(j_k-k)} = (-1)^{1+\dots+k+j_1+\dots+j_k}.$$

This agrees with Lagrange's formula, since  $I = \{1, \dots, k\}$ .  $\square$

**C.** Let  $A$  and  $B$  be  $k \times n$  and  $n \times k$  matrices (think of  $k < n$ ). For each multi-index  $I = (i_1, \dots, i_k)$ , denote by  $A_I$  and  $B_I$  the  $k \times k$ -matrices formed by respectively: columns of  $A$  and rows of  $B$  with the indices  $i_1, \dots, i_k$ .

**The determinant of the  $k \times k$ -matrix  $AB$  is given by the following Binet–Cauchy formula:<sup>3</sup>**

$$\det AB = \sum_I (\det A_I)(\det B_I).$$

Note that when  $k = n$ , this turns into the multiplicative property of determinants:  $\det(AB) = (\det A)(\det B)$ . Our second proof of it can be generalized to establish the formula of Binet–Cauchy. Namely, let  $\mathbf{a}_1, \dots, \mathbf{a}_n$  denote columns of  $A$ . Then the  $j$ th column of  $C = AB$  is the linear combination:  $\mathbf{c}_j = \mathbf{a}_1 b_{1j} + \dots + \mathbf{a}_n b_{nj}$ . Using linearity in each  $\mathbf{c}_j$ , we find:

$$\det[\mathbf{c}_1, \dots, \mathbf{c}_k] = \sum_{1 \leq i_1, \dots, i_k \leq k} \det[\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_k}] b_{i_1 1} \cdots b_{i_k k}.$$

If any two of the indices  $i_\alpha$  coincide,  $\det[\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_k}] = 0$ . Thus the sum is effectively taken over all *permutations*  $\begin{pmatrix} 1 & \cdots & k \\ i_1 & \cdots & i_k \end{pmatrix}$  on the set<sup>4</sup>  $\{i_1, \dots, i_k\}$ . Reordering the columns  $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_k}$  in the increasing order of the indices (an paying the “fees”  $\pm 1$  according to parities of permutations) we obtain the sum over all multi-indices of length  $k$ :

$$\sum_{i'_1 < \dots < i'_k} \det[\mathbf{a}_{i'_1}, \dots, \mathbf{a}_{i'_k}] \sum_{\sigma} \varepsilon(\sigma) b_{i_1 1} \cdots b_{i_k k}.$$

The sum on the right is taken over permutations  $\sigma' = \begin{pmatrix} i'_1 & \cdots & i'_k \\ i_1 & \cdots & i_k \end{pmatrix}$ . It is equal to  $\det B_I$ , where  $I = (i'_1, \dots, i'_k)$ .  $\square$

**Corollary 1.** *If  $k > n$ ,  $\det AB = 0$ .*

<sup>3</sup>After Jacques **Binet** (1786–1856) and Augustin Louis **Cauchy** (1789–1857).

<sup>4</sup>Remember that in a set, elements are unordered!

This is because no multi-indices of length  $k > n$  can be formed from  $\{1, \dots, n\}$ . In the oppositely extreme case  $k = 1$ , Binet–Cauchy’s formula turns into the expression  $\mathbf{u}^t \mathbf{v} = \sum u_i v_i$  for the dot product of coordinate vectors. A “Pythagorean” interpretation of the following identity will come to light in the next chapter, in connection with volumes of parallelepipeds.

Corollary 2.  $\det AA^t = \sum_I (\det A_I)^2$ .

### EXERCISES

110. Prove that the following determinant is equal to 0:

$$\begin{vmatrix} 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & c & d \\ 0 & 0 & 0 & e & f \\ p & q & r & s & t \\ v & w & x & y & z \end{vmatrix}. \quad \zeta$$

111. Compute determinants:

$$\begin{vmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{vmatrix}, \quad \begin{vmatrix} \cosh x & \sinh x \\ \sinh x & \cosh x \end{vmatrix}, \quad \begin{vmatrix} \cos x & \sin y \\ \sin x & \cos y \end{vmatrix}. \quad \checkmark$$

112. Compute determinants:

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{vmatrix}, \quad \begin{vmatrix} 0 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{vmatrix}, \quad \begin{vmatrix} 1 & i & 1+i \\ -i & 1 & 0 \\ 1-i & 0 & 1 \end{vmatrix}. \quad \checkmark$$

113. List all the 24 permutations of  $\{1, 2, 3, 4\}$ , find the length and the sign of each of them.  $\zeta$

114. Find the length of the following permutation:

$$\left( \begin{array}{cccccccc} 1 & 2 & \dots & k & k+1 & k+2 & \dots & 2k \\ 1 & 3 & \dots & 2k-1 & 2 & 4 & \dots & 2k \end{array} \right). \quad \checkmark$$

115. Find the maximal possible length of permutations of  $\{1, \dots, n\}$ .  $\zeta$

116. Find the length of a permutation  $\left( \begin{array}{ccc} 1 & \dots & n \\ i_1 & \dots & i_n \end{array} \right)$  given the length  $l$  of the permutation  $\left( \begin{array}{ccc} 1 & \dots & n \\ i_n & \dots & i_1 \end{array} \right)$ .  $\checkmark$

117. Prove that inverse permutations have the same length.  $\zeta$

118. Compare parities of permutations of the letters  $a, g, h, i, l, m, o, r, t$  in the words *logarithm* and *algorithm*.  $\zeta$

**119.** Represent the permutation  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$  as composition of a minimal number of transpositions. ✓

**120.** Do products  $a_{13}a_{24}a_{53}a_{41}a_{35}$  and  $a_{21}a_{13}a_{34}a_{55}a_{42}$  occur in the defining formula for determinants of size 5? ✓

**121.** Find the signs of the elementary products  $a_{23}a_{31}a_{42}a_{56}a_{14}a_{65}$  and  $a_{32}a_{43}a_{14}a_{51}a_{66}a_{25}$  in the definition of determinants of size 6 by computing the numbers of inverted pairs of indices. ✓

**122.** Compute the determinants

$$\begin{vmatrix} 13247 & 13347 \\ 28469 & 28569 \end{vmatrix}, \quad \begin{vmatrix} 246 & 427 & 327 \\ 1014 & 543 & 443 \\ -342 & 721 & 621 \end{vmatrix}. \quad \checkmark$$

**123.** The numbers 195, 247, and 403 are divisible by 13. Prove that the following determinant is also divisible by 13:  $\begin{vmatrix} 1 & 9 & 5 \\ 2 & 4 & 7 \\ 4 & 0 & 3 \end{vmatrix}$ . ✗

**124.** Professor Dumbel writes his office and home phone numbers as a  $7 \times 1$ -matrix  $O$  and  $1 \times 7$ -matrix  $H$  respectively. Help him compute  $\det(OH)$ . ✓

**125.** How does a determinant change if all its  $n$  columns are rewritten in the opposite order? ✓

**126.\*** Solve the equation  $\begin{vmatrix} 1 & x & x^2 & \dots & x^n \\ 1 & a_1 & a_1^2 & \dots & a_1^n \\ 1 & a_2 & a_2^2 & \dots & a_2^n \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n & a_n^2 & \dots & a_n^n \end{vmatrix} = 0$ , where all  $a_1, \dots, a_n$  are given distinct numbers. ✓

**127.** Prove that an anti-symmetric matrix of size  $n$  has zero determinant if  $n$  is odd. ✗

**128.** How do similarity transformations of a given matrix affect its determinant? ✓

**129.** Prove that the adjoint matrix of an upper (lower) triangular matrix is upper (lower) triangular.

**130.** Which triangular matrices are invertible?

**131.** Compute the determinants: (\* is a wild card):

$$(a) \begin{vmatrix} * & * & * & a_n \\ * & * & \dots & 0 \\ * & a_2 & 0 & \dots \\ a_1 & 0 & \dots & 0 \end{vmatrix}, \quad (b) \begin{vmatrix} * & * & a & b \\ * & * & c & d \\ e & f & 0 & 0 \\ g & h & 0 & 0 \end{vmatrix}. \quad \checkmark$$

**132.** Compute determinants using cofactor expansions:

$$(a) \begin{vmatrix} 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 1 & 1 \\ 0 & 2 & 0 & 1 \end{vmatrix}, \quad (b) \begin{vmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{vmatrix}. \quad \checkmark$$

**133.** Compute inverses of matrices using the Cofactor Theorem:

$$(a) \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \quad (b) \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}. \quad \checkmark$$

**134.** Solve the systems of linear equations  $A\mathbf{x} = \mathbf{b}$  where  $A$  is one of the matrices of the previous exercise, and  $\mathbf{b} = [1, 0, 1]^t$ .  $\checkmark$

**135.** Compute

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

**136.** Express  $\det(\text{adj}(A))$  of the adjoint matrix via  $\det A$ .  $\checkmark$

**137.** Which integer matrices have integer inverses?  $\checkmark$

**138.** Solve systems of equations using Cramer's rule:

$$(a) \begin{array}{rcl} 2x_1 - x_2 - x_3 & = & 4 \\ 3x_1 + 4x_2 - 2x_3 & = & 11 \\ 3x_1 - 2x_2 + 4x_3 & = & 11 \end{array}, \quad (b) \begin{array}{rcl} x_1 + 2x_2 + 4x_3 & = & 31 \\ 5x_1 + x_2 + 2x_3 & = & 29 \\ 3x_1 - x_2 + x_3 & = & 10 \end{array}. \quad \checkmark$$

**139.\*** Compute determinants:

$$(a) \begin{vmatrix} 0 & x_1 & x_2 & \dots & x_n \\ x_1 & 1 & 0 & \dots & 0 \\ x_2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & 0 & \dots & 0 & 1 \end{vmatrix}, \quad (b) \begin{vmatrix} a & 0 & 0 & 0 & 0 & b \\ 0 & a & 0 & 0 & b & 0 \\ 0 & 0 & a & b & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 \\ 0 & c & 0 & 0 & d & 0 \\ c & 0 & 0 & 0 & 0 & d \end{vmatrix} \quad \frac{1}{4} \checkmark.$$

**140.\*** Let  $P_{ij}$ ,  $1 \leq i < j \leq 4$ , denote the  $2 \times 2$ -minor of a  $2 \times 4$ -matrix formed by the columns  $i$  and  $j$ . Prove the following **Plücker identity**<sup>5</sup>

$$P_{12}P_{34} - P_{13}P_{24} + P_{14}P_{23} = 0. \quad \checkmark$$

<sup>5</sup>After Julius **Plücker** (1801–1868).

**141.** The **cross product** of two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^3$  is defined by

$$\mathbf{x} \times \mathbf{y} := \left( \begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}, \begin{vmatrix} x_3 & x_1 \\ y_3 & y_1 \end{vmatrix}, \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \right).$$

Prove that the length  $|\mathbf{x} \times \mathbf{y}| = \sqrt{|\mathbf{x}|^2|\mathbf{y}|^2 - \langle \mathbf{x}, \mathbf{y} \rangle^2}$ .  $\zeta$

**142.\*** Prove that  $a_n + \frac{1}{a_{n-1} + \frac{1}{a_{n-2} + \frac{1}{\dots + \frac{1}{a_1 + \frac{1}{a_0}}}} = \frac{\Delta_n}{\Delta_{n-1}}$ ,

where  $\Delta_n = \begin{vmatrix} a_0 & 1 & 0 & \dots & 0 \\ -1 & a_1 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & -1 & a_{n-1} & 1 \\ 0 & \dots & 0 & -1 & a_n \end{vmatrix}$ .  $\zeta$

**143.\*** Compute:  $\begin{vmatrix} \lambda & -1 & 0 & \dots & 0 \\ 0 & \lambda & -1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \dots & 0 & \lambda & -1 \\ a_n & a_{n-1} & \dots & a_2 & \lambda + a_1 \end{vmatrix}$ .  $\checkmark$

**144.\*** Compute:  $\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \binom{2}{1} & \binom{3}{1} & \dots & \binom{n}{1} \\ 1 & \binom{3}{2} & \binom{4}{2} & \dots & \binom{n+1}{2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \binom{n}{n-1} & \binom{n+1}{n-1} & \dots & \binom{2n-2}{n-1} \end{vmatrix}$ .  $\zeta \checkmark$

**145.\*** Prove **Vandermonde's identity**<sup>6</sup>

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i). \quad \zeta$$

**146.\*** Compute:  $\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2^3 & 3^3 & \dots & n^3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 2^{2n-1} & 3^{2n-1} & \dots & n^{2n-1} \end{vmatrix}$ .  $\zeta \checkmark$

<sup>6</sup>After Alexandre-Theóphile **Vandermonde** (1735–1796).



### 3 Vector Spaces

In four words, the subject of Linear Algebra can be described as *geometry* of vector spaces.

#### Axioms

By definition, a **vector space** is a set, equipped with operations of **addition** and **multiplication by scalars** which are required to satisfy certain **axioms**:

The set will be denoted here by  $\mathcal{V}$ , and its elements referred to as **vectors**. Here are the axioms.

(i) The sum of two vectors  $\mathbf{u}$  and  $\mathbf{v}$  is a vector (denoted  $\mathbf{u} + \mathbf{v}$ ); the result of multiplication of a vector  $\mathbf{v}$  by a scalar  $\lambda$  is a vector (denoted  $\lambda\mathbf{v}$ ).

(ii) Addition of vectors is commutative and associative:

$$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}, \quad (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w}) \quad \text{for all } \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{V}.$$

(iii) There exists the **zero vector** (denoted by  $\mathbf{0}$ ) such that

$$\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v} \quad \text{for every } \mathbf{v} \in \mathcal{V}.$$

(iv) For every vector  $\mathbf{u}$  there exists the **opposite** vector, denoted by  $-\mathbf{u}$ , such that

$$-\mathbf{u} + \mathbf{u} = \mathbf{0}.$$

(v) Multiplication by scalars is distributive: For all vectors  $\mathbf{u}, \mathbf{v}$  and scalars  $\lambda, \mu$  we have

$$(\lambda + \mu)(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v} + \mu\mathbf{u} + \mu\mathbf{v}.$$

(vi) Multiplication by scalars is associative in the following sense: For every vector  $\mathbf{u}$  and all scalars  $\lambda, \mu$  we have:

$$(\lambda\mu)\mathbf{u} = \lambda(\mu\mathbf{u}).$$

(vii) Multiplication by scalars 0 and 1 acts on every vector  $\mathbf{u}$  as

$$0\mathbf{u} = \mathbf{0}, \quad 1\mathbf{u} = \mathbf{u}.$$

We have to add to this definition the following comment about **scalars**. Taking one of the sets  $\mathbb{R}$  or  $\mathbb{C}$  of real or complex numbers on the role of scalars one obtains the definition of **real** vector spaces or **complex** vector spaces. In fact these two choices will suffice for all our major goals. The reader may assume that we use the symbol  $\mathbb{K}$  to cover both cases  $\mathbb{K} = \mathbb{R}$  and  $\mathbb{K} = \mathbb{C}$  in one go.

On the other hand, any **field**  $\mathbb{K}$  would qualify on the role of scalars, and this way one arrives at the notion of  $\mathbb{K}$ -vector spaces. By a **field** one means a set  $\mathbb{K}$  equipped with two operations: addition and multiplication. Both are assumed to be commutative and associative, and satisfying the distributive law:  $a(b + c) = ab + ac$ . Besides, it is required that there exist elements 0 and 1 such that  $a + 0 = a$  and  $1a = a$  for all  $a \in \mathbb{K}$ . Then, it is required that every  $a \in \mathbb{K}$  has the opposite  $-a$  such that  $-a + a = 0$ , and every *non-zero*  $a \in \mathbb{K}$  has its *inverse*  $a^{-1}$  such that  $a^{-1}a = 1$ . To the examples of fields  $\mathbb{C}$  and  $\mathbb{R}$ , we can add (omitting many other available examples): the field  $\mathbb{Q}$  of rational numbers; the field  $\mathcal{A} \subset \mathbb{C}$  of all **algebraic numbers** (i.e. roots of polynomials in one variable with rational coefficients); the field  $\mathbb{Z}_p$  of integers modulo a given prime number  $p$ . For instance, the set  $\mathbb{Z}_2 = \{0, 1\}$  of remainders modulo 2 with the usual arithmetics of remainders ( $0+0 = 0 = 1+1$ ,  $0+1 = 1 = 1+0$ ,  $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0$ ,  $1 \cdot 1 = 1$ ) can be taken on the role of scalars. This gives rise to the definition of  $\mathbb{Z}_2$ -vector spaces useful in computer science and logic.

To reiterate: it is essential that division by all non-zero scalars is defined. Therefore the set  $\mathbb{Z}$  of all integers and the set  $\mathbb{F}[x]$  of all polynomials in one indeterminate  $x$  with coefficients in a field  $\mathbb{F}$  are not fields, and do not qualify on the role of scalars in the definition of vector spaces, because the division is not always possible. However the field  $\mathbb{Q}$  of all rational numbers and the field  $\mathbb{F}(x)$  of all rational functions with coefficients in a field  $\mathbb{F}$  are O.K.

## Examples

The above definition of vector spaces is *doubly* abstract: not only it neglects to specify the set  $\mathcal{V}$  of vectors, but it does not even tell us anything explicit about the nature of the operations of addition of vectors and multiplication of vectors by scalars. To find various examples of vector spaces we should figure out which operations would be good candidates to satisfy the axioms (i–vii). It turns out that in the majority of useful examples, the operations are *pointwise addition of functions and multiplication of functions by scalars*.

**Example 1.** Let  $S$  be *any* set, and  $\mathcal{V}$  be the set of *all* functions on  $S$  with values in  $\mathbb{K}$ . We will denote this set by  $\mathbb{K}^S$ . The sum and multiplication by scalars are defined on  $\mathbb{K}^S$  as pointwise operations with functions. Namely, given two functions  $f, g$  and a scalar  $\lambda$ , the values of the sum  $f + g$  and the product  $\lambda f$  at a point  $s \in S$  are

$$(f + g)(s) = f(s) + g(s), \quad (\lambda f)(s) = \lambda(f(s)).$$

It is immediate to check that  $\mathcal{V} = \mathbb{K}^S$  equipped with these operations satisfies the axioms (i–vii). Thus  $\mathbb{K}^S$  is a  $\mathbb{K}$ -vector space.

**Example 1a.** Let  $S$  be the set of  $n$  elements  $1, 2, \dots, n$ . Then the space  $\mathbb{K}^S$  is the coordinate space  $\mathbb{K}^n$  (e.g.  $\mathbb{R}^S = \mathbb{R}^n$  and  $\mathbb{C}^S = \mathbb{C}^n$ ). Namely, each function on the set  $\{1, \dots, n\}$  is specified by the column  $\mathbf{x} = (x_1, \dots, x_n)^t$  of its values, and the usual operations with such columns coincide with pointwise operations with the functions.

**Example 1b.** Let  $S$  be the set of all ordered pairs  $(i, j)$ , where  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ . Then the vector space  $\mathbb{K}^S$  is the space of  $m \times n$ -matrices  $A$  whose entries  $a_{ij}$  lie in  $\mathbb{K}$ . The operations of addition of matrices and their multiplication by scalars coincide with pointwise operations with the functions.

**Example 2.** Let  $\mathcal{V}$  be a  $\mathbb{K}$ -vector space. Consider the set  $\mathcal{V}^S$  of all functions on a given set  $S$  with values in  $\mathcal{V}$ . Elements of  $\mathcal{V}$  can be added and multiplied by scalars. Respectively the *vector-valued* functions can be added and multiplied by scalars in the pointwise fashion. Thus,  $\mathcal{V}^S$  is an example of a  $\mathbb{K}$ -vector space.

**Example 3.** A non-empty subset  $\mathcal{W}$  in a vector space  $\mathcal{V}$  is called a **linear subspace** (or simply **subspace**) if linear combinations  $\lambda \mathbf{u} + \mu \mathbf{v}$  of vectors from  $\mathcal{W}$  with arbitrary coefficients lie in  $\mathcal{W}$ . In particular, for every  $\mathbf{u} \in \mathcal{W}$ ,  $-\mathbf{u} = (-1)\mathbf{u} \in \mathcal{W}$ , and  $\mathbf{0} = 0\mathbf{u} \in \mathcal{W}$ . A subspace of a vector space satisfies the axioms of a vector space on its own (since the operations are the same as in  $\mathcal{V}$ ). Thus every subspace of a  $\mathbb{K}$ -vector space is an example of a  $\mathbb{K}$ -vector space.

**Example 3a.** For instance, all upper triangular  $n \times n$ -matrices (lower triangular, block triangular, block diagonal, diagonal matrices — the reader can continue this line of examples) form subspaces in the space of all  $n \times n$ -matrices, and therefore provide examples of vector spaces.

**Example 3b.** The set of all polynomials (say, in one variable),<sup>7</sup> form a subspace in the space  $\mathbb{R}^{\mathbb{R}}$  of all real-valued functions on the

---

<sup>7</sup>As well as sets of all continuous, differentiable, 5 times continuously differentiable, infinitely differentiable, Riemann-integrable, measurable, etc. functions, introduced in Mathematical Analysis.

number line and therefore provide examples of real vector spaces. More generally, polynomials with coefficients in  $\mathbb{K}$  (as well as such polynomials of degree not exceeding 7) form examples of  $\mathbb{K}$ -vector spaces.

**Example 3c.** Linear forms or quadratic forms in  $\mathbb{K}^n$  form subspaces in the space  $\mathbb{K}^{\mathbb{K}^n}$  of all  $\mathbb{K}$ -valued functions on  $\mathbb{K}^n$ , and thus provide examples of  $\mathbb{K}$ -vector spaces.

**Example 3d.** All bilinear forms of two vectors  $\mathbf{v} \in \mathbb{K}^m$ ,  $\mathbf{w} \in \mathbb{K}^n$  form a subspace in the space of all functions on the Cartesian product<sup>8</sup>  $\mathbb{K}^m \times \mathbb{K}^n$  with values in  $\mathbb{K}$ . Hence they form a  $\mathbb{K}$ -vector space.

## Morphisms

The modern ideology requires objects of mathematical study to be organized into *categories*. This means that in addition to specifying *objects* of interest, one should also specify *morphisms*, i.e. maps between them. The **category of vector spaces** is obtained by taking vector spaces for objects, and linear maps for morphisms.

By definition, a function  $A : \mathcal{V} \rightarrow \mathcal{W}$  from a vector space  $\mathcal{V}$  to a vector space  $\mathcal{W}$  is called a **linear map** if it *respects* the operations with vectors, i.e. if it maps linear combinations of vectors to linear combinations of their images with the same coefficients:

$$A(\lambda\mathbf{u} + \mu\mathbf{v}) = \lambda A\mathbf{u} + \mu A\mathbf{v} \quad \text{for all } \mathbf{u}, \mathbf{v} \in \mathcal{V} \text{ and } \lambda, \mu \in \mathbb{K}.$$

With a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ , one associates two subspaces, one in  $\mathcal{V}$ , called the **null space**, or the **kernel** of  $A$  and denoted  $\text{Ker } A$ , and the other in  $\mathcal{W}$ , called the **range** of  $A$  and denoted  $A(\mathcal{V})$ :

$$\begin{aligned} \text{Ker } A &:= \{\mathbf{v} \in \mathcal{V} : A\mathbf{v} = \mathbf{0}\}, \\ A(\mathcal{V}) &:= \{\mathbf{w} \in \mathcal{W} : \mathbf{w} = A\mathbf{v} \text{ for some } \mathbf{v} \in \mathcal{V}\}. \end{aligned}$$

A linear map is **injective**, i.e. maps different vectors to different ones, exactly when its kernel is trivial. Indeed, if  $\text{Ker } A \neq \{\mathbf{0}\}$ , then it contains non-zero vectors mapped to the same point  $\mathbf{0}$  in  $\mathcal{W}$  as  $\mathbf{0}$  from  $\mathcal{V}$ . This makes the map  $A$  non-injective. *Vice versa*, if  $A$  is non-injective, i.e. if  $A\mathbf{v} = A\mathbf{v}'$  for some  $\mathbf{v} \neq \mathbf{v}'$ , then  $\mathbf{u} = \mathbf{v} - \mathbf{v}' \neq \mathbf{0}$  lies in  $\text{Ker } A$ . This makes the kernel nontrivial.

---

<sup>8</sup>**Cartesian product** of two sets  $A$  and  $B$  is defined as the set of all ordered pairs  $(a, b)$  of elements  $a \in A$  and  $b \in B$ .

When the range of a map is the whole target space,  $A(\mathcal{V}) = \mathcal{W}$ , the map is called **surjective**. If a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$  is **bijective**, i.e. both injective and surjective, it establishes a one-to-one correspondence between  $\mathcal{V}$  and  $\mathcal{W}$  in a way that respects vector operations. Then one says that  $A$  establishes an **isomorphism** between the vector spaces  $\mathcal{V}$  and  $\mathcal{W}$ . Two vector spaces are called **isomorphic** (written  $\mathcal{V} \cong \mathcal{W}$ ) if there exists an isomorphism between them.

**Example 4.** Let  $\mathcal{V} = \mathcal{W}$  be the space  $\mathbb{K}[x]$  of all polynomials in one indeterminate  $x$  with coefficients from  $\mathbb{K}$ . The **differentiation**  $d/dx : \mathbb{K}[x] \rightarrow \mathbb{K}[x]$  is a linear map defined by

$$\frac{d}{dx}(a_0 + a_1x + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

It is surjective, with the kernel consisting of constant polynomials.<sup>9</sup>

**Example 5.** Linear combinations  $\lambda A + \mu B$  of linear maps  $A, B : \mathcal{V} \rightarrow \mathcal{W}$  are linear. Therefore all linear maps from  $\mathcal{V}$  to  $\mathcal{W}$  form a subspace in the space of all vector-valued functions  $\mathcal{V} \rightarrow \mathcal{W}$ . The vector space of linear maps from  $\mathcal{V}$  to  $\mathcal{W}$  is usually denoted by<sup>10</sup>  $\text{Hom}(\mathcal{V}, \mathcal{W})$ .

**Example 5a.** The space of **linear functions** (or **linear forms**) on  $\mathcal{V}$ , i.e. linear maps  $\mathcal{V} \rightarrow \mathbb{K}$ , is called the space **dual** to  $\mathcal{V}$ , and is denoted by  $\mathcal{V}^*$ .

The following formal construction indicates that *every vector space can be identified with a subspace in a space of functions with pointwise operations of addition and multiplication by scalars*.

**Example 5b.** Given a vector  $\mathbf{v} \in \mathcal{V}$  and a linear function  $f \in \mathcal{V}^*$ , the value  $f(\mathbf{v}) \in \mathbb{K}$  is defined. We can consider it not as a function  $f$  of  $\mathbf{v}$ , but as a function of  $f$  defined by  $\mathbf{v}$ . This way, to a vector  $\mathbf{v}$  we associate the function  $E_{\mathbf{v}} : \mathcal{V}^* \rightarrow \mathbb{K}$  defined by evaluating all linear functions  $\mathcal{V} \rightarrow \mathbb{K}$  on the vector  $\mathbf{v}$ . The function  $E_{\mathbf{v}}$  is linear, since  $(\lambda f + \mu g)(\mathbf{v}) = \lambda f(\mathbf{v}) + \mu g(\mathbf{v})$ . The linear function  $E_{\mathbf{v}}$  is an element of the second dual space  $(\mathcal{V}^*)^*$ . The formula  $f(\lambda \mathbf{v} + \mu \mathbf{w}) = \lambda f(\mathbf{v}) + \mu f(\mathbf{w})$ , expressing linearity of linear functions, shows that  $E_{\mathbf{v}}$  depends linearly on  $\mathbf{v}$ . Thus the **evaluation map**  $E : \mathbf{v} \mapsto E_{\mathbf{v}}$  is a linear map  $\mathcal{V} \rightarrow (\mathcal{V}^*)^*$ . One can show<sup>11</sup> that  $E$  is **injective**

<sup>9</sup>When  $\mathbb{K}$  contains  $\mathbb{Q}$  (e.g.  $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ ), but not when  $\mathbb{K}$  contains  $\mathbb{Z}_p$ .

<sup>10</sup>From **homomorphism**, a word roughly synonymous to the terms *linear map* and *morphism*.

<sup>11</sup>Although we are not going to do this, as it would drag us into the boredom of general set theory and *transfinite induction*.

*and thus provides an isomorphism between  $\mathcal{V}$  and its range  $E(\mathcal{V}) \subset (\mathcal{V}^*)^*$ .*

The previous result and examples suggest that vector spaces need not be described abstractly and raises the suspicion that the axiomatic definition is misleading as it obscures the actual nature of vectors as functions subject to the pointwise algebraic operations. Here are however some examples where vectors do not come *naturally* as functions.

**Example 6a.** Geometric vectors (see Section 1 of Chapter 1), and forces and velocities in physics, are not introduced as functions.

**Example 6b.** Rational functions are defined as ratios  $P/Q$  of polynomials  $P$  and  $Q$ . Morally they are functions, but technically they are not. More precisely, the domain of  $P/Q$  is the non-empty set of points  $x$  where  $Q(x) \neq 0$ , but it varies with the function. All rational functions do form a vector space, but there is not a single point  $x$  at which all of them defined. The addition operation is not defined as pointwise, but is introduced instead by means of the formula:  $P/Q + P'/Q' = (PQ' + QP')/QQ'$ .

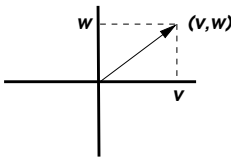


Figure 25

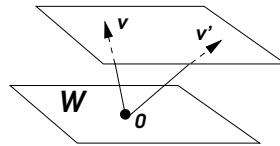


Figure 26

**Example 6c.** Vector spaces frequently occur in *number theory* and *field theory* in connection with **field extensions**, i.e. inclusions  $\mathbb{K} \subset \mathbb{F}$  of one field as a subfield into another. As examples, we already have:  $\mathbb{Q} \subset \mathcal{A} \subset \mathbb{C}$ ,  $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ , and  $\mathbb{K} \subset \mathbb{K}(x)$ . Given a field extension  $\mathbb{K} \subset \mathbb{F}$ , it is often useful to temporarily forget that elements of  $\mathbb{F}$  can be multiplied, but still remember that they can be multiplied by elements of  $\mathbb{K}$ . This way,  $\mathbb{F}$  becomes a  $\mathbb{K}$ -vector space (e.g.  $\mathbb{C}$  is a real plane). Vectors here, i.e. elements of  $\mathbb{F}$ , are “numbers” rather than “functions.”

More importantly, various abstract constructions of new vector spaces from given ones are used regularly, and it would be very awkward to express the resulting vector space as a space of functions even when the given spaces are expressed this way. Here are two such constructions.

## Direct Sums and Quotients

**Example 7.** Given two vector spaces  $\mathcal{V}$  and  $\mathcal{W}$ , their **direct sum**  $\mathcal{V} \oplus \mathcal{W}$  (Figure 25) is defined as the set of all ordered pairs  $(\mathbf{v}, \mathbf{w})$ , where  $\mathbf{v} \in \mathcal{V}$ ,  $\mathbf{w} \in \mathcal{W}$ , equipped with the component-wise operations:

$$\lambda(\mathbf{v}, \mathbf{w}) = (\lambda\mathbf{v}, \lambda\mathbf{w}), \quad (\mathbf{v}, \mathbf{w}) + (\mathbf{v}', \mathbf{w}') = (\mathbf{v} + \mathbf{v}', \mathbf{w} + \mathbf{w}').$$

Of course, one can similarly define the direct sum of several vector spaces. E.g.  $\mathbb{K}^n = \mathbb{K} \oplus \cdots \oplus \mathbb{K}$  ( $n$  times).

**Example 7a.** Given a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ , its **graph** is defined as a subspace in the direct sum  $\mathcal{V} \oplus \mathcal{W}$ :

$$\text{Graph } A = \{(\mathbf{v}, \mathbf{w}) \in \mathcal{V} \oplus \mathcal{W} : \mathbf{w} = A\mathbf{v}\}.$$

**Example 8.** The **quotient space** of a vector space  $\mathcal{V}$  by a subspace  $\mathcal{W}$  is defined as follows. Two vectors  $\mathbf{v}$  and  $\mathbf{v}'$  (Figure 26) are called *equivalent modulo*  $\mathcal{W}$ , if  $\mathbf{v} - \mathbf{v}' \in \mathcal{W}$ . This way, all vectors from  $\mathcal{V}$  become partitioned into equivalence classes. These equivalence classes form the quotient vector space  $\mathcal{V}/\mathcal{W}$ .

More precisely, denote by  $\pi : \mathcal{V} \rightarrow \mathcal{V}/\mathcal{W}$  the **canonical projection**, which assigns to a vector  $\mathbf{v}$  its equivalence class modulo  $\mathcal{W}$ . This class can be symbolically written as  $\mathbf{v} + \mathcal{W}$ , a notation emphasizing that the class consists of all vectors obtained from  $\mathbf{v}$  by adding arbitrary vectors from  $\mathcal{W}$ . Alternatively, one may think of  $\mathbf{v} + \mathcal{W}$  as a “plane” obtained from  $\mathcal{W}$  as *translation* by the vector  $\mathbf{v}$ . When  $\mathbf{v} \in \mathcal{W}$ , we have  $\mathbf{v} + \mathcal{W} = \mathcal{W}$ . When  $\mathbf{v} \notin \mathcal{W}$ ,  $\mathbf{v} + \mathcal{W}$  is not a linear subspace in  $\mathcal{V}$ . We will call it an **affine subspace** parallel to  $\mathcal{W}$ .

The set  $\mathcal{V}/\mathcal{W}$  of all affine subspaces in  $\mathcal{V}$  parallel to  $\mathcal{W}$  is equipped with algebraic operations of addition and multiplication by scalars in such a way that the *canonical projection*  $\pi : \mathcal{V} \rightarrow \mathcal{V}/\mathcal{W}$  becomes a *linear map*. In fact this condition leaves no choices, since it requires that for every  $\mathbf{u}, \mathbf{v} \in \mathcal{V}$  and  $\lambda, \mu \in \mathbb{K}$ ,

$$\lambda\pi(\mathbf{u}) + \mu\pi(\mathbf{v}) = \pi(\lambda\mathbf{u} + \mu\mathbf{v}).$$

In other words, the linear combination of given equivalence classes must coincide with the equivalence class containing the linear combination  $\lambda\mathbf{u} + \mu\mathbf{v}$  of arbitrary representatives  $\mathbf{u}, \mathbf{v}$  of these classes. It is important here that picking different representatives  $\mathbf{u}'$  and  $\mathbf{v}'$  will result in a new linear combination  $\lambda\mathbf{u}' + \mu\mathbf{v}'$  which is however equivalent to the previous one. Indeed, the difference  $\lambda(\mathbf{u} - \mathbf{u}') + \mu(\mathbf{v} - \mathbf{v}')$  lies in  $\mathcal{W}$  since  $\mathbf{u} - \mathbf{u}'$  and  $\mathbf{v} - \mathbf{v}'$  do. Thus linear combinations in  $\mathcal{V}/\mathcal{W}$  are well-defined.

**Example 8a.** Projecting 3D images to a 2-dimensional screen is described in geometry by the canonical projection  $\pi$  from the 3D space  $\mathcal{V}$  to the plane  $\mathcal{V}/\mathcal{W}$  of the screen along the line  $\mathcal{W}$  of the eye sight (Figure 27).

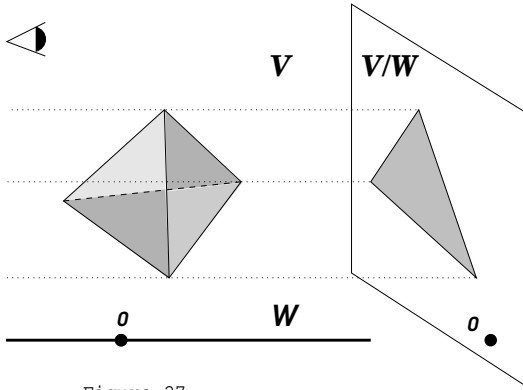


Figure 27

**Example 8b.** The direct sum  $\mathcal{V} \oplus \mathcal{W}$  contains  $\mathcal{V}$  and  $\mathcal{W}$  as subspaces consisting of the pairs  $(\mathbf{v}, \mathbf{0})$  and  $(\mathbf{0}, \mathbf{w})$  respectively. The quotient of  $\mathcal{V} \oplus \mathcal{W}$  by  $\mathcal{W}$  is canonically identified with  $\mathcal{V}$ , because each pair  $(\mathbf{v}, \mathbf{w})$  is equivalent modulo  $\mathcal{W}$  to  $(\mathbf{v}, \mathbf{0})$ . Likewise,  $(\mathcal{V} \oplus \mathcal{W}) / \mathcal{V} = \mathcal{W}$ .

**Example 8c.** Let  $\mathcal{V} = \mathbb{R}[x]$  be the space of polynomials with real coefficients, and  $\mathcal{W}$  the subspace of polynomials divisible by  $x^2 + 1$ . Then the quotient space  $\mathcal{V}/\mathcal{W}$  can be identified with the plane  $\mathbb{C}$  of complex numbers, and the projection  $\pi : \mathbb{R}[x] \rightarrow \mathbb{C}$  with the map  $P \mapsto P(i)$  of evaluating a polynomial  $P$  at  $x = i$ . Indeed, polynomials  $P$  and  $P'$  are equivalent modulo  $\mathcal{W}$  if and only if  $P - P'$  is divisible by  $x^2 + 1$ , in which case  $P(i) = P'(i)$ . *Vice versa*, if  $P(i) = P'(i)$ , then  $P(-i) = P'(-i)$  (since the polynomials are real), and hence  $P - P'$  is divisible by  $(x - i)(x + i) = x^2 + 1$ .

**Example 8d.** For every linear map  $A : \mathcal{V} \rightarrow \mathcal{V}'$ , there is a canonical isomorphism  $\tilde{A} : \mathcal{V}/\text{Ker } A \rightarrow A(\mathcal{V})$  between the quotient by the kernel of  $A$ , and its range. Namely,  $A\mathbf{u} = A\mathbf{v}$  if and only if  $\mathbf{u} - \mathbf{v} \in \text{Ker } A$ , i.e. whenever  $\mathbf{u}$  is equivalent to  $\mathbf{v}$  modulo the kernel. Thus, *one can think of every linear map as the projection of the source space onto the range along the null space*. This is a manifestation of a general **homomorphism theorem** in algebra, which in the context of vector spaces can be formally stated this way:

**Theorem.** *Every linear map  $A : \mathcal{V} \rightarrow \mathcal{V}'$  is uniquely represented as the composition  $A = i\tilde{A}\pi$  of the canonical projection  $\pi : \mathcal{V} \rightarrow \mathcal{V}/\text{Ker } A$  with the isomorphism  $\tilde{A} : \mathcal{V}/\text{Ker } A \rightarrow$*



$A(\mathcal{V})$  followed by the inclusion  $i : A(\mathcal{V}) \subset \mathcal{V}'$ :

$$\begin{array}{ccc} \mathcal{V} & \xrightarrow{A} & \mathcal{V}' \\ \pi \downarrow & & \cup i \\ \mathcal{V}/\text{Ker } A & \xrightarrow[\tilde{A}]{\cong} & A(\mathcal{V}) \end{array} .$$

## Quaternions

The assumption that scalars commute under multiplication is reasonable because they usually do, but it is not strictly necessary. Here is an important example: vector spaces over a **skew-filed**, namely the skew-filed  $\mathbb{H}$  of **quaternions**.

By definition,  $\mathbb{H} = \mathbb{C}^2 = \mathbb{R}^4$  consists of quaternions

$$q = z + wj = (a + bi) + (c + di)j = a + bi + cj + dk,$$

where  $z = a + bi$  and  $w = c + di$  are complex numbers, and  $k = ij$ . The multiplication is determined by the requirements:  $i^2 = j^2 = -1$ ,  $ij = -ji$ , associativity, and bilinearity over  $\mathbb{R}$ . Namely:

$$\begin{aligned} q'q &= (z' + w'j)(z + wj) = z'z + w'jwj + z'wj + w'jz \\ &= (z'z - w'\bar{w}) + (z'w + w'\bar{z})j, \end{aligned}$$

where we use that  $j(x + yi) = (x - yi)j$  for all real  $x, y$ . Equivalently, in purely real notation,  $1, i, j, k$  form the standard basis of  $\mathbb{H} = \mathbb{R}^4$ , and the product is specified by the multiplication table:

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

The quaternion

$$q^* = \bar{z} - wj = a - bi - cj - dk$$

is called **adjoint** or **conjugate** to  $q$ . We have:

$$\begin{aligned} q^*q &= (\bar{z} - wj)(z + wj) = \bar{z}z + w\bar{w} + (\bar{z}w - w\bar{z})j \\ &= |z|^2 + |w|^2 = a^2 + b^2 + c^2 + d^2 = |q|^2. \end{aligned}$$

By  $|q|$  we denote here the **norm** or **absolute value** of quaternion  $q$ . The norm coincides with the Euclidean length  $\sqrt{a^2 + b^2 + c^2 + d^2}$

of the vector  $q \in \mathbb{R}^4$ . Note that  $(q^*)^* = q$ , and hence  $qq^* = |q^*|^2 = |q|^2 = q^*q$ . It follows, that if  $q \neq \mathbf{0}$ , then

$$q^{-1} = \frac{q^*}{|q|^2} = |q|^{-2}(a - bi - cj - dk)$$

is the quaternion **inverse** to  $q$ , i.e.  $q^{-1}q = 1 = qq^{-1}$ . We conclude that although  $\mathbb{H}$  is not a field, since multiplication is not commutative, it shares with fields the property that all non-zero elements of  $\mathbb{H}$  are invertible.

In the definition of an  $\mathbb{H}$ -vector space, one should be cautious about only the axiom (vi): associativity of multiplication by scalars. Namely, there are two versions of this axiom:

$$(qq')\mathbf{u} = q(q'\mathbf{u}) \quad \text{and} \quad \mathbf{v}(qq') = (\mathbf{v}q)q'.$$

Using the first or the second one obtains the category of **left** or **right** quaternionic vector space. The actual difference is not in the side of the vector on which the scalars are written — this difference is purely typographical — but in the order of the factors: in the left case  $\mathbf{v}$  is first multiplied by  $q'$ , and in the right by  $q$ .

Some people prefer to deal with left, other with right quaternionic spaces, but in fact it is a matter of religion and hence does not matter. Namely, a left vector space can be converted into a right one (and *vice versa*) by defining the new multiplication by  $q$  as the old multiplication by  $q^*$ . The trick is that conjugation  $q \mapsto q^*$  is not exactly an automorphism of  $\mathbb{H}$  because it changes the order of factors:  $(q_1q_2)^* = q_2^*q_1^*$ . We prefer to work with *right* quaternionic vector spaces, and the following example explains *why*.

Define the **coordinate quaternionic space**  $\mathbb{H}^n$  as the set of all  $n$ -columns of quaternions, added component-wise, and multiplied by scalars  $q \in \mathbb{H}$  on the right:

$$\begin{bmatrix} q_1 \\ \cdot \\ \cdot \\ q_n \end{bmatrix} + \begin{bmatrix} q'_1 \\ \cdot \\ \cdot \\ q'_n \end{bmatrix} = \begin{bmatrix} q_1 + q'_1 \\ \cdot \\ \cdot \\ q_n + q'_n \end{bmatrix}, \quad \begin{bmatrix} q_1 \\ \cdot \\ \cdot \\ q_n \end{bmatrix} q = \begin{bmatrix} q_1q \\ \cdot \\ \cdot \\ q_nq \end{bmatrix}.$$

Clearly,  $\mathbb{H}^n$  is a *right* quaternionic vector space.

Let  $A$  be an  $m \times n$  matrix with entries  $a_{ij} \in \mathbb{H}$ , and  $\mathbf{x} \in \mathbb{H}^n$ . Then the usual matrix product  $\mathbf{y} = A\mathbf{x}$  yields a vector  $\mathbf{y} \in \mathbb{H}^m$ :

$$y_i = a_{i1}x_1 + \cdots + a_{in}x_n, \quad i = 1, \dots, m.$$

**The matrix multiplication**  $\mathbf{x} \mapsto \mathbf{y} = A\mathbf{x}$  defines an  $\mathbb{H}$ -linear map  $A : \mathbb{H}^n \rightarrow \mathbb{H}^m$ . Namely,  $A$  is not only additive, but it also commutes with multiplication by quaternionic scalars:  $(A\mathbf{x})q = A(\mathbf{x}q)$ . The point is that the matrix entries  $a_{ij}$  are applied to the components  $x_j$  of the vectors on the left, while the scalar  $q$  is applied on the right, and hence the order of these operations is irrelevant. For left vector spaces, linear maps  $\mathbf{y} = A\mathbf{x}$  would correspond to matrix multiplication formulas  $y_i = x_1a_{i1} + \cdots + x_na_{in}$  that look a bit weird.

### EXERCISES

**147.** Give an example of a “vector space” that satisfies all axioms except the last one:  $1\mathbf{u} = \mathbf{u}$  for all  $\mathbf{u}$ .  $\zeta$

**148.** Prove that the axiom:  $0\mathbf{u} = \mathbf{0}$  for all  $\mathbf{u}$ , in the definition of vector spaces is redundant, i.e. can be derived from remaining axioms.  $\zeta$

**149.** Derive from axioms of vector spaces that  $(-1)\mathbf{u} = -\mathbf{u}$  for all  $\mathbf{u}$ .  $\zeta$

**150.\*** Prove that every non-zero element of  $\mathbb{Z}_p$  is invertible.  $\zeta$

**151.** Verify that  $\mathbb{K}^S$  and  $\mathcal{V}^S$  are vector spaces.

**152.** How many vectors are there in  $\mathbb{Z}_p$ -vector space  $\mathbb{Z}_p^n$ ?  $\text{Hom}(\mathbb{Z}_p^n, \mathbb{Z}_p^m)$ ?  $\checkmark$

**153.** Show that in  $\mathbb{K}[x]$ , polynomials of degree  $n$  do not form a subspace, but polynomials of degree  $\leq n$  do.  $\zeta$

**154.** Prove that intersection of subspaces is a subspace.

**155.** How many vectors are there in the  $\mathbb{Z}_p$ -vector space of strictly upper triangular  $n \times n$ -matrices?  $\checkmark$

**156.** Show that the map  $f \mapsto \int_a^b f(x) dx$  defined by integration of (say) polynomial functions is a linear form  $\mathbb{R}[x] \rightarrow \mathbb{R}$ .

**157.** Find the kernel and the range of the differentiation map  $D = \frac{d}{dx} : \mathbb{K}[x] \rightarrow \mathbb{K}[x]$ , when  $\mathbb{K} = \mathbb{Z}_p$ .  $\checkmark$

**158.** For  $\mathcal{V} = \mathbb{K}^n$ , verify that the map  $E : \mathcal{V} \rightarrow \mathcal{V}^{**}$  defined in Example 5b is an isomorphism.

**159.** Let  $\mathcal{W} \subset \mathcal{V}$  be any subset of  $\mathcal{V}$ . Define  $\mathcal{W}^\perp \subset \mathcal{V}^*$  as the set of all those linear functions which vanish on  $\mathcal{W}$ . Prove that  $\mathcal{W}^\perp$  is a subspace of  $\mathcal{V}^*$ . (It is called the **annihilator** of  $\mathcal{W}$ .)

**160.** Let  $\mathcal{W} \subset \mathcal{V}$  be a subspace. Establish a canonical isomorphism between the dual space  $(\mathcal{V}/\mathcal{W})^*$  and the annihilator  $\mathcal{W}^\perp \subset \mathcal{V}^*$ .  $\zeta$

**161.** Let  $B$  be a bilinear form on  $\mathcal{V} \times \mathcal{V}$ , i.e. a function  $(\mathbf{v}, \mathbf{w}) \mapsto B(\mathbf{v}, \mathbf{w})$  of pairs of vectors linear in each of them. Prove that the **left kernel** and **right kernel** of  $B$ , defined as  $\text{LKer}B = \{\mathbf{v} \mid B(\mathbf{v}, \mathbf{x}) = 0 \text{ for all } \mathbf{x} \in \mathcal{V}\}$  and  $\text{RKer}B = \{\mathbf{w} \mid B(\mathbf{x}, \mathbf{w}) = 0 \text{ for all } \mathbf{x} \in \mathcal{V}\}$ , are subspaces of  $\mathcal{V}$ , which coincide when  $B$  is symmetric or anti-symmetric.

**162.** Establish canonical isomorphisms between the spaces  $\text{Hom}(\mathcal{V}, \mathcal{W}^*)$ ,  $\text{Hom}(\mathcal{W}, \mathcal{V}^*)$ , and the space  $\mathcal{B}(\mathcal{V}, \mathcal{W})$  of all bilinear forms on  $\mathcal{V} \times \mathcal{W}$ .  $\zeta$

**163.** Describe all affine subspaces in  $\mathbb{R}^3$ .  $\checkmark$

**164.** Prove that the intersection of two affine subspaces, parallel to given linear ones, if non-empty, is an affine subspace parallel to the intersection of the given linear subspaces.  $\zeta$

**165.** Prove that for a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ ,  $\text{Ker } A = (\text{Graph } A) \cap \mathcal{V}$ .

**166.** Show that  $(\mathcal{V} \oplus \mathcal{W})^* = \mathcal{V}^* \oplus \mathcal{W}^*$ .  $\zeta$

**167.** Composing a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$  with a linear form  $f \in \mathcal{W}^*$  we obtain a linear form  $A^t f \in \mathcal{V}^*$ . Prove that this defines a linear map  $A^t : \mathcal{W}^* \rightarrow \mathcal{V}^*$ . (The map  $A^t$  is called **dual** or **adjoint** to  $A$ .) Show that  $(AB)^t = B^t A^t$ .

**168.** Given the kernel and the range of a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ , find the kernel and the range of the dual map  $A^t$ .  $\checkmark$

**169.** Show that numbers of the form  $a + b\sqrt{2}$ , where  $a, b \in \mathbb{Q}$ , form a subfield in  $\mathbb{R}$ , and a  $\mathbb{Q}$ -vector space.

**170.** For  $q = i \cos \theta + j \sin \theta$ , compute  $q^2$ ,  $q^{-1}$ .  $\checkmark$

**171.** Prove multiplicativity of the norm of quaternions:  $|q_1 q_2| = |q_1| |q_2|$ .  $\zeta$

**172.** Prove that in  $\mathbb{H}$ ,  $(q_1 q_2)^* = q_2^* q_1^*$ .

**173.** Prove that if  $f : \mathbb{H}^n \rightarrow \mathbb{H}$  is a quaternionic linear function, then  $qf$ , where  $q \in \mathbb{H}$ , is also a quaternionic linear function, but  $fq$  generally speaking not.

**174.** On the set  $\text{Hom}(\mathbb{H}^n, \mathbb{H}^m)$  of all  $\mathbb{H}$ -linear maps  $A : \mathbb{H}^n \rightarrow \mathbb{H}^m$ , define the structure of a right  $\mathbb{H}$ -vector space.  $\zeta$

**175.** Let  $x + yj \in \mathbb{C}^2$  be complex coordinates on  $\mathbb{H}$ . Show that multiplication by  $q = z + wj \in \mathbb{H}$  on the left is, generally speaking, not  $\mathbb{C}$ -linear, but on the right is, and find its  $2 \times 2$ -matrix.  $\checkmark$

**176.\*** Find all quaternionic square roots of  $-1$ , i.e. solve the equation  $q^2 = -1$  for  $q \in \mathbb{H}$ .  $\zeta \checkmark$

# Chapter 3

## Simple Problems

### 1 Dimension and Rank

#### Bases

Let  $\mathcal{V}$  be a  $\mathbb{K}$ -vector space. A subset  $V \subset \mathcal{V}$  (finite or infinite) is called a **basis** of  $\mathcal{V}$  if every vector of  $\mathcal{V}$  can be uniquely written as a (finite!) linear combination of vectors from  $V$ .

**Example 1.** Monomials  $x^k, k = 0, 1, 2, \dots$ , form a basis in the space  $\mathbb{K}[x]$  since every polynomial is uniquely written as a linear combination of monomials.

**Example 2.** In  $\mathbb{K}^n$ , every vector  $(x_1, \dots, x_n)^t$  is uniquely written as the linear combination  $x_1\mathbf{e}_1 + \dots + x_n\mathbf{e}_n$  of unit coordinate vectors  $\mathbf{e}_1 = (1, 0, \dots, 0)^t, \dots, \mathbf{e}_n = (0, \dots, 0, 1)^t$ . Thus, vectors  $\mathbf{e}_1, \dots, \mathbf{e}_n$  form a basis. It is called the **standard basis** of  $\mathbb{K}^n$ .

The notion of basis has two aspects which can be considered separately.

Let  $V \subset \mathcal{V}$  be *any* set of vectors. Linear combinations  $\lambda_1\mathbf{v}_1 + \dots + \lambda_k\mathbf{v}_k$ , where the vectors  $\mathbf{v}_i$  are taken from the subset  $V$ , and  $\lambda_i$  are arbitrary scalars, form a subspace in  $\mathcal{V}$ . (Indeed, sums and scalar multiples of linear combinations of vectors from  $V$  are also linear combinations of vectors from  $V$ .) This subspace is often denoted as  $\text{Span } V$ . One says that the set  $V$  **spans** the subspace  $\text{Span } V$ , or that  $\text{Span } V$  is **spanned** by  $V$ .

A set  $V$  of vectors is called **linearly independent**, if no vector from  $\text{Span } V$  can be represented as a linear combination of vectors from  $V$  in more than one way. To familiarize ourselves with this notion, let us give several reformulations of the definition. Here is

one: no two *distinct* linear combinations of vectors from  $V$  are equal to each other. Yet another one: if two linear combinations of vectors from  $V$  are equal:  $\alpha_1 \mathbf{v}_1 + \cdots + \alpha_k \mathbf{v}_k = \beta_1 \mathbf{v}_1 + \cdots + \beta_k \mathbf{v}_k$ , then their coefficients must be the same:  $\alpha_1 = \beta_1, \dots, \alpha_k = \beta_k$ . Subtracting one linear combination from the other, we arrive at one more reformulation: if  $\gamma_1 \mathbf{v}_1 + \cdots + \gamma_k \mathbf{v}_k = \mathbf{0}$  for some vectors  $\mathbf{v}_i \in V$ , then necessarily  $\gamma_1 = \cdots = \gamma_k = 0$ . In other words,  $V$  is linearly independent, if the vector  $\mathbf{0}$  can be represented as a linear combination of vectors from  $V$  only in the *trivial* fashion:  $\mathbf{0} = 0\mathbf{v}_1 + \cdots + 0\mathbf{v}_k$ . Equivalently, every **nontrivial linear combination** of vectors from  $V$  is not equal to zero:  $\gamma_1 \mathbf{v}_1 + \cdots + \gamma_k \mathbf{v}_k \neq \mathbf{0}$  whenever at least one of  $\gamma_i \neq 0$ .

Of course, a set  $V \subset \mathcal{V}$  is called **linearly dependent** if it is not linearly independent. Yet, it is useful to have an affirmative reformulation:  $V$  is linearly dependent if and only if some *nontrivial* linear combination of vectors from  $V$  vanishes, i.e.  $\gamma_1 \mathbf{v}_1 + \cdots + \gamma_k \mathbf{v}_k = \mathbf{0}$ , where at least one of the coefficients (say,  $\gamma_k$ ) is non-zero. Dividing by this coefficients and moving all other terms to the other side of the equality, we obtain one more reformulation: a set  $V$  is linearly dependent if one of its vectors can be represented as a linear combination of the others:  $\mathbf{v}_k = -\gamma_k^{-1} \gamma_1 \mathbf{v}_1 - \cdots - \gamma_k^{-1} \gamma_{k-1} \mathbf{v}_{k-1}$ .<sup>1</sup> Obviously, every set containing the vector  $\mathbf{0}$  is linearly dependent; every set containing two proportional vectors is linearly dependent; adding new vectors to a linearly dependent set leaves it linearly dependent.

Thus, a basis of  $\mathcal{V}$  is a linearly independent set of vectors that spans the whole space.

## Dimension

In this course, we will be primarily concerned with **finite dimensional** vector spaces, i.e. spaces which can be spanned by finitely many vectors. If such a set of vectors is linearly dependent, then one of its vectors is a linear combination of the others. Removing this vector from the set, we obtain a smaller set that still spans  $\mathcal{V}$ . Continuing this way, we arrive at a finite linearly independent set that spans  $\mathcal{V}$ . Thus, a finite dimensional vector space has a basis, consisting of finitely many elements. The number of elements in a basis does not depend (as we will see shortly) on the choice of the basis. This number is called the **dimension** of the vector space  $\mathcal{V}$  and is denoted  $\dim \mathcal{V}$ .

---

<sup>1</sup>It is essential here that division by all non-zero scalars is well-defined.

Let  $\mathbf{v}_1, \dots, \mathbf{v}_n$  be a basis of  $\mathcal{V}$ . Then every vector  $\mathbf{x} \in \mathcal{V}$  is uniquely written as  $\mathbf{x} = x_1\mathbf{v}_1 + \dots + x_n\mathbf{v}_n$ . We call  $(x_1, \dots, x_n)$  **coordinates** of the vector  $\mathbf{x}$  with respect to the basis  $\mathbf{v}_1, \dots, \mathbf{v}_n$ . For  $\mathbf{y} = y_1\mathbf{v}_1 + \dots + y_n\mathbf{v}_n \in \mathcal{V}$  and  $\lambda \in \mathbb{K}$ , we have:

$$\begin{aligned}\mathbf{x} + \mathbf{y} &= (x_1 + y_1)\mathbf{v}_1 + \dots + (x_n + y_n)\mathbf{v}_n, \\ \lambda\mathbf{x} &= (\lambda x_1)\mathbf{v}_1 + \dots + (\lambda x_n)\mathbf{v}_n.\end{aligned}$$

This means that operations of addition of vectors and multiplication by scalars are performed *coordinate-wise*. In other words, **the map**:

$$\mathbb{K}^n \rightarrow \mathcal{V}: (x_1, \dots, x_n)^t \mapsto x_1\mathbf{v}_1 + \dots + x_n\mathbf{v}_n$$

**defines an isomorphism of the coordinate space  $\mathbb{K}^n$  onto the vector space  $\mathcal{V}$  with a basis  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ .**

**Lemma.** *A set of  $n + 1$  vectors in  $\mathbb{K}^n$  is linearly dependent.*

**Proof.** Any two vectors in  $\mathbb{K}^1$  are proportional and therefore linearly dependent. We intend to prove the lemma by deducing from this that any 3 vectors in  $\mathbb{K}^2$  are linearly dependent, then deducing from this that any 4 vectors in  $\mathbb{K}^3$  are linearly dependent, and so on. Thus we only need to prove that *if every set of  $n$  vectors in  $\mathbb{K}^{n-1}$  is linearly dependent then every set of  $n + 1$  vectors in  $\mathbb{K}^n$  is linearly dependent too.*<sup>2</sup>

To this end, consider  $n + 1$  column vectors  $\mathbf{v}_1, \dots, \mathbf{v}_{n+1}$  of size  $n$  each. If the last entry in each column is 0, then  $\mathbf{v}_1, \dots, \mathbf{v}_{n+1}$  are effectively  $n - 1$ -columns. Hence some nontrivial linear combination of  $\mathbf{v}_1, \dots, \mathbf{v}_n$  is equal to  $\mathbf{0}$  (by the induction hypothesis), and thus the whole set is linearly dependent. Now consider the case when at least one column has the last entry non-zero. Reordering the vectors we may assume that it is the column  $\mathbf{v}_{n+1}$ . Subtracting the column  $\mathbf{v}_{n+1}$  with suitable coefficients  $\alpha_1, \dots, \alpha_n$  from  $\mathbf{v}_1, \dots, \mathbf{v}_n$  we can form  $n$  new columns  $\mathbf{u}_1 = \mathbf{v}_1 - \alpha_1\mathbf{v}_{n+1}, \dots, \mathbf{u}_n = \mathbf{v}_n - \alpha_n\mathbf{v}_{n+1}$  so that all of them have the last entries equal to zero. Thus  $\mathbf{u}_1, \dots, \mathbf{u}_n$  are effectively  $n - 1$ -vectors and are therefore linearly dependent:  $\beta_1\mathbf{u}_1 + \dots + \beta_n\mathbf{u}_n = \mathbf{0}$  for some  $\beta_1, \dots, \beta_n$  not all equal to 0. Thus

$$\beta_1\mathbf{v}_1 + \dots + \beta_n\mathbf{v}_n - (\alpha_1\beta_1 + \dots + \alpha_n\beta_n)\mathbf{v}_{n+1} = \mathbf{0}.$$

Here at least one of  $\beta_i \neq 0$ , and hence  $\mathbf{v}_1, \dots, \mathbf{v}_{n+1}$  are linearly dependent.  $\square$

---

<sup>2</sup>This way of reasoning is called **mathematical induction**. Put abstractly, it establishes a *sequence*  $P_n$  of propositions in two stages called respectively the **base** and **step** of induction: (i)  $P_1$  is true; (ii) for all  $n = 2, 3, 4, \dots$ , if  $P_{n-1}$  is true (the **induction hypothesis**) then  $P_n$  is true.

Corollaries. (1) *Any set of  $m > n$  vectors in  $\mathbb{K}^n$  is linearly dependent.*

(2)  *$\mathbb{K}^n$  and  $\mathbb{K}^m$  are not isomorphic unless  $n = m$ .*

(3) *Every finite dimensional vector space is isomorphic to exactly one of the spaces  $\mathbb{K}^n$ .*

(4) *In a finite dimensional vector space, all bases have the same number of elements. In particular, dimension is well-defined.*

(5) *Two finite dimensional vector spaces are isomorphic if and only if their dimensions are equal.*

Indeed, (1) is obvious because adding new vectors to a linearly dependent set leaves it linearly dependent. Since the standard basis in  $\mathbb{K}^m$  consists of  $m$  linearly independent vectors,  $\mathbb{K}^m$  cannot be isomorphic to  $\mathbb{K}^n$  if  $m > n$ . This implies (2) and hence (3), because two spaces isomorphic to a third one are isomorphic to each other. Now (4) follows, since the choice of a basis of  $n$  elements establishes an isomorphism of the space with  $\mathbb{K}^n$ . Rephrasing (3) in terms of dimensions yields (5).

**Example 3.** Let  $\mathcal{V}$  be a vector space of dimension  $n$ , and let  $\mathbf{v}_1, \dots, \mathbf{v}_n$  be a basis of it. Then every vector  $\mathbf{x} \in \mathcal{V}$  can be uniquely written as  $\mathbf{x} = x_1\mathbf{v}_1 + \dots + x_n\mathbf{v}_n$ . Here  $x_1, \dots, x_n$  can be considered as linear functions from  $\mathcal{V}$  to  $\mathbb{K}$ . Namely, the function  $x_i$  takes the value 1 on the vector  $\mathbf{v}_i$  and the value 0 on all  $\mathbf{v}_j$  with  $j \neq i$ . Every linear function  $f : \mathcal{V} \rightarrow \mathbb{K}$  takes on a vector  $\mathbf{x}$  the value  $f(\mathbf{x}) = x_1f(\mathbf{v}_1) + \dots + x_nf(\mathbf{v}_n)$ . Therefore  $f$  is the linear combination of  $x_1, \dots, x_n$  with the coefficients  $f(\mathbf{v}_1), \dots, f(\mathbf{v}_n)$ , i.e.  $x_1, \dots, x_n$  span the dual space  $\mathcal{V}^*$ . In fact, they are linearly independent, and thus form a basis of  $\mathcal{V}^*$ . Indeed, if a linear combination  $\gamma_1x_1 + \dots + \gamma_nx_n$  coincides with the identically zero function, then its values  $\gamma_i$  on the vectors  $\mathbf{v}_i$  must be all zeroes. We conclude that ***the dual space  $\mathcal{V}^*$  has the same dimension  $n$  as  $\mathcal{V}$  and is isomorphic to it.*** The basis  $x_1, \dots, x_n$  is called the **dual basis** of  $\mathcal{V}^*$  with respect to the basis  $\mathbf{v}_1, \dots, \mathbf{v}_n$  of  $\mathcal{V}$ .

**Remark.** Corollaries 3, 5, and Example 3 suggest that in a sense there is “only one”  $\mathbb{K}$ -vector space in each dimension  $n = 0, 1, 2, \dots$ , namely  $\mathbb{K}^n$ . The role of this fact, which is literally true if the uniqueness is understood *up to isomorphism*, should not be overestimated. An isomorphism  $\mathbb{K}^n \rightarrow \mathcal{V}$  is determined by the choice of a basis in  $\mathcal{V}$ , and is therefore not unique. For example, the space of polynomials of degree  $< n$  in one indeterminate  $x$  has dimension  $n$  and is isomorphic to  $\mathbb{K}^n$ . However, different isomorphisms may be useful



for different purposes. In elementary algebra one would use the basis  $1, x, x^2, \dots, x^{n-1}$ . In Calculus  $1, x, x^2/2, \dots, x^{n-1}/(n-1)!$  may be more common. In the theory of interpolation the basis of **Lagrange polynomials** is used:

$$L_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}.$$

Here  $x_1, \dots, x_n$  are given distinct points on the number line, and  $L_i(x_j) = 0$  for  $j \neq i$  and  $L_i(x_i) = 1$ . The theory of orthogonal polynomials leads to many other important bases, e.g. those formed by **Chebyshev polynomials**<sup>3</sup>  $T_k$ , or **Hermite polynomials**  $H_k$ :

$$T_k(x) = \cos(k \cos^{-1}(x)), \quad H_k(x) = e^{x^2} \frac{d^k}{dx^k} e^{-x^2}.$$

There is no preferred basis in an  $n$ -dimensional vector space  $\mathcal{V}$  (and hence no preferred isomorphism between  $\mathcal{V}$  and  $\mathbb{K}^n$ ).

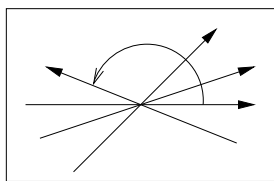


Figure 28

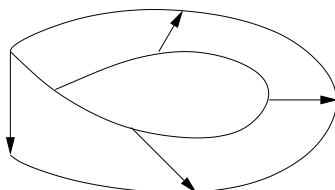


Figure 29

The lack of the preferred isomorphism becomes really important when *continuous families* of vector spaces get involved. For instance, consider on the plane  $\mathbb{R}^2$ , *all* subspaces of dimension 1 (Figure 28). When subspaces rotate, one can pick a basis vector in each of them, which would vary continuously, but when the angle of rotation approaches  $\pi$ , the *direction* of the vector disagrees with the initial direction of the same line. In fact it is impossible to choose bases in all the lines in a continuous fashion. The reason is shown on Figure 29: The surface formed by the continuous family of 1-dimensional subspaces in  $\mathbb{R}^2$  has the topology of a **Möbius band** (rather than a cylinder). The Möbius band is a first example of nontrivial *vector bundles*. Vector bundles are studied in Homotopic Topology. It turns out that among all  $k$ -dimensional vector bundles (i.e. continuous families of  $k$ -dimensional vector spaces) the most complicated are the bundles formed by *all*  $k$ -dimensional subspaces in the coordinate space of dimension  $n \gg k$ .

<sup>3</sup>After Pafnuty **Chebyshev** (1821– 1984).

**Corollary 6.** *A finite dimensional space  $\mathcal{V}$  is canonically isomorphic to its second dual  $\mathcal{V}^{**}$ .*

Here “canonically” means that *there is* a preferred isomorphism. Namely, the isomorphism is established by the map  $E : \mathcal{V} \rightarrow \mathcal{V}^{**}$  from Example 5b of Chapter 2, Section 3. Recall that to a vector  $\mathbf{v} \in \mathcal{V}$ , it assigns the linear function  $E_{\mathbf{v}} : \mathcal{V}^* \rightarrow \mathbb{K}$ , defined by evaluation of linear functions on the vector  $\mathbf{v}$ . The kernel of this map is trivial (e.g. because one can point a linear function that takes a non-zero value on a given non-zero vector). The range  $E(\mathcal{V})$  must be a subspace in  $\mathcal{V}^{**}$  isomorphic to  $\mathcal{V}$ . But  $\dim \mathcal{V}^{**} = \dim \mathcal{V}^* = \dim \mathcal{V}$ . Thus the range must be the whole space  $\mathcal{V}^{**}$ .

## Rank

In the previous subsection, we constructed a basis of a finite dimensional vector space by starting from a finite set that spans it and removing unnecessary vectors. Alternatively, one can construct a basis by starting from any linearly independent set and adding, one by one, new vectors linearly independent from the previous ones. Since the number of such vectors cannot exceed the dimension of the space, the process will stop when the vectors span the whole space and form therefore a basis. Thus we have proved that in a finite dimensional vector space, ***every linearly independent set of vectors can be completed to a basis.***<sup>4</sup> We are going to use this in the proof of the Rank Theorem.

The **rank** of a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$  is defined as the dimension of its range:  $\text{rk } A := \dim A(\mathcal{V})$ .

**Example.** Consider the map  $E_r : \mathbb{K}^n \rightarrow \mathbb{K}^m$  given by the block matrix  $E_r = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ , of size  $m \times n$ , where the left upper block is the identity matrix  $I_r$  of size  $r \times r$ , and the other three blocks are zero matrices of appropriate sizes. In standard coordinates  $(x_1, \dots, x_n)$  in  $\mathbb{K}^n$  and  $(y_1, \dots, y_m)$  in  $\mathbb{K}^m$ , the map  $E_r$  is given by the formulas  $y_1 = x_1, \dots, y_r = x_r, y_{r+1} = 0, \dots, y_m = 0$ . The range of  $E_r$  is the subspace of dimension  $r$  in  $\mathbb{K}^m$  given by the  $m - r$  equations  $y_{r+1} = \dots = y_m$ . Thus  $\text{rk } E_r = r$ . The kernel of  $E_r$  is the subspace of dimension  $n - r$  in  $\mathbb{K}^n$  given by  $r$  equations  $x_1 = \dots = x_r = 0$ . The map can be viewed geometrically as the projection along the kernel onto the range.

---

<sup>4</sup>Using the so called *transfinite induction* one can prove the same for infinite dimensional vector spaces as well.

**The Rank Theorem.** *A linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$  of rank  $r$  between two vector spaces of dimensions  $n$  and  $m$  is given by the matrix  $E_r$  in suitable bases of the spaces  $\mathcal{V}$  and  $\mathcal{W}$ .*

**Proof.** Let  $\mathbf{f}_1, \dots, \mathbf{f}_r$  be any basis in the range  $A(\mathcal{V}) \subset \mathcal{W}$ . Complete it to a basis of  $\mathcal{W}$  by choosing vectors  $\mathbf{f}_{r+1}, \dots, \mathbf{f}_m$  as explained above. Pick vectors  $\mathbf{e}_1, \dots, \mathbf{e}_r \in \mathcal{V}$  such that  $A\mathbf{e}_i = \mathbf{f}_i$ . (They exist because  $\mathbf{f}_i$  lie in the range of  $A$ .) Take vectors  $\mathbf{e}_{r+1}, \mathbf{e}_{r+2}, \dots$  to form a basis in the kernel of  $A$ . We claim that  $\mathbf{e}_1, \dots, \mathbf{e}_r, \mathbf{e}_{r+1}, \dots$  form a basis in  $\mathcal{V}$  (and in particular the total number of these vectors is equal to  $n$ ). The theorem follows from this, since  $A\mathbf{e}_i = \mathbf{f}_i$  for  $i = 1, \dots, r$ , and  $A\mathbf{e}_i = \mathbf{0}$  for  $i = r+1, \dots, n$ , and hence the matrix of  $A$  in these bases coincides with  $E_r$ .

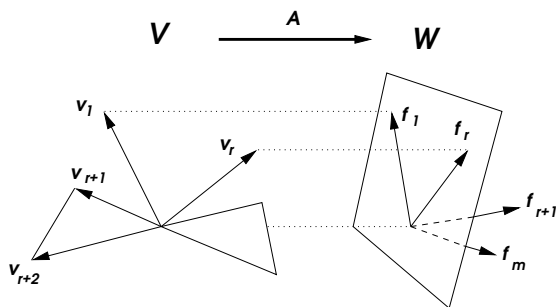


Figure 30

To justify the claim, we will show that every vector  $\mathbf{x} \in \mathcal{V}$  is uniquely written as a linear combination of  $\mathbf{e}_i$ . Indeed, we have:  $A\mathbf{x} = \alpha_1\mathbf{f}_1 + \dots + \alpha_r\mathbf{f}_r$  since  $A\mathbf{x}$  lies in the range of  $A$ . Then  $A(\mathbf{x} - \alpha_1\mathbf{e}_1 - \dots - \alpha_r\mathbf{e}_r) = \mathbf{0}$ , and hence  $\mathbf{x} - \alpha_1\mathbf{e}_1 - \dots - \alpha_r\mathbf{e}_r$  lies in the kernel of  $A$ . Therefore  $\mathbf{x} = \alpha_1\mathbf{e}_1 + \dots + \alpha_r\mathbf{e}_r + \alpha_{r+1}\mathbf{e}_{r+1} + \dots$ , i.e. the vectors  $\mathbf{v}_i$  span  $\mathcal{V}$ . On the other hand, if in the last equality we have  $\mathbf{x} = \mathbf{0}$ , then  $A\mathbf{x} = \alpha_1\mathbf{f}_1 + \dots + \alpha_r\mathbf{f}_r = \mathbf{0}$  and hence  $\alpha_1 = \dots = \alpha_r = 0$ , since  $\mathbf{f}_i$  are linearly independent in  $\mathcal{W}$ . Finally,  $\mathbf{0} = \alpha_{r+1}\mathbf{e}_{r+1} + \alpha_{r+2}\mathbf{e}_{r+2} + \dots$  implies that  $\alpha_{r+1} = \alpha_{r+2} = \dots = 0$  since  $\mathbf{e}_{r+1}, \mathbf{e}_{r+2}, \dots$  are linearly independent in  $\mathcal{V}$ .  $\square$

Let  $A$  be an  $m \times n$  matrix. It defines a linear map  $\mathbb{K}^n \rightarrow \mathbb{K}^m$ . The rank of this map is the dimension of the subspace in  $\mathbb{K}^m$  spanned by columns of  $A$ . It is called the **rank** of the matrix  $A$ . Applying the Rank Theorem to this linear map, we obtain the following result.

**Corollary.** *For every  $m \times n$ -matrix  $A$  of rank  $r$  there exist invertible matrices  $D$  and  $C$  of sizes  $m \times m$  and  $n \times n$  respectively such that  $D^{-1}AC = E_r$ .*

The Rank Theorem has the following reformulation. Let  $A : \mathcal{V} \rightarrow \mathcal{W}$  and  $A' : \mathcal{V}' \rightarrow \mathcal{W}'$  be two linear maps. They are called **equivalent** if there exist isomorphisms  $C : \mathcal{V}' \xrightarrow{\cong} \mathcal{V}$  and  $D : \mathcal{W}' \xrightarrow{\cong} \mathcal{W}$  such that  $DA' = AC$ . One expresses the last equality by saying that the following **square is commutative**:

$$\begin{array}{ccc} \mathcal{V}' & \xrightarrow{A'} & \mathcal{W}' \\ C \downarrow \cong & & \cong \downarrow D \\ \mathcal{V} & \xrightarrow{A} & \mathcal{W} \end{array} .$$

The Rank Theorem'. *Linear maps between finite dimensional spaces are equivalent if and only if they have the same rank.*

Indeed, when  $A' = D^{-1}AC$ , the ranges of  $A$  and  $A'$  must have the same dimension (since  $C$  and  $D$  are isomorphisms). Conversely, when  $\text{rk } A = r = \text{rk } A'$ , each  $A$  and  $A'$  is equivalent to  $E_r : \mathbb{K}^n \rightarrow \mathbb{K}^m$  by the Rank Theorem.

Below we discuss further corollaries and applications of the Rank Theorem.

## Adjoint Maps

Given a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ , one defines its **adjoint map**, acting between *dual* spaces in the opposite direction:  $A^t : \mathcal{W}^* \rightarrow \mathcal{V}^*$ . Namely, to a linear function  $\mathcal{W} \xrightarrow{\mathbf{a}} \mathbb{K}$ , the adjoint map  $A^t$  assigns the composition  $\mathcal{V} \xrightarrow{A} \mathcal{W} \xrightarrow{\mathbf{a}} \mathbb{K}$ , i.e.:

$$(A^t \mathbf{a})(\mathbf{x}) = \mathbf{a}(A\mathbf{x}) \quad \text{for all } \mathbf{x} \in \mathcal{V} \text{ and } \mathbf{a} \in \mathcal{W}^* .$$

In coordinates, suppose that  $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$  is given by  $m$  linear functions in  $n$  variables:

$$\begin{aligned} y_1 &= a_{11}x_1 + \cdots + a_{1n}x_n \\ &\dots \\ y_m &= a_{m1}x_1 + \cdots + a_{mn}x_n. \end{aligned}$$

These equalities show that the elements  $y_i$  of the dual basis in  $(\mathbb{K}^m)^*$  are mapped by  $A^t$  to the linear combinations  $a_{i1}x_1 + \cdots + a_{in}x_n$  of the elements  $x_j$  of the dual basis in  $(\mathbb{K}^n)^*$ . Therefore *columns* of the matrix representing the map  $A^t$  in these bases are *rows* of  $A$ . Thus, **matrices of adjoint maps with respect to dual bases are transposed to each other.**

**Corollary 1.** *Adjoint linear maps have the same rank.*

Indeed, when a map  $A : \mathcal{V} \rightarrow \mathcal{W}$  has the matrix  $E_r$  in suitable bases of  $\mathcal{V}$  and  $\mathcal{W}$ , the map  $A^t$  has the matrix  $E_r^t$  in respectively dual bases of  $\mathcal{W}^*$  and  $\mathcal{V}^*$ . Thus  $\text{rk } A^t = \text{rk } E_r^t = r$ .

**Remark.** Here is a more geometric way to understand this fact. According to the homomorphism theorem, the range of  $A : \mathcal{V} \rightarrow \mathcal{W}$  is a subspace in  $\mathcal{W}$  canonically isomorphic to  $\mathcal{V}/\text{Ker } A$ . The range of  $A^t$  is exactly the dual space  $(\mathcal{V}/\text{Ker } A)^*$  considered as the subspace in  $\mathcal{V}^*$  which consists of all those linear functions on  $\mathcal{V}$  that vanish on the  $\text{Ker } A$ . Since dual spaces have the same dimension, we conclude once again that  $\text{rk } A = \text{rk } A^t$ .

The range of the linear map  $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$  is spanned by columns of the matrix  $A$ . Therefore the rank of  $A$  is equal to the maximal number of linearly independent columns of  $A$ .

**Corollary 2.** *The maximal number of linearly independent rows of a matrix is equal to the maximal number of linearly independent columns of it.*

## Ranks and Determinants

**Corollary 3.** *The rank of a matrix is equal to the maximal size  $k$  for which there exists a  $k \times k$ -submatrix with a non-zero determinant.*

**Proof.** Suppose that a given  $m \times n$ -matrix has rank  $r$ . Then there exists a set of  $r$  linearly independent columns of it. These columns form an  $m \times r$ -matrix of rank  $r$ . Therefore there exists a set of  $r$  linearly independent rows of it. These rows form an  $r \times r$  matrix  $M$  of rank  $r$ . By Corollary of the Rank Theorem, this matrix can be written as the product  $M = DE_r C^{-1}$  where  $D$  and  $C$  are invertible  $r \times r$ -matrices, and  $E_r = I_r$  is the identity matrix of size  $r$ . Since invertible matrices have non-zero determinants, we conclude that  $\det M = (\det D)/(\det C) \neq 0$ .

On the other hand, let  $M'$  be a  $k \times k$ -submatrix of the given matrix, such that  $k > r$ . Then columns of  $M'$  are linearly dependent. Therefore one of them can be represented as a linear combination of the others. Since determinant don't change when from one of the columns, a linear combination of other columns is subtracted, we conclude that  $\det M' = 0$ .

## Systems of Linear Equations — Theory

Let  $Ax = \mathbf{b}$  be a system of  $m$  linear equations in  $n$  unknowns  $\mathbf{x}$  with the coefficient matrix  $A$  and the right hand side  $\mathbf{b}$ . Let  $r = \text{rk } A$ .

**Corollary 4.** (1) *The solution set to the homogeneous system  $Ax = \mathbf{0}$  is a linear subspace in  $\mathbb{K}^n$  of dimension  $n - r$  (namely, the kernel of  $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$ ).*

(2) *The system  $Ax = \mathbf{b}$  is consistent (i.e. has at least one solution) only when  $\mathbf{b}$  lies in a certain subspace of dimension  $r$  (namely, in the range of  $A$ ).*

(3) *When it does, the solution set to the system  $Ax = \mathbf{b}$  is an affine subspace in  $\mathbb{K}^n$  of dimension  $n - r$  parallel to the kernel of  $A$ .*

Indeed, this is obviously true in the special case  $A = E_r$ , and is therefore true in general due to the Rank Theorem.

A subspace (affine or linear) of dimension  $n - r$  in a space of dimension  $n$  is said to have **codimension**  $r$ . Thus, rephrasing Corollary 4, we can say that the solution space to a system  $Ax = \mathbf{b}$  is either empty (when the column  $\mathbf{b}$  does not lie in a subspace spanned by columns of  $A$ ), or is an affine subspace of codimension  $r$  parallel to the solution spaces of the corresponding homogeneous system  $Ax = \mathbf{0}$ . One calls the rank  $r$  of the matrix  $A$  also the **rank of the system**  $Ax = \mathbf{b}$ .

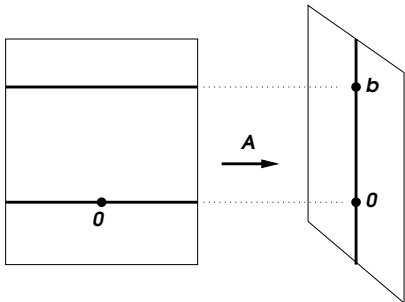


Figure 31

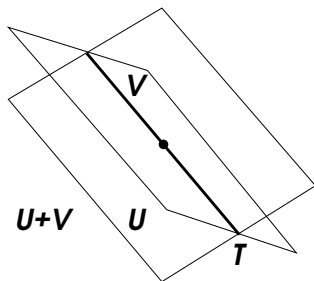


Figure 32

Consider now the case when the number of equations is equal to the number of unknowns.

**Corollary 5.** *When  $\det A \neq 0$ , the linear system  $Ax = \mathbf{b}$  of  $n$  linear equations with  $n$  unknowns has a unique solution for every  $\mathbf{b}$ , and when  $\det A = 0$ , solutions are non-unique for some (but not all)  $\mathbf{b}$  and do not exist for all others.*

Indeed, when  $\det A \neq 0$ , the matrix  $A$  is invertible, and  $\mathbf{x} = A^{-1}\mathbf{b}$  is the unique solution. When  $\det A = 0$ , the rank  $r$  of the system is smaller than  $n$ . Then the range of  $A$  has positive codimension, and the kernel has positive dimension, both equal to  $n - r$  (Figure 31).

## Dimension Counting

In 3-space, two distinct planes intersect in a line, and line meets a plane at a point. How do these geometric statements generalize to higher dimensions?

It follows from the Rank Theorem, that dimensions of the range and kernel of a linear map add up to the dimension of the domain space. We will use this fact to answer the above question.

**Corollary 6.** *If linear subspaces of dimensions  $k$  and  $l$  span together a subspace of dimension  $n$ , then their intersection is a linear subspace of dimension  $k + l - n$ .*

**Proof.** Let  $\mathcal{U}, \mathcal{V} \subset \mathcal{W}$  be linear subspaces of dimensions  $k$  and  $l$  in a vector space  $\mathcal{W}$ , and  $\mathcal{T} = \mathcal{U} \cap \mathcal{V}$  be their intersection (Figure 32). Denote by  $\mathcal{U} + \mathcal{V} \subset \mathcal{W}$  the subspace of dimension  $n$  spanned by vectors of  $\mathcal{U}$  and  $\mathcal{V}$ . Define a linear map  $A : \mathcal{U} \oplus \mathcal{V} \rightarrow \mathcal{W}$ , where  $\mathcal{U} \oplus \mathcal{V} = \{(\mathbf{u}, \mathbf{v}) | \mathbf{u} \in \mathcal{U}, \mathbf{v} \in \mathcal{V}\}$  is the direct sum, by  $A(\mathbf{u}, \mathbf{v}) = \mathbf{u} - \mathbf{v}$ . The range of  $A$  coincides with  $\mathcal{U} + \mathcal{V}$ . The kernel of  $A$  consists of all those pairs  $(\mathbf{u}, \mathbf{v})$ , where  $\mathbf{u} \in \mathcal{U}$  and  $\mathbf{v} \in \mathcal{V}$ , for which  $\mathbf{u} = \mathbf{v}$ . Therefore  $\text{Ker } A = \{(\mathbf{t}, \mathbf{t}) | \mathbf{t} \in \mathcal{T}\} \cong \mathcal{T}$ . Thus  $\dim(\mathcal{U} + \mathcal{V}) + \dim \mathcal{T} = \dim(\mathcal{U} \oplus \mathcal{V}) = \dim \mathcal{U} + \dim \mathcal{V}$ . We conclude that  $\dim \mathcal{T} = k + l - n$ .

## EXERCISES

**177.** Prove that columns of an invertible  $n \times n$ -matrix form a basis in  $\mathbb{K}^n$ , and vice versa: every basis in  $\mathbb{K}^n$  is thus obtained.

**178.** Find the dimension of the subspace in  $\mathbb{K}^4$  given by two equations:  $x_1 + x_2 + x_3 = 0$  and  $x_2 + x_3 + x_4 = 0$ . ✓

**179.** Find the dimension of the subspace in  $\mathbb{R}^{\mathbb{R}}$  spanned by functions  $\cos(x + \theta_1), \dots, \cos(x + \theta_n)$ , where  $\theta_1, \dots, \theta_n$  are given distinct angles. ✓

**180.\*** In the space of polynomials of degree  $< n$ , express the basis  $x^k, k = 0, 1, \dots, n-1$  of monomials in terms of the basis  $L_i, i = 1, \dots, n$ , of Lagrange polynomials. ✓

**181.** In  $\mathbb{R}[x]$ , find coordinates of the Chebyshev polynomials  $T_4$  in the basis of monomials  $x^k, k = 0, 1, 2, \dots$  ♪

**182.** Professor Dumbel writes his office and home phone numbers as a  $7 \times 1$ -matrix  $O$  and  $1 \times 7$ -matrix  $H$  respectively. Help him compute  $\text{rk}(OH)$ . ♪✓

**183.** Prove that  $\text{rk } A$  does not change if to a row of  $A$  a linear combination of other rows of  $A$  is added.

**184.** Prove that  $\text{rk}(A + B) \leq \text{rk } A + \text{rk } B$ .  $\zeta$

**185.** Following the proof of the Rank Theorem, find bases in the domain and the target spaces in which the following linear map  $A : \mathbb{K}^3 \rightarrow \mathbb{K}^3$

$$\begin{aligned}y_1 &= 2x_1 - x_2 - x_3 \\y_2 &= -x_1 + 2x_2 - x_3 \\y_3 &= -x_1 - x_2 + 2x_3\end{aligned}$$

has the matrix  $E_2$ . For which  $\mathbf{b} \in \mathbb{K}^3$  the system  $A\mathbf{x} = \mathbf{b}$  is consistent?  $\checkmark$

**186.** Given a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$ , its **right inverse** (respectively, **left inverse**) is defined as a linear map  $B : \mathcal{W} \rightarrow \mathcal{V}$  such that  $AB = \text{id}_{\mathcal{W}}$  (respectively,  $BA = \text{id}_{\mathcal{V}}$ ), where  $\text{id}_{\mathcal{V}}$  and  $\text{id}_{\mathcal{W}}$  denote the identity transformations on  $\mathcal{V}$  and  $\mathcal{W}$ . Prove that a right (left) inverse to  $A$  exists if and only if  $\text{rk } A = \dim \mathcal{W}$  ( $\text{rk } A = \dim \mathcal{V}$ ), and that neither is unique unless  $\dim \mathcal{V} = \dim \mathcal{W}$ .

**187.** Suppose that a system  $A\mathbf{x} = \mathbf{b}$  of  $m$  linear equations in 2009 unknowns has a unique solution for  $\mathbf{b} = (1, 0, \dots, 0)^t$ . Does this imply that: (a)  $\text{Ker } A = \{\mathbf{0}\}$ , (b)  $\text{rk } A = 2009$ , (c)  $m \geq 2009$ , (d)  $A^{-1}$  exists, (e)  $A^t A$  is invertible, (f)  $\det(AA^t) \neq 0$ , (g) rows of  $A$  are linearly independent, (h) columns of  $A$  are linearly independent?  $\checkmark$

**188.** Given  $A : \mathbb{K}^n \rightarrow \mathbb{K}^m$ , consider two **adjoint systems**:  $A\mathbf{x} = \mathbf{f}$  and  $A^t \mathbf{a} = \mathbf{b}$ . Prove that one of them (say,  $A\mathbf{x} = \mathbf{f}$ ) is consistent for a given right hand side vector ( $\mathbf{f} \in \mathbb{K}^m$ ) if and only if this vector is annihilated (i.e.  $\mathbf{a}(\mathbf{f}) = 0$ ) by all linear functions ( $\mathbf{a} \in (\mathbb{K}^m)^*$ ) satisfying the adjoint homogeneous system ( $A^t \mathbf{a} = \mathbf{0}$ ).  $\zeta$

**189.** Prove that two affine planes lying in a vector space are contained in an affine subspace of dimension  $\leq 5$ .

**190.** The solution set of a single non-trivial linear equation  $\mathbf{a}(\mathbf{x}) = b$  is called a **hyperplane** (affine if  $b \neq 0$  and linear if  $b = 0$ ). Show that a hyperplane is an (affine or linear) subspace of codimension 1.

**191.** Find possible codimensions of intersections of  $k$  linear hyperplanes.  $\checkmark$

**192.** Prove that every subspace in  $\mathbb{K}^n$  can be described as: (a) the range of a linear map; (b) the kernel of a linear map.

**193.** Classify linear subspaces in  $\mathbb{K}^n$  up to linear transformations of  $\mathbb{K}^n$ .  $\checkmark$

**194.\*** Classify *pairs* of subspaces in  $\mathbb{K}^n$  up to linear transformations.  $\checkmark$

**195.** Let  $\mathbb{K}$  be a *finite* field of  $q$  elements. Compute the number of: (a) vectors in a  $\mathbb{K}$ -vector space of dimension  $n$ , (b) bases in  $\mathbb{K}^n$ , (c)  $n \times r$ -matrices of rank  $r$ , (d) subspaces of dimension  $r$  in  $\mathbb{K}^n$ .  $\checkmark$

**196.\*** Prove that if a field has  $q$  elements, then  $q$  is a power of a prime.  $\zeta$



## 2 Gaussian Elimination

Evaluating the determinant of a  $20 \times 20$ -matrix directly from the definition of determinants requires 19 multiplications for each of the  $20! > 2 \cdot 10^{18}$  elementary products. On a typical PC that makes 1 *giga-flops* (i.e.  $10^9$  **F**loating point **O**perations **P**er **S**econd), this would take about  $4 \cdot 10^{10}$  seconds, which is a little longer than 1000 years. Algorithms based on Gaussian elimination allow your PC to evaluate much larger determinants in tiny fractions of a second.

### Row Reduction

Usually, solving a system of linear algebraic equations with coefficients given numerically we, using one of the equations, express the 1st unknown via the other unknowns and eliminate it from the remaining equations, then express the 2nd unknown from one of the remaining equations, etc., and finally arrive to an equivalent algebraic system which is easy to solve starting from the last equation and working backward. This computational procedure called **Gaussian elimination** can be conveniently organized as a sequence of operations with rows of the coefficient matrix of the system. Namely, we use three **elementary row operations**:

- transposition of two rows;
- division of a row by a non-zero scalar;
- subtraction of a multiple of one row from another one.

**Example 1.** Solving the system

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

by Gaussian elimination, we pull the 2nd equation up (since the 1st equation does not contain  $x_1$ ), divide it by 2 (in order to express  $x_1$  via  $x_2$ ) and subtract it 3 times from the 3rd equation in order to get rid of  $x_1$  therein. Then we use the 1st equation (which has become the 2nd one in our pile) in order to eliminate  $x_2$  from the 3rd equation. The coefficient matrix of the system is subject to the elementary row transformations:

$$\left[ \begin{array}{ccc|c} 0 & 1 & 2 & 3 \\ 2 & 4 & 0 & -2 \\ 3 & 5 & 1 & 0 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 2 & 4 & 0 & -2 \\ 0 & 1 & 2 & 3 \\ 3 & 5 & 1 & 0 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 3 & 5 & 1 & 0 \end{array} \right]$$

$$\mapsto \left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 0 & -1 & 1 & 3 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 3 & 6 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{array} \right].$$

The final “triangular” shape of the coefficient matrix is an example of the **row echelon form**. If read from bottom to top, it represents the system  $x_3 = 2$ ,  $x_2 + 2x_3 = 3$ ,  $x_1 + 2x_2 = -1$  which is ready to be solved by **back substitution**:  $x_3 = 2$ ,  $x_2 = 3 - 2x_3 = 3 - 4 = -1$ ,  $x_1 = -1 - 2x_2 = -1 + 2 = 1$ . The process of back substitution, expressed in the matrix form, consists of a sequence of elementary row operations of the third type:

$$\left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 1 & 2 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array} \right] \mapsto \left[ \begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array} \right].$$

The last matrix is an example of the **reduced row echelon form** and represents the system  $x_1 = 1$ ,  $x_2 = -1$ ,  $x_3 = 2$  which is “already solved”.

In general, Gaussian elimination is an algorithm of reducing an **augmented matrix** to a row-echelon form by means of elementary row operations. By an augmented matrix we mean simply a matrix subdivided into two blocks  $[A|B]$ . The augmented matrix of a linear system  $A\mathbf{x} = \mathbf{b}$  in  $n$  unknowns is  $[\mathbf{a}_1, \dots, \mathbf{a}_n|\mathbf{b}]$  where  $\mathbf{a}_1, \dots, \mathbf{a}_n$  are columns of  $A$ , but we will also make use of augmented matrices with  $B$  consisting of several columns. Operating with a row  $[a_1, \dots, a_n|b_1, \dots]$  of augmented matrices we will refer to the leftmost non-zero entry among  $a_j$  as the **leading entry**<sup>5</sup> of the row. We say that the augmented matrix  $[A|B]$  is in the **row echelon form of rank**  $r$  if the  $m \times n$ -matrix  $A$  satisfies the following conditions:

- each of the first  $r$  rows has the leading entry equal to 1;
- leading entries of the rows  $1, 2, \dots, r$  are situated respectively in the columns with indices  $j_1, \dots, j_r$  satisfying  $j_1 < j_2 < \dots < j_r$ ;
- all rows of  $A$  with indices  $i > r$  are zero.

Notice that a matrix in a row echelon has zero entries everywhere below and to the left of each leading entry. A row echelon form is called **reduced** (Figure 33) if all the entries in the columns  $j_1, \dots, j_r$  above the leading entries are also equal to zero.

<sup>5</sup>Also called **leading coefficient**, or **pivot**.

If the matrix  $A$  of a linear system is in the row echelon form and indeed has one or several zero rows on the bottom, then the system contains equations of the form  $0x_1 + \dots + 0x_n = b$ . If at least one of such  $b$  is non-zero, the system is **inconsistent** (i.e. has no solutions). If all of them are zeroes, the system is consistent and ready to be solved by back substitution.

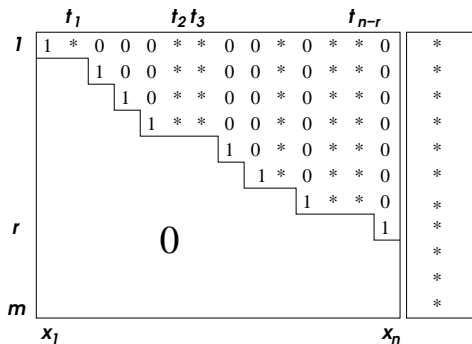


Figure 33

**Example 2.** The following augmented matrix is in the row echelon form of rank 2:

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

It corresponds to the system  $x_1 + 2x_2 + 3x_3 = 0$ ,  $x_3 = 2$ ,  $0 = 0$ . The system is consistent:  $x_3 = 2$ ,  $x_2 = t$ ,  $x_1 = -3x_3 - 2x_2 = -6 - 2t$  satisfy the system for any value of the parameter  $t$ .

We see that presence of leading entries in the columns  $j_1, \dots, j_r$  of the row echelon form allows one to express the unknowns  $x_{j_1}, \dots, x_{j_r}$  in terms of the unknowns  $x_j$  with  $j \neq j_1, \dots, j_r$ , while the values  $t_1, \dots, t_{n-r}$  of the unknowns  $x_j$ ,  $j \neq j_1, \dots, j_r$  remain completely ambiguous. In this case, **solutions to the linear system depend on the  $n - r$  parameters  $t_1, \dots, t_{n-r}$ .**

The algorithm of row reduction of an augmented matrix  $[A|B]$  to the row echelon form can be described by the following instructions. Let  $n$  be the number of columns of  $A$ . Then the algorithm consists of  $n$  steps. At the step  $l = 1, \dots, n$ , we assume that the matrix formed by the columns of  $A$  with the indices  $j = 1, \dots, l - 1$  is already in the row echelon form of some rank  $s < l$ , with the leading entries located

in some columns  $j_1 < \dots < j_s < l$ . The  $l$ -th step begins with locating the first non-zero entry in the column  $l$  below the row  $s$ . If none is found, the  $l$ -th step is over, since the columns  $1, \dots, l$  are already in the row echelon form of rank  $s$ . Otherwise the first non-zero entry is located in a row  $i (> s)$ , and the following operations are performed:

- (i) transposing the rows  $i$  and  $s + 1$  of the augmented matrix,
- (ii) dividing the whole row  $s + 1$  of the augmented matrix by the leading entry, which is now  $a_{s+1,l} (\neq 0)$ ,
- (iii) annihilating all the entries in the column  $l$  below the leading entry of the  $s + 1$ -st row by subtracting suitable multiples of the  $s + 1$ -st row of the augmented matrix from all rows with indices  $i > s + 1$ .

After that, the  $l$ -th step is over since the columns  $1, \dots, l$  are now in the row echelon form of rank  $s + 1$ .

When an augmented matrix  $[A|B]$  has been reduced to a row echelon form with the leading entries  $a_{1,j_1} = \dots = a_{r,j_r} = 1$ , the back substitution algorithm, which reduces it further to a row echelon form, consists of  $r$  steps which we number by  $l = r, r - 1, \dots, 1$  and perform in this order. On the  $l$ -th step, we subtract from each of the rows  $i = 1, \dots, l - 1$  of the augmented matrix, the  $l$ -th row multiplied by  $a_{i,j_l}$ , and thus annihilate all the entries of the column  $j_l$  above the leading entry.

## Applications

Row reduction algorithms allow one to compute efficiently determinants and inverses of square matrices given numerically, and to find a basis in the **null space**, **column space** and **row space** of a given rectangular matrix (i.e., speaking geometrically, in the kernel of the matrix, its range, and the range of the transposed matrix).

**Proposition 1.** *Suppose that an  $m \times n$ -matrix  $A$  has been reduced by elementary row operations to a row echelon form  $A'$  of rank  $r$  with the leading entries  $a_{1,j_1} = \dots = a_{r,j_r} = 1$ ,  $j_1 < \dots < j_r$ . Then*

- (1)  $\text{rk } A = \text{rk } A' = r$ ,
- (2) *rows  $1, \dots, r$  of  $A'$  form a basis in the row space of  $A$ ,*
- (3) *the columns of  $A$  with indices  $j_1, \dots, j_r$  form a basis in the column space of  $A$ .*

**Proof.** Elementary row operations do not change the space spanned by rows of the matrix. The non-zero rows of a row echelon form are linearly independent. The non-zero rows of a row echelon form are linearly independent. The non-zero rows of a row echelon form are linearly independent.

elon matrix are linearly independent and thus form a basis in the row space. In particular,  $\text{rk } A = \text{rk } A' = r$ .

The row operations change columns  $\mathbf{a}_1, \dots, \mathbf{a}_n$  of the matrix  $A$ , but preserve linear dependencies among them:  $\alpha_1 \mathbf{a}_1 + \dots + \alpha_n \mathbf{a}_n = \mathbf{0}$  if and only if  $\alpha_1 \mathbf{a}'_1 + \dots + \alpha_n \mathbf{a}'_n = \mathbf{0}$ . The  $r$  columns  $\mathbf{a}'_{j_1}, \dots, \mathbf{a}'_{j_r}$  of the matrix  $A'$  in the row echelon form which contain the leading entries are linearly independent. Therefore columns  $\mathbf{a}_{j_1}, \dots, \mathbf{a}_{j_r}$  of the matrix  $A$  are linearly independent too and hence form a basis in the column space of  $A$ .  $\square$

**Example 3.** The following row reduction

$$\begin{bmatrix} 1 & 2 & 3 & -1 \\ 2 & 4 & 5 & 1 \\ 3 & 6 & 8 & 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & -1 & 3 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

shows that the matrix has rank 2, rows  $(1, 2, 3, -1)$ ,  $(0, 0, 1, -3)$  form a basis in the row space, and columns  $(1, 2, 3)^t$ ,  $(3, 5, 8)^t$  a basis in the column space.

Suppose that the augmented matrix  $[A|\mathbf{b}]$  of the system  $A\mathbf{x} = \mathbf{b}$  has been transformed to a *reduced* row echelon form  $[A'|\mathbf{b}']$  with the leading entries positioned in the columns  $j_1 < j_2 < \dots < j_r$ . These columns are the unit coordinate vectors  $\mathbf{e}_1, \dots, \mathbf{e}_r$ , and the system is consistent only if  $\mathbf{b}'$  is their linear combination,  $\mathbf{b}' = b'_1 \mathbf{e}_1 + \dots + b'_r \mathbf{e}_r$ . Assuming that this is the case we can assign arbitrary values  $t_1, \dots, t_{n-r}$  to the unknowns  $x_j$ ,  $j \neq j_1, \dots, j_r$ , and express  $x_{j_1}, \dots, x_{j_r}$  as linear inhomogeneous functions of  $t_1, \dots, t_{n-r}$ . The general solution to the system will have the form  $\mathbf{x} = \mathbf{v}_0 + t_1 \mathbf{v}_1 + \dots + t_{n-r} \mathbf{v}_{n-r}$  of a linear combination of some  $n$ -dimensional vectors  $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{n-r}$ . We claim that ***the vectors  $\mathbf{v}_1, \dots, \mathbf{v}_{n-r}$  form a basis in the null space of the matrix  $A$ .*** Indeed, substituting  $t = 0$  we conclude that  $\mathbf{v}_0$  satisfies the equation  $A\mathbf{v}_0 = \mathbf{b}$ . Therefore  $\mathbf{x} - \mathbf{v}_0 = t_1 \mathbf{v}_1 + \dots + t_{n-r} \mathbf{v}_{n-r}$  form the general solution to the homogeneous system  $A\mathbf{x} = \mathbf{0}$ , i.e. the null space of  $A$ . In addition, we see that ***the solution set to the inhomogeneous system is the affine subspace in  $\mathbb{R}^n$  obtained from the null space by the translation through the vector  $\mathbf{v}_0$ .***

**Example 4.** Consider the system  $A\mathbf{x} = \mathbf{0}$  with the matrix  $A$  from Example 3. Transform the matrix to the reduced row echelon form:

$$\dots \mapsto \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 2 & 0 & 8 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The general solution to the system assumes the form

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} -2t_1 - 8t_2 \\ t_1 \\ 3t_2 \\ t_2 \end{bmatrix} = t_1 \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t_2 \begin{bmatrix} -8 \\ 0 \\ 3 \\ 1 \end{bmatrix}.$$

The columns  $(-2, 1, 0, 0)^t$  and  $(-8, 0, 3, 1)^t$  form therefore a basis in the null space of the matrix  $A$ .

**Proposition 2.** *Suppose that in the process of row reduction of an  $n \times n$  matrix  $A$  to a row echelon form  $A'$  row transpositions occurred  $k$  times, and the operations of division by leading entries  $\alpha_1, \dots, \alpha_r$  were performed. If  $\text{rk } A' < n$  then  $\det A = 0$ . If  $\text{rk } A' = n$  then  $\det A = (-1)^k \alpha_1 \dots \alpha_n$ .*

Indeed, each transposition of rows reverses the sign of the determinant, divisions of a row by  $\alpha$  divides the determinant by  $\alpha$ , and subtraction of a multiple of one row from another one does not change the determinant. Thus  $\det A = (-1)^k \alpha_1 \dots \alpha_r \det A'$ . The row echelon matrix is upper triangular. When  $\text{rk } A' = n$ , it has  $n$  leading 1's on the diagonal, and hence  $\det A' = 1$ . When  $r < n$  we have  $\det A' = 0$ .

**Proposition 3.** *Given an  $n \times n$ -matrix  $A$ , introduce the augmented matrix  $[A|I_n]$  (where  $I_n$  is the identity matrix) and transform it to the reduced row-echelon form  $[A'|B]$  by elementary row operations. If  $A' = I_n$  then  $B = A^{-1}$ .*

Indeed, the equality  $A' = I_n$  means that  $\text{rk } A = n$  and thus  $A^{-1}$  exists. Then the system  $A\mathbf{x} = \mathbf{b}$  has a unique solution for any  $\mathbf{b}$ , and for  $\mathbf{b} = \mathbf{e}_1, \dots, \mathbf{e}_n$  the corresponding solutions  $\mathbf{x} = A^{-1}\mathbf{e}_1, \dots, A^{-1}\mathbf{e}_n$  are the columns of the inverse matrix  $A^{-1}$ . These solutions can be found by simultaneous row reduction of the augmented matrices  $[A|\mathbf{e}_1], \dots, [A|\mathbf{e}_n]$  and thus coincide with the columns of the matrix  $B$  in the reduced row-echelon form  $[I_n|B]$ .

**Example 5.** Let us compute  $\det A$  and  $A^{-1}$  for the matrix of Example 1. We have:

$$\begin{aligned} \left[ \begin{array}{ccc|ccc} 0 & 1 & 2 & 1 & 0 & 0 \\ 2 & 4 & 0 & 0 & 1 & 0 \\ 3 & 5 & 1 & 0 & 0 & 1 \end{array} \right] &\mapsto \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 3 & 5 & 1 & 0 & 0 & 1 \end{array} \right] \mapsto \\ \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & -\frac{3}{2} & 1 \end{array} \right] &\mapsto \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & \frac{1}{3} & -\frac{1}{2} & \frac{1}{3} \end{array} \right]. \end{aligned}$$

Here one transposition of rows and divisions by 2 and by 3 were applied. Thus  $\det A = (-1) \cdot 2 \cdot 3 = -6$ , and the matrix is invertible. Back substitution eventually yields the inverse matrix:

$$\mapsto \left[ \begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 1 & 0 & \frac{1}{3} & 1 & -\frac{2}{3} \\ 0 & 0 & 1 & \frac{1}{3} & -\frac{1}{2} & \frac{1}{3} \end{array} \right] \mapsto \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{2}{3} & -\frac{3}{2} & \frac{4}{3} \\ 0 & 1 & 0 & \frac{1}{3} & 1 & -\frac{2}{3} \\ 0 & 0 & 1 & \frac{1}{3} & -\frac{1}{2} & \frac{1}{3} \end{array} \right].$$

**Remark.** Gaussian elimination algorithms are unlikely to work well for matrices depending on parameters. To see why, try row reduction in order to solve a linear system of the form  $(\lambda I - A)\mathbf{x} = \mathbf{0}$  depending on the parameter  $\lambda$ , or (even better!) apply Gaussian elimination to the system  $a_{11}x_1 + a_{12}x_2 = b_1$ ,  $a_{21}x_1 + a_{22}x_2 = b_2$  depending on 6 parameters  $a_{11}, a_{12}, a_{21}, a_{22}, b_1, b_2$ .

## LPU Decomposition

Gaussian elimination is an algorithm. The fact that it always works is a theorem. In this and next subsections, we reformulate this theorem (or rather an important special case of it) first in the language of matrix algebra, and then in geometric terms.

Recall that a square matrix  $A$  is called **upper triangular** (respectively **lower triangular**) if  $a_{ij} = 0$  for all  $i > j$  (respectively  $i < j$ ). We call  $P$  a **permutation matrix** if it is obtained from the identity matrix  $I_n$  by a permutation of columns. Such  $P$  is indeed the matrix of a linear transformation in  $\mathbb{K}^n$  defined as the permutation of coordinate axes.

**Theorem.** *Every invertible matrix  $M$  can be factored as the product  $M = LPU$  of a lower triangular matrix  $L$ , a permutation matrix  $P$ , and an upper triangular matrix  $U$ .*

The proof of this theorem is based on interpretation of elementary row operations in terms of matrix multiplication. Consider the following  $m \times m$ -matrices:

- $T_{ij}$  ( $i \neq j$ ), a **transposition matrix**, obtained by transposing the  $i$ -th and  $j$ -th columns of the identity matrix;
- $D_i(d)$  ( $d \neq 0$ ), a diagonal matrix, all of whose diagonal entries are equal to 1 except the  $i$ -th one, which is equal to  $1/d$ ;
- $L_{ij}(\alpha)$  ( $i > j$ ), a lower triangular matrix, all of whose diagonal entries are equal to 1, and all off-diagonal equal to 0 except the entry in  $i$ -th row and  $j$ -th column, which is equal to  $-\alpha$ .

Here are examples  $T_{13}$ ,  $D_2(3)$ , and  $L_{24}(-2)$  of size  $m = 4$ :

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{bmatrix}.$$

Elementary row operations on a given  $m \times n$ -matrix can be described as multiplication on the left by  $T_{ij}$ ,  $D_i(d)$ , or  $L_{ij}(\alpha)$ , which results respectively in transposing the  $i$ -th and  $j$ -th rows, dividing the  $i$ -th row by  $d$ , and subtracting the  $i$ -th row times  $\alpha$  from the  $j$ -th row. Note that inverses of elementary row operations are also elementary row operations. Thus, Gaussian elimination allows one to represent any matrix  $A$  as the product of a row echelon matrix with matrices of elementary row operations. In order to prove the  $LPU$  decomposition theorem, we will combine this idea with a modification of the Gaussian elimination algorithm.

Let  $M$  be an *invertible*  $n \times n$ -matrix. We apply the row reduction process to it, temporarily refraining from using permutations and divisions of rows and using only the row operations equivalent to left multiplication by  $L_{ij}(\alpha)$ . On the  $i$ -th step of the algorithm, if the  $i$ -th row does not contain a non-zero entry where expected, we don't swap it with the next row. Instead, we locate in *this* row the leading (i.e. leftmost non-zero) entry, which must exist since the matrix is invertible. When it is found in a column  $j$ , we subtract multiples of the row  $i$  from rows  $i + 1, \dots, n$  with such coefficients that all entries of these rows in the column  $j$  become annihilated.

**Example 7.** Let us illustrate the modified row reduction with the matrix taken from Example 1, and at the same time represent the process as matrix factorization. On the first step, we subtract the 1st row from the 2nd and 3rd 4 and 5 times respectively, and on the second step subtract the 2nd row times  $\frac{3}{2}$  from the 3rd. The lower triangular factors shown are *inverses* of the matrices  $L_{12}(4)$ ,  $L_{13}(5)$  and  $L_{23}(\frac{3}{2})$ . The leading entries are boldfaced:

$$\begin{aligned} \begin{bmatrix} 0 & \mathbf{1} & 2 \\ 2 & 4 & 0 \\ 3 & 5 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & \mathbf{1} & 2 \\ \mathbf{2} & 0 & -8 \\ 3 & 0 & -9 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \frac{3}{2} & 1 \end{bmatrix} \begin{bmatrix} 0 & \mathbf{1} & 2 \\ \mathbf{2} & 0 & -8 \\ 0 & 0 & \mathbf{3} \end{bmatrix}. \end{aligned}$$



Products of lower triangular matrices are lower triangular. As a result, applying the modified row reduction we obtain a factorization of the form  $M = LM'$ , where  $L$  is a lower triangular matrix with all diagonal entries equal to 1. Note that on the  $i$ th step of the algorithm, when a leading entry in the row  $i$  is searched, the leading entries of the previous rows can be in any columns  $j_1, \dots, j_{i-1}$ . The entries of the  $i$ -row situated in these columns have been annihilated at the previous steps. Therefore the leading entry of the  $i$ -th row will be found in a new column. This shows that the columns  $j_1, \dots, j_n$  of the leading entries found in the rows  $1, \dots, n$  are all distinct and thus form a permutation of  $\{1, \dots, n\}$ . We now write  $M' = PU$ , where  $P$  is the matrix of the permutation  $\binom{1, \dots, n}{j_1, \dots, j_n}$ . The operation  $M' \mapsto U = P^{-1}M'$  permutes rows of  $M'$  and places all leading entries of the resulting matrix  $U$  on the diagonal. Here is how this works in our example:

$$\begin{bmatrix} 0 & \mathbf{1} & 2 \\ \mathbf{2} & 0 & -8 \\ 0 & 0 & \mathbf{3} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \mathbf{2} & 0 & -8 \\ 0 & \mathbf{1} & 2 \\ 0 & 0 & \mathbf{3} \end{bmatrix}.$$

Since leading entries are leftmost non-zero entries in their rows, the matrix  $U$  turns out to be *upper* triangular. This completes the proof.

**Remarks.** (1) As it is seen from the proof, the matrix  $L$  in the  $LPU$  factorization can be required to have all diagonal entries equal to 1. Triangular matrices with this property are called **unipotent**. Alternatively, one can require that  $U$  is unipotent.

(2) When the permutation matrix  $P = I_n$ , one obtains the **LU decomposition**,  $M = LU$ , of *some* invertible matrices. Which ones? One can work backward and consider products  $LDU$  of a lower and upper triangular unipotent matrices  $L$  and  $U$  with an invertible diagonal matrix  $D$  in between (the so called **LDU decomposition**). A choice of such matrices depends on a number of arbitrary parameters:  $n(n-1)/2$  for each  $L$  and  $U$ , and  $n$  non-zero parameters for  $D$ , i.e. totally  $n^2$ . This is equal to the total number of matrix elements, suggesting that a *typical*  $n \times n$ -matrix admits an  $LDU$  factorization.

(3) This heuristic claim can be made precise. As illustrated by the above example of  $LPU$  decomposition, when  $P \neq I_n$ , certain entries of the resulting factor  $U$  come out equal to 0. This is because some entries of the matrix  $M'$  on the *right* of leading ones are annihilated at previous steps of row reduction. As a result, such decompositions involve fewer than  $n^2$  arbitrary parameters, and hence cover a positive codimension locus in the matrix space. Thus, the bulk of the space is covered by factorizations  $LPU$  with  $P = I_n$ .

## Flags and Bruhat cells

A sequence  $\mathcal{V}_1 \subset \mathcal{V}_2 \subset \cdots \subset \mathcal{V}_n$  of nested subspaces is said to form a **flag** in the space  $\mathcal{V} = \mathcal{V}_n$ . When  $\dim \mathcal{V}_k = k$  for all  $k = 1, \dots, n$ , the flag is called **complete**.

Given a basis  $\mathbf{f}_1, \dots, \mathbf{f}_n$  in  $\mathcal{V}$ , one can associate to it the **standard coordinate flag** (Figure 34)

$$\text{Span}(\mathbf{f}_1) \subset \text{Span}(\mathbf{f}_1, \mathbf{f}_2) \subset \cdots \subset \text{Span}(\mathbf{f}_1, \dots, \mathbf{f}_n) = \mathcal{V}.$$

Let  $U : \mathcal{V} \rightarrow \mathcal{V}$  be an invertible linear transformation *preserving* the standard coordinate flag. Then the matrix of  $U$  in the given basis is upper triangular. Indeed, since  $U(\mathcal{V}_k) \subset \mathcal{V}_k$ , the vector  $U\mathbf{f}_k$  is a linear combination of  $\mathbf{f}_1, \dots, \mathbf{f}_k$ , i.e.  $U\mathbf{f}_k = \sum_{i \leq k} u_{ik}\mathbf{f}_i$ . Since this is true for all  $k$ , the matrix  $[u_{ik}]$  is upper triangular. Reversing this argument, we find that if the matrix of  $U$  is upper triangular, then  $U$  preserves the flag.

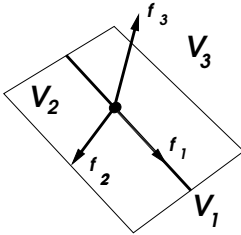


Figure 34

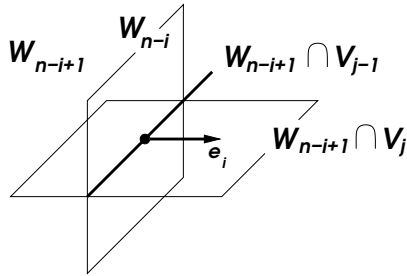


Figure 35

Conversely, given a complete flag  $\mathcal{V}_1 \subset \cdots \subset \mathcal{V}_n = \mathbb{K}^n$ , one can pick a basis  $\mathbf{f}_1$  in the line  $\mathcal{V}_1$ , then complete it to a basis  $\mathbf{f}_1, \mathbf{f}_2$  in the plane  $\mathcal{V}_2$ , and so on, until a basis  $\mathbf{f}_1, \dots, \mathbf{f}_n$  in the whole space  $\mathcal{V}_n$  is obtained, such that  $\mathcal{V}_k = \text{Span}(\mathbf{f}_1, \dots, \mathbf{f}_k)$  for each  $k$ . This shows that **every complete flag in  $\mathbb{K}^n$  can be obtained from any other by an invertible linear transformation**. Indeed, the linear transformation, defined in terms of the standard basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  of  $\mathbb{K}^n$  by  $\sum x_i \mathbf{e}_i \mapsto \sum x_i \mathbf{f}_i$ , transforms the standard coordinate flag  $\text{Span}(\mathbf{e}_1) \subset \cdots \subset \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_n)$  into the given flag  $\mathcal{V}_1 \subset \cdots \subset \mathcal{V}_n$ .

**Example 8.** Let  $P_\sigma : \mathbb{K}^n \rightarrow \mathbb{K}^n$  act by a permutation  $\sigma = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix}$  of coordinate axes. It transforms the *standard* coordinate flag into a **coordinate flag**

$$\mathbf{F}_\sigma : \text{Span}(\mathbf{e}_{i_1}) \subset \text{Span}(\mathbf{e}_{i_1}, \mathbf{e}_{i_2}) \subset \cdots \subset \text{Span}(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_n}) = \mathbb{K}^n,$$

called so because all the spaces are spanned by vectors of the standard basis. There are  $n!$  such flags, one for each permutation. For instance,  $\mathbf{F}_{\text{id}}$  is the standard coordinate flag. When  $\sigma = \begin{pmatrix} 1 & \cdots & n \\ n & \cdots & 1 \end{pmatrix}$ , the flag **opposite** to the standard one is obtained:

$$\text{Span}(\mathbf{e}_n) \subset \text{Span}(\mathbf{e}_n, \mathbf{e}_{n-1}) \subset \cdots \subset \text{Span}(\mathbf{e}_n, \dots, \mathbf{e}_1).$$

Transformation of  $\mathbb{K}^n$  defined by *lower* triangular matrices are exactly those that preserve this flag.

**Theorem.** *Every complete flag in  $\mathbb{K}^n$  can be transformed into exactly one of  $n!$  coordinate flags by invertible linear transformations preserving one of them (e.g. the flag opposite to the standard one).*

**Proof.** Let  $\mathbf{F}$  be a given complete flag in  $\mathbb{K}^n$ ,  $\mathbf{F}_{\text{id}}$  the standard coordinate flag,  $M$  a linear transformation such that  $\mathbf{F} = M(\mathbf{F}_{\text{id}})$ , and  $M = LP_\sigma U$  its LPU decomposition. Since  $U(\mathbf{F}_{\text{id}}) = \mathbf{F}_{\text{id}}$ , and  $P_\sigma(\mathbf{F}_{\text{id}}) = \mathbf{F}_\sigma$ , we find that  $\mathbf{F} = L(\mathbf{F}_\sigma)$ . Therefore the given flag  $\mathbf{F}$  is transformed into a coordinate flag  $\mathbf{F}_\sigma$  by  $L^{-1}$ , which is lower triangular and thus preserves the flag opposite to  $\mathbf{F}_{\text{id}}$ .

It remains to show that the same flag  $\mathbf{F}$  cannot be transformed this way into two different coordinate flags  $\mathbf{F}_\sigma$ . Let  $\mathcal{V}_j$ ,  $\dim \mathcal{V}_j = j$ , denote the spaces of the flag  $\mathbf{F}$ , and  $\mathcal{W}_{n-i} = \text{Span}(\mathbf{e}_n, \dots, \mathbf{e}_{i+1})$  the spaces of the flag opposite to the standard one,  $\text{codim } \mathcal{W}_{n-i} = i$ . Invertible transformations preserving the spaces  $\mathcal{W}_{n-i}$  can change their intersections with  $\mathcal{V}_j$ , but cannot change the dimensions of these intersections. Thus it suffices to show that, in the case of the flag  $\mathbf{F}_\sigma$ , the permutation  $\sigma$  is uniquely determined by these dimensions.

Note that  $\mathbf{e}_i \in \mathcal{W}_{n-i+1}$  but  $\mathbf{e}_i \notin \mathcal{W}_{n-i}$  (Figure 35), i.e. the quotient (1-dimensional!) space  $\mathcal{W}_{n-i+1}/\mathcal{W}_{n-i}$  is spanned by the image of  $\mathbf{e}_i$ . Suppose that in the flag  $\mathbf{F}_\sigma$ , the vector  $\mathbf{e}_i$  first occurs in the subspace  $\mathcal{V}_j$ , i.e.  $\sigma(j) = i$ . Consider the increasing sequence of spaces  $\mathcal{V}_1 \subset \cdots \subset \mathcal{V}_n = \mathbb{K}^n$ , their intersections with  $\mathcal{W}_{n-i+1}$ , and the projections of these intersections to the quotient space  $\mathcal{W}_{n-i+1}/\mathcal{W}_{n-i}$ . Examining the ranges of these maps and their dimensions, we find the sequence of  $j-1$  zeroes followed by  $n-j$  ones. Thus  $j = \sigma^{-1}(i)$  is determined by the flag.  $\square$

**Remark.** The theorem solves the following *classification* problem: In a vector space equipped with a fixed complete flag  $\mathcal{W}_1 \subset \cdots \subset \mathcal{W}_n$ , classify all complete flags up to invertible linear transformations preserving the fixed flag. According to the theorem, there are  $n!$  equivalence classes determined by dimensions of intersections of spaces of

the flags with the spaces of the fixed flag. The equivalence classes are known as **Bruhat cells**. This formulation also shows that the Gaussian elimination algorithm can be understood as a solution to a *simple* geometric classification problem. One can give a purely geometric proof of the above theorem (and hence a new proof of the *LPU* decomposition) by refining the argument in the proof of the Rank Theorem. the Rank Theorem, Gaussian elimination, and Bruhat cells under the same roof.

### EXERCISES

**197.** Solve systems of linear equations: ✓

$$\begin{array}{lll} 2x_1 - x_2 - x_3 = 4 & x_1 + x_2 - 3x_3 = -1 & 2x_1 + x_2 + x_3 = 2 \\ 3x_1 + 4x_2 - 2x_3 = 11 & 2x_1 + x_2 - 2x_3 = 1 & x_1 + 3x_2 + x_3 = 5 \\ 3x_1 - 2x_2 + 4x_3 = 11 & x_1 + x_2 + x_3 = 3 & x_1 + x_2 + 5x_3 = -7 \\ & x_1 + 2x_2 - 3x_3 = 1 & 2x_1 + 3x_2 - 3x_3 = 14 \end{array}$$

$$\begin{array}{ll} x_1 - 2x_2 + x_3 + x_4 = 1 & x_1 - 2x_2 + 3x_3 - 4x_4 = 4 \\ x_1 - 2x_2 + x_3 - x_4 = -1 & x_2 - x_3 + x_4 = -3 \\ x_1 - 2x_2 + x_3 + 5x_4 = 5 & x_1 + 3x_2 - 3x_4 = 1 \\ & -7x_2 + 3x_3 + x_4 = -3 \end{array}$$

$$\begin{array}{ll} 2x_1 + 3x_2 - x_3 + 5x_4 = 0 & 3x_1 + 4x_2 - 5x_3 + 7x_4 = 0 \\ 3x_1 - x_2 + 2x_3 - 7x_4 = 0 & 2x_1 - 3x_2 + 3x_3 - 2x_4 = 0 \\ 4x_1 + x_2 - 3x_3 + 6x_4 = 0 & 4x_1 + 11x_2 - 13x_3 + 16x_4 = 0 \\ x_1 - 2x_2 + 4x_3 - 7x_4 = 0 & 7x_1 - 2x_2 + x_3 + 3x_4 = 0 \end{array}$$

$$\begin{array}{l} x_1 + x_2 + x_3 + x_4 + x_5 = 7 \\ 3x_1 + 2x_2 + x_3 + x_4 - 3x_5 = -2 \\ x_2 + 2x_3 + 2x_4 + 6x_6 = 23 \\ 5x_1 + 4x_2 + 3x_3 + 3x_4 - x_5 = 12 \end{array}$$

**198.\*** Find those  $\lambda$  for which the system is consistent: ✓

$$\begin{array}{l} 2x_1 - x_2 + x_3 + x_4 = 1 \\ x_1 + 2x_2 - x_3 + 4x_4 = 2 \\ x_1 + 7x_2 - 4x_3 + 11x_4 = \lambda \end{array}$$

**199.** For each of the following matrices, find the rank and bases in the null, column, and row spaces: ✓

$$(a) \begin{bmatrix} 0 & 4 & 10 & 1 \\ 4 & 8 & 18 & 7 \\ 10 & 18 & 40 & 17 \\ 1 & 7 & 17 & 3 \end{bmatrix} \quad (b) \begin{bmatrix} 14 & 2 & 6 & 8 & 2 \\ 6 & 104 & 21 & 9 & 17 \\ 7 & 6 & 3 & 4 & 1 \\ 35 & 30 & 15 & 20 & 5 \end{bmatrix}$$

$$(c) \begin{bmatrix} 1 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 2 & 5 \\ 0 & 0 & 1 & 3 & 6 \\ 1 & 2 & 3 & 14 & 32 \\ 4 & 5 & 6 & 32 & 77 \end{bmatrix} \quad (d) \begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 4 & 1 \\ 1 & 1 & 1 & 5 \\ 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad (e) \begin{bmatrix} 2 & 1 & 3 & -1 \\ 3 & -1 & 2 & 0 \\ 1 & 3 & 4 & -2 \\ 4 & -3 & 1 & 1 \end{bmatrix}.$$

**200.** For each of the following matrices, compute the determinant and the inverse matrix, and an *LUP* decomposition: ✓

$$(a) \begin{bmatrix} 2 & 2 & -3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{bmatrix} \quad (b) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (c) \begin{bmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{bmatrix}.$$

**201.** Prove that  $D_i^{-1}(d) = D_i(d^{-1})$  and  $L_{ij}^{-1}(\alpha) = L_{ij}(-\alpha)$ .

**202.** Prove that the inverse of a permutation matrix  $P$  is  $P^t$ .

**203.** Prove that every invertible matrix  $M$  has an **LUP decomposition**  $M = LUP$  where  $L$  is lower triangular,  $U$  upper triangular, and  $P$  is a permutation matrix, and compute such factorizations for the matrices from the previous exercise. ♣

**204.** Prove that every invertible matrix  $M$  has an **PLU decomposition**  $M = PLU$ . ♣

**205.** Prove that every invertible matrix has factorizations of the form  $UPL$ ,  $PUL$ , and  $ULP$ , where  $L$ ,  $U$ , and  $P$  stand for lower triangular, upper triangular, and permutation matrices respectively. ♣

**206.** List all *coordinate* complete flags in  $\mathbb{K}^3$ .

**207.** For each permutation matrix  $P$  of size  $4 \times 4$ , describe all upper triangular matrices  $U$  which can occur as a result of the modified Gaussian algorithm from the proof of the *LPU* decomposition theorem. For each permutation, find the maximal number of non-zero entries of  $U$ .

**208.\*** Compute the **dimension** of each Bruhat cell, i.e. the number of parameters on which flags in the equivalence class of  $\mathbf{F}_\sigma$  depend. ✓

**209.\*** When  $\mathbb{K}$  is a finite field of  $q$  elements, find the number of *all* complete flags in  $\mathbb{K}^n$ . ✓

**210.\*** Prove that the number of Bruhat cells of dimension  $l$  is equal to the coefficient at  $q^l$  in the product (called **q-factorial**) ♣

$$[n]_q! := (1+q)(1+q+q^2) \cdots (1+q+q^2+\cdots+q^{n-1}).$$



### 3 The Inertia Theorem

We study here the classification of quadratic forms and some generalizations of this problem. The answer actually depends on properties of the field of scalars  $\mathbb{K}$ . Our first goal will be to examine the case  $\mathbb{K} = \mathbb{R}$ . We begin however with a key argument that remains valid in general.

#### Orthogonal Bases

We will assume here that the field  $\mathbb{K}$  does *not* contain  $\mathbb{Z}_2$ , i.e. that  $1 + 1 \neq 0$  in  $\mathbb{K}$ . Then, for any  $\mathbb{K}$ -vector space, there is a one-to-one correspondence between symmetric bilinear forms and quadratic forms:

$$Q(\mathbf{x}) = Q(\mathbf{x}, \mathbf{x}), \quad Q(\mathbf{x}, \mathbf{y}) = \frac{1}{2}[Q(\mathbf{x} + \mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})].$$

Let  $\dim \mathcal{V} = n$ ,  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$  be a basis of  $\mathcal{V}$ , and  $(x_1, \dots, x_n)$  corresponding coordinates. In these coordinates, the quadratic form  $Q$  is written as:

$$Q(\mathbf{x}) = \sum_{i=1}^n \sum_{j=1}^n q_{ij} x_i x_j.$$

The coefficients  $q_{ij}$  here are the values  $Q(\mathbf{f}_i, \mathbf{f}_j)$  of the corresponding symmetric bilinear form:

$$Q(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \sum_{j=1}^n x_i q_{ij} y_j.$$

These coefficients form a matrix, also denoted  $Q$ , which is symmetric:  $q_{ij} = q_{ji}$  for all  $i, j = 1, \dots, n$ . The basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$  is called  **$Q$ -orthogonal** if  $Q(\mathbf{f}_i, \mathbf{f}_j) = 0$  for all  $i \neq j$ , i.e. if the coefficient matrix is diagonal.

**Lemma.** *Every quadratic form in  $\mathbb{K}^n$  has an orthogonal basis.*

**Proof.** We use induction on  $n$ . For  $n = 1$  the requirement is empty. Let us construct a  $Q$ -orthogonal basis in  $\mathbb{K}^n$  assuming that every quadratic form in  $\mathbb{K}^{n-1}$  has an orthogonal basis. If  $Q$  is the identically zero quadratic form, then the corresponding symmetric bilinear form is identically zero too, and so any basis will be

$Q$ -orthogonal. If the quadratic form  $Q$  is not identically zero, then there exists a vector  $\mathbf{f}_1$  such that  $Q(\mathbf{f}_1) \neq 0$ . Let  $\mathcal{V}$  be the subspace in  $\mathbb{K}^n$  consisting of all vectors  $Q$ -orthogonal to  $\mathbf{f}_1$ :  $\mathcal{V} = \{\mathbf{x} \in \mathbb{K}^n \mid Q(\mathbf{f}_1, \mathbf{x}) = 0\}$ . This subspace does *not* contain  $\mathbf{f}_1$  and is given by 1 linear equation. Thus  $\dim \mathcal{V} = n - 1$ . Let  $\{\mathbf{f}_2, \dots, \mathbf{f}_n\}$  be a basis in  $\mathcal{V}$  orthogonal with respect to the symmetric bilinear form obtained by restricting  $Q$  to this subspace. Such a basis exists by the induction hypothesis. Therefore  $Q(\mathbf{f}_i, \mathbf{f}_j) = 0$  for all  $1 < i < j$ . Besides,  $Q(\mathbf{f}_1, \mathbf{f}_i) = 0$  for all  $i > 1$ , since  $\mathbf{f}_i \in \mathcal{V}$ . Thus  $\{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_n\}$  is a  $Q$ -orthogonal basis of  $\mathbb{K}^n$ .  $\square$

**Corollary.** *For every symmetric  $n \times n$ -matrix  $Q$  with entries from  $\mathbb{K}$  there exists an invertible matrix  $C$  such that  $C^t Q C$  is diagonal.*

The diagonal entries here are the values  $Q(\mathbf{f}_1), \dots, Q(\mathbf{f}_n)$ .

## Inertia Indices

Consider the case  $\mathbb{K} = \mathbb{R}$ .

Given a quadratic form  $Q$  in  $\mathbb{R}^n$ , we pick a  $Q$ -orthogonal basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$  and then *rescale* those of the basis vectors for which  $Q(\mathbf{f}_i) \neq 0$ :  $\mathbf{f}_i \mapsto \tilde{\mathbf{f}}_i = |Q(\mathbf{f}_i)|^{-1/2} \mathbf{f}_i$ . After such rescaling, the non-zero coefficients  $Q(\tilde{\mathbf{f}}_i)$  of the quadratic form will become  $\pm 1$ . Reordering the basis so that terms with positive coefficients come first, and negative next, we transform  $Q$  to the normal form:

$$Q = X_1^2 + \dots + X_p^2 - X_{p+1}^2 - \dots - X_{p+q}^2, \quad p + q \leq n.$$

Note that by restricting  $Q$  to the subspace  $X_{p+1} = \dots = X_n = 0$  of dimension  $p$  we obtain a quadratic form on this subspace which is **positive** (or **positive definite**), i.e. takes on positive values everywhere outside the origin.

**Proposition.** *The numbers  $p$  and  $q$  of positive and negative squares in the normal form are equal to the maximal dimensions of the subspaces in  $\mathbb{R}^n$  where the quadratic form  $Q$  (respectively,  $-Q$ ) is positive.*

*Proof.* The quadratic form  $Q = X_1^2 + \dots + X_p^2 - X_{p+1}^2 - \dots - X_{p+q}^2$  is non-positive everywhere on the subspace  $\mathcal{W}$  of dimension  $n - p$  given by the equations  $X_1 = \dots = X_p = 0$ . Let us show that the existence of a subspace  $\mathcal{V}$  of dimension  $p + 1$  where the quadratic form is positive leads to a contradiction. Indeed, the subspaces  $\mathcal{V}$  and  $\mathcal{W}$  would



intersect in a subspace of dimension at least  $(p+1) + (n-p) - n = 1$ , containing therefore non-zero vectors  $\mathbf{x}$  with  $Q(\mathbf{x}) > 0$  and  $Q(\mathbf{x}) \leq 0$ . Thus,  $Q$  is positive on some subspace of dimension  $p$  and cannot be positive on any subspace of dimension  $> p$ . Likewise,  $-Q$  is positive on some subspace of dimension  $q$  and cannot be positive on any subspace of dimension  $> q$ .  $\square$

The maximal dimensions of positive subspaces of  $Q$  and  $-Q$  are called respectively **positive** and **negative inertia indices** of a quadratic form in question. By definition, inertia indices of a quadratic form do not depend on the choice of a coordinate system. Our Proposition implies that the normal forms with different pairs of values of  $p$  and  $q$  are pairwise non-equivalent. This establishes the Inertia Theorem (as stated in Section 4 of Chapter 1).

**Theorem.** *Every quadratic form in  $\mathbb{R}^n$  by a linear change of coordinates can be transformed to exactly one of the normal forms:*

$$X_1^2 + \dots + X_p^2 - X_{p+1}^2 - \dots - X_{p+q}^2, \quad \text{where } 0 \leq p + q \leq n.$$

The matrix formulation of the Inertia Theorem reads:

*Every real symmetric matrix  $Q$  can be transformed to exactly one of the diagonal forms* 
$$\begin{bmatrix} I_p & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -I_q & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$$
 *by transformations of the form*  $Q \mapsto C^t Q C$  *defined by invertible real matrices  $C$ .*

## Complex Quadratic Forms

Consider the case  $\mathbb{K} = \mathbb{C}$ .

**Theorem.** *Every quadratic form in  $\mathbb{C}^n$  can be transformed by linear changes of coordinates to exactly one of the normal forms:*

$$z_1^2 + \dots + z_r^2, \quad \text{where } 0 \leq r \leq n.$$

**Proof.** Given a quadratic form  $Q$ , pick a  $Q$ -orthogonal basis in  $\mathbb{C}^n$ , order it in such a way that vectors  $\mathbf{f}_1, \dots, \mathbf{f}_r$  with  $Q(\mathbf{f}_i) \neq 0$  come first, and then rescale these vectors by  $\mathbf{f}_i \mapsto \sqrt{Q(\mathbf{f}_i)}\mathbf{f}_i$ .

In particular, we have proved that *every complex symmetric matrix*  $Q$  can be transformed to exactly one of the forms  $\begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$  by the transformations of the form  $Q \mapsto C^t Q C$  defined by invertible complex matrices  $C$ . As it follows from the Rank Theorem, here  $r = \text{rk } Q$ , the rank of the coefficient matrix of the quadratic form. This guarantees that the normal forms with different values of  $r$  are pairwise non-equivalent, and thus completes the proof.  $\square$

To establish the geometrical meaning of  $r$ , consider a more general situation.

Given a quadratic form  $Q$  on a  $\mathbb{K}$ -vector space  $\mathcal{V}$ , its **kernel** is defined as the subspace of  $\mathcal{V}$  consisting of all vectors which are  $Q$ -orthogonal to all vectors from  $\mathcal{V}$ :

$$\text{Ker } Q := \{\mathbf{z} \in \mathcal{V} \mid Q(\mathbf{z}, \mathbf{v}) = 0 \text{ for all } \mathbf{v} \in \mathcal{V}\}$$

Note that the values  $Q(\mathbf{x}, \mathbf{y})$  do not change when a vector from the kernel is added to either of  $\mathbf{x}$  and  $\mathbf{y}$ . As a result, the symmetric bilinear form  $Q$  descends to the *quotient space*  $\mathcal{V}/\text{Ker } Q$ .

The **rank** of a quadratic form  $Q$  on  $\mathbb{K}^n$  is defined as the codimension of  $\text{Ker } Q$ . For example, the quadratic form  $z_1^2 + \cdots + z_r^2$  on  $\mathbb{K}^n$  corresponds to the symmetric bilinear form  $x_1 y_1 + \cdots + x_r y_r$ , and has the kernel of codimension  $r$  defined by the equations  $z_1 = \cdots = z_r = 0$ .

## Conics

The set of all solutions to one polynomial equation in  $\mathbb{K}^n$ :

$$F(x_1, \dots, x_n) = 0$$

is called a **hypersurface**. When the polynomial  $F$  does not depend on one of the variables (say,  $x_n$ ), the equation  $F(x_1, \dots, x_{n-1}) = 0$  defines a hypersurface in  $\mathbb{K}^{n-1}$ . Then solution set in  $\mathbb{K}^n$  is called a **cylinder**, since it is the Cartesian product of the hypersurface in  $\mathbb{K}^{n-1}$  and the line of arbitrary values of  $x_n$ .

Hypersurfaces defined by polynomial equations of degree 2 are often referred to as **conics** — a name reminiscent of conic sections, which are “hypersurfaces” in  $\mathbb{K}^2$ . The following application of the Inertia Theorem allows one to classify all conics in  $\mathbb{R}^n$  up to **equivalence** defined by compositions of translations with invertible linear transformations.

**Theorem.** *Every conic in  $\mathbb{R}^n$  is equivalent to either the cylinder over a conic in  $\mathbb{R}^{n-1}$ , or to one of the conics:*

$$\begin{aligned}
 x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2 &= 1, & 0 \leq p \leq n, \\
 x_1^2 + \cdots + x_p^2 &= x_{p+1}^2 + \cdots + x_n^2, & 0 \leq p \leq n/2, \\
 x_n &= x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{n-1}^2, & 0 \leq p \leq (n-1)/2,
 \end{aligned}$$

*known as hyperboloids, cones, and paraboloids respectively.*

For  $n = 3$ , all types of “hyperboloids” (of which the first type contains spheres and ellipsoids) are shown in Figures 36, and cones and paraboloids in Figure 37.

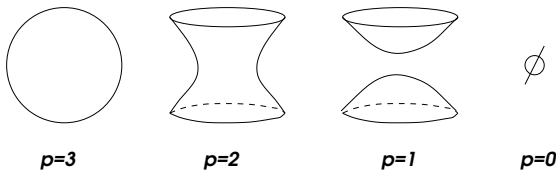


Figure 36

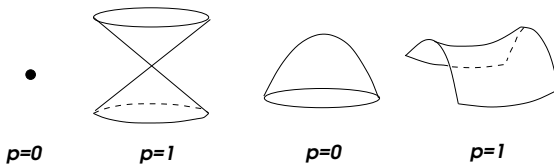


Figure 37

**Proof.** Given a degree 2 polynomial  $F = Q(\mathbf{x}) + \mathbf{a}(\mathbf{x}) + c$ , where  $Q$  is a non-zero quadratic form,  $\mathbf{a}$  a linear form, and  $c$  a constant. we can apply a linear change of coordinates to transform  $Q$  to the form  $\pm x_1^2 \pm \cdots \pm x_r^2$ , where  $r \leq n$ , and then use the completion of squares in the variables  $x_1, \dots, x_r$  to make the remaining linear form independent of  $x_1, \dots, x_r$ . When  $r = n$ , the resulting equations  $\pm x_1^2 \pm \cdots \pm x_n^2 = C$  (where  $C$  is a new constant) define hyperboloids (when  $C \neq 0$ ), or cones (when  $C = 0$ ). When  $r < n$ , we can take the remaining *linear* part of the function  $F$  (together with the constant) for a new,  $r + 1$ -st coordinate, provided that this linear part is non-constant. When  $r = n - 1$ , we obtain the equations of paraboloids. When  $r < n - 1$ , or if  $r = n - 1$ , but the linear function was constant, the function  $F$ , written in new coordinates, does not depend on the last of them, and this defines the cylinder over a conic in  $\mathbb{R}^{n-1}$ .  $\square$

Classification of conics in  $\mathbb{C}^n$  is obtained in the same way, but the answer looks simpler, since there are no signs  $\pm$  in the normal forms of quadratic forms over  $\mathbb{C}$ .

**Theorem.** *Every conic in  $\mathbb{C}^n$  is equivalent to either the cylinder over a conic in  $\mathbb{C}^{n-1}$ , or to one of the three conics:*

$$z_1^2 + \cdots + z_n^2 = 1, \quad z_1^2 + \cdots + z_n^2 = 0, \quad z_n = z_1^2 + \cdots + z_{n-1}^2.$$

**Example.** Let  $Q$  be a non-degenerate quadratic form with *real* coefficients in 3 variables. According to the previous (real) classification theorem, the conic  $Q(x_1, x_2, x_3) = 1$  can be transformed by a real change of coordinates into one of the 4 normal forms shown on Figure 36. The same real change of coordinates identifies the set of *complex* solutions to the equation  $Q(z_1, z_2, z_3) = 1$  with that of the normal form:  $\pm z_1^2 \pm z_2^2 + \pm z_3^2 = 1$ . However,  $-z$  becomes  $z$  after the change  $z \mapsto \sqrt{-1}z$ , which identifies the set of complex solutions with the **complex sphere** in  $\mathbb{C}^3$ , given by the equation  $z_1^2 + z_2^2 + z_3^2 = 1$ . Thus, various complex conics equivalent to the complex sphere and given by equations with real coefficients, “expose” themselves in  $\mathbb{R}^3$  by various *real forms*: real spheres or ellipsoids, hyperboloids of one or two sheets (as shown on figure 36), or even remain invisible (when the set of real points is empty).

**Remark.** The same holds true in general: various hyperboloids (as well as cones or paraboloids) of the real classification theorem are real forms of complex conics defined by the same equations. They become equivalent when complex changes of coordinates are allowed. In this sense, the three normal forms of the last theorem represent hyperboloids, cones and paraboloids of the previous one.

## Hermitian and Anti-Hermitian Forms

We introduce here a variant of the notion of a quadratic form which makes sense in complex vector spaces. It has no direct analogues over arbitrary fields, but it plays a central role in geometry and mathematical physics.

Let  $\mathcal{V}$  be a  $\mathbb{C}$ -vector space. A function<sup>6</sup>  $P : \mathcal{V} \times \mathcal{V} \rightarrow \mathbb{C}$  is called a **sesquilinear form** if it is linear in the second argument, i.e.

$$P(\mathbf{z}, \lambda\mathbf{x} + \mu\mathbf{y}) = \lambda P(\mathbf{z}, \mathbf{x}) + \mu P(\mathbf{z}, \mathbf{y}) \quad \text{for all } \lambda, \mu \in \mathbb{C} \text{ and } \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{V},$$

---

<sup>6</sup>We leave it to the reader to examine the possibility when the function  $P$  is defined on the product  $\mathcal{V} \times \mathcal{W}$  of two different spaces.

and **semilinear** (or **antilinear**) in the first one:

$$P(\lambda \mathbf{x} + \mu \mathbf{y}, \mathbf{z}) = \bar{\lambda}P(\mathbf{x}, \mathbf{z}) + \bar{\mu}P(\mathbf{y}, \mathbf{z}) \quad \text{for all } \lambda, \mu \in \mathbb{C} \text{ and } \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{V}.$$

When  $P$  is sesquilinear, the form  $P^*$  defined by

$$P^*(\mathbf{x}, \mathbf{y}) := \overline{P(\mathbf{y}, \mathbf{x})}$$

is also sesquilinear, and is called **Hermitian adjoint**<sup>7</sup> to  $P$ . When  $P^* = P$ , i.e.

$$P(\mathbf{y}, \mathbf{x}) = \overline{P(\mathbf{x}, \mathbf{y})} \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathcal{V},$$

the form  $P$  is called **Hermitian symmetric**. When  $P^* = -P$ , i.e.

$$P(\mathbf{y}, \mathbf{x}) = -\overline{P(\mathbf{x}, \mathbf{y})} \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathcal{V},$$

the form  $P$  is called **Hermitian anti-symmetric**. When  $P$  is Hermitian symmetric,  $iP$  is Hermitian anti-symmetric (and *vice versa*) since  $\bar{i} = -i$ . Every sesquilinear form is uniquely written as the sum of an Hermitian symmetric and Hermitian anti-symmetric form:

$$P = H + Q, \quad H = \frac{1}{2}(P + P^*), \quad Q = \frac{1}{2}(P - P^*).$$

In coordinates, when  $\mathbf{x} = \sum x_i \mathbf{e}_i$  and  $\mathbf{y} = \sum y_j \mathbf{e}_j$ , we have

$$P(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^m \sum_{j=1}^n \bar{x}_i p_{ij} y_j, \quad \text{where } p_{ij} = P(\mathbf{e}_i, \mathbf{e}_j).$$

The coefficients  $p_{ij}$  of a sesquilinear form can be arbitrary complex numbers, and form a square matrix which we also denote by  $P$ . The Hermitian adjoint form has the coefficient matrix, denoted  $P^*$ , whose entries are  $p_{ij}^* = P(\mathbf{e}_j, \mathbf{e}_i) = \overline{p_{ji}}$ . Thus two complex square matrices,  $P$  and  $P^*$ , are **Hermitian adjoint** if they are obtained from each other by transposition and entry-wise complex conjugation:

$$P^* = \bar{P}^t.$$

A complex square matrix  $P$  is called **Hermitian** if  $P^* = P$ , and **anti-Hermitian** if  $P^* = -P$ .

To any Hermitian symmetric sesquilinear form on a  $\mathbb{C}$ -vector space  $\mathcal{V}$ , there corresponds an **Hermitian quadratic form**, or simply **Hermitian form**,  $\mathbf{z} \mapsto H(\mathbf{z}, \mathbf{z})$ . Following our abuse-of-notation convention, we denote this form by the same letter  $H$ , i.e. put

$$H(\mathbf{z}) := H(\mathbf{z}, \mathbf{z}) \quad \text{for all } \mathbf{z} \in \mathcal{V}.$$

The values  $H(\mathbf{z})$  of an Hermitian form are *real*:  $H(\mathbf{z}, \mathbf{z}) = \overline{H(\mathbf{z}, \mathbf{z})}$ .

<sup>7</sup>After French mathematician Charles **Hermite** (1822–1901).

In coordinates  $\mathbf{z} = \sum z_i \mathbf{e}_i$ , an Hermitian form is written as

$$H(\mathbf{z}) = \sum_{i=1}^n \sum_{j=1}^n \bar{z}_i h_{ij} z_j,$$

where  $h_{ij} = \overline{h_{ji}}$ . For example, the Hermitian form

$$|\mathbf{z}|^2 = |z_1|^2 + \cdots + |z_n|^2,$$

corresponds to the sesquilinear form

$$\langle \mathbf{x}, \mathbf{y} \rangle = \bar{x}_1 y_1 + \cdots + \bar{x}_n y_n,$$

which plays the role of the **Hermitian dot product** in  $\mathbb{C}^n$ . Note that  $|\mathbf{z}|^2 > 0$  unless  $\mathbf{z} = \mathbf{0}$ . An Hermitian form on a vector space  $\mathcal{V}$  is called **positive definite** (or simply **positive**) if all of its values outside the origin are positive.

Since  $H(\mathbf{z}, \mathbf{w}) + H(\mathbf{w}, \mathbf{z}) = 2 \operatorname{Re} H(\mathbf{z}, \mathbf{w})$ , we have:

$$\operatorname{Re} H(\mathbf{z}, \mathbf{w}) = \frac{1}{2} [H(\mathbf{z} + \mathbf{w}) - H(\mathbf{z}) - H(\mathbf{w})],$$

$$\operatorname{Im} H(\mathbf{z}, \mathbf{w}) = \operatorname{Re} H(i\mathbf{z}, \mathbf{w}) = \frac{1}{2} [H(i\mathbf{z} + \mathbf{w}) - H(i\mathbf{z}) - H(\mathbf{w})],$$

i.e. a Hermitian symmetric sesquilinear form is uniquely determined by the corresponding Hermitian quadratic form.

**Theorem.** *Every Hermitian form  $H$  in  $\mathbb{C}^n$  can be transformed by a  $\mathbb{C}$ -linear change of coordinates to exactly one of the normal forms*

$$|z_1|^2 + \cdots + |z_p|^2 - |z_{p+1}|^2 - \cdots - |z_{p+q}|^2, \quad 0 \leq p + q \leq n.$$

**Proof.** It is the same as in the case of the Inertia Theorem for real quadratic forms. We pick a vector  $\mathbf{f}_1$  such that  $H(\mathbf{f}_1) = \pm 1$ , and consider the subspace  $\mathcal{V}_1$  consisting of all vectors  $H$ -orthogonal to  $\mathbf{f}_1$ . It does not contain  $\mathbf{f}_1$  (since  $H(\mathbf{f}_1, \mathbf{f}_1) = H(\mathbf{f}_1) \neq 0$ ), and has codimension 1. We consider the Hermitian form obtained by restricting  $H$  to  $\mathcal{V}_1$  and proceed the same way, i.e. pick a vector  $\mathbf{f}_2 \in \mathcal{V}_1$  such that  $H(\mathbf{f}_2) = \pm 1$ , and pass to the subspace  $\mathcal{V}_2$  consisting of all vectors of  $\mathcal{V}_1$  which are  $H$ -orthogonal to  $\mathbf{f}_2$ . The process stops when we reach a subspace  $\mathcal{V}_r$  of codimension  $r$  in  $\mathbb{C}^n$  such that the restriction of the form  $H$  to  $\mathcal{V}_r$  vanishes identically. Then we pick

any basis  $\{\mathbf{f}_{r+1}, \dots, \mathbf{f}_n\}$  in  $\mathcal{V}_r$ . The vectors  $\mathbf{f}_1, \dots, \mathbf{f}_n$  form a basis in  $\mathbb{C}^n$  which is  $H$ -orthogonal (since  $H(\mathbf{f}_i, \mathbf{f}_j) = 0$  for all  $i < j$  by construction), and  $H(\mathbf{f}_i, \mathbf{f}_i) = \pm 1$  (for  $i \leq r$ ) or  $= 0$  for  $i > r$ . Reordering the vectors  $\mathbf{f}_1, \dots, \mathbf{f}_r$  so that those with the values  $+1$  come first, we obtain the required normal form for  $H$ , where  $p+q = r$ .

To prove that the normal forms with different pairs of values of  $p$  and  $q$  are non-equivalent to each other, we show (the same way as in the case of real quadratic forms) that *the number  $p$  ( $q$ ) of positive (respectively negative) squares in the normal form is equal to the maximal dimension of a subspace where the Hermitian form  $H$  (respectively  $-H$ ) is positive definite*.  $\square$ .

To any given Hermitian anti-symmetric sesquilinear form  $Q$ , there corresponds an **anti-Hermitian form**  $Q(\mathbf{z}) := Q(\mathbf{z}, \mathbf{z})$ , which takes on purely imaginary values, and determines the given sesquilinear form uniquely. Applying the theorem to the *Hermitian* form  $iQ$ , we obtain the following result.

**Corollary 1.** *An anti-Hermitian form  $Q$  in  $\mathbb{C}^n$  can be transformed by a  $\mathbb{C}$ -linear change of coordinates to exactly one of the normal forms*

$$i|z_1|^2 + \dots + i|z_p|^2 - i|z_{p+1}|^2 - \dots - i|z_{p+q}|^2, \quad 0 \leq p+q \leq n.$$

Using matrix notation, we can express the Hermitian dot product by  $\mathbf{x}^* \mathbf{y}$  (where  $\mathbf{x}^* = \bar{\mathbf{x}}^t$ ), and respectively the values of an arbitrary sesquilinear form by  $P(\mathbf{x}, \mathbf{y}) = \mathbf{x}^* P \mathbf{y}$ . Making a linear change of variables  $\mathbf{x} = C \mathbf{x}'$ ,  $\mathbf{y} = C \mathbf{y}'$ , we find  $\mathbf{x}^* P \mathbf{y} = (\mathbf{x}')^* P' \mathbf{y}'$ , where  $P'$  is the coefficient matrix of the same form in the new coordinates. The value  $p'_{ij} = P(C \mathbf{e}_i, C \mathbf{e}_j)$  is the product of the  $i$ th row of  $C^*$  with  $P$  and the  $j$ th column of  $C$ . Thus  $P' = C^* P C$ . Therefore the previous results have the following matrix reformulations.

**Corollary 2.** *Any Hermitian (anti-Hermitian) matrix can be transformed to exactly one of the normal forms*

$$\begin{bmatrix} I_p & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -I_q & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \left( \text{respectively} \begin{bmatrix} iI_p & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -iI_q & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \right).$$

*by transformations of the form  $P \mapsto C^* P C$  defined by invertible complex matrices  $C$ .*

It follows that  $p+q$  is equal to the rank of the coefficient matrix of the (anti-)Hermitian form.

## Sylvester's Rule

Let  $H$  be a Hermitian  $n \times n$ -matrix. Denote by  $\Delta_0 = 1$ ,  $\Delta_1 = h_{11}$ ,  $\Delta_2 = h_{11}h_{22} - h_{12}h_{21}$ ,  $\dots$ ,  $\Delta_n = \det H$  the minors formed by the intersection of the first  $k$  rows and columns of  $H$ ,  $k = 1, 2, \dots, n$  (Figure 38). They are called **leading minors** of the matrix  $H$ . Note that  $\det H = \det H^t = \det \bar{H} = \overline{\det H}$  is real, and the same is true for each  $\Delta_k$ , since it is the determinant of an Hermitian  $k \times k$ -matrix. The following result is due to the English mathematician James **Sylvester** (1814–1897).

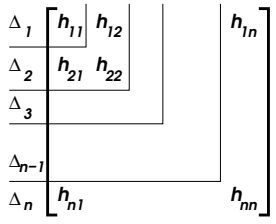


Figure 38

**Theorem.** *Suppose that an Hermitian  $n \times n$ -matrix  $H$  has non-zero leading minors. Then the negative inertia index of the corresponding Hermitian form is equal to the number of sign changes in the sequence  $\Delta_0, \Delta_1, \dots, \Delta_n$ .*

**Remark.** The hypothesis that  $\det H \neq 0$  means that the Hermitian form is **non-degenerate**, or equivalently, that its kernel is trivial. In other words, for each non-zero vector  $\mathbf{x}$  there exists  $\mathbf{y}$  such that  $H(\mathbf{x}, \mathbf{y}) \neq 0$ . Respectively, the assumption that all leading minors are non-zero means that *restrictions of the Hermitian forms to all spaces of the standard coordinate flag*

$$\text{Span}(\mathbf{e}_1) \subset \text{Span}(\mathbf{e}_1, \mathbf{e}_2) \subset \dots \subset \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_k) \subset \dots$$

*are non-degenerate.* The proof of the theorem consists in classifying such Hermitian forms up to linear changes of coordinates that *preserve the flag.*

**Proof.** As before, we inductively construct an  $H$ -orthogonal basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$  and normalize the vectors so that  $H(\mathbf{f}_i) = \pm 1$ , requiring however that each  $\mathbf{f}_k \in \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_k)$ . When such vectors  $\mathbf{f}_1, \dots, \mathbf{f}_{k-1}$  are already found, the vector  $\mathbf{f}_k$ ,  $H$ -orthogonal to them, can be found (by the Rank Theorem) in the  $k$ -dimensional space of



the flag, and can be assumed to satisfy  $H(\mathbf{f}_k) = \pm 1$ , since the Hermitian form on this space is non-degenerate. Thus, ***an Hermitian form non-degenerate on each space of the standard coordinate flag can be transformed to one (and in fact exactly one) of the  $2^n$  normal forms  $\pm|z_1|^2 \pm \dots \pm|z_n|^2$  by a linear change of coordinates preserving the flag.***

In matrix form, this means that there exists an invertible *upper triangular matrix*  $C$  such that  $D = C^*HC$  is diagonal with all diagonal entries equal to  $\pm 1$ . Note that transformations of the form  $H \mapsto C^*HC$  may change the determinant but preserve its sign:

$$\det(C^*HC) = (\det C^*)(\det H)(\det C) = \det H |\det C|^2.$$

When  $C$  is upper triangular, the same holds true for all leading minors, i.e. each  $\Delta_k$  has the same sign as the leading  $k \times k$ -minor of the diagonal matrix  $D$  with the diagonal entries  $d_1, \dots, d_n$  equal  $\pm 1$ . The latter minors form the sequence  $1, d_1, d_1d_2, \dots, d_1 \dots d_k, \dots$ , where the sign is changed each time as  $d_k = -1$ . Thus the total number of sign changes is equal to the number of negative squares in the normal form.  $\square$

When the form  $H$  is positive definite, its restrictions to any subspace is positive definite and hence non-degenerate automatically. We obtain the following corollaries.

**Corollary 1.** *Any positive definite Hermitian form in  $\mathbb{C}^n$  can be transformed into  $|z_1|^2 + \dots + |z_n|^2$  by a linear change of coordinates preserving a given complete flag.*

**Corollary 2.** *A Hermitian form in  $\mathbb{C}^n$  is positive definite if and only if all of its leading minors are positive.*

Note that the standard basis of  $\mathbb{C}^n$  is **orthonormal** with respect to the Hermitian dot product  $\langle \mathbf{x}, \mathbf{y} \rangle = \sum \bar{x}_i y_i$ , i.e.  $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$  for  $i \neq j$ , and  $\langle \mathbf{e}_i, \mathbf{e}_i \rangle = 1$ .

**Corollary 3.** *Every Hermitian form in  $\mathbb{C}^n$  has an orthonormal basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_n\}$  such that  $\mathbf{f}_k \in \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_k)$ .*

**Remarks.** (1) The process of replacing a given basis  $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  with a new basis, orthonormal with respect to a given positive definite Hermitian form and such that each  $\mathbf{f}_k$  is a linear combination of  $\mathbf{e}_1, \dots, \mathbf{e}_k$ , is called **Gram–Schmidt orthogonalization**.

(2) Results of this subsection hold true for quadratic forms in  $\mathbb{R}^n$ . Namely, our reasoning can be easily adjusted to this case. Note also that every real symmetric matrix is Hermitian.

## Finite Fields

Consider the case  $\mathbb{K} = \mathbb{Z}_p$ , the field of integers modulo a prime number  $p \neq 2$ . It consists of  $p$  elements corresponding to possible remainders  $0, 1, 2, \dots, p-1$  of integers divided by  $p$ . It is indeed a field due to some facts of elementary number theory. Namely, when an integer  $a$  is not divisible by  $p$ , it follows from the Euclidean algorithm, that the greatest common divisor of  $a$  and  $p$ , which is 1, can be represented as their linear combination:  $1 = ma + np$ . Modulo  $p$ , this means that  $m$  is inverse to  $a$ . Thus every non-zero element of  $\mathbb{Z}_p$  is invertible.

As we have seen, in classification of quadratic forms, it is important to know which scalars are complete squares.

**Examples.** (1) Let  $Q = ax^2$  and  $Q' = a'x^2$  be two non-zero quadratic forms on  $\mathbb{K}^1$  (i.e.  $a, a' \in \mathbb{K} - \{0\}$ ). Rescaling  $x$  to  $cx$ , where  $c$  can be any element from  $\mathbb{K} - \{0\}$ , transforms  $Q$  into  $ac^2x^2$ . Thus, the quadratic forms in  $\mathbb{K}^1$  are equivalent if and only if  $a' = ac^2$  for some non-zero  $c$ . i.e. if the ratio  $a'/a$  is a complete square in  $\mathbb{K} - \{0\}$ .

(2) When  $\mathbb{K} = \mathbb{C}$ , every element is a complete square, so there is only one equivalence class of *non-zero* quadratic forms in  $\mathbb{C}^1$ . When  $\mathbb{K} = \mathbb{R}$ , there are two such classes according to the sign of the coefficient (because complete squares are exactly the positive reals).

(3) When  $\mathbb{K} = \mathbb{Z}_p$ , there are  $p-1$  non-zero quadratic forms which are divided into two equivalence classes. One class can be represented by the normal form  $x^2$  and consists of those quadratic forms whose coefficient is a complete square,  $a = c^2 \neq 0$ . There are  $(p-1)/2$  such forms, i.e. a half of all non-zero ones, since each complete square  $a = c^2$  has exactly two different square roots:  $c$  and  $-c$ . Let  $\varepsilon \neq 0$  be any non-square. Then, when  $c^2$  runs all squares,  $\varepsilon c^2$  runs all the  $(p-1)/2$  non-squares. Thus  $Q = \varepsilon x^2$  can be taken for the normal form in the other equivalence class.

(4) In  $\mathbb{Z}_{13}$ , there are 12 non-zero elements represented by the integers  $\pm 1, \dots, \pm 6$ , their squares are  $1, 4, -4, 3, -1, -3$  respectively, and the non-squares are  $\pm 2, \pm 5, \pm 6$ . Any of them (e.g. 2) can be taken for  $\varepsilon$ . Thus, every non-zero quadratic form on  $\mathbb{Z}_{13}^1$  is equivalent to either  $x^2$  or  $2x^2$ . This example suggests that there may be no choice of the normal form  $\varepsilon x^2$  good for all  $\mathbb{Z}_p$  at once.

**Theorem.** *Every non-zero quadratic form on  $\mathbb{Z}_p^n$ ,  $p \neq 2$ , is equivalent to exactly one of the forms*

$$x_1^2 + x_2^2 + \dots + x_r^2, \quad \varepsilon x_1^2 + x_2^2 + \dots + x_r^2, \quad 1 \leq r \leq n.$$

**Proof.** First note that both normal forms have rank  $r$ . Since the rank of the coefficient matrix  $Q$  of a quadratic form does not change under the transformations  $C^tQC$  defined by invertible matrices  $C$ , it suffices to prove that a quadratic form of a fixed rank  $r > 0$  is equivalent to exactly one of the two normal forms.

Next, the symmetric bilinear form corresponding to the quadratic form  $Q$  of rank  $r$  has kernel  $\text{Ker}(Q)$  (non-trivial when  $r < n$ ) and defines a *non-degenerate* symmetric bilinear form on the quotient space  $\mathbb{K}^n / \text{Ker}(Q)$  of dimension  $r$ . Thus, it suffices to prove that a non-degenerate quadratic form on  $\mathbb{K}^r = \mathbb{Z}_p^r$  is equivalent to exactly one of the two normal forms.

The normal forms, considered as non-degenerate quadratic forms on  $\mathbb{Z}_p^r$ , are not equivalent to each other. Indeed, they have diagonal coefficient matrices with determinants equal 1 and  $\varepsilon$  respectively, of which the first one is a square in  $\mathbb{Z}_p$ , and the second is not. But for equivalent non-degenerate quadratic forms, the ratio of the determinants is a complete square:  $\det(C^tQC)/(\det Q) = (\det C)^2$ .

To transform a non-degenerate quadratic form  $Q$  on  $\mathbb{Z}_p^r$  to one of the normal forms, we can construct a  $Q$ -orthogonal basis  $\{\mathbf{f}_1, \dots, \mathbf{f}_r\}$  and thus reduce  $Q$  to the form  $a_1x_1^2 + \dots + a_rx_r^2$ . Here  $a_i = Q(\mathbf{f}_i) \neq 0$ . We would like to show that a better choice of a basis can be made, such that  $Q(\mathbf{f}_i) = 1$  for all  $i > 1$ . Let us begin with the case  $r = 2$ .

**Lemma.** *Given non-zero  $a, b \in \mathbb{Z}_p$ , there exist  $(x, y) \in \mathbb{Z}_p^2$  such that  $ax^2 + by^2 = 1$ .*

Indeed, when each of  $x$  and  $y$  runs all  $p$  possible values (including 0) each of  $ax^2$  and  $1 - by^2$  takes on  $(p - 1)/2 + 1$  different values. Since the total number exceeds  $p$ , we must have  $ax^2 = 1 - by^2$  for some  $x$  and  $y$ .  $\square$

Thus, given a non-degenerate quadratic form  $P = ax^2 + by^2$  in  $\mathbb{Z}_p^2$ , there exists  $\mathbf{f} \in \mathbb{Z}_p^2$ , such that  $P(\mathbf{f}) = 1$ . Taking a second vector  $P$ -orthogonal to  $\mathbf{f}$ , we obtain a new basis in which  $P$  takes on the form  $a'x^2 + b'y^2$  with  $a' = 1$  and  $b' \neq 0$ .

We can apply this trick  $r - 1$  times to the quadratic form  $Q = a_1x_1^2 + \dots + a_rx_r^2$  using two of the variables at a time, and end up with the form where  $a_r = a_{r-1} = \dots = a_2 = 1$ . Finally, rescaling  $x_1$  as in Example 3, we can make  $a_1$  equal either 1 or  $\varepsilon$ .

**Remark.** Readers comfortable with arbitrary finite fields can easily check that our proof and the theorem remain true over any finite field  $\mathbb{K} \supset \mathbb{Z}_p$ ,  $p \neq 2$ , with any non-square in  $\mathbb{K}$  taken in the role of  $\varepsilon$ .

### The Case of $\mathbb{K} = \mathbb{Z}_2$ .

This is a peculiar world where  $2 = 0$ ,  $-1 = 1$ , and where therefore the usual one-to-one correspondence between quadratic and symmetric bilinear forms is broken, and the distinction between symmetric and anti-symmetric forms lost.

Yet, consider a symmetric bilinear form  $Q$  on  $\mathbb{Z}_2^n$ :

$$Q(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n \sum_{j=1}^n x_i q_{ij} y_j, \text{ where } q_{ij} = q_{ji} = 0 \text{ or } 1 \text{ for all } i, j.$$

The corresponding quadratic form  $Q(\mathbf{x}) := Q(\mathbf{x}, \mathbf{x})$  still exists, but satisfies  $Q(\mathbf{x} + \mathbf{y}) = Q(\mathbf{x}) + 2Q(\mathbf{x}, \mathbf{y}) + Q(\mathbf{y}) = Q(\mathbf{x}) + Q(\mathbf{y})$  and hence defines a *linear* function  $\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ . This linear function can be identically zero, i.e.  $Q(\mathbf{x}, \mathbf{x}) = 0$  for all  $\mathbf{x}$ , in which case the bilinear form  $Q$  is called **even**. This happens exactly when all the diagonal entries of the coefficient matrix vanish:  $q_{ii} = Q(\mathbf{e}_i, \mathbf{e}_i) = 0$  for all  $i$ . Otherwise the bilinear form  $Q$  is called **odd**. We begin with classifying *even non-degenerate* forms. As it is implied by the following theorem, such forms exist only in  $\mathbb{Z}_2$ -spaces of even dimension  $n = 2k$ .

**Theorem.** *Every even non-degenerate symmetric bilinear form  $Q$  on  $\mathbb{Z}_2^n$  in a suitable coordinate system is given by the formula:*

$$Q(\mathbf{x}, \mathbf{y}) = x_1 y_2 + x_2 y_1 + \cdots + x_{2k-1} y_{2k} + x_{2k} y_{2k-1}. \quad (i)$$

**Proof.** Pick any  $\mathbf{f}_1 \neq \mathbf{0}$  and find  $\mathbf{f}_2$  such that  $Q(\mathbf{f}_1, \mathbf{f}_2) = 1$ . Such  $\mathbf{f}_2$  must exist since  $Q$  is non-degenerate. In  $\text{Span}(\mathbf{f}_1, \mathbf{f}_2)$ , we have:  $Q(x_1 \mathbf{f}_1 + x_2 \mathbf{f}_2, y_1 \mathbf{f}_1 + y_2 \mathbf{f}_2) = x_1 y_2 + x_2 y_1$ , since  $Q$  is even, i.e.  $Q(\mathbf{f}_1, \mathbf{f}_1) = Q(\mathbf{f}_2, \mathbf{f}_2) = 0$ .

Let  $\mathcal{V}$  denote the space of all vectors  $Q$ -orthogonal to  $\text{Span}(\mathbf{f}_1, \mathbf{f}_2)$ . It is given by two linear equations:  $Q(\mathbf{f}_1, \mathbf{x}) = 0$ ,  $Q(\mathbf{f}_2, \mathbf{x}) = 0$ , which are independent (since  $\mathbf{x} = \mathbf{f}_1$  satisfies the first one but not the second, and  $\mathbf{x} = \mathbf{f}_2$  the other way around). Therefore  $\text{codim } \mathcal{V} = 2$ . If  $\mathbf{v} \in \mathcal{V}$  is  $Q$ -orthogonal to all vectors from  $\mathcal{V}$ , then being  $Q$ -orthogonal to  $\mathbf{f}_1$  and  $\mathbf{f}_2$ , it lies in  $\text{Ker } Q$ , which is trivial. This shows that the restriction of the bilinear form  $Q$  to  $\mathcal{V}$  is non-degenerate. We can continue our construction inductively, i.e. find  $\mathbf{f}_3, \mathbf{f}_4 \in \mathcal{V}$  such that  $Q(\mathbf{f}_3, \mathbf{f}_4) = 1$ , take their  $Q$ -orthogonal complement in  $\mathcal{V}$ , and so on. At the end we obtain a basis  $\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_{2k-1}, \mathbf{f}_{2k}$  such that  $Q(\mathbf{f}_{2i-1}, \mathbf{f}_{2i}) = 1 = Q(\mathbf{f}_{2i}, \mathbf{f}_{2i-1})$  for  $i = 1, \dots, k$ , and  $Q(\mathbf{f}_i, \mathbf{f}_j) = 0$  for all other pairs of indices. In the coordinate system corresponding to this basis, the form  $Q$  is given by (i).  $\square$

Whenever  $Q$  is given by the formula (i), let us call the basis a **Darboux basis**<sup>8</sup> of  $Q$ .

Consider now the case of *odd non-degenerate* forms. Let  $\mathcal{W} \subset \mathbb{Z}_2^n$  denote the subspace given by one linear equation  $Q(\mathbf{x}) = 0$ . It has dimension  $n - 1$ . The restriction to it of the bilinear form  $Q$  is even, but possibly degenerate. Consider vectors  $\mathbf{y}$   $Q$ -orthogonal to all vectors from  $\mathcal{W}$ . They are given by the system of  $n - 1$  linear equations:  $Q(\mathbf{w}_1, \mathbf{y}) = \dots = Q(\mathbf{w}_{n-1}, \mathbf{y}) = 0$ , where  $\mathbf{w}_1, \dots, \mathbf{w}_{n-1}$  is any basis of  $\mathcal{W}$ . Since  $Q$  is non-degenerate, and  $\mathbf{w}_i$  are linearly independent, these linear equations are also independent, and hence the solution space has *dimension* 1. Let  $\mathbf{f}_0$  be the non-zero solution vector, i.e.  $\mathbf{f}_0 \neq \mathbf{0}$ , and  $Q(\mathbf{f}_0, \mathbf{x}) = 0$  for all  $\mathbf{x} \in \mathcal{W}$ . There are two cases:  $\mathbf{f}_0 \in \mathcal{W}$  (Figure 39) and  $\mathbf{f}_0 \notin \mathcal{W}$  (Figure 40).

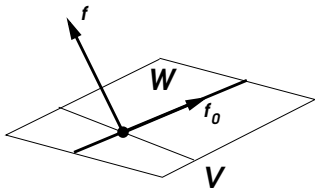


Figure 39

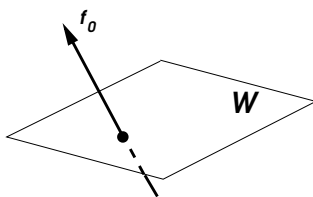


Figure 40

In the first case,  $\mathbf{f}_0$  spans the kernel of the form  $Q$  restricted to  $\mathcal{W}$ . We pick  $\mathbf{f}$  such that  $Q(\mathbf{f}, \mathbf{f}_0) = 1$ . Such  $\mathbf{f}$  exists (since  $Q$  is non-degenerate), but  $\mathbf{f} \notin \mathcal{W}$ , i.e.  $Q(\mathbf{f}) = 1$ . Let  $\mathcal{V}$  consist of all vectors of  $\mathcal{W}$  which are  $Q$ -orthogonal to  $\mathbf{f}$ . It is a subspace of codimension 1 in  $\mathcal{W}$ , which does not contain  $\mathbf{f}_0$ . Therefore the restriction of  $Q$  to  $\mathcal{V}$  is non-degenerate (and even). Let  $\{\mathbf{f}_1, \dots, \mathbf{f}_{2k}\}$  (with  $2k = n - 2$ ) be a Darboux basis in  $\mathcal{V}$ . Then  $\mathbf{f}, \mathbf{f}_0, \mathbf{f}_1, \dots, \mathbf{f}_{2k}$  form a basis in  $\mathbb{Z}_2^n$  such that in the corresponding coordinate system:

$$Q = xy + xy_0 + x_0y + \sum_{i=1}^k (x_{2i-1}y_{2i} + x_{2i}y_{2i-1}). \tag{ii}$$

In the second case,  $Q(\mathbf{f}_0, \mathbf{f}_0) = 1$ , so that the restriction of  $Q$  to  $\mathcal{W}$  is non-degenerate (and even). Let  $\{\mathbf{f}_1, \dots, \mathbf{f}_{2k}\}$  (with  $2k = n - 1$ ) be a Darboux basis in  $\mathcal{W}$ . Then  $\mathbf{f}_0, \mathbf{f}_1, \dots, \mathbf{f}_{2k}$  form a basis in  $\mathbb{Z}_2^n$  such that in the corresponding coordinate system:

$$Q = x_0y_0 + \sum_{i=1}^k (x_{2i-1}y_{2i} + x_{2i}y_{2i-1}). \tag{iii}$$

---

<sup>8</sup>After a French mathematician Jean-Gaston **Darboux** (1842–1917).

Corollary. *A non-degenerate symmetric bilinear form in  $\mathbb{Z}^n$  is equivalent to (iii) when  $n$  is odd, and to one of the forms (i) or (ii) when  $n$  is even.*

### The Case of $\mathbb{K} = \mathbb{Q}$

All previous problems of this section belong to Linear Algebra, which is Geometry, and hence are relatively easy. Classification of *rational* quadratic forms belongs to Arithmetic and is therefore much harder. Here we can only hope to whet reader's appetite for the theory which is one of the pinnacles of classical Number Theory, and refer to [5] for a serious introduction.

Of course, every non-degenerate quadratic form  $Q$  on  $\mathbb{Q}^n$  has a  $Q$ -orthogonal basis and hence can be written as

$$Q = a_1x_1^2 + \cdots + a_nx_n^2,$$

where  $a_1, \dots, a_n$  are non-zero rational numbers. Furthermore, by rescaling  $x_i$  we can make each  $a_i$  integer and *square free* (i.e. expressed as a signed product  $\pm p_1 \dots p_k$  of *distinct* primes). The problem is that such quadratic forms with different sets of coefficients can sometimes be transformed into each other by transformations mixing up the variables, and it is not obvious how to determine if this is the case. A necessary condition is that the inertia indices of equivalent rational forms must be the same, since such forms are equivalent over  $\mathbb{R}$ . However, there are many other requirements.

To describe them, let us start with writing integers and fractions using the *binary number system*, e.g.:

$$2009_{(10)} = 11111011001_{(2)}, \quad -\frac{1}{3} = -.010101\dots_{(2)}.$$

We usually learn in school that every rational (and even real) number can be represented by binary sequences, which are either finite or *infinite to the right*. What we usually don't learn in school is that rational numbers can also be represented by binary sequences *infinite to the left*. For instance,

$$-\frac{1}{3} = \frac{1}{1-2^2} = 1 + 2^2 + 2^4 + 2^6 + \cdots_{(10)} = \dots 1010101_{(2)}$$

For this, one should postulate that powers  $2^k$  of the base become smaller (!) as  $k$  increases, and moreover:  $\lim 2^k = 0$  as  $k \rightarrow +\infty$ .

Just as the *standard algorithms* for the addition and multiplication of finite binary fractions can be extended to binary fractions infinite to the right, they can be extended to such fractions infinite to the left. While the former possibility leads to completing the field  $\mathbb{Q}$  into  $\mathbb{R}$ , the latter one gives rise to another completion, denoted  $\mathbb{Q}_{(2)}$ . In fact the same construction can be repeated with any *prime base*  $p$  each time leading to a different completion,  $\mathbb{Q}_{(p)}$ , called the **field of  $p$ -adic numbers**.

If two quadratic forms with rational coefficients are equivalent over  $\mathbb{Q}$  they must be equivalent not only over  $\mathbb{R}$  (denoted in this context by  $\mathbb{Q}_{(\infty)}$ ), but also over  $\mathbb{Q}_{(p)}$  for each  $p = 2, 3, 5, 7, 11, \dots$

Classification of quadratic forms over each  $\mathbb{Q}_{(p)}$  is relatively tame. For instance, it can be shown that over  $\mathbb{Q}_{(2)}$ , there are 16 (respectively 15 and 8) equivalence classes of quadratic forms of rank  $r$  when  $r > 2$  (respectively  $r = 2$  and  $r = 1$ ). However, the classification of quadratic forms over  $\mathbb{Q}$  is most concisely described by the following celebrated theorem.<sup>9</sup>

**Theorem.** *Two quadratic forms with rational coefficients are equivalent over  $\mathbb{Q}$  if and only if they are equivalent over each  $\mathbb{Q}_{(p)}$ ,  $p = 2, 3, 5, 7, \dots, \infty$ .*

These infinitely many equivalence conditions are not independent. Remarkably, *if all but any one of them are satisfied, then the last one is satisfied too*. It follows, for example, that if two rational quadratic forms are equivalent over every  $p$ -adic field, then they are equivalent over  $\mathbb{R}$ .

### EXERCISES

**211.** Find orthogonal bases and inertia indices of quadratic forms: ✓

$$x_1x_2 + x_2^2, \quad x_1^2 + 4x_1x_2 + 6x_2^2 - 12x_2x_3 + 18x_3^2, \quad x_1x_2 + x_2x_3 + x_3x_1.$$

**212.** Prove that  $Q = \sum_{1 \leq i < j \leq n} x_i x_j$  is positive definite.

**213.** A minor of a square matrix formed by rows and columns with the same indices is called **principal**. Prove that all principal minors of the coefficient matrix of a positive definite quadratic form are positive.

**214.\*** Let  $\mathbf{a}_1, \dots, \mathbf{a}_p$  and  $\mathbf{b}_1, \dots, \mathbf{b}_q$  be linear forms in  $\mathbb{R}^n$ , and let  $Q(\mathbf{x}) = \mathbf{a}_1^2(\mathbf{x}) + \dots + \mathbf{a}_p^2(\mathbf{x}) - \mathbf{b}_1^2(\mathbf{x}) - \dots - \mathbf{b}_q^2(\mathbf{x})$ . Prove that the positive and negative inertia indices of  $Q$  do not exceed  $p$  and  $q$  respectively. ♯

---

<sup>9</sup>This is essentially a special case of the **Minkowski–Hasse theorem** named after Hermann **Minkowski** (1864–1909) and Helmut **Hasse** (1898–1979).

**215.** Find the place of surfaces  $x_1x_2 + x_2x_3 = \pm 1$  and  $x_1x_2 + x_2x_3 + x_3x_1 = \pm 1$  in the classification of conics in  $\mathbb{R}^3$ .

**216.** Examine normal forms of hyperboloids in  $\mathbb{R}^4$  and find out how many connected components (“sheets”) each of them has.  $\checkmark$

**217.** Find explicitly a  $\mathbb{C}$ -linear transformation that identifies the sets of complex solutions to the equations  $xy = 1$  and  $x^2 + y^2 = 1$ .

**218.** Find the rank of the quadratic form  $z_1^2 + 2iz_1z_2 - z_2^2$ .

**219.** Define the **kernel** of an *anti*-symmetric bilinear form  $A$  on a vector space  $\mathcal{V}$  as the subspace  $\text{Ker } A := \{\mathbf{z} \in \mathcal{V} \mid A(\mathbf{z}, \mathbf{x}) = 0 \text{ for all } \mathbf{x} \in \mathcal{V}\}$ , and prove that the form descends to the quotient space  $\mathcal{V}/\text{Ker } A$ .

**220.** Classify conics in  $\mathbb{C}^2$  up to linear inhomogeneous transformations.  $\checkmark$

**221.** Find the place of the complex conic  $z_1^2 - 2iz_1z_2 - z_2^2 = iz_1 + z_2$  in the classification of conics in  $\mathbb{C}^2$ .  $\checkmark$

**222.** Classify all conics in  $\mathbb{C}^3$  up to linear inhomogeneous transformations.

**223.** Prove that there are  $3n - 1$  equivalence classes of conics in  $\mathbb{C}^n$ .

**224.** Check that  $P^* = P^t$  if and only if  $A$  is real.

**225.** Show that diagonal entries of an Hermitian matrix are real, and of anti-Hermitian imaginary.

**226.** Find all complex matrices which are symmetric and anti-Hermitian simultaneously.  $\checkmark$

**227.\*** Prove that a sesquilinear form  $P$  of  $\mathbf{z}, \mathbf{w} \in \mathbb{C}^n$  can be expressed in terms of its values at  $\mathbf{z} = \mathbf{w}$ , and find such an expression.  $\checkmark$

**228.** Define sesquilinear forms  $P : \mathbb{C}^m \times \mathbb{C}^n \rightarrow \mathbb{C}$  of pairs of vectors  $(\mathbf{z}, \mathbf{w})$  taken from two different spaces, and prove that  $P(\mathbf{z}, \mathbf{w}) = \langle \mathbf{z}, P\mathbf{w} \rangle$ , where  $P$  is the  $m \times n$ -matrix of coefficients of the form, and  $\langle \cdot, \cdot \rangle$  is the Hermitian dot product in  $\mathbb{C}^m$ .  $\checkmark$

**229.** Prove that under changes of variables  $\mathbf{v} = D\mathbf{v}'$ ,  $\mathbf{w} = C\mathbf{w}'$  the coefficient matrices of sesquilinear forms are transformed as  $P \mapsto D^*PC$ .

**230.** Prove that  $\langle A\mathbf{z}, \mathbf{w} \rangle = \langle \mathbf{z}, B\mathbf{w} \rangle$  for all  $\mathbf{z} \in \mathbb{C}^m$ ,  $\mathbf{w} \in \mathbb{C}^n$  if and only if  $A = B^*$ . Here  $\langle \cdot, \cdot \rangle$  denote *Hermitian* dot products in  $\mathbb{C}^n$  or  $\mathbb{C}^m$ .  $\checkmark$

**231.** Prove that  $(AB)^* = B^*A^*$ .  $\checkmark$

**232.** Prove that for (anti-)Hermitian matrices  $A$  and  $B$ , the **commutator** matrix  $AB - BA$  is (anti-)Hermitian.

**233.** Find out which of the following forms are Hermitian or anti-Hermitian and transform them to the appropriate normal forms:  $\checkmark$

$$\bar{z}_1z_2 - \bar{z}_2z_1, \quad \bar{z}_1z_2 + \bar{z}_2z_1, \quad \bar{z}_1z_1 + i\bar{z}_2z_1 - i\bar{z}_1z_2 - \bar{z}_2z_2.$$

**234.** Prove that for every symmetric matrix  $Q$  all of whose leading minors are non-zero there exists a *unipotent* upper triangular matrix  $C$  such that



$D = C^tQC$  is diagonal, and express the diagonal entries of  $D$  in terms of the leading minors. ✓

**235.** Use Sylvester's rule to find inertia indices of quadratic forms: ✓

$$x_1^2 + 2x_1x_2 + 2x_2x_3 + 2x_1x_4, \quad x_1x_2 - x_2^2 + x_3^2 + 2x_2x_4 + x_4^2.$$

**236.** Compute determinants and inertia indices of quadratic forms:

$$x_1^2 - x_1x_2 + x_2^2, \quad x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3.$$

**237.** Prove positivity of the quadratic form  $\sum_{i=1}^n x_i^2 - \sum_{1 \leq i < j \leq n} x_i x_j$ .

**238.\*** Prove that when the square of a linear form is added to a positive quadratic form, the determinant of the coefficient matrix increases. ♣

**239.** In  $\mathbb{Z}_{11}$ , compute multiplicative inverses of all non-zero elements, find all non-square elements, and find out if any of the quadratic forms  $x_1x_2$ ,  $x_1^2 + x_1x_2 + 3x_2^2$ ,  $2x_1^2 + x_1x_2 - 2x_2^2$  are equivalent to each other in  $\mathbb{Z}_{11}^2$ .

**240.** Prove that when  $p$  is a prime of the form  $4k - 1$ , then every non-degenerate quadratic form in  $\mathbb{Z}_p^n$  is equivalent to one of the two normal forms  $\pm x_1^2 + x_2^2 + \dots + x_n^2$ . ♣

**241.** Prove that in a suitable coordinate system  $(u, v, w)$  in the space  $\mathbb{Z}_p^3$  of symmetric  $2 \times 2$ -matrices  $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$  over  $\mathbb{Z}_p$ , the determinant  $ac - b^2$  takes on the form  $u^2 + v^2 + w^2$ .

**242.** For  $\mathbf{x} \in \mathbb{Z}_2^n$ , show that  $\sum a_i x_i^2 = \sum a_i x_i$ .

**243.** Show that on  $\mathbb{Z}_2^2$ , there are 4 non-degenerate symmetric bilinear forms, and find how they are divided into 2 equivalence classes. ♣

**244.** Let  $Q$  be a quadratic form in  $n$  variables  $x_1, \dots, x_n$  over  $\mathbb{Z}_2$ , i.e. a sum of monomials  $x_i x_j$ . Associate to it a function of  $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^n$  given by the formula:  $B_Q(\mathbf{x}, \mathbf{y}) = Q(\mathbf{x} + \mathbf{y}) + Q(\mathbf{x}) + Q(\mathbf{y})$ . Prove that  $B_Q$  is an even bilinear form.

**245.\*** Let  $\mathcal{Q}$  and  $\mathcal{B}$  denote vector  $\mathbb{Z}_2$ -spaces of quadratic and symmetric bilinear forms on  $\mathbb{Z}_2^n$  respectively. Denote by  $p : \mathcal{Q} \rightarrow \mathcal{B}$  the linear map  $Q \mapsto B_Q$ , and by  $q : \mathcal{B} \rightarrow \mathcal{Q}$  the linear map that associates to a symmetric bilinear form  $B$  the quadratic form  $Q(\mathbf{x}) = B(\mathbf{x}, \mathbf{x})$ . Prove that the range of  $p$  consists of all even forms and thus coincides with the kernel of  $q$ , and that the range of  $q$  in its turn coincides with the kernel of  $p$ , i.e. consists of all "diagonal" quadratic forms  $Q = \sum a_i x_i^2$ .

**246.** Show that in  $\mathbb{Q}_{(2)}$ , the field of 2-adic numbers,  $-1 = \dots 11111$ .

**247.\*** Compute the (unsigned!) binary representation of  $1/3$  in  $\mathbb{Q}_{(2)}$ . ♣

**248.\*** Prove that every non-zero 2-adic number is invertible in  $\mathbb{Q}_{(2)}$ . ♣

**249.\*** Prove that a 2-adic unit  $\dots *** 1$ . (where  $*$  is a wild card) is a square in  $\mathbb{Q}_{(2)}$  if and only if it has the form  $\dots *** 001$ .

**250.\*** Prove that over the field  $\mathbb{Q}_{(2)}$ , there are 8 equivalence classes of quadratic forms in one variable. ♣

**251.\*** Let  $\mathbb{K}$ ,  $\mathbb{K}^\times$ ,  $(\mathbb{K}^\times)^2$  and  $\mathcal{V} := \mathbb{K}^\times/(\mathbb{K}^\times)^2$  stand for: any field, the set of non-zero elements in it, complete squares in  $\mathbb{K}^\times$ , and equivalence classes of all non-zero elements modulo complete squares. Show that  $\mathcal{V}$ , equipped with the operation, induced by multiplication in  $\mathbb{K}^\times$ , is a  $\mathbb{Z}_2$ -vector space. Show that when  $\mathbb{K} = \mathbb{C}, \mathbb{R}$ , or  $\mathbb{Q}_{(2)}$ ,  $\dim \mathcal{V} = 0, 1$  and  $3$  respectively.

**252.** Let  $Q$  and  $Q'$  be quadratic forms in  $n$  variables with *integer* coefficients. Prove that if these forms can be transformed into each other by linear changes of variables with coefficients in  $\mathbb{Z}$ , then  $\det Q = \det Q'$ . (Thus,  $\det Q$ , which is called the **discriminant** of  $Q$ , depends only on the equivalence class of  $Q$ .)

# Chapter 4

## Eigenvalues

### 1 The Spectral Theorem

#### Hermitian Spaces

Given a  $\mathbb{C}$ -vector space  $\mathcal{V}$ , an **Hermitian inner product** in  $\mathcal{V}$  is defined as a Hermitian symmetric sesquilinear form such that the corresponding Hermitian quadratic form is positive definite. A space  $\mathcal{V}$  equipped with an Hermitian inner product  $\langle \cdot, \cdot \rangle$  is called a **Hermitian space**.<sup>1</sup>

The inner square  $\langle \mathbf{z}, \mathbf{z} \rangle$  is interpreted as the square of the **length**  $|\mathbf{z}|$  of the vector  $\mathbf{z}$ . Respectively, the **distance** between two points  $\mathbf{z}$  and  $\mathbf{w}$  in an Hermitian space is defined as  $|\mathbf{z} - \mathbf{w}|$ . Since the Hermitian inner product is positive, distance is well-defined, symmetric, and positive (unless  $\mathbf{z} = \mathbf{w}$ ). In fact it satisfies the **triangle inequality**<sup>2</sup>:

$$|\mathbf{z} - \mathbf{w}| \leq |\mathbf{z}| + |\mathbf{w}|.$$

This follows from the **Cauchy – Schwarz inequality**:

$$|\langle \mathbf{z}, \mathbf{w} \rangle|^2 \leq \langle \mathbf{z}, \mathbf{z} \rangle \langle \mathbf{w}, \mathbf{w} \rangle,$$

where the equality holds if and only if  $\mathbf{z}$  and  $\mathbf{w}$  are linearly dependent. To derive the triangle inequality, write:

$$\begin{aligned} |\mathbf{z} - \mathbf{w}|^2 &= \langle \mathbf{z} - \mathbf{w}, \mathbf{z} - \mathbf{w} \rangle = \langle \mathbf{z}, \mathbf{z} \rangle - \langle \mathbf{z}, \mathbf{w} \rangle - \langle \mathbf{w}, \mathbf{z} \rangle + \langle \mathbf{w}, \mathbf{w} \rangle \\ &\leq |\mathbf{z}|^2 + 2|\mathbf{z}||\mathbf{w}| + |\mathbf{w}|^2 = (|\mathbf{z}| + |\mathbf{w}|)^2. \end{aligned}$$

---

<sup>1</sup>Other terms used are **unitary space** and finite dimensional **Hilbert space**.

<sup>2</sup>This makes a Hermitian space a **metric space**.

To prove the Cauchy–Schwarz inequality, note that it suffices to consider the case  $|\mathbf{w}| = 1$ . Indeed, when  $\mathbf{z} = \mathbf{0}$ , both sides vanish, and when  $\mathbf{w} \neq \mathbf{0}$ , both sides scale the same way when  $\mathbf{w}$  is normalized to the unit length. So, assuming  $|\mathbf{w}| = 1$ , we put  $\lambda := \langle \mathbf{w}, \mathbf{z} \rangle$  and consider the **projection**  $\lambda \mathbf{w}$  of the vector  $\mathbf{z}$  to the line spanned by  $\mathbf{w}$ . The difference  $\mathbf{z} - \lambda \mathbf{w}$  is **orthogonal** to  $\mathbf{w}$ :  $\langle \mathbf{w}, \mathbf{z} - \lambda \mathbf{w} \rangle = \langle \mathbf{w}, \mathbf{z} \rangle - \lambda \langle \mathbf{w}, \mathbf{w} \rangle = 0$ . From positivity of inner squares, we have:

$$0 \leq \langle \mathbf{z} - \lambda \mathbf{w}, \mathbf{z} - \lambda \mathbf{w} \rangle = \langle \mathbf{z}, \mathbf{z} - \lambda \mathbf{w} \rangle = \langle \mathbf{z}, \mathbf{z} \rangle - \lambda \langle \mathbf{z}, \mathbf{w} \rangle.$$

Since  $\langle \mathbf{z}, \mathbf{w} \rangle = \overline{\langle \mathbf{w}, \mathbf{z} \rangle} = \bar{\lambda}$ , we conclude that  $|\mathbf{z}|^2 \geq |\langle \mathbf{z}, \mathbf{w} \rangle|^2$  as required. Notice that the equality holds true only when  $\mathbf{z} = \lambda \mathbf{w}$ .

**All Hermitian spaces of the same dimension are isometric** (or **Hermitian isomorphic**), i.e. isomorphic through isomorphisms respecting Hermitian inner products. Namely, as it follows from the Inertia Theorem for Hermitian forms, every Hermitian space has an **orthonormal basis**, i.e. a basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  such that  $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$  for  $i \neq j$  and  $= 1$  for  $i = j$ . In the coordinate system corresponding to an orthonormal basis, the Hermitian inner product takes on the standard form:

$$\langle \mathbf{z}, \mathbf{w} \rangle = \bar{z}_1 w_1 + \dots + \bar{z}_n w_n.$$

An orthonormal basis is not unique. Moreover, as it follows from the proof of Sylvester’s rule, one can start with any basis  $\mathbf{f}_1, \dots, \mathbf{f}_n$  in  $\mathcal{V}$  and then construct an orthonormal basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  such that  $\mathbf{e}_k \in \text{Span}(\mathbf{f}_1, \dots, \mathbf{f}_k)$ . This is done inductively; namely, when  $\mathbf{e}_1, \dots, \mathbf{e}_{k-1}$  have already been constructed, one subtracts from  $\mathbf{f}_k$  its projection to the space  $\text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_{k-1})$ :

$$\tilde{\mathbf{f}}_k = \mathbf{f}_k - \langle \mathbf{e}_1, \mathbf{f}_k \rangle \mathbf{e}_1 - \dots - \langle \mathbf{e}_{k-1}, \mathbf{f}_k \rangle \mathbf{e}_{k-1}.$$

The resulting vector  $\tilde{\mathbf{f}}_k$  lies in  $\text{Span}(\mathbf{f}_1, \dots, \mathbf{f}_{k-1}, \mathbf{f}_k)$  and is orthogonal to  $\text{Span}(\mathbf{f}_1, \dots, \mathbf{f}_{k-1}) = \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_{k-1})$ . Indeed,

$$\langle \mathbf{e}_i, \tilde{\mathbf{f}}_k \rangle = \langle \mathbf{e}_i, \mathbf{f}_k \rangle - \sum_{j=1}^{k-1} \langle \mathbf{e}_j, \mathbf{f}_k \rangle \langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0.$$

for all  $i = 1, \dots, k-1$ . To construct  $\mathbf{e}_k$ , one normalizes  $\tilde{\mathbf{f}}_k$  to the unit length:

$$\mathbf{e}_k := \langle \tilde{\mathbf{f}}_k, \tilde{\mathbf{f}}_k \rangle^{-1/2} \tilde{\mathbf{f}}_k.$$

The above algorithm of replacing a given basis with an orthonormal one is known as **Gram–Schmidt orthogonalization**.

## Normal Operators

Let  $A : \mathcal{V} \rightarrow \mathcal{W}$  be a linear map between two Hermitian spaces. Its **Hermitian adjoint** (or simply **adjoint**) is defined as the linear map  $A^* : \mathcal{W} \rightarrow \mathcal{V}$  characterized by the property

$$\langle A^* \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{w}, A\mathbf{v} \rangle \quad \text{for all } \mathbf{v} \in \mathcal{V}, \mathbf{w} \in \mathcal{W}.$$

One way to look at this construction is to realize that an Hermitian inner product on a vector space  $\mathcal{U}$  allows one to assign to each vector  $\mathbf{z} \in \mathcal{U}$  a  $\mathbb{C}$ -linear function  $\langle \mathbf{z}, \cdot \rangle$  (i.e. the function  $\mathcal{U} \rightarrow \mathbb{C}$  whose value at  $\mathbf{w} \in \mathcal{U}$  is equal to  $\langle \mathbf{z}, \mathbf{w} \rangle$ ). Moreover, since the inner product is non-degenerate, each  $\mathbb{C}$ -linear function on  $\mathcal{U}$  is represented this way by a unique vector. Thus, given  $\mathbf{w} \in \mathcal{W}$ , one introduces a  $\mathbb{C}$ -linear function on  $\mathcal{V}$ :  $\mathbf{v} \mapsto \langle \mathbf{w}, A\mathbf{v} \rangle$ , and defines  $A^* \mathbf{w}$  to be the unique vector in  $\mathcal{V}$  that represents this linear function.

Examining the defining identity of the adjoint map in coordinate systems in  $\mathcal{V}$  and  $\mathcal{W}$  corresponding to orthonormal bases, we conclude that the matrix of  $A^*$  in such bases is the Hermitian adjoint to  $A$ , i.e.  $A^* = \bar{A}^t$ . Indeed, in matrix product notation,

$$\langle \mathbf{w}, A\mathbf{v} \rangle = \mathbf{w}^* A\mathbf{v} = (A^* \mathbf{w})^* \mathbf{v} = \langle A^* \mathbf{w}, \mathbf{v} \rangle.$$

Note that  $(A^*)^* = A$ , and that  $\langle A\mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{v}, A^* \mathbf{w} \rangle$  for all  $\mathbf{v} \in \mathcal{V}$  and  $\mathbf{w} \in \mathcal{W}$ .

Consider now linear maps  $A : \mathcal{V} \rightarrow \mathcal{V}$  from an Hermitian space to itself. To such a map, one can associate a sesquilinear form:  $A(\mathbf{z}, \mathbf{w}) := \langle \mathbf{z}, A\mathbf{w} \rangle$ . *Vice versa*, every sesquilinear form corresponds this way to a unique linear transformation. (It is especially obvious when the inner product is written in the standard form  $\langle \mathbf{z}, \mathbf{w} \rangle = \mathbf{z}^* \mathbf{w}$  using an orthonormal basis.) In particular, one can define Hermitian ( $A^* = A$ ) and anti-Hermitian ( $A^* = -A$ ) linear maps which correspond to Hermitian and anti-Hermitian forms respectively.

A linear map  $A : \mathcal{V} \rightarrow \mathcal{V}$  on a Hermitian vector space is called **normal**<sup>3</sup> if it commutes with its Hermitian adjoint:  $A^*A = AA^*$ .

**Examples 1.** Hermitian and anti-Hermitian transformations are normal.

**Example 2.** An invertible linear transformation  $U : \mathcal{V} \rightarrow \mathcal{V}$  is called **unitary** if it preserves inner products:

$$\langle U\mathbf{z}, U\mathbf{w} \rangle = \langle \mathbf{z}, \mathbf{w} \rangle \quad \text{for all } \mathbf{z}, \mathbf{w} \in \mathcal{V}.$$

---

<sup>3</sup>The term **normal operator** is frequently in use.

Equivalently,  $\langle \mathbf{z}, (U^*U - I)\mathbf{w} \rangle = 0$  for all  $\mathbf{z}, \mathbf{w} \in \mathcal{V}$ . Taking  $\mathbf{z} = (U^*U - I)\mathbf{w}$ , we conclude that  $(U^*U - I)\mathbf{w} = \mathbf{0}$  for all  $\mathbf{w} \in \mathcal{V}$ , and hence  $U^*U = I$ . Thus, for a unitary map  $U$ ,  $U^{-1} = U^*$ . The converse statement is also true (and easy to check by starting from  $U^{-1} = U^*$  and reversing our computation). Since every invertible transformation commutes with its own inverse, we conclude that *unitary transformations are normal*.

**Example 3.** Every linear transformation  $A : \mathcal{V} \rightarrow \mathcal{V}$  can be uniquely written as the sum  $A = B + C$  of Hermitian ( $B = (A + A^*)/2$ ) and ant-Hermitian ( $C = (A - A^*)/2$ ) operators. We claim that *an operator is normal if and only if its Hermitian and anti-Hermitian parts commute*. Indeed,  $A^* = B - C$ ,  $AA^* = B^2 - BC + CB - C^2$ ,  $A^*A = B^2 + BC - CB - C^2$ , and hence  $AA^* = A^*A$  if and only if  $BC = CB$ .

## The Spectral Theorem for Normal Operators

Let  $A : \mathcal{V} \rightarrow \mathcal{V}$  be a linear transformation,  $\mathbf{v} \in \mathcal{V}$  a vector, and  $\lambda \in \mathbb{C}$  a scalar. The vector  $\mathbf{v}$  is called an **eigenvector** of  $A$  with the **eigenvalue**  $\lambda$ , if  $\mathbf{v} \neq \mathbf{0}$ , and  $A\mathbf{v} = \lambda\mathbf{v}$ . In other words,  $A$  preserves the line spanned by the vector  $\mathcal{V}$  and acts on this line as the multiplication by  $\lambda$ .

**Theorem.** *A linear transformation  $A : \mathcal{V} \rightarrow \mathcal{V}$  on a finite dimensional Hermitian vector space is normal if and only if  $\mathcal{V}$  has an orthonormal basis of eigenvectors of  $A$ .*

**Proof.** In one direction, the statement is almost obvious: If a basis consists of eigenvectors of  $A$ , then the matrix of  $A$  in this basis is diagonal. When the basis is orthonormal, the matrix of the adjoint operator  $A^*$  in this basis is adjoint to the matrix of  $A$  and is also diagonal. Since all diagonal matrices commute, we conclude that  $A$  is normal. Thus, it remains to prove that, conversely, every normal operator has an orthonormal basis of eigenvectors. We will prove this in four steps.

**Step 1. Existence of eigenvalues.** We need to show that there exists a scalar  $\lambda \in \mathbb{C}$  such that the system of linear equations  $A\mathbf{x} = \lambda\mathbf{x}$  has a non-trivial solution. Equivalently, this means that the linear transformation  $\lambda I - A$  has a non-trivial kernel. Since  $\mathcal{V}$  is finite dimensional, this can be re-stated in terms of the determinant of the matrix of  $A$  (in any basis) as

$$\det(\lambda I - A) = 0.$$

This relation, understood as an equation for  $\lambda$ , is called the **characteristic equation** of the operator  $A$ . When  $A = 0$ , it becomes  $\lambda^n = 0$ , where  $n = \dim \mathcal{V}$ . In general, it is a degree- $n$  polynomial equation

$$\lambda^n + p_1\lambda^{n-1} + \cdots + p_{n-1}\lambda + p_n = 0,$$

where the coefficients  $p_1, \dots, p_n$  are certain algebraic expressions of matrix entries of  $A$  (and hence are complex numbers). According to the Fundamental Theorem of Algebra, this equation has a complex solution, say  $\lambda_0$ . Then  $\det(\lambda_0 I - A) = 0$ , and hence the system  $(\lambda_0 - A)\mathbf{x} = \mathbf{0}$  has a non-trivial solution,  $\mathbf{v} \neq \mathbf{0}$ , which is therefore an eigenvector of  $A$  with the eigenvalue  $\lambda_0$ .

**Remark.** Solutions to the system  $A\mathbf{x} = \lambda_0\mathbf{x}$  form a linear subspace  $\mathcal{W}$  in  $\mathcal{V}$ , namely the kernel of  $\lambda_0 I - A$ , and eigenvectors of  $A$  with the eigenvalue  $\lambda_0$  are exactly all non-zero vectors in  $\mathcal{W}$ . Slightly abusing terminology,  $\mathcal{W}$  is called the **eigenspace** of  $A$  corresponding to the eigenvalue  $\lambda_0$ . Obviously,  $A(\mathcal{W}) \subset \mathcal{W}$ . Subspaces with such property are called  **$A$ -invariant**. Thus eigenspaces of a linear transformation  $A$  are  $A$ -invariant.

**Step 2.**  *$A^*$ -invariance of eigenspaces of  $A$ .* Let  $\mathcal{W} \neq \{\mathbf{0}\}$  be the eigenspace of a normal operator  $A$  corresponding to the eigenvalue  $\lambda$ . Then for every  $\mathbf{w} \in \mathcal{W}$ ,

$$A(A^*\mathbf{w}) = A^*(A\mathbf{w}) = A^*(\lambda\mathbf{w}) = \lambda(A^*\mathbf{w}).$$

Therefore  $A^*\mathbf{w} \in \mathcal{W}$ , i.e. the eigenspace  $\mathcal{W}$  is  $A^*$ -invariant.

**Step 3.** *Invariance of orthogonal complements.* Let  $\mathcal{W} \subset \mathcal{V}$  be a linear subspace. Denote by  $\mathcal{W}^\perp$  the **orthogonal complement** of the subspace  $\mathcal{W}$  with respect to the Hermitian inner product:

$$\mathcal{W}^\perp := \{\mathbf{v} \in \mathcal{V} \mid \langle \mathbf{w}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{w} \in \mathcal{W}\}.$$

Note that if  $\mathbf{e}_1, \dots, \mathbf{e}_k$  is a basis in  $\mathcal{W}$ , then  $\mathcal{W}^\perp$  is given by  $k$  linear equations  $\langle \mathbf{e}_i, \mathbf{v} \rangle = 0$ ,  $i = 1, \dots, k$ , and thus has dimension  $\geq n - k$ . On the other hand,  $\mathcal{W} \cap \mathcal{W}^\perp = \{\mathbf{0}\}$ , because no vector  $\mathbf{w} \neq \mathbf{0}$  can be orthogonal to itself:  $\langle \mathbf{w}, \mathbf{w} \rangle > 0$ . It follows from dimension counting formulas that  $\dim \mathcal{W}^\perp = n - k$ . Moreover, this implies that  $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^\perp$ , i.e. the whole space is represented as the direct sum of two orthogonal subspaces.

We claim that *if a subspace is both  $A$ - and  $A^*$ -invariant, then its orthogonal complement is also  $A$ - and  $A^*$ -invariant*. Indeed, suppose that  $A^*(\mathcal{W}) \subset \mathcal{W}$ , and  $\mathbf{v} \in \mathcal{W}^\perp$ . Then for any  $\mathbf{w} \in \mathcal{W}$ , we have:  $\langle \mathbf{w}, A\mathbf{v} \rangle = \langle A^*\mathbf{w}, \mathbf{v} \rangle = 0$ , since  $A^*\mathbf{w} \in \mathcal{W}$ . Therefore  $A\mathbf{v} \in \mathcal{W}^\perp$ , i.e.

$\mathcal{W}^\perp$  is  $A$ -invariant. By the same token, if  $\mathcal{W}$  is  $A$ -invariant, then  $\mathcal{W}^\perp$  is  $A^*$ -invariant.

**Step 4.** *Induction on  $\dim \mathcal{V}$ .* When  $\dim \mathcal{V} = 1$ , the theorem is obvious. Assume that the theorem is proved for normal operators in spaces of dimension  $< n$ , and prove it when  $\dim \mathcal{V} = n$ .

According to Step 1, a normal operator  $A$  has an eigenvalue  $\lambda$ , and let  $\mathcal{W} \neq \{\mathbf{0}\}$  be the corresponding eigenspace. If  $\mathcal{W} = \mathcal{V}$ , then the operator is scalar,  $A = \lambda I$ , and *any* orthonormal basis in  $\mathcal{V}$  will consist of eigenvectors of  $A$ . If  $\mathcal{W} \neq \mathcal{V}$ , then (by Steps 2 and 3) both  $\mathcal{W}$  and  $\mathcal{W}^\perp$  are  $A$ - and  $A^*$ -invariant and have dimensions  $< n$ . The *restrictions* of the operators  $A$  and  $A^*$  to each of these subspaces still satisfy  $AA^* = A^*A$  and  $\langle A^*\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, A\mathbf{y} \rangle$  for all  $\mathbf{x}, \mathbf{y}$ . Therefore these restrictions remain adjoint to each other normal operators on  $\mathcal{W}$  and  $\mathcal{W}^\perp$ . Applying the induction hypothesis, we can find orthonormal bases of eigenvectors of  $A$  in each  $\mathcal{W}$  and  $\mathcal{W}^\perp$ . The union of these bases form an orthonormal basis of eigenvectors of  $A$  in  $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^\perp$ .  $\square$

**Remark.** Note that Step 1 is based on the Fundamental Theorem of Algebra, but does not use normality of  $A$  and applies to any  $\mathbb{C}$ -linear transformation. Furthermore, Step 2 actually applies to any commuting transformations and shows that if  $AB = BA$  then eigenspaces of  $A$  are  $B$ -invariant. The fact that  $B = A^*$  is used in Step 3.

**Corollary 1.** *A normal operator has a diagonal matrix in a suitable orthonormal basis.*

**Corollary 2.** *Let  $A : \mathcal{V} \rightarrow \mathcal{V}$  be a normal operator,  $\lambda_i$  distinct roots of its characteristic polynomial,  $m_i$  their multiplicities, and  $\mathcal{W}_i$  corresponding eigenspaces. Then  $\dim \mathcal{W}_i = m_i$ , and  $\sum \dim \mathcal{W}_i = \dim \mathcal{V}$ .*

Indeed, this is true for transformations defined by any diagonal matrices. For normal operators, in addition  $\mathcal{W}_i \perp \mathcal{W}_j$  when  $i \neq j$ . In particular we have the following corollary.

**Corollary 3.** *Eigenvectors of a normal operator corresponding to different eigenvalues are orthogonal.*

Here is a matrix version of the Spectral Theorem.

**Corollary 4.** *A square complex matrix  $A$  commuting with its adjoint matrix  $A^*$  can be transformed to a diagonal form by transformations  $A \mapsto U^*AU$  defined by unitary matrices  $U$ .*



Note that for unitary matrices,  $U^* = U^{-1}$ , and therefore the above transformations coincide with similarity transformations  $A \mapsto U^{-1}AU$ . This is how the matrix  $A$  of a linear transformation changes under a change of the basis. When both the old and new bases are orthonormal, the transition matrix  $U$  must be unitary (because in old and new coordinates the Hermitian inner product has the same standard form:  $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^* \mathbf{y}$ ). The result follows.

## Unitary Transformations

Note that if  $\lambda$  is an eigenvalue of a unitary operator  $U$  then  $|\lambda| = 1$ . Indeed, if  $\mathbf{x} \neq \mathbf{0}$  is a corresponding eigenvector, then  $\langle \mathbf{x}, \mathbf{x} \rangle = \langle U\mathbf{x}, U\mathbf{x} \rangle = \lambda \bar{\lambda} \langle \mathbf{x}, \mathbf{x} \rangle$ , and since  $\langle \mathbf{x}, \mathbf{x} \rangle \neq 0$ , it implies  $\lambda \bar{\lambda} = 1$ .

**Corollary 5.** *A transformation is unitary if and only if in a suitable orthonormal basis its matrix is diagonal, and the diagonal entries are complex numbers of the absolute value 1.*

On the complex line  $\mathbb{C}$ , multiplication by  $\lambda$  with  $|\lambda| = 1$  and  $\arg \lambda = \theta$  defines the rotation through the angle  $\theta$ . We will call this transformation on the complex line a **unitary rotation**. We arrive therefore to the following geometric characterization of unitary transformations.

**Corollary 6.** *Unitary transformations in an Hermitian space of dimension  $n$  are exactly unitary rotations (through possibly different angles) in  $n$  mutually perpendicular complex directions.*

## Orthogonal Diagonalization

**Corollary 7.** *A linear operator is Hermitian (respectively anti-Hermitian) if and only if in a suitable orthonormal basis its matrix is diagonal with all real (respectively imaginary) diagonal entries.*

Indeed, if  $A\mathbf{x} = \lambda\mathbf{x}$  and  $A^* = \pm A$ , we have:

$$\lambda \langle \mathbf{x}, \mathbf{x} \rangle = \langle \mathbf{x}, A\mathbf{x} \rangle = \langle A^* \mathbf{x}, \mathbf{x} \rangle = \pm \bar{\lambda} \langle \mathbf{x}, \mathbf{x} \rangle.$$

Therefore  $\lambda = \pm \bar{\lambda}$  provided that  $\mathbf{x} \neq \mathbf{0}$ , i.e. eigenvalues of a Hermitian operator are real and of anti-Hermitian imaginary. *Vice versa*, a real diagonal matrix is obviously Hermitian, and imaginary anti-Hermitian.

Recall that (anti-)Hermitian operators correspond to (anti-)Hermitian forms  $A(\mathbf{x}, \mathbf{y}) := \langle \mathbf{x}, A\mathbf{y} \rangle$ . Applying the Spectral Theorem and reordering the basis eigenvectors in the monotonic order of the corresponding eigenvalues, we obtain the following classification results for forms.

**Corollary 8.** *In a Hermitian space of dimension  $n$ , an Hermitian form can be transformed by unitary changes of coordinates to exactly one of the normal forms*

$$\lambda_1|z_1|^2 + \cdots + \lambda_n|z_n|^2, \quad \lambda_1 \geq \cdots \geq \lambda_n.$$

**Corollary 9.** *In a Hermitian space of dimension  $n$ , an anti-Hermitian form can be transformed by unitary changes of coordinates to exactly one of the normal forms*

$$i\omega_1|z_1|^2 + \cdots + i\omega_n|z_n|^2, \quad \omega_1 \geq \cdots \geq \omega_n.$$

Uniqueness follows from the fact that eigenvalues and dimensions of eigenspaces are determined by the operators in a coordinate-less fashion.

**Corollary 10.** *In a complex vector space of dimension  $n$ , a pair of Hermitian forms, of which the first one is positive definite, can be transformed by a choice of a coordinate system to exactly one of the normal forms:*

$$|z_1|^2 + \cdots + |z_n|^2, \quad \lambda_1|z_1|^2 + \cdots + \lambda_n|z_n|^2, \quad \lambda_1 \geq \cdots \geq \lambda_n.$$

This is the **Orthogonal Diagonalization Theorem** for Hermitian forms. It is proved in two stages. First, applying the Inertia Theorem to the positive definite form one transforms it to the standard form; the 2nd Hermitian form changes accordingly but remains arbitrary at this stage. Then, applying Corollary 8 of the Spectral Theorem, one transforms the 2nd Hermitian form to its normal form by transformations preserving the 1st one.

Note that one can take the positive definite sesquilinear form corresponding to the 1st Hermitian form for the Hermitian inner product, and describe the 2nd form as  $\langle \mathbf{z}, A\mathbf{z} \rangle$ , where  $A$  is an operator Hermitian with respect to this inner product. The operator, its eigenvalues, and their multiplicities are thus defined by the given pair of forms in a coordinate-less fashion. This guarantees that pairs with different collections  $\lambda_1 \geq \dots \lambda_n$  of eigenvalues are non-equivalent to each other.

## Singular Value Decomposition

**Theorem.** *Let  $A : \mathcal{V} \rightarrow \mathcal{W}$  be a linear map or rank  $r$  between Hermitian spaces of dimensions  $n$  and  $m$  respectively. Then there exist orthonormal bases:  $\mathbf{v}_1, \dots, \mathbf{v}_n$  of  $\mathcal{V}$  and  $\mathbf{w}_1, \dots, \mathbf{w}_m$  of  $\mathcal{W}$ , and positive reals  $\mu_1 \geq \dots \geq \mu_r$ , such that*

$$A\mathbf{v}_1 = \mu_1\mathbf{w}_1, \dots, A\mathbf{v}_r = \mu_r\mathbf{w}_r, \quad A\mathbf{v}_{r+1} = \dots = A\mathbf{v}_n = \mathbf{0}.$$

**Proof.** For  $\mathbf{x}, \mathbf{y} \in \mathcal{V}$ , put<sup>4</sup>

$$H(\mathbf{x}, \mathbf{y}) := \langle A\mathbf{x}, A\mathbf{y} \rangle = \langle \mathbf{x}, A^*A\mathbf{y} \rangle.$$

This is an Hermitian sesquilinear form on  $\mathcal{V}$  (thus obtained by pulling the Hermitian inner product on  $\mathcal{W}$  back to  $\mathcal{V}$  by means of  $A$ ). It is **non-negative** (i.e.  $H(\mathbf{x}, \mathbf{x}) \geq 0$  for all  $\mathbf{x} \in \mathcal{V}$ ), and corresponds to the Hermitian operator  $H := A^*A$ . The eigenspace of  $H$  corresponding to the eigenvalue 0 coincides with the kernel of  $A$ . Indeed,  $H\mathbf{x} = \mathbf{0}$  implies  $|A\mathbf{x}| = 0$ , i.e.  $A\mathbf{x} = \mathbf{0}$ .

Applying the Spectral Theorem to  $H$ , we obtain an orthonormal basis of  $\mathcal{V}$  consisting of eigenvectors  $\mathbf{v}_1, \dots, \mathbf{v}_r$  of  $H$  with *positive* eigenvalues,  $\lambda_1 \geq \dots \geq \lambda_r > 0$ , and eigenvectors  $\mathbf{v}_{r+1}, \dots, \mathbf{v}_n$  lying in the kernel of  $A$ . For  $i \leq r$ , put  $\mathbf{w}_i = \lambda_i^{-1/2}A\mathbf{v}_i$ . We have:

$$\langle \mathbf{w}_i, \mathbf{w}_j \rangle = \sqrt{\frac{1}{\lambda_i\lambda_j}} \langle A\mathbf{v}_i, A\mathbf{v}_j \rangle = \sqrt{\frac{1}{\lambda_i\lambda_j}} \langle \mathbf{v}_i, A^*A\mathbf{v}_j \rangle = \sqrt{\frac{\lambda_j}{\lambda_i}} \langle \mathbf{v}_i, \mathbf{v}_j \rangle,$$

which is equal to 1 when  $i = j$  and 0 when  $i \neq j$ . Thus  $\mathbf{w}_1, \dots, \mathbf{w}_r$  form an orthonormal basis in the range of  $A$ . Completing it to an orthonormal basis of  $\mathcal{W}$ , we obtain the required result with  $\mu_i = \sqrt{\lambda_i}$ .

**Remark.** When  $A\mathbf{v} = \mu\mathbf{w}$  and  $A^*\mathbf{w} = \mu\mathbf{v}$  for unit vectors  $\mathbf{v}$  and  $\mathbf{w}$ , they are called **right** and **left singular vectors** of  $A$  corresponding to the **singular value**  $\mu$ . The next reformulation provides the **singular value decomposition** of a matrix.

**Corollary.** *For every complex  $m \times n$ -matrix  $A$  of rank  $r$  there exist: unitary matrices  $U$  and  $V$  of sizes  $m$  and  $n$  respectively, and a diagonal  $r \times r$ -matrix  $M$  with positive diagonal entries, such that*

$$A = U^* \begin{bmatrix} M & 0 \\ 0 & 0 \end{bmatrix} V.$$

---

<sup>4</sup>Note that the 1st inner product is in  $\mathcal{W}$  while the 2nd one is in  $\mathcal{V}$ .

## Complexification

Since  $\mathbb{R} \subset \mathbb{C}$ , every complex vector space can be considered as a real vector space simply by “forgetting” that one can multiply by non-real scalars. This operation is called **realification**; applied to a  $\mathbb{C}$ -vector space  $\mathcal{V}$ , it produces an  $\mathbb{R}$ -vector space, denoted  $\mathcal{V}^{\mathbb{R}}$ , of real dimension twice the complex dimension of  $\mathcal{V}$ .

In the reverse direction, to a real vector space  $\mathcal{V}$  one can associate a complex vector space,  $\mathcal{V}^{\mathbb{C}}$ , called the **complexification** of  $\mathcal{V}$ . As a real vector space, it is the direct sum of two copies of  $\mathcal{V}$ :

$$\mathcal{V}^{\mathbb{C}} := \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{V}\}.$$

Thus the addition is performed componentwise, while the multiplication by complex scalars  $\alpha + i\beta$  is introduced with the thought in mind that  $(\mathbf{x}, \mathbf{y})$  stands for  $\mathbf{x} + i\mathbf{y}$ :

$$(\alpha + i\beta)(\mathbf{x}, \mathbf{y}) := (\alpha\mathbf{x} - \beta\mathbf{y}, \beta\mathbf{x} + \alpha\mathbf{y}).$$

This results in a  $\mathbb{C}$ -vector space  $\mathcal{V}^{\mathbb{C}}$  whose complex dimension equals the real dimension of  $\mathcal{V}$ .

**Example.**  $(\mathbb{R}^n)^{\mathbb{C}} = \mathbb{C}^n = \{\mathbf{x} + i\mathbf{y} \mid \mathbf{x}, \mathbf{y} \in \mathbb{R}^n\}$ .

A productive point of view on complexification is that it is a complex vector space with an *additional structure* that “remembers” that the space was constructed from a real one. This additional structure is the operation of **complex conjugation**  $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x}, -\mathbf{y})$ . The operation in itself is a map  $\sigma : \mathcal{V}^{\mathbb{C}} \rightarrow \mathcal{V}^{\mathbb{C}}$ , satisfying  $\sigma^2 = \text{id}$ , which is **anti-linear** over  $\mathbb{C}$ . The latter means that  $\sigma(\lambda\mathbf{z}) = \bar{\lambda}\sigma(\mathbf{z})$  for all  $\lambda \in \mathbb{C}$  and all  $\mathbf{z} \in \mathcal{V}^{\mathbb{C}}$ . In other words,  $\sigma$  is  $\mathbb{R}$ -linear, but anti-commutes with multiplication by  $i$ :  $\sigma(i\mathbf{z}) = -i\sigma(\mathbf{z})$ .

Conversely, let  $\mathcal{W}$  be a complex vector space equipped with an anti-linear operator whose square is the identity<sup>5</sup>:

$$\sigma : \mathcal{W} \rightarrow \mathcal{W}, \quad \sigma^2 = \text{id}, \quad \sigma(\lambda\mathbf{z}) = \bar{\lambda}\sigma(\mathbf{z}) \quad \text{for all } \lambda \in \mathbb{C}, \mathbf{z} \in \mathcal{W}.$$

Let  $\mathcal{V}$  denote the *real* subspace in  $\mathcal{W}$  that consists of all  $\sigma$ -invariant vectors. We claim that  $\mathcal{W}$  is **canonically identified with the complexification of  $\mathcal{V}$** :  $\mathcal{W} = \mathcal{V}^{\mathbb{C}}$ . Indeed, every vector  $\mathbf{z} \in \mathcal{W}$  is uniquely written as the sum of  $\sigma$ -invariant and  $\sigma$ -anti-invariant vectors:

$$\mathbf{z} = \frac{1}{2}(\mathbf{z} + \sigma\mathbf{z}) + \frac{1}{2}(\mathbf{z} - \sigma\mathbf{z}).$$

---

<sup>5</sup>An transformation whose square is the identity is called an **involution**.

Since  $\sigma i = -i\sigma$ , multiplication by  $i$  transforms  $\sigma$ -invariant vectors to  $\sigma$ -anti-invariant ones, and *vice versa*. Thus,  $\mathcal{W}$  as a real space is the direct sum  $\mathcal{V} \oplus (i\mathcal{V}) = \{\mathbf{x} + i\mathbf{y} \mid \mathbf{x}, \mathbf{y} \in \mathcal{V}\}$ , where multiplication by  $i$  acts in the required for the complexification fashion:  $i(\mathbf{x} + i\mathbf{y}) = -\mathbf{y} + i\mathbf{x}$ .

The construction of complexification and its abstract description in terms of the complex conjugation operator  $\sigma$  are the tools that allow one to carry over results about complex vector spaces to real vector spaces. The idea is to consider real objects as complex ones *invariant* under the complex conjugation  $\sigma$ , and apply (or improve) theorems of complex linear algebra in a way that would *respect*  $\sigma$ .

**Example.** A real matrix can be considered as a complex one. This way an  $\mathbb{R}$ -linear map defines a  $\mathbb{C}$ -linear map (on the complexified space). More abstractly, given an  $\mathbb{R}$ -linear map  $A : \mathcal{V} \rightarrow \mathcal{V}$ , one can associate to it a  $\mathbb{C}$ -linear map  $A^{\mathbb{C}} : \mathcal{V}^{\mathbb{C}} \rightarrow \mathcal{V}^{\mathbb{C}}$  by  $A^{\mathbb{C}}(\mathbf{x}, \mathbf{y}) := (A\mathbf{x}, A\mathbf{y})$ . This map is *real* in the sense that it commutes with the complex conjugation:  $A^{\mathbb{C}}\sigma = \sigma A^{\mathbb{C}}$ .

*Vice versa*, let  $B : \mathcal{V}^{\mathbb{C}} \rightarrow \mathcal{V}^{\mathbb{C}}$  be a  $\mathbb{C}$ -linear map that commutes with  $\sigma$ :  $\sigma(B\mathbf{z}) = B\sigma(\mathbf{z})$  for all  $\mathbf{z} \in \mathcal{V}^{\mathbb{C}}$ . When  $\sigma(\mathbf{z}) = \pm\mathbf{z}$ , we find  $\sigma(B\mathbf{z}) = \pm B\mathbf{z}$ , i.e. the subspaces  $\mathcal{V}$  and  $i\mathcal{V}$  of real and imaginary vectors are  $B$ -invariant. Moreover, since  $B$  is  $\mathbb{C}$ -linear, we find that for  $x, \mathbf{y} \in \mathcal{V}$ ,  $B(\mathbf{x} + i\mathbf{y}) = B\mathbf{x} + iB\mathbf{y}$ . Thus  $B = A^{\mathbb{C}}$  where the linear operator  $A : \mathcal{V} \rightarrow \mathcal{V}$  is obtained by restricting  $B$  to  $\mathcal{V}$ .

## Euclidean Spaces

Let  $\mathcal{V}$  be a real vector space. A **Euclidean inner product** (or **Euclidean structure**) on  $\mathcal{V}$  is defined as a positive definite symmetric bilinear form  $\langle \cdot, \cdot \rangle$ . A real vector space equipped with a Euclidean inner product is called a **Euclidean space**. A Euclidean inner product allows one to talk about distances between points and angles between directions:

$$|\mathbf{x} - \mathbf{y}| = \sqrt{\langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y} \rangle}, \quad \cos \theta(\mathbf{x}, \mathbf{y}) := \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{|\mathbf{x}| |\mathbf{y}|}.$$

It follows from the Inertia Theorem that *every finite dimensional Euclidean vector space has an orthonormal basis*. In coordinates corresponding to an orthonormal basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  the inner product is given by the standard formula:

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i,j=1}^n x_i y_j \langle \mathbf{e}_i, \mathbf{e}_j \rangle = x_1 y_1 + \dots + x_n y_n.$$

Thus, every Euclidean space  $\mathcal{V}$  of dimension  $n$  can be identified with the **coordinate Euclidean space**  $\mathbb{R}^n$  by an isomorphism  $\mathbb{R}^n \rightarrow \mathcal{V}$  respecting inner products. Such an isomorphism is not unique, but can be composed with any invertible linear transformation  $U : \mathcal{V} \rightarrow \mathcal{V}$  preserving the Euclidean structure:

$$\langle U\mathbf{x}, U\mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathcal{V}.$$

Such transformations are called **orthogonal**.

A Euclidean structure on a vector space  $\mathcal{V}$  allows one to identify the space with its dual  $\mathcal{V}^*$  by the rule that to a vector  $\mathbf{v} \in \mathcal{V}$  assigns the linear function on  $\mathcal{V}$  whose value at a point  $\mathbf{x} \in \mathcal{V}$  is equal to the inner product  $\langle \mathbf{v}, \mathbf{x} \rangle$ . Respectively, given a linear map  $A : \mathcal{V} \rightarrow \mathcal{W}$  between Euclidean spaces, the adjoint map  $A^t : \mathcal{W}^* \rightarrow \mathcal{V}^*$  can be considered as a map between the spaces themselves:  $A^t : \mathcal{W} \rightarrow \mathcal{V}$ . The defining property of the adjoint map reads:

$$\langle A^t \mathbf{w}, \mathbf{v} \rangle = \langle \mathbf{w}, A\mathbf{v} \rangle \quad \text{for all } \mathbf{v} \in \mathcal{V} \text{ and } \mathbf{w} \in \mathcal{W}.$$

Consequently matrices of adjoint maps  $A$  and  $A^t$  with respect to orthonormal bases of the Euclidean spaces  $\mathcal{V}$  and  $\mathcal{W}$  are transposed to each other.

As in the case of Hermitian spaces, one easily derives that a linear transformation  $U : \mathcal{V} \rightarrow \mathcal{V}$  is orthogonal if and only if  $U^{-1} = U^t$ . In the matrix form, the relation  $U^t U = I$  means that columns of  $U$  form an orthonormal set in the coordinate Euclidean space.

Our nearest goal is obtain real analogues of the Spectral Theorem and its corollaries. One way to do it is to combine corresponding complex results with complexification. Let  $\mathcal{V}$  be a Euclidean space. We extend the inner product to the complexification  $\mathcal{V}^{\mathbb{C}}$  in such a way that it becomes an Hermitian inner product. Namely, for all  $\mathbf{x}, \mathbf{y}, \mathbf{x}', \mathbf{y}' \in \mathcal{V}$ , put

$$\langle \mathbf{x} + i\mathbf{y}, \mathbf{x}' + i\mathbf{y}' \rangle = \langle \mathbf{x}, \mathbf{x}' \rangle + \langle \mathbf{y}, \mathbf{y}' \rangle + i\langle \mathbf{x}, \mathbf{y}' \rangle - i\langle \mathbf{y}, \mathbf{x}' \rangle.$$

It is straightforward to check that this form on  $\mathcal{V}^{\mathbb{C}}$  is sesquilinear and Hermitian symmetric. It is also positive definite since  $\langle \mathbf{x} + i\mathbf{y}, \mathbf{x} + i\mathbf{y} \rangle = |\mathbf{x}|^2 + |\mathbf{y}|^2$ . Note that changing the signs of  $\mathbf{y}$  and  $\mathbf{y}'$  preserves the real part and reverses the imaginary part of the form. In other words, for all  $\mathbf{z}, \mathbf{w} \in \mathcal{V}^{\mathbb{C}}$ , we have:

$$\langle \sigma(\mathbf{z}), \sigma(\mathbf{w}) \rangle = \overline{\langle \mathbf{z}, \mathbf{w} \rangle} (= \langle \mathbf{w}, \mathbf{z} \rangle).$$

This identity expresses the fact that the Hermitian structure of  $\mathcal{V}^{\mathbb{C}}$  came from a Euclidean structure on  $\mathcal{V}$ . When  $A : \mathcal{V}^{\mathbb{C}} \rightarrow \mathcal{V}^{\mathbb{C}}$  is a *real* operator, i.e.  $\sigma A \sigma = A$ , the Hermitian adjoint operator  $A^*$  is also real.<sup>6</sup> Indeed, since  $\sigma^2 = \text{id}$ , we find that for all  $\mathbf{z}, \mathbf{w} \in \mathcal{V}^{\mathbb{C}}$

$$\langle \sigma A^* \sigma \mathbf{z}, \mathbf{w} \rangle = \langle \sigma \mathbf{w}, A^* \sigma \mathbf{z} \rangle = \langle A \sigma \mathbf{w}, \sigma \mathbf{z} \rangle = \langle \sigma A \mathbf{w}, \sigma \mathbf{z} \rangle = \langle \mathbf{z}, A \mathbf{w} \rangle,$$

i.e.  $\sigma A^* \sigma = A^*$ . In particular, complexifications of orthogonal ( $U^{-1} = U^t$ ), **symmetric** ( $A^t = A$ ), **anti-symmetric** ( $A^t = -A$ ), **normal** ( $A^t A = A A^t$ ) operators in a Euclidean space are respectively unitary, Hermitian, anti-Hermitian, normal operators on the complexified space, commuting with the complex conjugation.

## The Real Spectral Theorem

**Theorem.** *Let  $\mathcal{V}$  be a Euclidean space, and  $A : \mathcal{V} \rightarrow \mathcal{V}$  a normal operator. Then in the complexification  $\mathcal{V}^{\mathbb{C}}$ , there exists an orthonormal basis of eigenvectors of  $A^{\mathbb{C}}$  which is invariant under complex conjugation and such that the eigenvalues corresponding to conjugated eigenvectors are conjugated.*

**Proof.** Applying the complex Spectral Theorem to the normal operator  $B = A^{\mathbb{C}}$ , we obtain a decomposition of the complexified space  $\mathcal{V}^{\mathbb{C}}$  into a direct orthogonal sum of eigenspaces  $\mathcal{W}_1, \dots, \mathcal{W}_r$  of  $B$  corresponding to distinct complex eigenvalues  $\lambda_1, \dots, \lambda_r$ . Note that if  $\mathbf{v}$  is an eigenvector of  $B$  with an eigenvalue  $\mu$ , then  $B \sigma \mathbf{v} = \sigma B \mathbf{v} = \sigma(\mu \mathbf{v}) = \bar{\mu} \sigma \mathbf{v}$ , i.e.  $\sigma \mathbf{v}$  is an eigenvector of  $B$  with the conjugate eigenvalue  $\bar{\mu}$ . This shows that if  $\lambda_i$  is a non-real eigenvalue, then its conjugate  $\bar{\lambda}_i$  is also one of the eigenvalues of  $B$  (say,  $\lambda_j$ ), and the corresponding eigenspaces are conjugated:  $\sigma(\mathcal{W}_i) = \mathcal{W}_j$ . By the same token, if  $\lambda_k$  is real, then  $\sigma(\mathcal{W}_k) = \mathcal{W}_k$ . This last equality means that  $\mathcal{W}_k$  itself is the complexification of a real space, namely of the  $\sigma$ -invariant part of  $\mathcal{W}_k$ . It coincides with the space  $\text{Ker}(\lambda_k I - A) \subset \mathcal{V}$  of real eigenvectors of  $A$  with the eigenvalue  $\lambda_k$ . Thus, to construct a required orthonormal basis, we take: for each real eigenspace  $\mathcal{W}_k$ , a Euclidean orthonormal basis in the corresponding real eigenspace, and for each pair  $\mathcal{W}_i, \mathcal{W}_j$  of complex conjugate eigenspaces, an Hermitian orthonormal basis  $\{\mathbf{f}_\alpha\}$  in  $\mathcal{W}_i$  and the conjugate basis  $\{\sigma(\mathbf{f}_\alpha)\}$  in  $\mathcal{W}_j = \sigma(\mathcal{W}_i)$ . The vectors of all these bases altogether form an orthonormal basis of  $\mathcal{V}^{\mathbb{C}}$  satisfying our requirements.  $\square$

---

<sup>6</sup>This is obvious in the matrix form: In a real orthonormal basis of  $\mathcal{V}$  (which is a complex orthonormal basis of  $\mathcal{V}^{\mathbb{C}}$ )  $A$  has a real matrix, so that  $A^* = A^t$ . We use here a “hard way” to illustrate how various aspects of  $\sigma$ -invariance fit together.

**Example 1.** Identify  $\mathbb{C}$  with the Euclidean plane  $\mathbb{R}^2$  in the usual way, and consider the operator  $(x + iy) \mapsto (\alpha + i\beta)(x + iy)$  of multiplication by given complex number  $\alpha + i\beta$ . In the basis  $1, i$ , it has the matrix

$$A = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}.$$

Since  $A^t$  represents multiplication by  $\alpha - i\beta$ , it commutes with  $A$ . Therefore  $A$  is normal. It is straightforward to check that

$$\mathbf{z} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} \quad \text{and} \quad \bar{\mathbf{z}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

are complex eigenvectors of  $A$  with the eigenvalues  $\alpha + i\beta$  and  $\alpha - i\beta$  respectively, and form an Hermitian orthonormal basis in  $(\mathbb{R}^2)^{\mathbb{C}}$ .

**Example 2.** If  $A$  is a linear transformation in  $\mathbb{R}^n$ , and  $\lambda_0$  is a non-real root of its characteristic polynomial  $\det(\lambda I - A)$ , then the system of linear equations  $A\mathbf{z} = \lambda_0\mathbf{z}$  has non-trivial solutions, which cannot be real though. Let  $\mathbf{z} = \mathbf{u} + i\mathbf{v}$  be a complex eigenvector of  $A$  with the eigenvalue  $\lambda_0 = \alpha + i\beta$ . Then  $\sigma\mathbf{z} = \mathbf{u} - i\mathbf{v}$  is an eigenvector of  $A$  with the eigenvalue  $\bar{\lambda}_0 = \alpha - i\beta$ . Since  $\lambda_0 \neq \bar{\lambda}_0$ , the vectors  $\mathbf{z}$  and  $\sigma\mathbf{z}$  are linearly independent over  $\mathbb{C}$ , and hence the real vectors  $\mathbf{u}$  and  $\mathbf{v}$  must be linearly independent over  $\mathbb{R}$ . Consider the plane  $\text{Span}(\mathbf{u}, \mathbf{v}) \subset \mathbb{R}^n$ . Since

$$A(\mathbf{u} - i\mathbf{v}) = (\alpha - i\beta)(\mathbf{u} - i\mathbf{v}) = (\alpha\mathbf{u} - \beta\mathbf{v}) - i(\beta\mathbf{u} + \alpha\mathbf{v}),$$

we conclude that  $A$  preserves this plane and in the basis  $\mathbf{u}, -\mathbf{v}$  in it (note the sign change!) acts by the matrix  $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ . If we assume in addition that  $A$  is normal (with respect to the standard Euclidean structure in  $\mathbb{R}^n$ ), then the eigenvectors  $\mathbf{z}$  and  $\sigma\mathbf{z}$  must be Hermitian orthogonal, i.e.

$$\langle \mathbf{u} - i\mathbf{v}, \mathbf{u} + i\mathbf{v} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{v}, \mathbf{v} \rangle + 2i\langle \mathbf{u}, \mathbf{v} \rangle = 0.$$

We conclude that  $\langle \mathbf{u}, \mathbf{v} \rangle = 0$  and  $|\mathbf{u}|^2 - |\mathbf{v}|^2 = 0$ , i.e.  $\mathbf{u}$  and  $\mathbf{v}$  are orthogonal and have the same length. Normalizing the length to 1, we obtain an orthonormal basis of the  $A$ -invariant plane, in which the transformation  $A$  acts as in Example 1. The geometry of this transformation is known to us from studying geometry of complex numbers: It is the composition of the rotation through the angle  $\arg(\lambda_0)$  with the expansion by the factor  $|\lambda_0|$ . We will call such a transformation of the Euclidean plane a **complex multiplication** or **multiplication by a complex scalar**,  $\lambda_0$ .



Corollary 1. *Given a normal operator on a Euclidean space, the space can be represented as a direct orthogonal sum of invariant lines and planes, on each of which the transformation acts as multiplication by a real or complex scalar respectively.*

Corollary 2. *A transformation in a Euclidean space is orthogonal if and only if the space can be represented as the direct orthogonal sum of invariant lines and planes on each of which the transformation acts as multiplication by  $\pm 1$  and rotation respectively.*

Corollary 3. *In a Euclidean space, every symmetric operator has an orthonormal basis of eigenvectors.*

Corollary 4. *Every quadratic form in a Euclidean space of dimension  $n$  can be transformed by an orthogonal change of coordinates to exactly one of the normal forms:*

$$\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2, \quad \lambda_1 \geq \cdots \geq \lambda_n.$$

Corollary 5. *In a Euclidean space of dimension  $n$ , every anti-symmetric bilinear form can be transformed by an orthogonal change of coordinates to exactly one of the normal forms*

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^r \omega_i (x_{2i-1} y_{2i} - x_{2i} y_{2i-1}), \quad \omega_1 \geq \cdots \geq \omega_r > 0, \quad 2r \leq n.$$

Corollary 6. *Every real normal matrix  $A$  can be written in the form  $A = U^* M U$  where  $U$  is an orthogonal matrix, and  $M$  is block-diagonal matrix with each block of size 1, or of size 2 of the form  $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ , where  $\alpha^2 + \beta^2 \neq 0$ .*

*If  $A$  is symmetric, then only blocks of size 1 are present (i.e.  $M$  is diagonal).*

*If  $A$  is anti-symmetric, then blocks of size 1 are zero, and of size 2 are of the form  $\begin{bmatrix} 0 & -\omega \\ \omega & 0 \end{bmatrix}$ , where  $\omega > 0$ .*

*If  $A$  is orthogonal, then all blocks of size 1 are equal to  $\pm 1$ , and blocks of size 2 have the form  $\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$ , where  $0 < \theta < \pi$ .*

## Courant–Fisher’s Minimax Principle

One of the consequences (equivalent to Corollary 4) of the Spectral Theorem is that a pair  $(Q, S)$  of quadratic forms in  $\mathbb{R}^n$  of which the first one is positive definite can be transformed by a linear change of coordinates to the normal form:

$$Q = x_1^2 + \cdots + x_n^2, \quad S = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2, \quad \lambda_1 \geq \cdots \geq \lambda_n.$$

The eigenvalues  $\lambda_1 \geq \cdots \geq \lambda_n$  form the **spectrum** of the pair  $(Q, S)$ . The following result gives a coordinate-less, geometric description of the spectrum.

**Theorem.** *The  $k$ -th greatest spectral number is given by*

$$\lambda_k = \max_{\mathcal{W}: \dim \mathcal{W}=k} \min_{\mathbf{x} \in \mathcal{W}-\mathbf{0}} \frac{S(\mathbf{x})}{Q(\mathbf{x})},$$

where the maximum is taken over all  $k$ -dimensional subspaces  $\mathcal{W} \subset \mathbb{R}^n$ , and minimum over all non-zero vectors in the subspace.

**Proof.** When  $\mathcal{W}$  is given by the equations  $x_{k+1} = \cdots = x_n = 0$ , the minimal ratio  $S(\mathbf{x})/Q(\mathbf{x})$ , achieved on vectors proportional to  $\mathbf{e}_k$ , is equal to  $\lambda_k$  because

$$\lambda_1 x_1^2 + \cdots + \lambda_k x_k^2 \geq \lambda_k (x_1^2 + \cdots + x_k^2) \quad \text{when } \lambda_1 \geq \cdots \geq \lambda_k.$$

Therefore it suffices to prove for every other  $k$ -dimensional subspace  $\mathcal{W}$  the minimal ratio cannot be greater than  $\lambda_k$ . For this, denote by  $\mathcal{V}$  the subspace of dimension  $n - k + 1$  given by the equations  $x_1 = \cdots = x_{k-1} = 0$ . Since  $\lambda_k \geq \cdots \geq \lambda_n$ , we have:

$$\lambda_k x_k^2 + \cdots + \lambda_n x_n^2 \leq \lambda_k (x_k^2 + \cdots + x_n^2),$$

i.e. for all non-zero vectors  $\mathbf{x}$  in  $\mathcal{V}$  the ratio  $S(\mathbf{x})/Q(\mathbf{x}) \leq \lambda_k$ . Now we invoke the dimension counting argument:  $\dim \mathcal{W} + \dim \mathcal{V} = k + (n - k + 1) = n + 1 > \dim \mathbb{R}^n$ , and conclude that  $\mathcal{W}$  has a non-trivial intersection with  $\mathcal{V}$ . Let  $\mathbf{x}$  be a non-zero vector in  $\mathcal{W} \cap \mathcal{V}$ . Then  $S(\mathbf{x})/Q(\mathbf{x}) \leq \lambda_k$ , and hence the minimum of the ratio  $S/Q$  on  $\mathcal{W} - \mathbf{0}$  cannot exceed  $\lambda_k$ .  $\square$

Applying Theorem to the pair  $(Q, -S)$  we obtain yet another characterization of the spectrum:

$$\lambda_k = \min_{\mathcal{W}: \dim \mathcal{W}=n-k} \max_{\mathbf{x} \in \mathcal{W}-\mathbf{0}} \frac{S(\mathbf{x})}{Q(\mathbf{x})}.$$

Formulating some applications, we assume that the space  $\mathbb{R}^n$  is Euclidean, and refer to the spectrum of the pair  $(Q, S)$  where  $Q = |\mathbf{x}|^2$ , simply as the spectrum of  $S$ .

**Corollary 1.** *When a quadratic form increases, its spectral numbers do not decrease: If  $S \leq S'$  then  $\lambda_k \leq \lambda'_k$  for all  $k = 1, \dots, n$ .*

**Proof.** Indeed, since  $S/Q \leq S'/Q$ , the minimum of the ratio  $S/Q$  on every  $k$ -dimensional subspace  $\mathcal{W}$  cannot exceed that of  $S'/Q$ , which in particular remains true for that  $\mathcal{W}$  on which the maximum of  $S/Q$  equal to  $\lambda_k$  is achieved.

The following result is called **Cauchy's interlacing theorem**.

**Corollary 2.** *Let  $\lambda_1 \geq \dots \geq \lambda_n$  be the spectrum of a quadratic form  $S$ , and  $\lambda'_1 \geq \dots \geq \lambda'_{n-1}$  be the spectrum of the quadratic form  $S'$  obtained by restricting  $S$  to a given hyperplane  $\mathbb{R}^{n-1} \subset \mathbb{R}^n$ . Then:*

$$\lambda_1 \geq \lambda'_1 \geq \lambda_2 \geq \lambda'_2 \geq \dots \geq \lambda_{n-1} \geq \lambda'_{n-1} \geq \lambda_n.$$

**Proof.** Maximum over all  $k$ -dimensional subspaces  $\mathcal{W}$  cannot be smaller than maximum (of the same quantities) over subspaces lying inside the hyperplane. This proves that  $\lambda_k \geq \lambda'_k$ . Applying the same argument to  $-S$  and subspaces of dimension  $n - k - 1$ , we conclude that  $-\lambda_{k+1} \geq -\lambda'_k$ .  $\square$

An **ellipsoid** in a Euclidean space is defined as the level-1 set  $E = \{\mathbf{x} \mid S(\mathbf{x}) = 1\}$  of a positive definite quadratic form,  $S$ . It follows from the Spectral Theorem that every ellipsoid can be transformed by an orthogonal transformation to **principal axes**: a normal form

$$\frac{x_1^2}{\alpha_1^2} + \dots + \frac{x_n^2}{\alpha_n^2} = 1, \quad 0 < \alpha_1 \leq \dots \leq \alpha_n.$$

The vectors  $\mathbf{x} = \pm\alpha_k \mathbf{e}_k$  lie on the ellipsoid, and their lengths  $\alpha_k$  are called **semiaxes** of  $E$ . They are related to the spectral numbers  $\lambda_1 \geq \dots \geq \lambda_k > 0$  of the quadratic form by  $\alpha_k^{-1} = \sqrt{\lambda_k}$ . From Corollaries 1 and 2 respectively, we obtain:

*If one ellipsoid is enclosed by another, the semiaxes of the inner ellipsoid do not exceed corresponding semiaxes of the outer:*

*If  $E' \subset E$ , then  $\alpha'_k \leq \alpha_k$  for all  $k = 1, \dots, n$ .*

*Semiaxes of a given ellipsoid are interlaced by semiaxes of any section of it by a hyperplane passing through the center:*

*If  $E' = E \cap \mathbb{R}^{n-1}$ , then  $\alpha_k \leq \alpha'_k \leq \alpha_{k+1}$  for  $k = 1, \dots, n - 1$ .*

**EXERCISES**

**253.** Prove that if two vectors  $\mathbf{u}$  and  $\mathbf{v}$  in an Hermitian space are orthogonal, then  $|\mathbf{u}|^2 + |\mathbf{v}|^2 = |\mathbf{u} - \mathbf{v}|^2$ . Is the converse true?  $\checkmark$

**254.** Prove that for any vectors  $\mathbf{u}, \mathbf{v}$  in an Hermitian space,

$$|\mathbf{u} + \mathbf{v}|^2 + |\mathbf{u} - \mathbf{v}|^2 = 2|\mathbf{u}|^2 + 2|\mathbf{v}|^2.$$

Find a geometric interpretation of this fact.  $\checkmark$

**255.** Apply Gram–Schmidt orthogonalization to the basis  $\mathbf{f}_1 = \mathbf{e}_1 + 2i\mathbf{e}_2 + 2i\mathbf{e}_3$ ,  $\mathbf{f}_2 = \mathbf{e}_1 + 2i\mathbf{e}_2$ ,  $\mathbf{f}_3 = \mathbf{e}_1$  in the coordinate Hermitian space  $\mathbb{C}^3$ .

**256.** Apply Gram–Schmidt orthogonalization to the standard basis  $\mathbf{e}_1, \mathbf{e}_2$  of  $\mathbb{C}^2$  to construct an orthonormal basis of the Hermitian inner product  $\langle \mathbf{z}, \mathbf{w} \rangle = \bar{z}_1 w_1 + 2\bar{z}_1 w_2 + 2\bar{z}_2 w_1 + 5\bar{z}_2 w_2$ .

**257.** Let  $\mathbf{f} \in \mathcal{V}$  be a vector in an Hermitian space,  $\mathbf{e}_1, \dots, \mathbf{e}_k$  an orthonormal basis in a subspace  $\mathcal{W}$ . Prove that  $\mathbf{u} = \sum \langle \mathbf{e}_i, \mathbf{v} \rangle \mathbf{e}_i$  is the point of  $\mathcal{W}$  closest to  $\mathbf{v}$ , and that  $\mathbf{v} - \mathbf{u}$  is orthogonal to  $\mathcal{W}$ . (The point  $\mathbf{u} \in \mathcal{W}$  is called the **orthogonal projection** of  $\mathbf{v}$  to  $\mathcal{W}$ .)

**258.\*** Let  $\mathbf{f}_1, \dots, \mathbf{f}_N$  be a finite sequence of vectors in an Hermitian space. The Hermitian  $N \times N$ -matrix  $\langle \mathbf{f}_i, \mathbf{f}_j \rangle$  is called the **Gram matrix** of the sequence. Show that two finite sequences of vectors are isometric, i.e. obtained from each other by a unitary transformation, if and only if their Gram matrices are the same.

**259.** Prove that  $\langle A, B \rangle := \text{tr}(A^*B)$  defines an Hermitian inner product on the space  $\text{Hom}(\mathbb{C}^n, \mathbb{C}^m)$  of  $m \times n$ -matrices.

**260.** Let  $A_1, \dots, A_k : \mathcal{V} \rightarrow \mathcal{W}$  be linear maps between Hermitian spaces. Prove that if  $\sum A_i^* A_i = 0$ , then  $A_1 = \dots = A_k = 0$ .

**261.** Let  $A : \mathcal{V} \rightarrow \mathcal{W}$  be a linear map between Hermitian spaces. Show that  $B := A^*A$  and  $C = AA^*$  are Hermitian, and that the corresponding Hermitian forms  $B(\mathbf{x}, \mathbf{x}) := \langle \mathbf{x}, B\mathbf{x} \rangle$  in  $\mathcal{V}$  and  $C(\mathbf{y}, \mathbf{y}) := \langle \mathbf{y}, C\mathbf{y} \rangle$  in  $\mathcal{W}$  are non-negative. Under what hypothesis about  $A$  is the 1st of them positive? the 2nd one? are they both positive?

**262.** Let  $\mathcal{W} \subset \mathcal{V}$  be a subspace in an Hermitian space, and let  $P : \mathcal{V} \rightarrow \mathcal{V}$  be the map that to each vector  $\mathbf{v} \in \mathcal{V}$  assigns its orthogonal projection to  $\mathcal{W}$ . Prove that  $P$  is an Hermitian operator, and that  $P^2 = P$ , and that  $\text{Ker } P = \mathcal{W}^\perp$ . (It is called the **orthogonal projector** to  $\mathcal{W}$ .)

**263.** Prove that an  $n \times n$ -matrix is unitary if and only if its rows (or columns) form an orthonormal basis in the coordinate Hermitian space  $\mathbb{C}^n$ .

**264.** Prove that the determinant of a unitary matrix is a complex number of absolute value 1.

**265.** Prove that the **Cayley transform**:  $C \mapsto (I - C)/(I + C)$ , well-defined for linear transformations  $C$  such that  $I + C$  is invertible, transforms unitary

operators into anti-Hermitian and *vice versa*. Compute the square of the Cayley transform. ✓

**266.** Prove that the commutator  $AB - BA$  of anti-Hermitian operators  $A$  and  $B$  is anti-Hermitian.

**267.** Give an example of a normal  $2 \times 2$ -matrix which is not Hermitian, anti-Hermitian, or unitary.

**268.** Prove that for any  $n \times n$ -matrix  $A$  and any complex numbers  $\alpha, \beta$  of absolute value 1, the matrix  $\alpha A + \beta A^*$  is normal.

**269.** Prove that  $A : \mathcal{V} \rightarrow \mathcal{V}$  is normal if and only if  $|A\mathbf{x}| = |A^*\mathbf{x}|$  for all  $\mathbf{x} \in \mathcal{V}$ .

**270.** Prove that the characteristic polynomial  $\det(\lambda I - A)$  of a square matrix  $A$  does not change under similarity transformations  $A \mapsto C^{-1}AC$  and thus depends only on the linear operator defined by the matrix.

**271.** Show that if  $\lambda^n + p_1\lambda^{n-1} + \cdots + p_n$  is the characteristic polynomial of a matrix  $A$ , then  $p_n = (-1)^n \det A$ , and  $p_1 = -\operatorname{tr} A$ .

**272.** Prove that all roots of characteristic polynomials of Hermitian matrices are real.

**273.** Find eigenspaces and eigenvalues of an orthogonal projector to a subspace  $\mathcal{W} \subset \mathcal{V}$  in an Hermitian space.

**274.** Prove that every Hermitian operator  $P$  satisfying  $P^2 = P$  is an orthogonal projector. Does this remain true if  $P$  is not Hermitian?

**275.** Prove directly, i.e. not referring to the Spectral Theorem, that every Hermitian operator has an orthonormal basis of eigenvectors. ✎

**276.** Prove that if  $A$  and  $B$  are normal and  $AB = 0$ , then  $BA = 0$ .

**277.\*** Let  $A$  be a normal operator. Prove that the set of complex numbers  $\{\langle \mathbf{x}, A\mathbf{x} \rangle \mid |\mathbf{x}| = 1\}$  is a convex polygon whose vertices are eigenvalues of  $A$ . ✎

**278.** Prove that two (or several) commuting normal operators have a common orthonormal basis of eigenvectors. ✎

**279.** Prove that if  $A$  is normal and  $AB = BA$ , then  $AB^* = B^*A$ ,  $A^*B = BA^*$ , and  $A^*B^* = B^*A^*$ .

**280.** Prove that if  $(\lambda - \lambda_1) \cdots (\lambda - \lambda_n)$  is the characteristic polynomial of a normal operator  $A$ , then  $\sum |\lambda_i|^2 = \operatorname{tr}(A^*A)$ .

**281.** Classify up to linear changes of coordinates pairs  $(Q, A)$  of forms, where  $S$  is positive definite Hermitian, and  $A$  anti-Hermitian.

**282.** An Hermitian operator  $S$  is called **positive** (written:  $S \geq 0$ ) if  $\langle \mathbf{x}, S\mathbf{x} \rangle \geq 0$  for all  $\mathbf{x}$ . Prove that for every positive operator  $S$  there is a unique positive **square root** (denoted by  $\sqrt{S}$ ), i.e. a positive operator whose square is  $S$ .

**283.** Using Singular Value Decomposition theorem with  $m = n$ , prove that every linear transformation  $A$  of an Hermitian space has a **polar decomposition**  $A = SU$ , where  $S$  is positive, and  $U$  is unitary.

**284.** Prove that the polar decomposition  $A = SU$  is unique when  $A$  is invertible; namely  $S = \sqrt{AA^*}$ , and  $U = S^{-1}A$ . What are polar decompositions of non-zero  $1 \times 1$ -matrices?

**285.** Describe the complexification of  $\mathbb{C}^n$  considered as a real vector space.

**286.** Let  $\sigma$  be the complex conjugation operator on  $\mathbb{C}^n$ . Consider  $\mathbb{C}^n$  as a real vector space. Show that  $\sigma$  is symmetric and orthogonal.

**287.** Prove that every orthogonal transformation in  $\mathbb{R}^3$  is either a rotation through an angle  $\theta$ ,  $0 \leq \theta \leq \pi$ , about some axis, or the composition of such a rotation with the reflection about the plane perpendicular to the axis.

**288.** Find an orthonormal basis in  $\mathbb{C}^n$  in which the transformation defined by the cyclic permutation of coordinates:  $(z_1, z_2, \dots, z_n) \mapsto (z_2, \dots, z_n, z_1)$  is diagonal.

**289.** In the coordinate Euclidean space  $\mathbb{R}^n$  with  $n \leq 4$ , find real and complex normal forms of orthogonal transformations defined by various permutations of coordinates.

**290.** Transform to normal forms by orthogonal transformations:

- (a)  $x_1x_2 + x_3x_4$ , (b)  $2x_1^2 - 4x_1x_2 + x_2^2 - 4x_2x_3$ ,  
 (c)  $5x_1^2 + 6x_2^2 + 4x_3^2 - 4x_1x_2 - 8x_1x_3 - 4x_2x_3$ .

**291.** In Euclidean spaces, classify all operators which are both orthogonal and anti-symmetric.

**292.** Let  $\mathcal{U}$  and  $\mathcal{V}$  be two subspaces of dimension 2 in the Euclidean 4-space. Consider the map  $T : \mathcal{V} \rightarrow \mathcal{V}$  defined as the composition:  $\mathcal{V} \subset \mathbb{R}^4 \rightarrow \mathcal{U} \subset \mathbb{R}^4 \rightarrow \mathcal{V}$ , where the arrows are the orthogonal projections to  $\mathcal{U}$  and  $\mathcal{V}$  respectively. Prove that  $T$  is positive, and that its eigenvalues have the form  $\cos \phi$ ,  $\cos \psi$  where  $\phi, \psi$  are certain angles,  $0 \leq \phi, \psi \leq \pi/2$ .

**293.** Solve **Gelfand's problem**: In the Euclidean 4-space, classify pairs of planes passing through the origin up to orthogonal transformations of the space. ♣

**294.** Prove that every ellipsoid in  $\mathbb{R}^n$  has pairwise perpendicular hyperplanes of bilateral symmetry.

**295.** Prove that every ellipsoid in  $\mathbb{R}^4$  has a plane section which is a circle. Does this remain true for ellipsoids in  $\mathbb{R}^3$ ?

**296.** Formulate and prove counterparts of Courant–Fisher's minimax principle and Cauchy's interlacing theorem for Hermitian forms.

**297.** Prove that semiaxes  $\alpha_1 \leq \alpha_2 \leq \dots$  of an ellipsoid in  $\mathbb{R}^n$  and semiaxes  $\alpha'_k \leq \alpha'_2 \leq \dots$  of its section by a linear subspaces of codimension  $k$  are related by the inequalities:  $\alpha_i \leq \alpha'_i \leq \alpha_{i+k}$ ,  $i = 1, \dots, n - k$ .

## 2 Jordan Canonical Forms

### Characteristic Polynomials and Root Spaces

Let  $\mathcal{V}$  be a finite dimensional  $\mathbb{K}$ -vector space. We do not assume that  $\mathcal{V}$  is equipped with any structure in addition to the structure of a  $\mathbb{K}$ -vector space. In this section, we study geometry of linear operators on  $\mathcal{V}$ . In other words, we study the problem of classification of linear operators  $A : \mathcal{V} \rightarrow \mathcal{V}$  up to **similarity** transformations  $A \mapsto C^{-1}AC$ , where  $C$  stands for arbitrary invertible linear transformations of  $\mathcal{V}$ .

Let  $n = \dim \mathcal{V}$ , and let  $A$  be the matrix of a linear operator with respect to some basis of  $\mathcal{V}$ . Recall that

$$\det(\lambda I - A) = \lambda^n + p_1\lambda^{n-1} + \cdots + p_{n-1}\lambda + p_n$$

is called the **characteristic polynomial** of  $A$ . In fact it does not depend on the choice of a basis. Indeed, under a change  $\mathbf{x} = C\mathbf{x}'$  of coordinates, the matrix of a linear operator  $\mathbf{x} \mapsto A\mathbf{x}$  is transformed into the matrix  $C^{-1}AC$  similar to  $A$ . We have:

$$\begin{aligned} \det(\lambda I - C^{-1}AC) &= \det[C^{-1}(\lambda I - A)C] = \\ &(\det C^{-1}) \det(\lambda I - A) (\det C) = \det(\lambda I - A). \end{aligned}$$

Therefore, the characteristic polynomial of a linear operator is well-defined (by the geometry of  $A$ ). In particular, ***coefficients of the characteristic polynomial do not change under similarity transformations.***

Let  $\lambda_0 \in \mathbb{K}$  be a root of the characteristic polynomial. Then  $\det(\lambda_0 I - A) = 0$ , and hence the system of homogeneous linear equations  $A\mathbf{x} = \lambda_0\mathbf{x}$  has a non-trivial solution,  $\mathbf{x} \neq \mathbf{0}$ . As before, we call any such solution an **eigenvector** of  $A$ , and call  $\lambda_0$  the corresponding to the **eigenvalue**. All solutions to  $A\mathbf{x} = \lambda_0\mathbf{x}$  (including  $\mathbf{x} = \mathbf{0}$ ) form a linear subspace in  $\mathcal{V}$ , called the **eigenspace** of  $A$  corresponding to the eigenvalue  $\lambda_0$ .

Let us change slightly our point of view on the eigenspace. It is the null space of the operator  $A - \lambda_0 I$ . Consider powers of this operator and their null spaces. If  $(A - \lambda_0 I)^k \mathbf{x} = \mathbf{0}$  for some  $k > 0$ , then then  $(A - \lambda_0 I)^l \mathbf{x} = \mathbf{0}$  for all  $l \geq k$ . Thus the null spaces are nested:

$$\text{Ker}(A - \lambda_0 I) \subset \text{Ker}(A - \lambda_0 I)^2 \subset \cdots \subset \text{Ker}(A - \lambda_0 I)^k \subset \cdots$$

On the other hand, since  $\dim \mathcal{V} < \infty$ , nested subspaces must stabilize, i.e. starting from some  $m > 0$ , we have:

$$\mathcal{W}_{\lambda_0} := \text{Ker}(A - \lambda_0 I)^m = \text{Ker}(A - \lambda_0 I)^{m+1} = \dots$$

We call the subspace  $\mathcal{W}_{\lambda_0}$  a **root space** of the operator  $A$ , corresponding to the root  $\lambda_0$  of the characteristic polynomial.

Note that if  $\mathbf{x} \in \mathcal{W}_{\lambda_0}$ , then  $A\mathbf{x} \in \mathcal{W}_{\lambda_0}$ , because  $(A - \lambda_0 I)^m A\mathbf{x} = A(A - \lambda_0 I)^m \mathbf{x} = A\mathbf{0} = \mathbf{0}$ . Thus a root space is  $A$ -invariant. Denote by  $\mathcal{U}_{\lambda_0}$  the range of  $(A - \lambda_0 I)^m$ . It is also  $A$ -invariant, since if  $\mathbf{x} = (A - \lambda_0 I)^m \mathbf{y}$ , then  $A\mathbf{x} = A(A - \lambda_0 I)^m \mathbf{y} = (A - \lambda_0 I)^m (A\mathbf{y})$ .

**Lemma.**  $\mathcal{V} = \mathcal{W}_{\lambda_0} \oplus \mathcal{U}_{\lambda_0}$ .

**Proof.** Put  $B := (A - \lambda_0 I)^m$ , so that  $\mathcal{W}_{\lambda_0} = \text{Ker } B$ ,  $\mathcal{U}_{\lambda_0} = B(\mathcal{V})$ . Let  $\mathbf{x} = B\mathbf{y} \in \text{Ker } B$ . Then  $B\mathbf{x} = \mathbf{0}$ , i.e.  $\mathbf{y} \in \text{Ker } B^2$ . But  $\text{Ker } B^2 = \text{Ker } B$  by the assumption that  $\text{Ker } B = \mathcal{W}_{\lambda_0}$  is the root space. Thus  $\mathbf{y} \in \text{Ker } B$ , and hence  $\mathbf{x} = B\mathbf{y} = \mathbf{0}$ . This proves that  $\text{Ker } B \cap B(\mathcal{V}) = \{\mathbf{0}\}$ . Therefore the subspace in  $\mathcal{V}$  spanned by  $\text{Ker } B$  and  $B(\mathcal{V})$  is their direct sum. On the other hand, for any operator,  $\dim \text{Ker } B + \dim B(\mathcal{V}) = \dim \mathcal{V}$ . Thus, the subspace spanned by  $\text{Ker } B$  and  $B(\mathcal{V})$  is the whole space  $\mathcal{V}$ .

**Corollary 1.** *Root spaces of the restriction of  $A$  to  $\mathcal{U}_{\lambda_0}$  are exactly those root spaces  $\mathcal{W}_\lambda$  of  $A$  in the whole space  $\mathcal{V}$ , which correspond to roots  $\lambda \neq \lambda_0$ .*

**Proof.** It suffices to prove that if  $\lambda \neq \lambda_0$  is another root of the characteristic polynomial, then  $\mathcal{W}_\lambda \subset \mathcal{U}_{\lambda_0}$ . Indeed,  $\mathcal{W}_\lambda$  is invariant with respect to  $A - \lambda_0 I$ , but contains no eigenvectors of  $A$  with eigenvalue  $\lambda_0$ . Therefore  $A - \lambda_0 I$  and all powers of it are invertible on  $\mathcal{W}_\lambda$ . Thus  $\mathcal{W}_\lambda$  lies in the range  $\mathcal{U}_{\lambda_0}$  of  $B = (A - \lambda_0 I)^m$ .

**Corollary 2.** *Suppose that  $(\lambda - \lambda_1)^{m_1} \dots (\lambda - \lambda_r)^{m_r}$  is the characteristic polynomial of  $A : \mathcal{V} \rightarrow \mathcal{V}$ , where  $\lambda_1, \dots, \lambda_r \in \mathbb{K}$  are pairwise distinct roots. Then  $\mathcal{V}$  is the direct sum of root spaces:*

$$\mathcal{V} = \mathcal{W}_{\lambda_1} \oplus \dots \oplus \mathcal{W}_{\lambda_r}.$$

**Proof.** By induction on  $r$ , it follows from Corollary 1 that the subspace  $\mathcal{W} \subset \mathcal{V}$  spanned by root spaces  $\mathcal{W}_{\lambda_i}$  is their direct sum and moreover,  $\mathcal{V} = \mathcal{W} \oplus \mathcal{U}$ , where  $\mathcal{U}$  is the intersection of all  $\mathcal{U}_{\lambda_i}$ . Furthermore, the characteristic polynomial of  $A$  restricted to  $\mathcal{U}$  has none of  $\lambda_i$  as a root. From our assumption that the characteristic polynomial of  $A$  factors into  $\lambda - \lambda_i$ , it follows however that  $\dim \mathcal{U} = 0$ .



Indeed, the characteristic polynomial of  $A$  is equal to the product of the characteristic polynomials of its restrictions to  $\mathcal{W}$  and  $\mathcal{U}$  (because the matrix of  $A$  in a suitable basis of a direct sum is block diagonal). Hence the factor corresponding to  $\mathcal{U}$  must be of degree 0.

**Remarks.** (1) We will see later that dimensions of the root spaces coincide with multiplicities of the roots:  $\dim \mathcal{W}_{\lambda_i} = m_i$ .

(2) The restriction of  $A$  to  $\mathcal{W}_{\lambda_i}$  has the property that some power of  $A - \lambda_i I$  vanishes. A linear operator some power of which vanishes is called **nilpotent**. Our next task will be to study the geometry of nilpotent operators.

(3) Our assumption that the characteristic polynomial factors completely over  $\mathbb{K}$  is automatically satisfied in the case  $\mathbb{K} = \mathbb{C}$  due to the Fundamental Theorem of Algebra. Thus, we have proved for every linear operator on a finite dimensional complex vector space, that the space decomposes in a canonical fashion into the direct sum of invariant subspaces on each of which the operator differs from a nilpotent one by scalar summand.

## Nilpotent Operators

**Example.** Introduce a nilpotent linear operator  $N : \mathbb{K}^n \rightarrow \mathbb{K}^n$  by describing its action on vectors of the standard basis:

$$N\mathbf{e}_n = \mathbf{e}_{n-1}, \quad N\mathbf{e}_{n-1} = \mathbf{e}_{n-2}, \quad \dots, \quad N\mathbf{e}_2 = \mathbf{e}_1, \quad N\mathbf{e}_1 = \mathbf{0}.$$

Then  $N^n = 0$  but  $N^{n-1} \neq 0$ . We will call  $N$ , as well as any operator similar to it, a **regular nilpotent** operator. The matrix of  $N$  in the standard basis has the form

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \end{bmatrix}.$$

It has the range of dimension  $n - 1$  spanned by  $\mathbf{e}_1, \dots, \mathbf{e}_{n-1}$  and the null space of dimension 1 spanned by  $\mathbf{e}_1$ .

**Proposition.** *Let  $N : \mathcal{V} \rightarrow \mathcal{V}$  be a nilpotent operator on a  $\mathbb{K}$ -vector space of finite dimension. Then the space can be decomposed into the direct sum of  $N$ -invariant subspaces, on each of which  $N$  is regular.*

**Proof.** We use induction on  $\dim \mathcal{V}$ . When  $\dim \mathcal{V} = 0$ , there is nothing to prove. Now consider the case when  $\dim \mathcal{V} > 0$ .

The range  $N(\mathcal{V})$  is  $N$ -invariant, and  $\dim N(\mathcal{V}) < \dim \mathcal{V}$  (since otherwise  $N$  could not be nilpotent). By the induction hypothesis, there space  $N(\mathcal{V})$  can be decomposed into the direct sum of  $N$ -invariant subspaces, on each of which  $N$  is regular. Let  $l$  be the number of these subspaces,  $n_1, \dots, n_l$  their dimensions, and  $\mathbf{e}_1^{(i)}, \dots, \mathbf{e}_{n_i}^{(i)}$  a basis in the  $i$ th subspace such that  $N$  acts on the basis vectors as in Example:

$$\mathbf{e}_{n_i}^{(i)} \mapsto \dots \mapsto \mathbf{e}_1^{(i)} \mapsto \mathbf{0}.$$

Since each  $\mathbf{e}_{n_i}^{(i)}$  lies in the range of  $N$ , we can pick a vector  $\mathbf{e}_{n_i+1}^{(i)} \in \mathcal{V}$  such that  $N\mathbf{e}_{n_i+1}^{(i)} = \mathbf{e}_{n_i}^{(i)}$ . Note that  $\mathbf{e}_1^{(1)}, \dots, \mathbf{e}_1^{(l)}$  form a basis in  $(\text{Ker } N) \cap N(\mathcal{V})$ . We complete it to a basis

$$\mathbf{e}_1^{(1)}, \dots, \mathbf{e}_1^{(l)}, \mathbf{e}_1^{(l+1)}, \dots, \mathbf{e}_1^{(r)}$$

of the whole null space  $\text{Ker } N$ . We claim that *all the vectors*  $\mathbf{e}_j^{(i)}$  form a basis in  $\mathcal{V}$ , and therefore the  $l + r$  subspaces

$$\text{Span}(\mathbf{e}_1^{(i)}, \dots, \mathbf{e}_{n_i}^{(i)}, \mathbf{e}_{n_i+1}^{(i)}), \quad i = 1, \dots, l, l + 1, \dots, r,$$

(of which the last  $r - l$  are 1-dimensional) form a decomposition of  $\mathcal{V}$  into the direct sum with required properties.

To justify the claim, notice that the subspace  $\mathcal{U} \subset \mathcal{V}$  spanned by  $n_1 + \dots + n_l = \dim N(\mathcal{V})$  vectors  $\mathbf{e}_j^{(i)}$  with  $j > 1$  is mapped by  $N$  onto the space  $N(\mathcal{V})$ . Therefore: those vectors form a basis of  $\mathcal{U}$ ,  $\dim \mathcal{U} = \dim N(\mathcal{V})$ , and  $\mathcal{U} \cap \text{Ker } N = \{\mathbf{0}\}$ . On the other hand, vectors  $\mathbf{e}_j^{(i)}$  with  $j = 1$  form a basis of  $\text{Ker } N$ , and since  $\dim \text{Ker } N + \dim N(\mathcal{V}) = \dim \mathcal{V}$ , together with the above basis of  $\mathcal{U}$ , they form a basis of  $\mathcal{V}$ .  $\square$

**Corollary 1.** *The matrix of a nilpotent operator in a suitable basis is block diagonal with regular diagonal blocks (as in Example) of certain sizes  $n_1 \geq \dots \geq n_r > 0$ .*

The basis in which the matrix has this form, as well as the decomposition into the direct sum of invariant subspaces as described in Proposition, are not canonical, since choices are involved on each step of induction. However, the dimensions  $n_1 \geq \dots \geq n_r > 0$  of the subspaces turn out to be uniquely determined by the geometry of the operator.

To see why, introduce the following **Young tableaux** (Figure 41). It consist of  $r$  rows of identical square cells. The lengths of the rows represent dimensions  $n_1 \geq n_2 \geq \dots \geq n_r > 0$  of invariant subspaces, and in the cells of each row we place the basis vectors of the corresponding subspace, so that the operator  $N$  sends each vector to its left neighbor (and vectors of the leftmost column to  $\mathbf{0}$ ).

$e_1^{(1)}$	$e_2^{(1)}$	$e_3^{(1)}$			$e_{n_r}^{(1)}$	$e_{n_1}^{(1)}$
$e_1^{(2)}$	$e_2^{(2)}$	$e_3^{(2)}$		$e_{n_2}^{(2)}$		
$e_1^{(3)}$	$e_2^{(3)}$	$e_3^{(3)}$		$e_{n_3}^{(3)}$		
$e_1^{(r-1)}$	$e_2^{(r-1)}$					
$e_1^{(r)}$						

Figure 41

The format of the tableaux is determined by the **partition** of the total number  $n$  of cells (equal to  $\dim \mathcal{V}$ ) into the sum  $n_1 + \dots + n_r$  of positive integers. Reading the same format *by columns*, we obtain another partition  $n = m_1 + \dots + m_d$ , called **transposed** to the first one, where  $m_1 \geq \dots \geq m_d > 0$  are the heights of the columns. Obviously, two transposed partitions determine each other.

It follows from the way how the cells are filled with vectors  $e_j^{(i)}$ , that the vectors in the columns 1 through  $k$  form a basis of the space  $\text{Ker } N^k$ . Therefore

$$m_k = \dim \text{Ker } N^k - \dim \text{Ker } N^{k-1}, \quad k = 1, \dots, d.$$

**Corollary 2.** *Consider the flag of subspaces defined by a nilpotent operator  $N : \mathcal{V} \rightarrow \mathcal{V}$ :*

$$\text{Ker } N \subset \text{Ker } N^2 \subset \dots \subset \text{Ker } N^d = \mathcal{V}$$

*and the partition of  $n = \dim V$  into the summands  $m_k = \dim \text{Ker } N^k - \dim \text{Ker } N^{k-1}$ . Then summands of the transposed partition  $n = n_1 + \dots + n_r$  are the dimensions of the regular nilpotent blocks of  $N$  (described in Proposition and Corollary 1).*

**Corollary 3.** *The number of equivalence classes of nilpotent operators on a vector space of dimension  $n$  is equal to the number of partitions of  $n$ .*

## The Jordan Canonical Form Theorem

We proceed to classification of linear operators  $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$  up to similarity transformations.

**Theorem.** *Every complex matrix is similar to a block diagonal normal form with each diagonal block of the form:*

$$\begin{bmatrix} \lambda_0 & 1 & 0 & \dots & 0 \\ 0 & \lambda_0 & 1 & \dots & 0 \\ & & \dots & & \\ 0 & 0 & \dots & \lambda_0 & 1 \\ 0 & 0 & \dots & 0 & \lambda_0 \end{bmatrix}, \quad \lambda_0 \in \mathbb{C},$$

*and such a normal form is unique up to permutations of the blocks.*

The block diagonal matrices described in the theorem are called **Jordan canonical forms** (or **Jordan normal forms**). Their diagonal blocks are called **Jordan cells**.

It is instructive to analyze a Jordan canonical form before going into the proof of the theorem. The characteristic polynomial of a Jordan cell is  $(\lambda - \lambda_0)^m$  where  $m$  is the size of the cell. The characteristic polynomial of a block diagonal matrix is equal to the product of characteristic polynomials of the diagonal blocks. Therefore the characteristic polynomial of the whole Jordan canonical form is the product of factors  $(\lambda - \lambda_i)^{m_i}$ , one per Jordan cell. Thus the diagonal entries of Jordan cells are roots of the characteristic polynomial. After subtracting the scalar matrix  $\lambda_0 I$ , Jordan cells with  $\lambda_i = \lambda_0$  (and only these cells) become nilpotent. Therefore the root space  $\mathcal{W}_{\lambda_0}$  is exactly the direct sum of those subspaces on which the Jordan cells with  $\lambda_i = \lambda_0$  operate.

**Proof of Theorem.** Everything we need has been already established in the previous two subsections.

Thanks to the Fundamental Theorem of Algebra, the characteristic polynomial  $\det(\lambda I - A)$  of a complex  $n \times n$ -matrix  $A$  factor into the product of powers of distinct linear factors:  $(\lambda - \lambda_1)^{n_1} \dots (\lambda - \lambda_r)^{n_r}$ . According to Corollary 2 of Lemma, the space  $\mathbb{C}^n$  is decomposed in a canonical fashion into the direct sum  $\mathcal{W}_{\lambda_1} \oplus \dots \oplus \mathcal{W}_{\lambda_r}$  of  $A$ -invariant root subspaces. On each root subspace  $\mathcal{W}_{\lambda_i}$ , the operator  $A - \lambda_i I$  is nilpotent. According to Proposition, the root space  $\mathcal{W}_{\lambda_i}$  is represented (in a non-canonical fashion) as the direct sum of invariant subspaces on each of which  $A - \lambda_i I$  acts as a regular nilpotent. Since

the scalar operator  $\lambda_i I$  leaves every subspace invariant, this means that  $\mathcal{W}_{\lambda_i}$  is decomposed into the direct sum of  $A$ -invariant subspaces, on each of which  $A$  acts as a Jordan cell with the eigenvalue  $\lambda_0 = \lambda_i$ . Thus, existence of a basis in which  $A$  is described by a Jordan normal form is established.

To prove uniqueness, note that the root spaces  $\mathcal{W}_{\lambda_i}$  are intrinsically determined by the operator  $A$ , and the partition of  $\dim \mathcal{W}_{\lambda_i}$  into the sizes of Jordan cells with the eigenvalue  $\lambda_i$  is uniquely determined, according to Corollary 2 of Proposition, by the geometry of the operator  $A - \lambda_i I$  nilpotent on  $\mathcal{W}_{\lambda_i}$ . Therefore the exact structure of the Jordan normal form of  $A$  (i.e. the numbers and sizes of Jordan cells for each of the eigenvalues  $\lambda_i$ ) is uniquely determined by  $A$ , and only the ordering of the diagonal blocks remains ambiguous.  $\square$

**Corollary 1.** *Dimensions of root spaces  $\mathcal{W}_{\lambda_i}$  coincide with multiplicities of  $\lambda_i$  as roots of the characteristic polynomial.*

**Corollary 2.** *If the characteristic polynomial of a complex matrix has only simple roots, then the matrix is diagonalizable, i.e. is similar to a diagonal matrix.*

**Corollary 3.** *Every operator  $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$  in a suitable basis is described by the sum  $D + N$  of two commuting matrices, of which  $D$  is diagonal, and  $N$  strictly upper triangular.*

**Corollary 4.** *Every operator on a complex vector space of finite dimension can be represented as the sum  $D + N$  of two commuting operators, of which  $D$  is diagonalizable and  $N$  nilpotent.*

**Remark.** We used that  $\mathbb{K} = \mathbb{C}$  only to factor the characteristic polynomial of the matrix  $A$  into linear factors. Therefore the same results hold true over any field  $\mathbb{K}$  such that all non-constant polynomials from  $\mathbb{K}[\lambda]$  factor into linear factors. Such fields are called **algebraically closed**. In fact (see [8]) every field  $\mathbb{K}$  is contained in an algebraically closed field. Thus every linear operator  $A : \mathbb{K}^n \rightarrow \mathbb{K}^n$  can be brought to a Jordan normal form by transformations  $A \mapsto C^{-1}AC$ , where however entries of  $C$  and scalars  $\lambda_0$  in Jordan cells may belong to a larger field  $\mathbb{F} \supset \mathbb{K}$ .<sup>7</sup> We will see how this works when  $\mathbb{K} = \mathbb{R}$  and  $\mathbb{F} = \mathbb{C}$ .

---

<sup>7</sup>For this,  $\mathbb{F}$  does not have to be algebraically closed, but only needs to contain all roots of  $\det(\lambda I - A)$ .

## The Real Case

Let  $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  be an  $\mathbb{R}$ -linear operator. It acts<sup>8</sup> on the complexification  $\mathbb{C}^n$  of the real space, and commutes with the complex conjugation operator  $\sigma : \mathbf{x} + i\mathbf{y} \mapsto \mathbf{x} - i\mathbf{y}$ .

The characteristic polynomial  $\det(\lambda I - A)$  has real coefficients, but its roots  $\lambda_i$  can be either real or come in pair of complex conjugated roots (of the same multiplicity). Consequently, the complex root spaces  $\mathcal{W}_{\lambda_i}$ , which are defined as null spaces in  $\mathbb{C}^n$  of sufficiently high powers of  $A - \lambda_i I$ , come in two types. If  $\lambda_i$  is real, then the root space is *real* in the sense that it is  $\sigma$ -invariant, and thus is the complexification of the real root space  $\mathcal{W}_{\lambda_i} \cap \mathbb{R}^n$ . If  $\lambda_i$  is not real, and  $\bar{\lambda}_i$  is its complex conjugate, then  $\mathcal{W}_{\lambda_i}$  and  $\mathcal{W}_{\bar{\lambda}_i}$  are different root spaces of  $A$ , but they are transformed into each other by  $\sigma$ . Indeed,  $\sigma A = A\sigma$ , and  $\sigma\lambda_i = \bar{\lambda}_i\sigma$ . Therefore, if  $\mathbf{z} \in \mathcal{W}_{\lambda_i}$ , i.e.  $(A - \lambda_i I)^d \mathbf{z} = \mathbf{0}$  for some  $d$ , then  $\mathbf{0} = \sigma(A - \lambda_i I)^d \mathbf{z} = (A - \bar{\lambda}_i I)^d \sigma\mathbf{z}$ , and hence  $\sigma\mathbf{z} \in \mathcal{W}_{\bar{\lambda}_i}$ . This allows one to obtain the following improvement for the Jordan Canonical Form Theorem applied to real matrices.

**Theorem.** *A real linear operator  $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  can be represented by the matrix in a Jordan normal form with respect to a basis of the complexified space  $\mathbb{C}^n$  invariant under complex conjugation.*

**Proof.** In the process of construction bases in  $\mathcal{W}_{\lambda_i}$  in which  $A$  has a Jordan normal form, we can use the following procedure. When  $\lambda_i$  is real, we take the real root space  $\mathcal{W}_{\lambda_i} \cap \mathbb{R}^n$  and take in it a real basis in which the matrix of  $A - \lambda_i I$  is block diagonal with regular nilpotent blocks. This is possible due to Proposition applied to the case  $\mathbb{K} = \mathbb{R}$ . This real basis serves then as a  $\sigma$ -invariant complex basis in the complex root space  $\mathcal{W}_{\lambda_i}$ . When  $\mathcal{W}_{\lambda_i}$  and  $\mathcal{W}_{\bar{\lambda}_i}$  is a pair of complex conjugated root spaces, then we take a required basis in one of them, and then apply  $\sigma$  to obtain such a basis in the other. Taken together, the bases form a  $\sigma$ -invariant set of vectors.  $\square$

Of course, for each Jordan cell with a non-real eigenvalue  $\lambda_0$ , there is another Jordan cell of the same size with the eigenvalue  $\bar{\lambda}_0$ . Moreover, if  $\mathbf{e}_1, \dots, \mathbf{e}_m$  is the basis in the  $A$ -invariant subspace of the first cell, i.e.  $A\mathbf{e}_k = \lambda_0\mathbf{e}_k + \mathbf{e}_{k-1}$ ,  $k = 2, \dots, m$ , and  $A\mathbf{e}_1 = \lambda_0\mathbf{e}_1$ , then the  $A$ -invariant subspace corresponding to the other cell comes with the complex conjugate basis  $\bar{\mathbf{e}}_1, \dots, \bar{\mathbf{e}}_m$ , where  $\bar{\mathbf{e}}_k = \sigma\mathbf{e}_k$ . The direct sum  $\mathcal{U} := \text{Span}(\mathbf{e}_1, \dots, \mathbf{e}_m, \bar{\mathbf{e}}_1, \dots, \bar{\mathbf{e}}_m)$  of the two subspaces is

---

<sup>8</sup>Strictly speaking, it is the complexification  $A^{\mathbb{C}}$  of  $A$  that acts on  $\mathbb{C}^n = (\mathbb{R}^n)^{\mathbb{C}}$ , but we will denote it by the same letter  $A$ .

both  $A$ - and  $\sigma$ -invariant and thus is a complexification of the real  $A$ -invariant subspace  $\mathcal{U} \cap \mathbb{R}^n$ . We use this to describe a real normal form for the action of  $A$  on this subspace.

Namely, let  $\lambda_0 = \alpha - i\beta$ , and write each basis vector  $\mathbf{e}_k$  in terms of its real and imaginary part:  $\mathbf{e}_k = \mathbf{u}_k - i\mathbf{v}_k$ . Then the real vectors  $\mathbf{u}_k$  and  $\mathbf{v}_k$  form a real basis in the real part of the complex 2-dimensional space spanned by  $\mathbf{e}_k$  and  $\bar{\mathbf{e}}_k = \mathbf{u}_k + i\mathbf{v}_k$ . Thus, we obtain a basis  $\mathbf{u}_1, \mathbf{v}_1, \mathbf{u}_2, \mathbf{v}_2, \dots, \mathbf{u}_m, \mathbf{v}_m$  in the subspace  $\mathcal{U} \cap \mathbb{R}^n$ . The action of  $A$  on this basis is found from the formulas:

$$\begin{aligned} A\mathbf{u}_1 + iA\mathbf{v}_1 &= (\alpha - i\beta)(\mathbf{u}_1 + i\mathbf{v}_1) = (\alpha\mathbf{u}_1 + \beta\mathbf{v}_1) + i(-\beta\mathbf{u}_1 + \alpha\mathbf{v}_1), \\ A\mathbf{u}_k + iA\mathbf{v}_k &= (\alpha\mathbf{u}_k + \beta\mathbf{v}_k + \mathbf{u}_{k-1}) + i(-\beta\mathbf{u}_k + \alpha\mathbf{v}_k + \mathbf{v}_{k-1}), \quad k > 1. \end{aligned}$$

**Corollary 1.** *A linear operator  $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$  is represented in a suitable basis by a block diagonal matrix with the diagonal blocks that are either Jordan cells with real eigenvalues, or have the form ( $\beta \neq 0$ ):*

$$\begin{bmatrix} \alpha & -\beta & 1 & 0 & 0 & \dots & 0 & 0 \\ \beta & \alpha & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha & -\beta & 1 & 0 & \dots & 0 \\ 0 & 0 & \beta & \alpha & 0 & 1 & \dots & 0 \\ & & & & \dots & & & \\ 0 & & \dots & 0 & \alpha & -\beta & 1 & 0 \\ 0 & & \dots & 0 & \beta & \alpha & 0 & 1 \\ 0 & 0 & \dots & & 0 & 0 & \alpha & -\beta \\ 0 & 0 & \dots & & 0 & 0 & \beta & \alpha \end{bmatrix}.$$

**Corollary 2.** *If two real matrices are related by a complex similarity transformation, then they are related by a real similarity transformation.*

**Remark.** The proof meant here is that if two real matrices are similar over  $\mathbb{C}$  then they have the same Jordan normal form, and thus they are similar over  $\mathbb{R}$  to the same real matrix, as described in Corollary 1. However, Corollary 2 can be proved directly, without a reference to the Jordan Canonical Form Theorem. Namely, if two real matrices,  $A$  and  $A'$ , are related by a complex similarity transformation:  $A' = C^{-1}AC$ , we can rewrite this as  $CA' = AC$ , and taking  $C = B + iD$  where  $B$  and  $D$  are real, obtain:  $BA' = AB$  and  $DA' = AD$ . The problem now is that neither  $B$  nor  $D$  is guaranteed to be invertible. Yet, there must exist an invertible linear combination  $E = \lambda B + \mu D$ , for if the polynomial  $\det(\lambda B + \mu D)$  of  $\lambda$  and  $\mu$

vanishes identically, then  $\det(B + iD) = 0$  too. For invertible  $E$ , we have  $EA' = AE$  and hence  $A' = E^{-1}AE$ .

### EXERCISES

**298.** Let  $A, B : \mathcal{V} \rightarrow \mathcal{V}$  be two commuting linear operators, and  $p$  and  $q$  two polynomials in one variable. Show that the operators  $p(A)$  and  $q(B)$  commute.

**299.** Prove that if  $A$  commutes with  $B$ , then root spaces of  $A$  are  $B$ -invariant.

**300.** Let  $\lambda_0$  be a root of the characteristic polynomial of an operator  $A$ , and  $m$  its multiplicity. What are possible values for the dimension of the eigenspace corresponding to  $\lambda_0$ ?

**301.** Let  $\mathbf{v} \in \mathcal{V}$  be a non-zero vector, and  $\mathbf{a} : \mathcal{V} \rightarrow \mathbb{K}$  a non-zero linear function. Find eigenvalues and eigenspaces of the operator  $\mathbf{x} \mapsto \mathbf{a}(\mathbf{x})\mathbf{v}$ .

**302.** Let  $\mathcal{V}_n \subset \mathbb{K}[x]$  be the space of all polynomials of degree  $< n$ . Prove that the differentiation  $\frac{d}{dx} : \mathcal{V}_n \rightarrow \mathcal{V}_n$  is a regular nilpotent operator.

**303.** Prove that a square matrix satisfies its own characteristic equation; namely, if  $p$  denotes the characteristic polynomial of a matrix  $A$ , then  $p(A) = 0$ . (This identity is called the **Hamilton–Cayley equation**.)

**304.** Is there an  $n \times n$ -matrix  $A$  such that  $A^2 \neq 0$  but  $A^3 = 0$ : (a) if  $n = 2$ ? (b) if  $n = 3$ ?

**305.** Classify similarity classes of nilpotent  $4 \times 4$ -matrices.

**306.** Prove that the number of similarity classes of unipotent  $n \times n$ -matrices is equal to the number of partitions of  $n$ .

**307.** Find Jordan normal forms of the following matrices: ✓

$$(a) \begin{bmatrix} 1 & 2 & 0 \\ 0 & 2 & 0 \\ -2 & -2 & 1 \end{bmatrix}, \quad (b) \begin{bmatrix} 4 & 6 & 0 \\ -3 & -5 & 0 \\ -3 & -6 & 1 \end{bmatrix}, \quad (c) \begin{bmatrix} 13 & 16 & 16 \\ -5 & -7 & -6 \\ -6 & -8 & -7 \end{bmatrix},$$

$$(d) \begin{bmatrix} 3 & 0 & 8 \\ 3 & -1 & -6 \\ -2 & 0 & -5 \end{bmatrix}, \quad (e) \begin{bmatrix} -4 & 2 & 10 \\ -4 & 3 & 7 \\ -3 & 1 & 7 \end{bmatrix}, \quad (f) \begin{bmatrix} 7 & -12 & -2 \\ 3 & -4 & 0 \\ -2 & 0 & 2 \end{bmatrix},$$

$$(g) \begin{bmatrix} -2 & 8 & 6 \\ -4 & 10 & 6 \\ 4 & -8 & -4 \end{bmatrix}, \quad (h) \begin{bmatrix} 0 & 3 & 3 \\ -1 & 8 & 6 \\ 2 & -14 & -10 \end{bmatrix}, \quad (i) \begin{bmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{bmatrix},$$

$$(j) \begin{bmatrix} 1 & -1 & 2 \\ 3 & -3 & 6 \\ 2 & -2 & 4 \end{bmatrix}, \quad (k) \begin{bmatrix} -1 & 1 & 1 \\ -5 & 21 & 17 \\ 6 & -26 & -21 \end{bmatrix}, \quad (l) \begin{bmatrix} 3 & 7 & -3 \\ -2 & -5 & 2 \\ -4 & -10 & 3 \end{bmatrix},$$

$$(m) \begin{bmatrix} 8 & 30 & -14 \\ -6 & -19 & 9 \\ -6 & -23 & 11 \end{bmatrix}, \quad (n) \begin{bmatrix} 9 & 22 & -6 \\ -1 & -4 & 1 \\ 8 & 16 & -5 \end{bmatrix}, \quad (o) \begin{bmatrix} 4 & 5 & -2 \\ -2 & -2 & 1 \\ -1 & -1 & 1 \end{bmatrix}.$$



- 308.** Find all matrices commuting with a regular nilpotent.
- 309.** Compute powers of Jordan cells.  $\zeta$
- 310.** Prove that if some power of a complex matrix is the identity, then the matrix is diagonalizable.
- 311.** Prove that transposed square matrices are similar.
- 312.** Prove that  $\text{tr } A = \sum \lambda_i$  and  $\det A = \prod \lambda_i$ , where  $\lambda_1, \dots, \lambda_n$  are all roots of the characteristic polynomial (not necessarily distinct).
- 313.** Find complex eigenvectors and eigenvalues of rotations on the Euclidean plane.
- 314.** Classify all linear operators in  $\mathbb{R}^2$  up to linear changes of coordinates.
- 315.** Consider real traceless  $2 \times 2$ -matrices  $\begin{bmatrix} a & b \\ c & -a \end{bmatrix}$  as points in the 3-dimensional space with coordinates  $a, b, c$ . Sketch the partition of this space into similarity classes.



# Hints

8.  $\overrightarrow{AA'} = 3\overrightarrow{AM}/2$ .
14.  $\cos^2 \theta \leq 1$ .
19. Rotate the regular  $n$ -gon through  $2\pi/n$ .
22. Take  $X = A$  first.
23.  $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$ .
24. If  $a + b + c + d = 0$ , then  $2(b + c)(c + d) = a^2 - b^2 + c^2 - d^2$ .
25.  $XA^2 = |\overrightarrow{OX} - \overrightarrow{OA}|^2 = 2R^2 - 2\langle \overrightarrow{OX}, \overrightarrow{OA} \rangle$  if  $O$  is the center.
26. Consider projections of the vertices to any line.
27. Project faces to an arbitrary plane and compute signed areas.
28.  $Q(-x, -y) = Q(x, y)$  for a quadratic form  $Q$ .
31.  $AX^2 + CY^2$  is even in  $X$  and  $Y$ .
32.  $Q(-x, y) = Q(x, y)$  only if  $b = 0$ .
35.  $\cos \theta = 4/5$ .
38.  $x^2 + 4xy = (x + 2y)^2 - 4y^2$ .
42.  $e = |AB|/|AC|$  is the slope of the secting plane.
43. Show that the sum of distances to the foci of an ellipse from points on a tangent line is minimal at the tangency point; then reflect the source of light about the line.
52. Compute  $(\cos \theta + i \sin \theta)^3$ .
54. Divide  $P$  by  $z - z_0$  with a remainder.
57.  $(z - z_0)(z - \bar{z}_0)$  is real.
58. Apply Vieta's formula.
67. Draw the regions of the plane where the quadratic forms  $Q > 0$ .
70. First apply the Inertia Theorem to make  $Q = x_1^2 + x_2^2$ .
74. In each  $a^k b^{m-k}$ , each  $a$  comes from one of  $m$  factors  $(a + b)$ .
76. Take  $x_1 = x$ ,  $x_2 = \dot{x}$ .

- 80.**  $\frac{3n(n+1)}{2} - n^2 = \frac{n(n+3)}{2} > \frac{n^2}{2}$ .
- 83.** Write  $\mathbf{x} = \sum x_i \mathbf{e}_i$ .
- 94.** Pick two  $2 \times 2$ -matrices at random.
- 97.** Compute  $BAC$ , where  $B$  and  $C$  are two inverses of  $A$ .
- 98.** Compute  $(B^{-1}A^{-1})(AB)$  and  $(AB)(B^{-1}A^{-1})$ .
- 99.** Consider  $1 \times 2$  and  $2 \times 1$  matrices.
- 101.** Solve  $D^{-1}AC = I$  for  $D$  and  $C$ .
- 104.** Which  $2 \times 2$ -matrices are anti-symmetric?
- 109.** Start with any non-square matrix.
- 110.** Each elementary product contains a zero factor.
- 113.** There are 12 even and 12 odd permutations.
- 115.** Permutation  $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$  has length  $\binom{n}{2}$ .
- 117.** Pairs of indices inverted by  $\sigma$  and  $\sigma^{-1}$  are the same.
- 118.** The transformation: *logarithm*  $\rightarrow$  *lagorithm*  $\rightarrow$  *algorithm* consists of two transpositions.
- 123.**  $247 = 2 \cdot 100 + 4 \cdot 10 + 7$ .
- 127.**  $\det(-A) = (-1)^n \det A$ .
- 139.** Apply the 1st of the “cool formulas.”
- 140.** Compute the determinant of a  $4 \times 4$ -matrix the last two of whose rows repeat the first two.
- 141.** Apply Binet–Cauchy’s formula to the  $2 \times 3$  matrix whose rows are  $\mathbf{x}^t$  and  $\mathbf{y}^t$ .
- 142.** Show that  $\Delta_n = a_n \Delta_{n-1} + \Delta_{n-2}$ .
- 144.** Use the defining property of **Pascal’s triangle**:  $\binom{m}{k} = \binom{m-1}{k} + \binom{m-1}{k-1}$ .
- 145.** Use the fact of algebra that a polynomial in  $(x_1, \dots, x_n)$ , which vanishes when  $x_i = x_j$ , is divisible by  $x_i - x_j$ .
- 146.** Divide the  $k$ th column by  $k$  and apply Vandermonde’s identity.
- 147.** Redefine multiplication by scalars as  $\lambda \mathbf{u} = \mathbf{0}$  for all  $\lambda \in \mathbb{K}$  and all  $\mathbf{u} \in \mathcal{V}$ .
- 148.**  $0\mathbf{u} = (0+0)\mathbf{u} = 0\mathbf{u} + 0\mathbf{u}$ .
- 149.**  $(-1)\mathbf{u} + \mathbf{u} = (-1+1)\mathbf{u} = 0\mathbf{u} = \mathbf{0}$ .
- 150.** Use the Euclidean algorithm (see e.g. [3]) to show that for relatively prime  $k$  and  $p$ , the least positive integer of the form  $mk + np$  is equal to 1.
- 153.** There is no  $\mathbf{0}$  among polynomials of a fixed degree.
- 160.** To a linear form  $f : \mathcal{V}/\mathcal{W} \rightarrow \mathbb{K}$ , associate  $\mathcal{V} \xrightarrow{\pi} \mathcal{V}/\mathcal{W} \xrightarrow{f} \mathbb{K}$ .

- 162.** Given  $B : \mathcal{V} \rightarrow \mathcal{W}^*$ , show that evaluation  $(B\mathbf{v})(\mathbf{w})$  of the linear form  $B\mathbf{v} \in \mathcal{W}^*$  on  $\mathbf{w} \in \mathcal{W}$  defines a bilinear form.
- 164.** Translate given linear subspaces by any vector in the intersection of the affine ones.
- 166.** A linear function on  $\mathcal{V} \oplus \mathcal{W}$  is uniquely determined by its restrictions to  $\mathcal{V}$  and  $\mathcal{W}$ .
- 171.** Compute  $q_1 q_2 q_2^* q_1^*$ .
- 174.** Introduce multiplication by scalars  $q \in \mathbb{H}$  as  $A \mapsto q^* A$ .
- 176.**  $|q|^2 = |-1| = 1$ .
- 181.**  $\cos 4\theta + i \sin 4\theta = (\cos \theta + i \sin \theta)^4$ .
- 182.**  $H : \mathbb{R}^7 \rightarrow \mathbb{R}^1$ .
- 184.** The space spanned by columns of  $A$  and  $B$  contains columns of  $A+B$ .
- 188.**  $(A^t \mathbf{a})(\mathbf{x}) = \mathbf{a}(A\mathbf{x})$  for all  $\mathbf{x} \in \mathbb{K}^n$  and  $\mathbf{a} \in (\mathbb{K}^m)^*$ .
- 196.** Prove that in a finite field, multiples of 1 form a subfield isomorphic to  $\mathbb{Z}_p$  where  $p$  is a prime.
- 203.** Modify the Gaussian elimination algorithm of Section 2 by permuting unknowns (instead of equations).
- 204.** Apply the *LUP* decomposition to  $M^t$ .
- 205.** Apply *LPU*, *LUP*, and *PLU* decompositions to  $M^{-1}$ .
- 210.** When  $\mathbb{K}$  has  $q$  elements, each cell of dimension  $l$  has  $q^l$  elements.
- 214.** Consider the map  $\mathbb{R}^n \rightarrow \mathbb{R}^{p+q}$  defined by the linear forms.
- 227.**  $P = A + iB$  where both  $A$  and  $B$  are Hermitian.
- 228.**  $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^* \mathbf{y}$ .
- 230.**  $\langle \mathbf{z}, \mathbf{w} \rangle = \mathbf{z}^* \mathbf{w}$ .
- 231.** Use the previous exercise.
- 233.** The normal forms are:  $i|Z_1|^2 - i|Z_2|^2$ ,  $|Z_1|^2 - |Z_2|^2$ ,  $|Z_1|^2$ .
- 238.** Take the linear form for one of new coordinates.
- 240.** Prove that  $-1$  is a non-square.
- 243.** There are 1 even and 3 odd non-degenerate forms.
- 247.**  $\frac{1}{3} = 1 - \frac{2}{3}$ .
- 248.** Start with inverting 2-adic units  $\cdots * * * 1$ . (\* is a wild card).
- 250.** Use the previous exercise.
- 275.** Find an eigenvector, and show that its orthogonal complement is invariant.
- 277.** Compute  $\langle \mathbf{x}, A\mathbf{x} \rangle$  for  $\mathbf{x} = \sum t_i \mathbf{v}_i$ , where  $\{\mathbf{v}_i\}$  is an orthonormal basis of eigenvectors, and  $\sum t_i^2 = 1$ .
- 278.** If  $AB = BA$ , then eigenspaces of  $A$  are  $B$ -invariant.
- 293.** Use the previous exercise.

**309.** Use Newton's binomial formula.

# Answers

1.  $mg/2, mg\sqrt{3}/2$ .
2. 18 min (reloading time excluded).
6. It rotates with the same angular velocity along a circle centered at the barycenter of the triangle formed by the centers of the given circles.
10.  $3/4$ .
13.  $7\overrightarrow{OA} = \overrightarrow{OA'} + 2\overrightarrow{OB'} + 4\overrightarrow{OC'}$  for any  $O$ .
15.  $3/2$ .
17.  $2\langle \mathbf{u}, \mathbf{v} \rangle = |\mathbf{u} + \mathbf{v}|^2 - |\mathbf{u}|^2 - |\mathbf{v}|^2$ .
18. (b) No.
30. (a)  $\pm(\sqrt{\alpha^2 - \beta^2}, 0)$ , (b)  $\pm(\sqrt{\alpha^2 + \beta^2}, 0)$ .
33. Yes,  $k(x^2 + y^2)$ .
34.  $y = \pm x$ ; level curves of (a) are ellipses, of (c) hyperbolas.
35.  $2X^2 - Y^2 = 1$ .
38. 2nd ellipse, 1st & 4th hyperbolas.
39. A pair of intersecting lines,  $x - 1 = \pm(2y - 1)$ .
44. Yes; Yes (0); Yes.
45. (a)  $\frac{1+5i}{13}$ ; (b)  $\frac{1-i\sqrt{3}}{2}$ .
47.  $|z|^{-2}$ .
48.  $\pm i\sqrt{3}$ .
50. (a)  $\sqrt{2}, -\pi/4$ ; (b)  $2, -\pi/3$ .
51.  $\frac{-1+i\sqrt{3}}{2}$ .
55.  $2 \pm i$ ;  $i\frac{1\pm\sqrt{5}}{2}$ ;  $1 + i, 1 + i$ ;  $1 \pm \frac{\sqrt{6-i\sqrt{2}}}{2}$ .
56.  $-2, 1 \pm i\sqrt{3}; i, \frac{\pm\sqrt{3}-i}{2}; \pm i\sqrt{2}, \pm i\sqrt{2}; \frac{\sqrt{3}\pm i}{2}, \frac{\sqrt{3}\pm i}{2}; \pm i, \pm \frac{\sqrt{3}\pm i}{2}$ .
59.  $a_k = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n} z_{i_1} \cdots z_{i_k}$ .
60. For normal forms,  $y^2$  and 0 can be taken.

63. Yes, some non-equivalent equations represent the empty set.  
 65.  $m = n = r = 2$ .  
 69.  $n(n+1)$ .  
 71. The ODEs  $\dot{x} = ax$  and  $\dot{x} = a'x$  are non-equivalent whenever  $a \neq a'$ .  
 77.  $\dot{X}_1 = iX_1$ ,  $\dot{X}_2 = -iX_2$ .  
 78.  $x_1 = c_1e^{\lambda t}$ ,  $x_2 = c_2e^{\lambda t}$ , and  $y_1 = (c_1 + c_2t)e^{\lambda t}$ ,  $y_2 = c_2e^{\lambda t}$ .  
 79.  $\frac{n(n+1)}{2}$ .  
 81. yes, no, no, yes, no, yes, yes, no.  
 84.  $E = \mathbf{va}$ , i.e.  $e_{ij} = v_i a_j$ ,  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ .

85. 
$$\begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}.$$

86. Check your answers using associativity, e.g.  $(CB)A = C(BA)$ .

Other answers:  $BAC = \begin{bmatrix} 3 & 1 \\ 3 & 3 \end{bmatrix}$ ,  $ACB = \begin{bmatrix} 0 & -2 \\ 3 & 6 \end{bmatrix}$ .

91. 
$$\begin{bmatrix} \cos 1^\circ & -\sin 1^\circ \\ \sin 1^\circ & \cos 1^\circ \end{bmatrix}.$$

92. If  $B = A^k$ , then  $b_{i,i+k} = 1$ , and all other  $b_{ij} = 0$ .  
 93. (a) If  $A$  is  $m \times n$ ,  $B$  must be  $n \times m$ . (b) Both must be  $n \times n$ .  
 95. Exactly when  $AB = BA$ .  
 96. Those with all  $a_{ii} \neq 0$ .  
 102. No; yes (of  $x, y \in \mathbb{R}^1$ ); yes (in  $\mathbb{R}^2$ ).  
 103.  $I$ .  
 105.  $S = 2x_1y_1 + x_1y_2 + x_2y_1$ ,  $A = x_1y_2 - x_2y_1$ .  
 106.  $(\sum x_i)(\sum y_i)$  and  $\sum_{i \neq j} x_i y_j / 2$ .  
 107. No, only if  $AB = BA$ .  
 111.  $1; 1; \cos(\mathbf{x} + \mathbf{y})$ .  
 112.  $2, 1; -2$ .  
 114.  $k(k-1)/2$ .  
 116.  $n(n-1)/2 - l$ .  
 119. E.g.  $\tau_{14}\tau_{34}\tau_{25}$ .  
 120. No; yes.  
 121.  $+$  (6 inverted pairs);  $+$  (8 inverted pairs).  
 122.  $-1\ 522\ 200; -29\ 400\ 000$ .  
 124.  $0$ .  
 125. Changes sign, if  $n = 4k + 2$  for some  $k$ , and remains unchanged otherwise.



126.  $x = a_1, \dots, a_n$ .

128. Leave it unchanged.

131. (a)  $(-1)^{n(n-1)/2} a_1 a_2 \cdots a_n$ , (b)  $(ad - bc)(eh - fg)$ .

132. (a) 9, (b) 5.

133. (a)  $\begin{bmatrix} -\frac{5}{18} & \frac{7}{18} & \frac{1}{18} \\ \frac{1}{18} & -\frac{5}{18} & \frac{7}{18} \\ \frac{7}{18} & \frac{1}{18} & -\frac{5}{18} \end{bmatrix}$ , (b)  $\begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix}$ .

134. (a)  $\mathbf{x} = [-\frac{2}{9}, \frac{1}{3}, \frac{1}{9}]^t$ , (b)  $\mathbf{x} = [1, -1, 1]^t$ .

136.  $(\det A)^{n-1}$ , where  $n$  is the size of  $A$ .

137. Those with determinants  $\pm 1$ .

138. (a)  $x_1 = 3, x_2 = x_3 = 1$ , (b)  $x_1 = 3, x_2 = 4, x_3 = 5$ .

139. (a)  $-x_1^2 - \cdots - x_n^2$ , (b)  $(ad - bc)^3$ .

143.  $\lambda^n + a_1 \lambda^{n-1} + \cdots + a_{n-1} \lambda + a_n$ .

144. 1.

146.  $1!3!5! \cdots (2n-1)!$ .

152.  $p^n; p^{mn}$ .

155.  $p^{n(n-1)/2}$ .

157.  $\text{Ker } D = \mathbb{K}[x^p] \subset \mathbb{K}[x]$ .

163. Points, lines, and planes.

168.  $\text{Ker } A^t = A(\mathcal{V})^\perp$ ,  $A^t(\mathcal{W}^*) = (\mathcal{V}/\text{Ker } A)^* \subset \mathcal{V}^*$ .

170.  $-1; -q$ .

175.  $\begin{bmatrix} z & -\bar{w} \\ w & \bar{z} \end{bmatrix}$ .

176.  $\{bi + cj + dk \mid b^2 + c^2 + d^2 = 1\}$ .

178. 2.

179. 2, if  $n > 1$ .

180.  $x^k = x_1^k L_1(x) + \cdots + x_n^k L_n(x)$ ,  $k = 0, \dots, n-1$ .

182. 1.

185. The system is consistent whenever  $b_1 + b_2 + b_3 = 0$ .

187. (a) Yes, (b) yes, (c) yes, (d) no, (e) yes, (f) no, (g) no, (h) yes.

191.  $0 \leq \text{codim} \leq k$ .

193. Two subspaces are equivalent if and only if they have the same dimension.

194. The equivalence class of an ordered pair  $\mathcal{U}, \mathcal{V}$  of subspaces is determined by  $k := \dim U$ ,  $l := \dim \mathcal{V}$ , and  $r := \dim(\mathcal{U} + \mathcal{V})$ , where  $k, l \leq r \leq n$  can be arbitrary.

- 195.** (a)  $q^n$ ; (b)  $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ ;  
 (c)  $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{r-1})$ ;  
 (d)  $(q^n - 1)(q^n - q) \cdots (q^n - q^{r-1}) / (q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})$ .

**197.**  $x_1 = 3, x_2 = 1, x_3 = 1$ ; inconsistent;  $x_1 = 1, x_2 = 2, x_3 = -2$ ;  
 $x_1 = 2t_1 - t_2, x_2 = t_1, x_3 = t_2, x_4 = 1$ ;

$x_1 = -8, x_2 = 3 + t, x_3 = 6 + 2t, x_4 = t$ ;  $x_1 = x_2 = x_3 = x_4 = 0$ ;  
 $x_1 = \frac{3}{17}t_1 - \frac{13}{17}t_2, x_2 = \frac{19}{17}t_1 - \frac{29}{17}t_2, x_3 = t_1, x_4 = t_2$ ;

$x_1 = -16 + t_1 + t_2 + 5t_3, x_2 = 23 - 2t_1 - 2t_2 - 6t_3, x_3 = t_1, x_4 = t_2, x_5 = t_3$ .

**198.**  $\lambda = 5$ .

**199.** (a)  $\text{rk} = 2$ , (b)  $\text{rk} = 2$ , (c)  $\text{rk} = 3$ , (d)  $\text{rk} = 4$ , (e)  $\text{rk} = 2$ .

**200.** Inverse matrices are:

$$\begin{bmatrix} 1 & -4 & -3 \\ 1 & -5 & -3 \\ -1 & 6 & 4 \end{bmatrix}, \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & -1 & 0 & 0 \\ -3 & 2 & 0 & 0 \\ 31 & -19 & 3 & -4 \\ -23 & 14 & -2 & 3 \end{bmatrix}.$$

**208.**  $\binom{n}{2} - l(\sigma)$ , where  $l(\sigma)$  is the length of the permutation.

**209.**  $[n]_q! := [1]_q[2]_q \cdots [n]_q$  (called **q-factorial**), where  $[k]_q := \frac{q^k - 1}{q - 1}$ .

**211.** Inertia indices  $(p, q) = (1, 1), (2, 0), (1, 2)$ .

**216.** Empty for  $p = 0$ , has 2 components for  $p = 1$ , and 1 for  $p = 2, 3, 4$ .

**220.**  $z_1^2 + z_2^2 = 1, z_1^2 + z_2^2 = 0, z_2 = z_1^2, z_1^2 = 1, z_1^2 = 0$ .

**221.** Two parallel lines.

**226.** Those all of whose entries are imaginary.

**227.**  $P(\mathbf{z}, \mathbf{w}) =$

$$\frac{1}{2} [P(\mathbf{z} + \mathbf{w}, \mathbf{z} + \mathbf{w}) + iP(i\mathbf{z} + \mathbf{w}, i\mathbf{z} + \mathbf{w}) - (1 + i)(P(\mathbf{z}, \mathbf{z}) + P(\mathbf{w}, \mathbf{w}))].$$

**234.**  $d_{ii} = \Delta_i / \Delta_{i-1}$ .

**235.**  $(p, q) = (2, 2), (3, 1)$ .

**253.** No.

**254.** The sum of the squares of all sides of a parallelogram is equal to the sum of the squares of the diagonals.

**265.** id.

$$\mathbf{307.} \text{ (a) } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix} \text{ (b) } \begin{bmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ (c) } \begin{bmatrix} -3 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{ (e) } \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix} \text{ (f) } \begin{bmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ (k) } \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \text{ (l) } \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix}.$$

# Bibliography

- [1]
- [2] D. K. Faddeev, I. S. Sominsky. *Problems in Linear Algebra*. 8th edition, Nauka, Moscow, 1964 (in Russian).
- [3] A. P. Kiselev. *Kiselev's Geometry / Book I. Planimetry*. Adapted from Russian by Alexander Givental. Sumizdat, El Cerrito, 2006.
- [4] A. P. Kiselev. *Kiselev's Geometry / Book II. Stereometry*. Adapted from Russian by Alexander Givental. Sumizdat, El Cerrito, 2008.
- [5] J.-P. Serre. *A Course in Arithmetic*.
- [6] Ronald Solomon. *Abstract Algebra*. Thomson — Brooks/Cole, Belmont, CA, 2002.
- [7] Berezin
- [8] Van der Waerden
- [9] Hermann Weyl. *Space. Time. Matter*.

# Index

- absolute value, 18, 67
- addition of vectors, 59
- additivity, 5
- adjoint linear map, 119
- adjoint map, 70, 78
- adjoint matrix, 50
- adjoint quaternion, 67
- adjoint systems, 82
- affine subspace, 65
- algebraic number, 60
- algebraically closed field, 143
- annihilator, 69
- anti-Hermitian form, 105
- anti-Hermitian matrix, 103
- anti-symmetric form, 37
- anti-symmetric operator, 129
- antilinear function, 103
- argument of complex number, 19
- associative, 34
- associativity, 2
- augmented matrix, 84
- axiom, 59
- axis of symmetry, 14
  
- Bézout, 22
- Bézout's theorem, 22
- back substitution, 84
- barycenter, 7
- basis, 3, 71
- bijective, 63
- bilinear form, 36
- bilinearity, 5
- Binet, 54
- Binet–Cauchy formula, 54
- binomial coefficient, 30
- binomial formula, 30
- block, 46
- block triangular matrix, 46
  
- Bruhat cell, 94
  
- canonical form, 24
- canonical projection, 65
- Cartesian coordinates, 6
- Cartesian product, 62
- category of vector spaces, 62
- Cauchy, 54
- Cauchy – Schwarz inequality, 8, 117
- Cauchy's interlacing theorem, 133
- Cayley transform, 134
- change of coordinates, 34
- characteristic equation, 121
- characteristic polynomial, 137
- Chebyshev, 75
- Chebyshev polynomials, 75
- classification theorem, 24
- codimension, 80
- cofactor, 49
- cofactor expansion, 49, 52
- column space, 86
- commutative square, 78
- commutativity, 2
- commutator, 114
- complementary multi-index, 52
- complete flag, 92
- completing squares, 12
- complex conjugate, 17
- complex conjugation, 126
- complex multiplication, 130
- complex sphere, 102
- complex vector space, 60
- complexification, 126
- composition, 33
- conic section, 9
- conics, 100
- conjugate quaternion, 67
- coordinate Euclidean space, 128

- coordinate flag, 92
- coordinate quaternionic space, 68
- coordinate space, 32
- coordinate system, 3
- coordinate vector, 32
- coordinates, 3, 73
- Cramer's rule, 51
- cross product, 58
- cylinder, 100
  
- Dandelin, 10
- Dandelin's spheres, 9
- Darboux, 111
- Darboux basis, 111
- Descartes, 6
- determinant, 28, 41
- diagonal, 39
- diagonalizable matrix, 143
- differentiation, 63
- dimension, 72
- dimension of Bruhat cell, 95
- direct sum, 65
- directed segment, 1
- directrix, 15
- discriminant, 20, 116
- distance, 117
- distributive law, 18, 32
- distributivity, 2
- dot product, 5, 36
- dual basis, 74
- dual map, 70
- dual space, 63
  
- eccentricity, 15
- eigenspace, 121, 137
- eigenvalue, 26, 120, 137
- eigenvector, 120, 137
- elementary product, 41
- elementary row operations, 83
- ellipse, 10
- ellipsoid, 133
- equivalent, 23
- equivalent conics, 100
- equivalent linear maps, 78
- Euclidean inner product, 127
- Euclidean space, 127
- Euclidean structure, 127
- evaluation, 32
- evaluation map, 63
- even form, 110
- even permutation, 42
  
- field, 18, 60
- field extension, 64
- field of  $p$ -adic numbers, 113
- finite dimensional spaces, 72
- flag, 92
- focus of ellipse, 10
- focus of hyperbola, 14
- focus of parabola, 15
  
- Gaussian elimination, 83
- Gelfand's problem, 136
- Gram matrix, 134
- Gram–Schmidt process, 107, 118
- graph, 65
  
- Hamilton–Cayley equation, 146
- Hasse, 113
- head, 1
- Hermite, 103
- Hermite polynomials, 75
- Hermitian adjoint, 103, 119
- Hermitian adjoint matrix, 103
- Hermitian anti-symmetric form, 103
- Hermitian dot product, 104
- Hermitian form, 103
- Hermitian inner product, 117
- Hermitian isomorphic, 118
- Hermitian matrix, 103
- Hermitian quadratic form, 103
- Hermitian space., 117
- Hermitian symmetric form, 103
- Hilbert space, 117
- Hirani, 15
- homogeneity, 5
- homogeneous system, 80
- homomorphism, 63
- homomorphism theorem, 66
- hyperbola, 10
- hyperplane, 82
- hypersurface, 100
  
- identity matrix, 34
- identity permutation, 42
- imaginary part, 17
- imaginary unit, 17

- inconsistent system, 85
- indices in inversion, 42
- induction hypothesis, 73
- inertia index, 99
- injective, 62
- inner product, 5
- invariant subspace, 121
- inverse matrix, 35
- inverse quaternion, 68
- inverse transformation, 35
- inversion of indices, 42
- involution, 126
- isometric Hermitian spaces, 118
- isomorphic spaces, 63
- isomorphism, 63
  
- Jordan canonical form, 142
- Jordan cell, 27, 142
- Jordan normal form, 142
- Jordan system, 27
  
- kernel, 62
- kernel of form, 100, 114
  
- Lagrange, 52
- Lagrange polynomials, 75
- Lagrange's formula, 52
- law of cosines, 6
- LDU decomposition, 91
- leading coefficient, 84
- leading entry, 84
- leading minors, 106
- left inverse, 82
- left kernel, 69
- left singular vector, 125
- left vector space, 68
- length, 117
- length of permutation, 42
- linear combination, 2
- linear form, 32, 63
- linear function, 32, 63
- linear map, 33, 62
- linear subspace, 61
- linear transformation, 35
- linearity, 32
- linearly dependent, 72
- linearly independent, 71
- Linnaeus, 23
  
- lower triangular, 38, 89
- LPU decomposition, 89
- LU decomposition, 91
- LUP decomposition, 95
  
- Möbius band, 75
- mathematical induction, 73
- matrix, 31
- matrix entry, 31
- matrix product, 32, 33
- metric space, 117
- Minkowski, 113
- Minkowski–Hasse theorem, 113
- minor, 49, 52
- multi-index, 52
- multiplication by scalar, 2
- multiplication by scalars, 59
- multiplicative, 18
- multiplicity, 20
  
- nilpotent operator, 139
- non-degenerate Hermitian form, 106
- non-negative form, 125
- nontrivial linear combination, 72
- norm of quaternion, 67
- normal form, 24
- normal operator, 119, 129
- null space, 62, 86
  
- odd form, 110
- odd permutation, 42
- opposite coordinate flag, 93
- opposite vector, 59
- orthogonal, 118
- orthogonal basis, 97
- orthogonal complement, 121
- orthogonal diagonalization, 124
- orthogonal projection, 134
- orthogonal projector, 134
- orthogonal transformation, 128
- orthogonal vectors, 6
- orthonormal basis, 107, 118, 127
  
- parabola, 13
- partition, 141
- Pascal's triangle, 150
- permutation, 41
- permutation matrix, 89
- pivot, 84

- Plücker, 57  
Plücker identity, 57  
PLU decomposition, 95  
polar, 19  
polar decomposition, 136  
positive definite, 98  
positive Hermitian form, 104  
positive operator, 135  
positivity, 5  
power of matrix, 39  
principal axes, 14, 133  
principal minor, 113  
projection, 118  
Pythagorean theorem, 6
- q-factorial, 95, 156  
quadratic curve, 9  
quadratic form, 11, 25, 37  
quadratic formula, 20  
quaternions, 67  
quotient space, 65
- range, 62  
rank, 25, 76  
rank of linear system, 80  
rank of matrix, 77  
real part, 17  
real spectral theorem, 129  
real vector space, 60  
realification, 126  
reduced row echelon form, 84  
regular nilpotent, 139  
right inverse, 82  
right kernel, 69  
right singular vector, 125  
right vector space, 68  
ring, 31  
root of unity, 21  
root space, 138  
row echelon form, 84  
row echelon form of rank  $r$ , 84  
row space, 86
- scalar, 59, 60  
scalar product, 5  
semiaxes, 133  
semiaxis of ellipse, 13  
semilinear function, 103  
sesquilinear form, 102  
sign of permutation, 41  
similarity, 137  
similarity transformation, 35  
simple problems, 29  
singular value, 125  
singular value decomposition, 125  
skew-symmetric, 67  
span, 71  
spectral theorem, 120  
spectrum, 26, 132  
square matrix, 34  
square root, 21, 135  
standard basis, 33, 71  
standard coordinate flag, 92  
surjective, 63  
Sylvester, 106  
symmetric bilinear form, 37  
symmetric matrix, 38  
symmetric operator, 129  
symmetry, 5  
system of linear equations, 38
- tail, 1  
total anti-symmetry, 44  
transition matrix, 35  
transposed bilinear form, 36  
transposed partition, 141  
transposition, 36  
transposition matrix, 89  
transposition permutation, 42  
triangle inequality, 8, 117
- unipotent matrix, 91  
unit vector, 5  
unitary rotation, 123  
unitary space, 117  
unitary transformation, 119  
upper triangular, 38, 89
- Vandermonde, 58  
Vandermonde's identity, 58  
vector, 1, 59  
vector space, 28, 59  
vector sum, 2  
Vieta, 22  
Vieta's theorem, 22
- Young tableaux, 141

zero vector, 2, 59