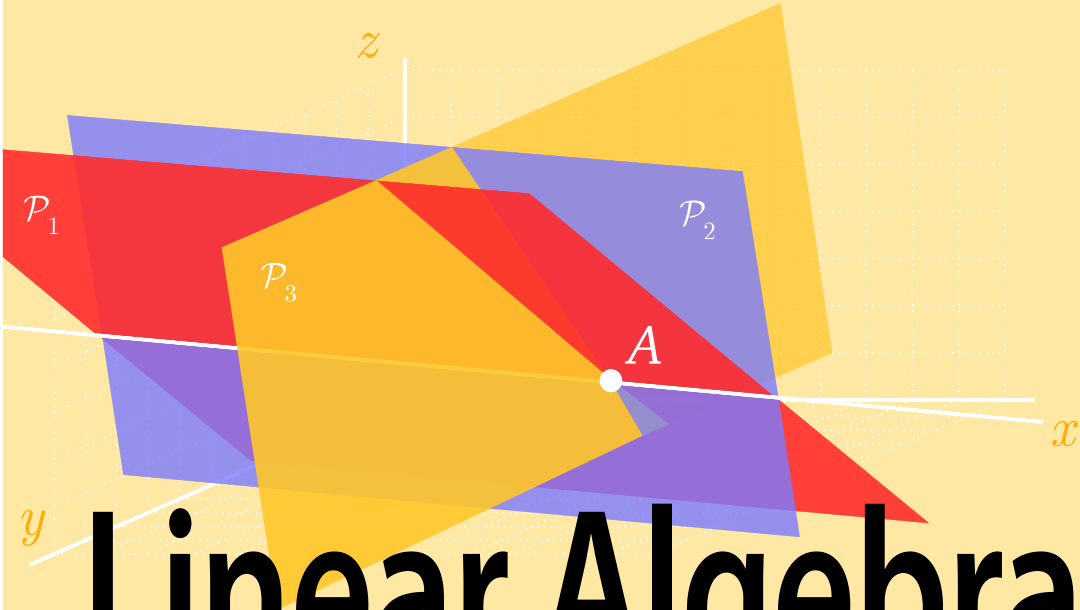
Linear Algebra, Theory and Algorithms



Linear Algebra

Theory and Algorithms

A Teaching Instrument for My Students

By V. Mikaelian

- *Lecture Notes,*
- *Algorithms with Examples,*
- *Exercises and Quizzes with Solutions*
- *Video Lectures*

Edition of 2021

Download at: bit.ly/LAdownload

Linear Algebra, Theory and Algorithms. By V. Mikaelian.
Edition of July 15, 2021.

Contents

Introduction

"Un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté."
Évariste Galois

These notes are a *teaching instrument* based on more than 15 years of experience in lecturing linear algebra. I recorded them bearing *three main objectives* in mind:

1. My course needed a *very clear* introduction to modern linear algebra, in which each concept is explained in detail, and is illustrated by *examples* to be as understandable to students as possible. An average student should understand the material with only minimal help from my side.[1]
2. Since linear algebra is one of the most applicable areas of mathematics, special attention need be paid to *algorithms* and *problem solving* techniques.[2]
3. *Reasonable balance* for the amount of abstract algebra evolved in a linear algebra introduction[3] need be found, and the *theoretical background* of the presented methods need be fully revealed.[4]

A general outline: Part 1 starts with examples of real, rational, complex and modular spaces to prepare the student for the general concepts of field F, and of space F^n over F. Some elements of analytic geometry in $\mathbb{R}^2$ and $\mathbb{R}^3$ are used to practice with vectors and operations on them. This part can well be omitted by students familiar with vectors, fields and their basic properties.

[1] I am aware that certain explanations may be too detailed, and certain examples may be too evident for some students. This typically means that something caused questions by my students in past years, and I re-wrote those parts to answer all questions in detail.

[2] Having students from different departments, such as computer science, mathematics, engineering, business, etc., I know that their priorities may be different.

[3] To show what I mean under *reasonable balance*, let me explain how the important algebraic notion of *field* is covered. In the past I came across students who learned linear algebra *over real numbers* $\mathbb{R}$ *only*, and years later for some applications they discovered that there are matrices, linear equations, eigenvectors over $\mathbb{Z}_p$ or over $\mathbb{C}$, as well. Most of the fundamental consteps in linear algebra, such as the systems of linear equations, elementary operations, matrices, reduced row-echelon forms, determinants, transformations, eigenvectors, etc..., live over any field, and it is *not* reasonable to teach them over $\mathbb{R}$ only, hoping that the students will learn their analogs for, say $\mathbb{Z}_p$, somewhere in the future in a programming-related course or in Wikipedia. On the other hand, evolving elements of fields theory, such as characteristics of fields, extensions, etc., would make the entrance to linear algebra too heavy for freshman students, especially for those outside pure mathematics. In order to achieve *reasonable balance* between these two trends, this course covers the linear algebra material focusing on the "most popular" fields $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$ mainly. Definition of abstract field F is given, but the text is not assuming that a student necessarily remembers all nine points of that definition, see Agreement 4.3 below.

[4] I believe that clearness and transparency cannot be achieved, if the full *logic* and *beauty* of the mathematical theory are sacrificed for the sake of "simplicity". Thirst for oversimplification sometimes turns the linear algebra texts to parodies of linear algebra. See Évariste Galois quote in the epigraph above.

Then in Part 2 and Part 3 the systems of linear equations and matrices are discussed on general fields. Gaussian row-elimination, row-echelon form and the reduced row-echelon form, factorization of matrices into elementary matrices are the main study tools in these parts.

The accumulated material on fields, vectors, matrices, polynomials, etc., allows to define abstract vector spaces in Part 4. Bases and dimension of spaces, coordinate systems, change of basis in spaces are introduced. Then a series of computational methods are offered in Part 5.

Part 6 is an introduction to determinants and their basic applications. The determinants earlier used to be central technical tools to study almost all other concepts of linear algebra. But later introduction of more efficient methods shifted attention away from determinants.[5]

Part 7 introduces linear transformations and related objects, such as kernel and range of transformations, operations with transformations, etc.

Study of transformations is continued in Part 8 using eigenvalues and eigenvectors. Diagonalization, invariant subspace, the Jordan normal form are considered.

Part 9 is dedicated to inner product spaces and orthogonality. Orthogonal and symmetric transformations, the Spectral Theorem, the orthogonal diagonalization are discussed.

Structure of the text: In each chapter the theory is followed by algorithms to accomplish certain types of tasks. The theory and the algorithms[6] are illustrated by many examples. As my experience shows, these examples very much help the students to undersad the topic. Besides, there are a few optional sections highlighted as "Applications".

Each chapter is concluded by *Exercises* section. These exercises mostly are from homeworks of the past years. *Solutions and hints* to selected exercises of each chapter can be found on page 325.

The *Syllabus* of the Linear Algebra 104 course can be found on page 11. Not all the sections of these lecture notes are included in the actually taught course, and in the included sections not all parts are mandatory.[7]

The *quizzes* I offered during the courses in 2017–2019 are given on page 307. The full solutions to all quizzes are provided.

The most up-to-date version of these lecture notes and some other related material can be downloaded from the online drive at: `bit.ly/LAdownload`

To submit your *feedback* please go: `bit.ly/LAfback`

I thank fortune for bringing me to the problems I describe here.[8]

V. Mikaelian, 2016–2021

---

[5]As a student I was taught linear algebra over $\mathbb{R}$ mainly, starting the study by determinants. Then the determinants were used, say, to solve systems of linear equations, to compute the inverse matrices (which are too inefficient methods as Remark 19.2 and Remark 19.7 stress), or to study linear dependence (which is too unnatural, as linear independence of vectors, say, $v_1 = (2,4,1)$, $v_2 = (0,3,2)$, $v_3 = (0,0,5)$ naturally follows from definitions of independence, and there is no need to sail to the combinatorial concept of the determinant $D = \begin{vmatrix} 2&4&1\\0&3&2\\0&0&5 \end{vmatrix} = 2\cdot 3\cdot 5 = 30$ in order to deduce the same fact from inequality $30 \neq 0$). Saying this, I also do *not* follow the modern fashion of "irrational fear of determinants" which intentionally avoids any usage of determinants, as it is done in some sources in recent decades.

[6]The algorithms are highlighted in the table of Contents, so that one can easily find the specific algorithm.

[7]So following the Syllabus will help the students to get closer correlation with actual lectures.

[8]This sentence is borrowed from B.I. Plotkin's *"Seven Lectures on the Universal Algebraic Geometry"*.

The Linear Algebra Course Syllabus

Linear Algebra 104 course covers most part of the current lecture notes. This detailed Syllabus will help you to identify those chapters and sections which actually are in the course. The Syllabus is separated to 15 weeks, and videos for each section are mentioned within respective week.

Week 1

1. The Pyramid of Linear Algebra.
Video: VidIntroduction 1, VidIntroduction 2, VidIntroduction 3.

1. Introduction to Vectors, Spaces and Fields

2. Vectors in real spaces $\mathbb{R}^2$, $\mathbb{R}^3$, $\mathbb{R}^n$. Operations with vectors. The main algebraic properties of real spaces. The rational space $\mathbb{Q}^n$.
Reading: Sections 1.1, 1.2.
Video: VidSection 01.1, VidSection 01.2.

3. The dot product in $\mathbb{R}^n$. Norm of the vectors and angle between vectors. Cauchy-Schwarz inequality. Triangle inequality. Pythagoras Theorem. Projections of vectors.
Reading: Section 1.3.
Video: VidSection 01.3.a, VidSection 01.3.b.

Week 2

4. Lines in the space $\mathbb{R}^2$. The vector, parametric, normal, general forms of lines in $\mathbb{R}^2$ (Example 2.4 is optional).
Reading: Section 2.1.
Video: VidSection 02.1.a, VidSection 02.1.b.

5. Planes in the space $\mathbb{R}^3$. The vector, parametric, normal, general forms of planes in $\mathbb{R}^3$. The cross product. Lines in the space $\mathbb{R}^3$. The vector, parametric, normal, general forms of lines (examples 2.8, 2.9, 2.11 are optional).
Reading: Section 2.2.
Video: VidSection 02.2.a, VidSection 02.2.b, VidSection 02.2.c.

6. Introduction to complex numbers.
Reading: Appendices C.1, C.2.
Video: VidAppendix C.1.a, VidAppendix C.1.b, VidAppendix C.1.c.

Week 3

7. The complex space $\mathbb{C}^n$. The main algebraic properties of complex spaces.
Reading: Section 3.1.
Video: VidSection 03.1.

8. Modular arithmetic.
Reading: *Appendices B.1, B.2* (may be covered in Discrete Mathematics course already).

9. The finite modular space $\mathbb{Z}_p^n$. The main algebraic properties of modular spaces.
Reading: Section 3.2.
Video: VidSection 03.2.a, VidSection 03.2.b.

10. Definition of field. The space F^n over the field F. The main algebraic properties of the space F^n. The "first step of abstraction".
Reading: Sections 4.1, 4.2.
Video: VidSection 04.1, VidSection 04.2.

2. Systems of Linear Equations

11. Systems of linear equations and their solutions. Geometrical interpretation.
Reading: Section 5.1.
Video: VidSection 05.1.

WEEK 4

12. Elementary operations with systems of linear equations. First examples of consistent and inconsistent systems.
Reading: Section 5.2.
Video: VidSection 05.2.a, VidSection 05.2.b.

13. Matrices over fields.
Reading: Section 6.1.
Video: VidSection 06.1.

14. Elementary operations with matrices. Writing the elimination process by matrices. The row-equivalence of matrices.
Reading: Section 6.2.
Video: VidSection 06.2.

15. The row-echelon form of matrices. Bringing a matrix to a row-echelon form.
Reading: Section 6.3.
Video: VidSection 06.3.a, VidSection 06.3.b.

16. Solving the system of linear equations by the basic method. The homogeneous systems.
Reading: Section 7.1.
Video: VidSection 07.1.a VidSection 07.1.b.

WEEK 5

17. The reduced row-echelon form of a matrix. Bringing a matrix to the reduced row-echelon form.
Reading: Section 7.2 (the first half).
Video: VidSection 07.2.a.

18. Solving the system of linear equations by the Gauss-Jordan method.
Reading: Section 7.2 (the second half).
Video: VidSection 07.2.b.

19. Uniqueness of the reduced row-echelon form (proof of Theorem 7.13 is optional). Rank of a matrix.
Reading: Section 7.3.
Video: VidSection 07.3.a, VidSection 07.3.b.

3. Matrix Algebra

20. Matrix addition and multiplication. The main algebraic properties of addition of matrices, of multiplication of a matrix by a scalar, and of multiplication of matrices.
Reading: Section 8.1.
Video: VidSection 08.1.a, VidSection 08.1.b.

21. The transposed matrix.
Reading: Section 8.2 (the first half).
Video: VidSection 08.2.a.

22. The inverse matrix.
Reading: Section 8.2 (the second half).
Video: VidSection 08.2.b.

WEEK 6

23. Interpretation of systems of linear equations and of elementary operations by matrices. The single matrix representing the elimination process.
Reading: Section 9.1.
Video: VidSection 09.1.a, VidSection 09.1.b.

24. The equivalent conditions for invertible matrices.
Reading: Section 9.2.
Video: VidSection 09.2.

25. Computing the inverse matrix by Gauss-Jordan method.
Reading: Section 9.3.
Video: VidSection 09.3.

4. Abstract Vector Spaces

26. The abstract spaces over fields. The main examples.
Reading: Section 10.1.
Video: VidSection 10.1.a, VidSection 10.1.b.

WEEK 7

27. Subspaces in spaces. Intersections and sums of subspaces.
Reading: Section 10.2.
Video: VidSection 10.2.a, VidSection 10.2.b.

28. Linear dependence and independence. The basic properties.
Reading: Section 11.1.
Video: VidSection 11.1.a, VidSection 11.1.b.

29. Spanning sets for spaces.
Reading: Section 11.2 (the first half).
Video: VidSection 11.2.a.

30. Bases for spaces. Uniqueness of representation. Theorem on equal cardinalities of bases. Dimension of space. Properties of bases.
Reading: Section 11.2 (the second half).
Video: VidSection 11.2.b, VidSection 11.2.c.

∼ Spring Break ∼

WEEK 8

31. Coordinate systems. Main examples.
Reading: Section 12.1.
Video: VidSection 12.1.

32. Basic properties of coordinate systems.
Reading: Section 12.2.
Video: VidSection 12.2.

33. The change of basis matrix.
Reading: Section 13.1.
Video: VidSection 13.1.a, VidSection 13.1.b.

34. Computation of change of basis matrix.

Reading: Section 13.2.

Video: VidSection 13.2.

WEEK 9

5. Matrix Computations in Spaces

35. Row spaces and column spaces. Finding the row space and the column space.

Reading: Section 14.1.

Video: VidSection 14.1.a, VidSection 14.1.b.

36. The rank and linearly independent rows and columns. A criterion for invertible matrices. Subspaces and the reduced row-echelon form. The proof for Theorem 14.15 is optional.

Reading: Section 14.2.

Video: VidSection 14.2.

37. Finding a basis for a span of vectors, first method. Linear dependence detection.

Reading: Section 14.3 (the first half).

Video: VidSection 14.3.a.

38. Finding the maximal linearly independent subset. Finding a basis for a span of vectors, second method. Presenting a vector as a linear combination.

Reading: Section 14.3 (the second half).

Video: VidSection 14.3.b, VidSection 14.3.c.

WEEK 10

39. Null space of a matrix. Theorem on rank and nullity. Finding a basis for null space.

Reading: Section 15.1.

Video: VidSection 15.1.a, VidSection 15.1.b, VidSection 15.1.c.

40. Null spaces and solutions of homogeneous systems of equations. Solving a system of linear equations, the free columns method.

Reading: Section 15.2.

Video: VidSection 15.2.

41. Identifying the subspaces, detecting when a subspace sontains the other.

Reading: Section 16.1.

Video: VidSection 16.1.a, VidSection 16.1.b, VidSection 16.1.c.

42. (Optional) Computation of the sum and intersection of subspaces. Dimensions of the sum and the intersection (proof of Theorem 16.14 is optional).

Reading: Section 16.2, Section 16.3.

WEEK 11

6. Determinants and their Applications

43. Defining determinant by cofactor expansion. Computation of determinants of degree 2 and 3. *Section 17.1.*

Reading: Section 17.1.

Video: VidSection 17.1.a, VidSection 17.1.b.

44. Basic properties of determinants (all proofs optional).

Reading: Section 17.2.

Video: VidSection 17.2.

45. Determinants and matrix operations. Determinants of elementary matrices. Determinant of a product matrix. Determinant of a transpose.

Reading: Section 17.3.

Video: VidSection 17.3.

46. The triangle method for determinant computation.
Reading: Section 18.1.
Video: VidSection 18.1.

47. The Laplace expansion rule and method for determinant computation.
Reading: Section 18.2.
Video: VidSection 18.2.

48. Determinants and linear independence.
Reading: Section 19.2.
Video: VidSection 19.2.a, VidSection 19.2.b.

WEEK 12

7. Linear Transformations

49. Definition and main examples of transformations. *Section 20.1*.
50. The matrix of a linear transformation. *Section 20.2*.
51. Change of basis for linear transformations. *Section 20.3*.
52. The kernel transformation. *Section 21.1*.
53. The range of transformation, the sum of rank and nullity. *Section 21.2*.
54. Compositions of linear transformations. *Section 22.1*.
55. The inverse of a linear transformation. *Section 22.2*.
56. Sums and scalar multiples of transformations. *Section 22.3*.

8. Eigenvectors and Diagonalization

57. Eigenvectors and eigenvalues, definition and examples. *Section 23.1*.
58. Computation of eigenspace for a given eigenvalue. *Section 23.2*.
59. Polynomials over fields (optional). *Appendices D.1, D.2*.
60. Characteristic polynomials and the eigenvalues. *Section 23.3*.
61. Eigenvectors and linear independence, eigenbases. *Section 23.4*.
62. Similar matrices. *Section 24.1*.
63. Introduction to diagonalization. *Section 24.2*.
64. Diagonalization by geometric multiplicity. *Section 24.3*.
65. Diagonalization by algebraic multiplicity. *Section 24.4*.

9. Inner Product Spaces and Orthogonality

66. Orthogonal systems of vectors. *Section 27.1*.
67. The Gram-Schmidt process. *Section 27.2*.
68. Orthogonal matrices and orthogonal transformations. *Section 29.1*.
69. Symmetric matrices and symmetric transformations. *Section 29.3*.
70. Orthogonal diagonalizalion and the Spectral Theorem (proofs are optional). *Section 29.3*.

The Main *How To*'s

1. How to bring a matrix to a row-echelon form. *Algorithm 6.10*.
2. How to solve a system of linear equations, basic method. *Algorithm 7.1*.
3. How to bring a matrix to the reduced row-echelon form. *Algorithm 7.7*.
4. How to solve a system of linear equations, the Gauss-Jordan method. *Algorithm 7.8*.
5. How to detect if two matrices are row-equivalent.
6. How to compute the rank of a matrix by row-elimination.
7. How to compute the inverse matrix. *Algorithm 9.12*.
8. How to compute the change of basis matrix. *Algorithm 13.8*.
9. How to find the row space of a matrix. *Algorithm 14.7*.
10. How to find the column space of a matrix. *Algorithm 14.10*.
11. How to find a basis for a subspace (span of vectors), first method. *Algorithm 14.19*.
12. How to detect linear dependence. *Algorithm 14.23*.
13. How to find a maximal linearly independent subset. *Algorithm 14.24*.
14. How to find a basis for a subspace (span of vectors), second method. *Algorithm 14.27*.
15. How to present a vector as a linear combination. *Algorithm 14.29*.
16. How to find a basis for null space. *Algorithm 15.2*.
17. How to solve a system of linear equations, the free columns method. *Algorithm 15.7*.
18. How to compare subspaces. *Algorithm 16.1*.
19. How to find if a given subspace contains the other subspace. *Algorithm 16.3*.
20. * How to continue a basis of a subspace to a basis for the space. *Algorithm 16.6*.
21. * How to find the sum of two subspaces.
22. * How to find the intersection of two subspaces, basic method. *Algorithm 16.9*.
23. * How to find the intersection of two subspaces, handy method.
24. How to compute a determinant by triangle method. *Algorithm 18.1*.
25. How to compute a determinant by the Laplace Expansion. *Algorithm 18.6*.
26. * How to solve a square system of linear equations, Cramer's method.
27. * How to compute the inverse matrix, adjoint matrix method.
28. How to compute the matrix of a transformation. *Algorithm 20.12*.
29. How to compute the kernel and nullity of a transformation. *Algorithm 21.2*.
30. How to compute the range and rank of a transformation. *Algorithm 21.9*.
31. How to compute the eigenvectors associated to an eigenvalue. *Algorithm 23.10*.

32. How to diagonalize a matrix using geometric multiplicity. *Algorithm 24.16*.
33. How to diagonalize a matrix using algebraic multiplicity.
34. * How to find the Jordan decomposition of a matrix. *Algorithm 26.4*.
35. How to find an orthonormal basis. *Algorithm 27.6*.
36. * How to find a basis for the orthogonal complement by the left null space. *Algorithm 28.9*.
37. * How to detect if the given subspaces are orthogonal.
38. * How to find least square solutions for a system of linear equations. *Algorithm 28.26*.
39. * How to find a QR-factorization of a matrix. *Algorithm 29.14*.
40. How to orthogonally diagonalize a real matrix. *Algorithm 29.26*.

The items marked by an asterisk (*) are *not* a part of the Linear Algebra 104 course.

Part 1

Introduction to Vectors, Spaces and Fields

CHAPTER 1

The real space $\mathbb{R}^n$

"Man muss immer mit den einfachsten Beispielen anfangen."
David Hilbert

1.1. Vectors in the real space $\mathbb{R}^2$

Following the advice of Hilbert let us start with the simplest examples. Call the set of real numbers $\mathbb{R}$ (together with its operations $+$ and $\cdot$) a *field of scalars*, and take the Cartesian plane on it, i.e., the Cartesian product $\mathbb{R}^2 = \{(x,y) \,|\, x,y \in \mathbb{R}\}$ consisting of ordered pairs (x,y) with coordinates x and y. We build the *real 2-dimensional space* on the field $\mathbb{R}$ in two steps: setting up the vectors, and then defining their operations.

For each point $A=(x,y)$ set a *vector* $\overrightarrow{OA}$ which can be visualized as an arrow with the *initial point* or *tail* at the origin $O=(0,0)$, and the *terminal point* or *head* at A. Denote this vector by $\vec{v}=\overrightarrow{OA}$ as in Figure 1.1 (a). By definition, the vectors $v=(x,y)$ and $u=(x',y')$ are equal if and only if $x=x'$ and $y=y'$. We can also denote the vector using its coordinates: $\vec{v}=(x,y)$. Other alternative notations are $\vec{v}=[x,y]$ (the *row vector* notation) or $\vec{v}=\begin{bmatrix} x \\ y \end{bmatrix}$ (the *column vector* notation). Later we will see why such alternative notations may sometimes be preferable. In most cases we are going to omit the arrow sign in $\vec{v}$, and to write the vector by just v unless the arrow is needed for some reason. For example, we may write the *zero vector* as $\vec{0}=(0,0)$ (here the arrow stresses that $\vec{0}$ is a *vector*, while 0 is a *number*).

Can we also consider vectors the tails of which are other than the origin $O=(0,0)$? You may have used such vectors in school mathematics and physics, and now you are surprised why they were not covered above. We can introduce such vectors, but we

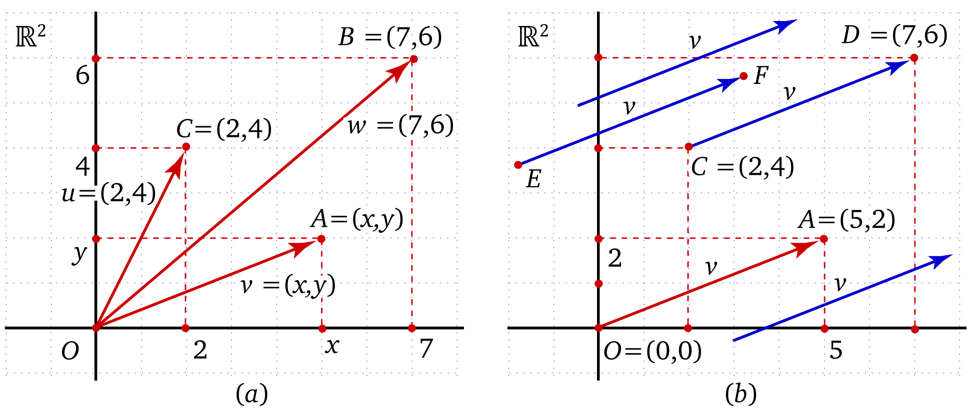


FIGURE 1.1. Setting up vectors in $\mathbb{R}^2$.

consider each of them to be *equal* to a respective vector with tail at the origin O. Namely, the vector $\overrightarrow{CD}$ is equal to the vector $v = \overrightarrow{OA}$, if v is obtained from $\overrightarrow{CD}$ by a *parallel translation* (i.e., by subtracting the tail's coordinates of $\overrightarrow{CD}$ from its head's coordinates). In Figure 1.1 (b) we have $\overrightarrow{CD} = \overrightarrow{OA} = v$ because $(7-2,\ 6-4) = (5,2)$. Notice that the coordinates of $\overrightarrow{CD}$ are *not* $(7,6)$ but $(5,2)$. We say that $\overrightarrow{OA}$ is the *standard position* of the vector $\overrightarrow{CD}$. More generally, u and v are equal, if we obtain one of them from the other by a parallel translation. In Figure 1.1 (b) we have $\overrightarrow{CD} = \overrightarrow{EF}$, and v is the standard position for both of them.

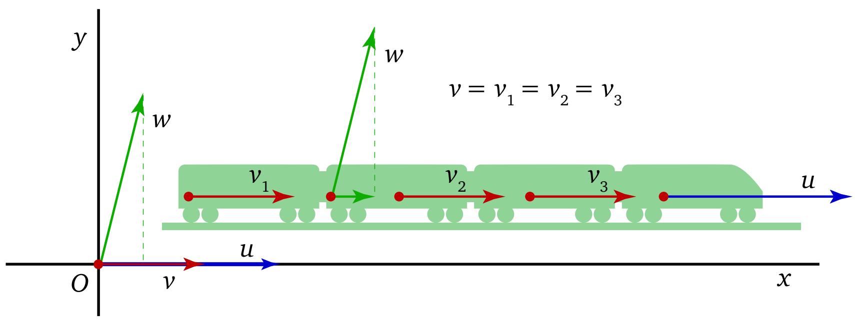


FIGURE 1.2. Forces applied at different points of an object.

Thus, a vector is defined as an "arrow" which has *length* and *direction*, but it does not matter at which position it "stands". In the nature this corresponds to *force* applied to an ideal object. The *strength (length)* and *direction* of the force do matter, but it does not matter at which point of the object it is applied. Visualize a group of people pushing a train of Figure 1.2. Three people push the train forward at equal strengths, across the equal vectors $v_1 = v_2 = v_3$. Although their forces are applied at different points, they have the same impact in pushing the train forward. The fourth person pushes stronger across the vector u. And the fifth person pushes in some other direction across w...

Define two main operations with vectors: *addition of vectors* and *multiplication of a vector by a scalar*. For any vectors $v_1 = (x_1, y_1)$ and $v_2 = (x_2, y_2)$ in $\mathbb{R}^2$ define their sum:

$$v_1 + v_2 = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2).$$

Or in other notation:

$$v_1 + v_2 = [x_1, y_1] + [x_2, y_2] = [x_1 + x_2,\ y_1 + y_2], \quad v_1 + v_2 = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} + \begin{bmatrix} x_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 \\ y_1 + y_2 \end{bmatrix}.$$

Geometrically this operation can be visualized in two ways shown in Figure 1.3: either by the parallelogram rule or by the head-to-tail rule (triangle rule).

Next for any vector $v = (x, y)$ and for any scalar $a \in \mathbb{R}$ define the product

$$a\,v = a(x, y) = (ax, ay).$$

Or in other notation:

$$av = a[x, y] = [ax, ay], \quad a\,v = a \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax \\ ay \end{bmatrix}.$$

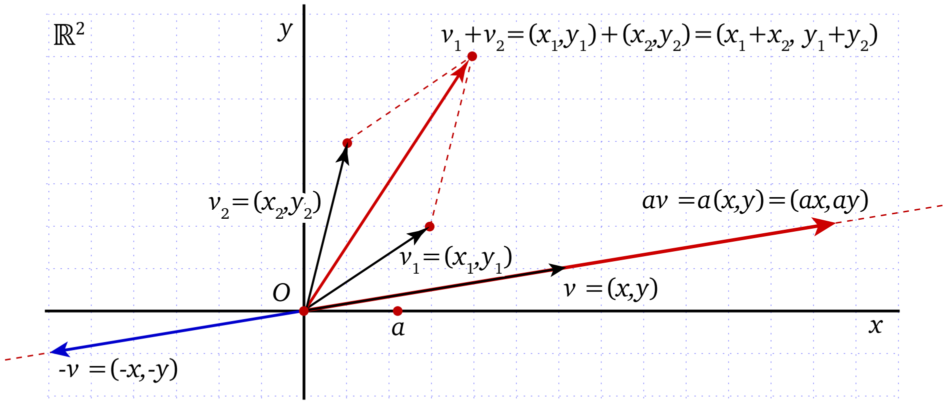


FIGURE 1.3. Addition and multiplication of vectors by scalar in $\mathbb{R}^2$.

av is the *scalar multiple* of v. Geometrically this operation can be visualized as stretching or compressing a vector a times as in Figure 1.3. If a is negative, then the direction of av is opposite to the direction of v.

If $u = av$ or $v = bu$ (for some scalars $a, b \in \mathbb{R}$), then the vectors u, v are said to be *parallel* or *collinear*.

For $a = -1$ and for any $v = (x, y)$ we have

$$-1v = \Big((-1)\cdot x, (-1)\cdot y\Big) = (-x, -y).$$

Denoting $-1v$ by $-v$ we will get the *opposite vector* for v:

$$-v + v = v + (-v) = \vec{0}$$

(see Figure 1.3). In general denote $v - u = v + (-u)$ (this subtraction is not a new operation in the space, but it is just a shorthand notation for $v + (-u)$. It is easy to check that $-(u + v) = -u - v,\ \ -(cv) = c(-v),\ \ u - v = -(v - u)$, etc.

1.2. The real spaces $\mathbb{R}^n$ and their main properties, the spaces $\mathbb{Q}^n$

You surely found introduction of the space $\mathbb{R}^2$ in previous section very detailed (and maybe rather boring). Thus we without many repetitions could introduce the *real 3-dimensional space* $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ and, more generally, the *real n-dimensional space* on the field of scalars $\mathbb{R}$:

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R},\ i = 1, \ldots, n\}$$

for any $n = 1, 2, 3, \ldots$ For a point $A = (x_1, x_2, \ldots, x_n)$ of this Cartesian product we set up the vector $\overrightarrow{OA}$, i.e., an ordered pair of points O and A, where O is the origin $O = (0, 0, \ldots, 0)$. We denote the vector $\overrightarrow{OA}$ as $\vec{v} = (x_1, x_2, \ldots, x_n)$, or by row- or column vector notations:

$$\vec{v} = [x_1, x_2, \cdots, x_n] \quad \text{or} \quad \vec{v} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix},$$

and in most cases we are going to omit the arrow sign in $\vec{v}$. The numbers $x_1, x_2, \dots, x_n$ are called the *coordinates* of v.

For $v_1 = (x_1, x_2, \dots, x_n)$ and $v_2 = (y_1, y_2, \dots, y_n)$ their *sum* is defined by

$$v_1 + v_2 = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

In, say, column vector notation this looks like:

$$v_1 + v_2 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

For any vector $v = (x_1, x_2, \dots, x_n)$ and any scalar $a \in \mathbb{R}$ define:

$$a\,v = a(x_1, x_2, \dots, x_n) = (ax_1, ax_2, \dots, ax_n).$$

And in column vector notation:

$$a\,v = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix}.$$

When $n = 3$, we still can visualize the vector addition either by parallelogram rule or by the head-to-tail rule like in example of Figure 1.4 below:

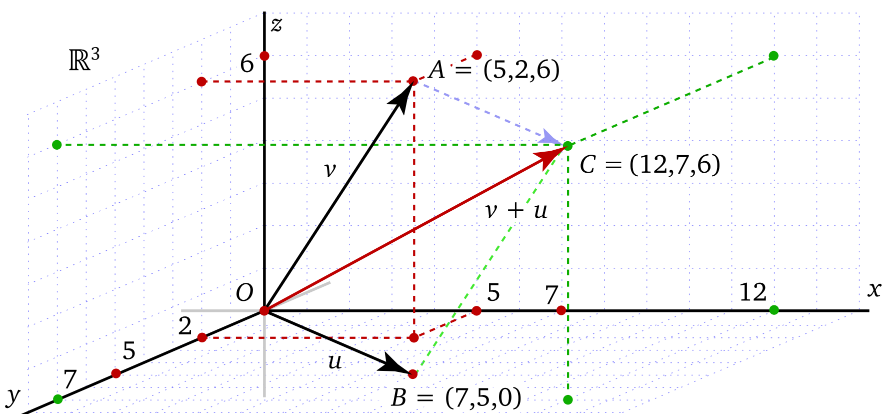


FIGURE 1.4. Vector operations in $\mathbb{R}^3$.

Notice a spacial case of real spaces: when $n = 1$, then $\mathbb{R}^n = \mathbb{R}^1 = \{(x)\,|\,x \in \mathbb{R}\}$. So we just have $(x) + (y) = (x + y)$ and $a(x) = (ax)$. I.e., $\mathbb{R}$ is a 1-dimensional space on the field $\mathbb{R}$.

Generalizing the concept of equal vectors of $\mathbb{R}^2$ we can also consider vectors $\overrightarrow{CD}$ with tails C other than O. Namely, if $C = (y_1, y_2, \dots, y_n)$ and $D = (z_1, z_2, \dots, z_n)$, then set the vector $\overrightarrow{CD}$ to be *equal* to $v = (x_1, x_2, \dots, x_n)$, where $x_i = z_i - y_i$ for all $i = 1, 2, \dots, n$ (the n-dimensional analog of parallel translation).

Let us collect the *main algebraic properties* for all real spaces $\mathbb{R}^n$:

Proposition 1.1. *The following properties hold for any vectors $u, v, w \in \mathbb{R}^n$ and scalars $a, b \in \mathbb{R}$:*

1. $u + v = v + u$; *(commutativity of vector addition)*
2. $(u+v)+w = u+(v+w)$; *(associativity of vector addition)*
3. *there is a vector* $0 \in \mathbb{R}^n$ *such that* $v + 0 = v$; *(existence of additive identity)*
4. *there is a vector* $-v \in \mathbb{R}^n$ *such that* $v + (-v) = 0$; *(existence of opposite vector)*
5. $a(u+v) = au + av$; *(distributivity of vector addition)*
6. $(a+b)v = av + bv$; *(distributivity of scalar addition)*
7. $(a \cdot b)v = a(bv)$; *(homogeneity of multiplication by scalar)*
8. $1v = v$. *(unitarity of multiplication by scalar)*

***Proof*.** These points are easy exercises to prove, and we demonstrate just some of them. As the zero vector $0 \in \mathbb{R}^n$ we may take the vector with all coordinates zero: $0 = \vec{0} = (0, 0, \dots, 0)$. For the given $v = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ we can take the opposite vector $-v = (-x_1, -x_2, \dots, -x_n)$. To prove distributivity of point (5) just notice that

$$a\big((x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n)\big) = \big(a(x_1 + y_1), a(x_2 + y_2), \dots, a(x_n + y_n)\big)$$

$$= (ax_1 + ay_1, ax_2 + ay_2, \dots, ax_n + ay_n) = a(x_1, x_2, \dots, x_n) + a(y_1, y_2, \dots, y_n).$$

$\square$

The reason why we call the points of Proposition 1.1 "main algebraic properties" is that they match the definition of the abstract vector space (see Definition 10.1), so this proposition actually means that $\mathbb{R}^n$ is a *vector space* over the real field $\mathbb{R}$.

Remark 1.2. We called $\mathbb{R}^n$ a "space". In intuitive meaning of that word, a *space* is an environment in which we have freedom to pick whatever location we want. For example, if the plane $\mathbb{R}^2$ contains two points A and B, then it also contains their midpoint M. The plane also contains a point C opposite to A (about the origin O), and a point D which is, say, 3 times further from O and is on the same direction as $\overrightarrow{OA}$.

All these points can be easily discovered in $\mathbb{R}^2$. Indeed, if $u = \overrightarrow{OA} = (x, y)$ and $v = \overrightarrow{OB} = (x', y')$, then M is found from $\overrightarrow{OM} = \frac{1}{2}(u+v) = \big(\frac{1}{2}(x+x'),\ \frac{1}{2}(y+y')\big)$, the point C is found from $\overrightarrow{OC} = -u = (-x,\ -y)$, and D is found from $\overrightarrow{OD} = 3u = (3x,\ 3y)$.

To have the listed points inside the space $\mathbb{R}^2$, the field of scalars $\mathbb{R}$ need have certain properties, such as, it need have the *sums*, the *products*, the *opposites* of any of its scalars. Also, with any non-zero scalar a it need contain the *inverse* $a^{-1} = \frac{1}{a}$.

Did you notice how the *numeric properties* of the field pre-determine the *geometric properties* of a space? This simple observation will become principal when we later study the abstract fields and spaces on them (see the question about the sets $\mathbb{N}^n$, $\mathbb{Z}^n$, $(0,5)^n$, $(-1,1)^n$ at the beginning of 4.1).

It sounds rather unexpected, but everything we constructed above starting from the field of *real* scalars $\mathbb{R}$ could be re-stated starting from the field of *rational* scalars $\mathbb{Q} = \{\frac{m}{k} \mid m, k \in \mathbb{Z};\ k \neq 0\}$. We can consider the Cartesian products:

$$\mathbb{Q}^2 = \{(x, y) \mid x, y \in \mathbb{Q}\},$$

$$\mathbb{Q}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{Q}\},$$

$$\mathbb{Q}^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in \mathbb{Q},\ i = 1, \dots, n\}.$$

In $\mathbb{Q}^n$ we can define addition of vectors because if $v_1, v_2 \in \mathbb{Q}^n$ then also $v_1 + v_2 \in \mathbb{Q}^n$ (the sum of any rational coordinates is rational). Also, for any $a \in \mathbb{Q}$ we have $av \in \mathbb{Q}^n$ (the product of any rational coordinates is rational). Call such spaces $\mathbb{Q}^n$ *rational spaces*.

Analogs of the main algebraic properties in Proposition 1.1 can be re-stated for rational spaces, and each of eight points can easily be verified.

Since any non-zero rational number $a = \frac{m}{k}$ has a rational inverse $\left(\frac{m}{k}\right)^{-1} = \frac{k}{m} \in \mathbb{Q}$, we can also divide each rational vector v by a to get another rational vector:

$$a^{-1}v = \left(\tfrac{m}{k}\right)^{-1} v = \tfrac{k}{m}(x_1, x_2, \ldots, x_n) = \left(\tfrac{k}{m}x_1,\ \tfrac{k}{m}x_2, \ldots, \tfrac{k}{m}x_n\right) \in \mathbb{Q}^n.$$

This means the analog of Remark 1.2 is valid for $\mathbb{Q}^n$ also.

How to visualize the rational spaces? The paintings of *Georges Seurat* perhaps give some insight of how the spaces $\mathbb{Q}^n$ could look like...

1.3. The dot product and the norm on $\mathbb{R}^n$

We will turn to other types of vector spaces later, but for now let us learn more on $\mathbb{R}^n$, and introduce *metrics* on $\mathbb{R}^n$, i.e., define *dot product* to measure length of vectors and angle between vectors using dot product.

Definition 1.3. For vectors $u = (x_1, x_2, \ldots, x_n)$ and $v = (y_1, y_2, \ldots, y_n)$ in $\mathbb{R}^n$ their (real) *dot product* is defined as

$$u \cdot v = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

In the literature dot product often is called *scalar product* or *inner product*, and it may also be denoted by (u, v) or by $\langle u, v \rangle$. Call vectors $u, v \in \mathbb{R}^n$ *orthogonal* or *perpendicular*, if $u \cdot v = 0$. We denote this fact by $\boldsymbol{u} \perp \boldsymbol{v}$.

Example 1.4. In $\mathbb{R}^2$ choose $u = (2,1)$, $v = (3,0)$, $w = (0,1)$.

$$\begin{aligned} u \cdot v &= 2 \cdot 3 + 1 \cdot 0 = 6, \\ u \cdot w &= 2 \cdot 0 + 1 \cdot 1 = 1, \\ v \cdot w &= 3 \cdot 0 + 0 \cdot 1 = 0. \end{aligned}$$

Notice that $v \cdot w = 0$, and so the vectors v and w are perpendicular.

Example 1.5. For $u = (1,2,-1)$, $v = (2,3,0)$, $w = (0,0,5) \in \mathbb{R}^3$ we have:

$$\begin{aligned} u \cdot v &= 1 \cdot 2 + 2 \cdot 3 + (-1) \cdot 0 = 7, \\ u \cdot w &= 1 \cdot 0 + 2 \cdot 0 + (-1) \cdot 5 = -5, \\ v \cdot w &= 2 \cdot 0 + 3 \cdot 0 + 0 \cdot 5 = 0. \end{aligned}$$

Again, $v \cdot w = 0$, and we get $v \perp w$.

Here are the *main algebraic properties* of dot products:

Proposition 1.6. *The following properties hold for any vectors $u, v, w \in \mathbb{R}^n$ and scalar $a \in \mathbb{R}$:*

1. $u \cdot v = v \cdot u$; *(symmetry)*
2. $(au) \cdot v = a(u \cdot v)$; *(homogenity)*
3. $(u + v) \cdot w = u \cdot w + v \cdot w$; *(distributivity)*
4. $v \cdot v \geq 0$, *and* $v \cdot v = 0$ *if and only if* $v = 0$. *(non-negativeness)*

The proofs of all points are easy exercises.

From this proposition it is very easy to deduce other properties, such as:

Corollary 1.7. *For any $u, v, w \in \mathbb{R}^n$ and $a \in \mathbb{R}$:*

1. $u \cdot (av) = a(u \cdot v)$;

2. $(u-v)\cdot w = u\cdot w - v\cdot w$;
3. $u\cdot(v+w) = u\cdot v + u\cdot w$ *and* $u\cdot(v-w) = u\cdot v - u\cdot w$.

Dot product can be used to define *norm* or *vector length* in spaces.

Definition 1.8. For a vector $v=(x_1,x_2,\ldots,x_n)\in\mathbb{R}^n$ its *norm* or *length* is defined as:

$$|v| = \sqrt{v\cdot v} = \sqrt{x_1^2+x_2^2+\cdots+x_n^2}.$$

The norm sometimes is also denoted by $\|v\|$.

Example 1.9. Like in previous example, take three vectors $u=(1,2,-1)$, $v=(2,3,0)$ and $w=(0,0,5)$ in $\mathbb{R}^3$. We then have the norms: $|u| = \sqrt{u\cdot u} = \sqrt{1^2+2^2+(-1)^2} = \sqrt{6}$, and $|v| = \sqrt{v\cdot v} = \sqrt{13}$, and $|w| = \sqrt{w\cdot w} = \sqrt{25} = 5$.

It is easy to prove that $|av| = |a|\cdot|v|$ for any $v\in\mathbb{R}^n$ and scalar a (here $|a|$ means absolute value of the number a, and $|v|$ means the norm of the vector v).

A vector v is called *normalized* vector or *unit* vector if $|v|=1$. We can normalize each non-zero vector: multiply it by a scalar a such that $|av|=1$ (just take $a=\frac{1}{|v|}$).

Vector length can be used to compute the *distance* between any two points A and B in $\mathbb{R}^n$. Namely, that distance is equal to the length of the vector $\overrightarrow{OB}-\overrightarrow{OA}=u-v$:

$$|AB| = |u-v| = \sqrt{(u-v)\cdot(u-v)}.$$

This distance sometimes is called *distance between two vectors*.

The following key fact is called *Cauchy-Schwarz* inequality or, sometimes, *Cauchy-Bunyakovsky* inequality:

Theorem 1.10 (Cauchy-Schwarz inequality)**.** *For any vectors $u,v\in\mathbb{R}^n$ we have:*

$$|u\cdot v| \le |u|\cdot|v|.$$

(Here $|u\cdot v|$ means the absolute value of the dot product $u\cdot v$ of two vectors, whereas the similarly looking $|u|\cdot|v|$ means the product of two numbers $|u|$ and $|v|$, i.e., the above dots $\bullet$ and $\cdot$ stand for different operations.)

Proof. The case when u or v is zero is evident. So assume $u,v\neq 0$, and consider the vector $w=\frac{u}{|u|}-\frac{v}{|v|}$. By above proposition and its corollary we have:

$$0\le w\cdot w = \Big(\frac{u}{|u|}-\frac{v}{|v|}\Big)\cdot\Big(\frac{u}{|u|}-\frac{v}{|v|}\Big) = \frac{u\cdot u}{|u|\cdot|u|} - \frac{u\cdot v}{|u|\cdot|v|} - \frac{v\cdot u}{|v|\cdot|u|} + \frac{v\cdot v}{|v|\cdot|v|} = 1-2\frac{u\cdot v}{|u|\cdot|v|}+1.$$

Then $2\,\frac{u\cdot v}{|u|\cdot|v|}\le 2$, and so $u\cdot v\le\frac{2}{2}\,|u|\cdot|v| = |u|\cdot|v|$. This completes the proof in case $u\cdot v\ge 0$. And when $u\cdot v<0$ just replace in $u\cdot v\le|u|\cdot|v|$ the vector u by $-u$. □

Two well-known theorems can be proved now:

Theorem 1.11 (Triangle inequality)**.** *For any vectors $u,v\in\mathbb{R}^n$ we have:*

$$|u+v| \le |u|+|v|.$$

Proof. Apply the Cauchy-Schwarz inequality below:

$$\begin{aligned}|u+v|^2 &= (u+v)\cdot(u+v) = u\cdot u + v\cdot u + u\cdot v + v\cdot v\\ &= |u|^2 + 2\,u\cdot v + |v|^2 \le |u|^2 + 2\,|u|\cdot|v| + |v|^2 = \big(|u|+|v|\big)^2.\end{aligned}$$

□

For any points A, B, C in the space $\mathbb{R}^n$ we may apply the above theorem for $u = \overrightarrow{AB}$ and $v = \overrightarrow{BC}$ to get:

$$|\overrightarrow{AC}| = |u + v| \leq |u| + |v| = |\overrightarrow{AB}| + |\overrightarrow{BC}|.$$

This is nothing but the familiar rule: *"The shortest path between two points is the straight line"* that you know from the school. We now see that this rule happens to be correct in n-dimensional space for *any* n also.

Theorem 1.12 (Pythagoras Theorem). *For any vectors $u, v \in \mathbb{R}^n$ the equality*

$$|u + v|^2 = |u|^2 + |v|^2$$

holds if and only if $u \perp v$.

***Proof*.** Proving the Triangle inequality we saw that

$$|u + v|^2 = |u|^2 + 2\,u \cdot v + |v|^2.$$

So the theorem holds if and only if the summand $2\,u \cdot v$ is equal to 0, i.e., if $u \perp v$. □

Why this theorem is more general than the traditional form of the Pythagoras Theorem that you knew? Firstly, this is an *if and only if* theorem. And, more remarkably, it holds in n-dimensional space for *any* n.

You perhaps recall the school definition of dot product for vectors on plane using the vector lengths and the cosine of angle between them: $\boldsymbol{u \cdot v = |u|\,|v| \cos(\varphi)}$. That formula, in fact, follows from a more general *definition of angle* by dot product in $\mathbb{R}^n$:

Definition 1.13. For vectors $u, v \in \mathbb{R}^n$ the *angle* φ between them is a number in $(-\pi, \pi]$ defined by:

$$\cos(\varphi) = \frac{u \cdot v}{|u|\,|v|}.$$

This definition is correct because according to the Cauchy-Schwarz inequality $\frac{u \cdot v}{|u|\,|v|}$ cannot be more than 1 by absolute value.

Example 1.14. Let us compute the angle between the vectors of the previous example: $u = (1, 2, -1)$, $v = (2, 3, 0)$ and $w = (0, 0, 5)$. The angle φ between u and v can be computed by:

$$\cos(\varphi) = \frac{u \cdot v}{|u|\,|v|} = \frac{8}{\sqrt{6 \cdot 13}}.$$

The angle θ between v and w can be computed by:

$$\cos(\theta) = \frac{v \cdot w}{|v|\,|w|} = \frac{0}{\sqrt{13 \cdot 25}} = 0.$$

I.e. $\theta = \pi/2$ and the vectors v and w are perpendicular.

And the angle τ between u and w can be computed by:

$$\cos(\tau) = \frac{u \cdot w}{|u|\,|w|} = -\frac{5}{\sqrt{6 \cdot 25}} = -\frac{1}{\sqrt{6}}.$$

The dot product can be used to define *projections of vectors*. Let us start by the case of the plane $\mathbb{R}^2$. Assume we want to find the distance $|AC|$ from a point A to a line ℓ in Figure 1.5 (a). The points OAC define a right triangle, and by Pythagoras Theorem the distance $|AC|$ will be found, if we find the other two sides $|OA|$ and $|OC|$ of OAC. The length $|OA|$ is known as it is the length of the vector $v = \overrightarrow{OA}$ (see Figure 1.5 (b)).

Let us compute the vector $v' = \overrightarrow{OC}$. We know its length $|v'| = |v| \cos(\theta)$. Next, take a point B on ℓ and set the vector $u = \overrightarrow{OB}$. Normalize it to get the vector $e = \frac{1}{|u|} u$ which has the same direction as u, and has the length 1. Since, clearly, $v' = |v'|\, e$, we have:

$$v' = |v| \cos(\theta)\, e = |v|\, \frac{u \cdot v}{|u|\,|v|}\, \frac{1}{|u|}\, u = \frac{u \cdot v}{|u|\,|u|}\, u = \frac{u \cdot v}{u \cdot u}\, u$$

(we replaced $|u|\,|u|$ by $u \cdot u$ because the angle between u and u is zero, so $\cos(0) = \frac{u \cdot u}{|u|\,|u|} = 1$, and $|u|\,|u| = u \cdot u$).

An important feature of $\dfrac{u \cdot v}{u \cdot u}$ is that it relies on *dot product only*, and can be considered *in any space* $\mathbb{R}^n$. So forgetting the 2-dimensional Figures 1.5, we can define projections for any $\mathbb{R}^n$. Call the vector

$$\mathbf{proj}_u(v) = \frac{u \cdot v}{u \cdot u}\, u \tag{1.1}$$

the *projection* of the vector $v \in \mathbb{R}^n$ onto the vector $u \in \mathbb{R}^n$.

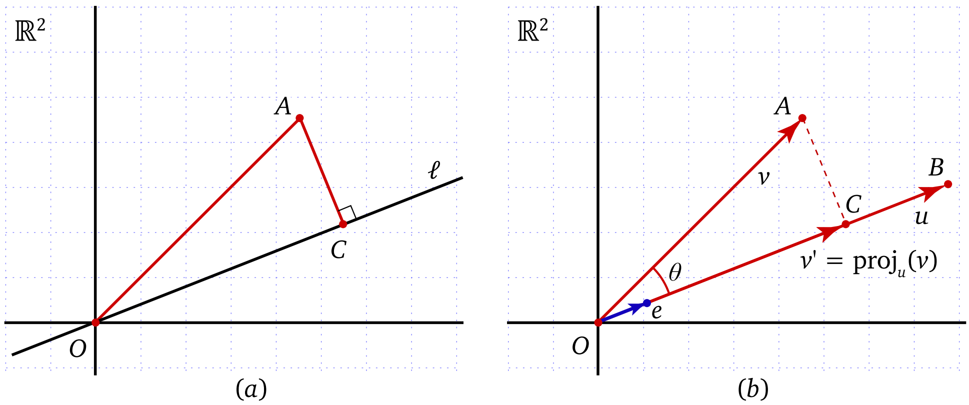


FIGURE 1.5. Vector projection in $\mathbb{R}^2$.

Example 1.15. Let us compute the projection $\text{proj}_u(v)$ of the vector $v = (3, 2)$ on the vector $u = (4, -5)$. We have

$$\text{proj}_u(v) = \frac{u \cdot v}{u \cdot u}\, u$$

$$= \frac{2}{41}(4, -5) = \left(\frac{8}{41}, -\frac{10}{41}\right)$$

Example 1.16. Suppose a triangle ABC is given in $\mathbb{R}^3$, and we know the vertices $A = (1, 0, 1)$ and $B = (2, 1, -1)$. We also know that the side AC is parallel to the vector $u = (3, 1, 1)$, and the angle at C is right. Can we find the vertex C?

First find the vector corresponding to side AB:

$$v = (2, 1, -1) - (1, 0, 1) = (1, 1, -2).$$

Its projection on u is

$$v' = \text{proj}_u(v) = \frac{2}{11}(3, 1, 1) = \left(\frac{6}{11}, \frac{2}{11}, \frac{2}{11}\right).$$

The vector $w = \overrightarrow{OC}$ clearly is the sum of $\overrightarrow{OA}$ and v'. So we get the point C as the head of the vector

$$\overrightarrow{OA} + v' = (1, 0, 1) + \left(\frac{6}{11}, \frac{2}{11}, \frac{2}{11}\right)$$
$$= \left(\frac{17}{11}, \frac{2}{11}, \frac{13}{11}\right).$$

Exercises

E.1.1. Find the coordinates of $\overrightarrow{AB}$, $3\overrightarrow{BC}$, $\frac{1}{2}\overrightarrow{CA}$ in $\mathbb{R}^2$, if $A = (1, 2)$, $B = (3, -2)$, $C = (0, 3)$.

E.1.2. The vectors $u = (2, 3, -2)$, $v = (5, -1, 2)$ are given in $\mathbb{R}^3$. Compute the vectors $2u + 3v$, $\frac{1}{2}(u - v)$, $\frac{v}{-2}$. Write the answers in row vector and column vector forms.

E.1.3. We are given the points $A=(1,0,-2)$, $B=(2,-1,3)$ and the vector $v=(1,2,5)$ in $\mathbb{R}^3$. Find the coordinates of the vector w and write it in column vector notation, if: **(1)** $w=-\overrightarrow{AB}+3v$. **(2)** $w=v-2\overrightarrow{BA}$.

E.1.4. The vector $v\in\mathbb{R}^3$ is given as $v=(x,4,y+2)$ and as $v=(1+y,2x,3)$. Find the values of the parameters x and y.

E.1.5. Is there a value $x\in\mathbb{R}$ for which the vectors $u=(3,0)$ and $v=(x,2)$ are collinear?

E.1.6. Three vectors are given in $\mathbb{R}^4$: $u=\begin{bmatrix}1\\2\\3\\1\end{bmatrix}$, $v=\begin{bmatrix}0\\1\\0\\3\end{bmatrix}$, $w=\begin{bmatrix}2\\3\\0\\-8\end{bmatrix}$. Compute the dot products $u\cdot v$, $u\cdot w$, $v\cdot w$. Are there orthogonal pairs among these vectors?

E.1.7. Find the length of the vectors $u=[1,3]$, $v=[2,0,3]$, $w=[0,1,-1,2]$.

E.1.8. Find the angle formed by the vectors u,v from Exercise E.1.2.

E.1.9. In $\mathbb{R}^3$ a cube is determined by vectors (three sides) $u=(2,2,0)$, $v=(-2,2,0)$, $w=(0,0,\sqrt{8})$. **(1)** Using vector operations only find the vertex A of the cube opposite to the vertex $O=(0,0,0)$ (so that OA is the main diagonal of the cube). **(2)** Find the length of the main diagonal OA. **(3)** Find the projection of the main diagonal on the vector u. **(4)** Find the distance from the point $C=(1,1,0)$ to the main diagonal of the cube.

E.1.10. Show that for any $u,v\in\mathbb{R}^3$ the length of $\text{proj}_u(v)$ is not more than the length of v. *Hint:* you may use the Cauchy-Schwartz inequality.

E.1.11. Do there exist vectors $u,v\in\mathbb{R}^n$ such that: **(1)** $|u|>2$, $|v|>2$, and $|u\cdot v|<4$? **(2)** $|u|<2$, $|v|<2$, and $|u\cdot v|>4$? *Hint*: here $|u\cdot v|$ is *not* a vector norm, but is the absolute value of the number $u\cdot v$.

E.1.12. The Great Pyramid of Giza (2580–2560 BC) is a 147 meters heigh geometric pyramid. Its base is a square with 230 meters long sides. Denote the base square by $ABCD$, and the apex by M. *Using vector calculus or projections find*: **(1)** the coordinates of M, **(2)** the length of the side CM, **(3)** the distance of point D from side BM (express the distance just by vector formula, the routine calculations are *not required* for this point). *Hint*: Put the pyramid into the space $\mathbb{R}^3$ so that $A=(0,0,0)$, $B=(230,0,0)$, $D=(0,230,0)$.

E.1.13. Let $x_1,\dots,x_n$ and $y_1,\dots,y_n$ be any sequences of real numbers. Prove the inequality: $\left(\sum_{i=1}^n x_iy_i\right)^2\le\sum_{i=1}^n x_i^2\cdot\sum_{i=1}^n y_i^2$. *Hint*: Use dot products.

E.1.14. **(1)** Prove point 2 of Proposition 1.6. **(2)** Deduce property 1 in Corollary 1.7 from the points of Proposition 1.6. **(3)** Deduce property 3 in Corollary 1.7 from the points of Proposition 1.6.

CHAPTER 2

Applications: Lines and planes in real spaces

Before we proceed we need some orientation. The central objects of study for linear algebra are the *abstract vector spaces over fields*, and the first three parts of this course prepare you for that study. In particular, Part 1 introduces basic examples of vector spaces: $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathbb{Z}_p^n$. The spaces $\mathbb{R}^n$ and $\mathbb{Q}^n$ were covered in sections 1.1–1.3, and in order to proceed to our main aim quickly we could now skip to sections 3.1, 3.2 to cover the spaces $\mathbb{C}^n$ and $\mathbb{Z}_p^n$. However, in this chapter we "stray from the right path" to study some vector-based analytic geometry in $\mathbb{R}^2$ and in $\mathbb{R}^3$ in order to show how efficient the vector methods can be. Also, some material from this chapter will be used as geometric illustrations later.

2.1. Lines in the space $\mathbb{R}^2$

The vectors language is very helpful to consider problems in different areas of mathematics. As an illustration let us study lines and planes in spaces $\mathbb{R}^2$, $\mathbb{R}^3$ to see how much simpler methods we may get compared to method of school geometry.

First consider a line ℓ passing through the origin O in $\mathbb{R}^2$ as in Figure 2.1 (a). Choose a *direction vector* d for the line ℓ, i.e., a non-zero vector the head point of which is on ℓ. Take an arbitrary point $A = (x, y)$ on the line. The vector $v = \overrightarrow{OA}$ can be constructed using the fixed vector d, since v is collinear to d: there is a $t \in \mathbb{R}$ such that $v = td$. That is, as t varies from $-\infty$ to $+\infty$ is head A "plots" the line ℓ.

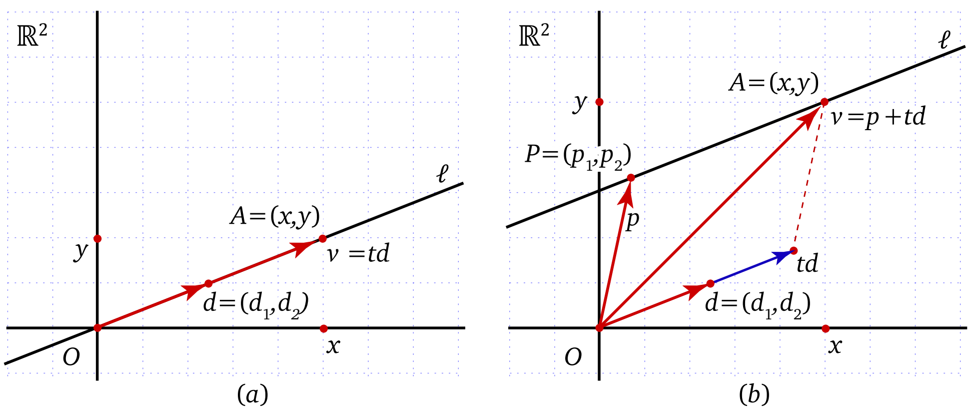


FIGURE 2.1. Constructing the vector form of a line in $\mathbb{R}^2$.

Now consider the general situation when ℓ is an arbitrary line as in Figure 2.1 (b). Fix some point P on ℓ and consider the *position vector* $p = \overrightarrow{OP}$. For an arbitrary point

$A=(x,y)$ taken on the line ℓ the vector $v=\overrightarrow{OA}$ can be presented using the fixed vectors d and p:

$$\boldsymbol{v}=\boldsymbol{p}+t\boldsymbol{d},$$

since td is collinear to d, and for suitable value $t\in\mathbb{R}$ the sum of p and td is v. Call this the *vector form* of the line ℓ with direction vector d and position vector p.

From the vector form we can derive another way to give a line. If $p=(p_1,p_2)$ and $d=(d_1,d_2)$, then

$$(x,y)=\vec{v}=\vec{p}+t\vec{d}=(p_1,p_2)+t(d_1,d_2)=(p_1+td_1,p_2+td_2),$$

which is equivalent to the system of two linear equations:

$$\begin{cases} \boldsymbol{x}=\boldsymbol{p_1}+\boldsymbol{t}\boldsymbol{d_1} \\ \boldsymbol{y}=\boldsymbol{p_2}+\boldsymbol{t}\boldsymbol{d_2}. \end{cases}$$

We call this *parametric form* of the line ℓ.

Example 2.1. Let us find the parametric form of the line ℓ with direction vector $d=(5,1)$ and passing via $P=(2,-2)$. As a position vector one clearly can take $p=(2,-2)$. The parametric form is:

$$\begin{cases} x=2+5t, \\ y=-2+t. \end{cases}$$

Example 2.2. Let us find five points on the line ℓ passing via the points $A=(1,2)$ and $B=(3,-4)$. This time the direction vector is not given, but we can take

$$d=\overrightarrow{AB}=(3-1,\ -4-2)=(2,\ -6).$$

As a position vector take, say, $p=(1,2)$. The parametric form is:

$$\begin{cases} x=1+2t, \\ y=2-6t. \end{cases}$$

To get five points on ℓ choose any five values of the parameter t, say, $t=1,2,3,4,5$, and accordingly compute: $C_1=(3,-4)$, $C_2=(5,-10)$, $C_3=(7,-16)$, $C_4=(9,-22)$, $C_5=(11,-28)$. Or we could take A as C_4, B as C_5.

Next study another way to characterize the line in a plane. Again, start by a line ℓ passing via the origin O. Choose a non-zero vector n orthogonal to ℓ. Notice that for any point A of ℓ the vector $\overrightarrow{OA}$ is orthogonal to n, as seen in Figure 2.2 (a). Denoting $v=\overrightarrow{OA}$ we can give ℓ by the form $n\cdot v=0$.

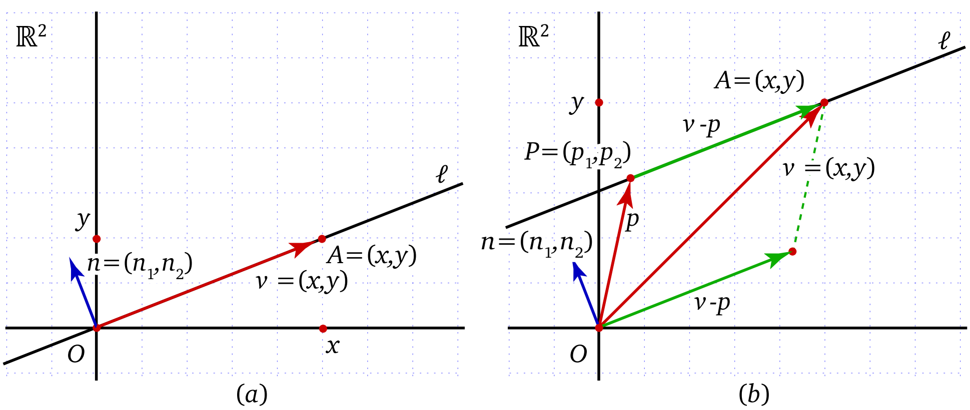


FIGURE 2.2. Constructing the normal form of a line in $\mathbb{R}^2$.

Now consider the general case when ℓ is any line in $\mathbb{R}^2$ as in Figure 2.2 (b). Fix some point P on it, and again consider the position vector $p = \overrightarrow{OP}$. The difference $v - p$ is orthogonal to n, and we have the following in terms of dot products:

$$\boldsymbol{n} \cdot (\boldsymbol{v} - \boldsymbol{p}) = \boldsymbol{0} \quad \text{or, equivalently,} \quad \boldsymbol{n} \cdot \boldsymbol{v} = \boldsymbol{n} \cdot \boldsymbol{p},$$

which we call a *normal form* of the line ℓ with normal vector n and position vector p.

Assume $n = (n_1, n_2)$, $p = (p_1, p_2)$ and $v = (x, y)$. Using these coordinates in the normal form $n \cdot v = n \cdot p$ we get:

$$(n_1, n_2) \cdot (x, y) = n_1 x + n_2 y = (n_1, n_2) \cdot (p_1, p_2) = n_1 p_1 + n_2 p_2.$$

Setting $a = n_1$, $b = n_2$ and $c = -(n_1 p_1 + n_2 p_2)$ we obtain the *general form* (or *equation*) of the line ℓ:

$$\boldsymbol{ax + by + c = 0}.$$

Notice that it is easy to get the normal and vector forms from each other. If, say, $d = (d_1, d_2)$ is a direction vector, then as a normal vector take $n = (-d_2, d_1)$ or $n = (d_2, -d_1)$. And if $n = (n_1, n_2)$ is a normal vector, then as a direction vector take $d = (-n_2, n_1)$.

Example 2.3. Let us write the normal form and the general form of the line ℓ that passes through the points $A = (3, 4)$ and $B = (-2, 5)$. As a direction vector d we may take, say $d = \overrightarrow{AB} = (-2 - 3, 5 - 4) = (-5, 1)$. Then as a normal vector we can choose $n = (1, 5)$. Taking $p = (3, 4)$ we have $n \cdot p = 1 \cdot 3 + 5 \cdot 4 = 23$. Thus as a general form we may take:

$$x + 5y - 23 = 0.$$

Example 2.4. (Optional) Find the distance of the point $A = (1, 2)$ from the line ℓ given in $\mathbb{R}^2$ by equation $-x - y + 7 = 0$. Firstly, find a position vector $p = (0, 7)$ for ℓ by assigning the value, say, $x = 0$ and computing respective $y = 7$. A normal vector of ℓ clearly is $n = (-1, -1)$ or, simpler, $n = (1, 1)$. Since parallel translation by the vector $-p$ does not change the distances, the distance from the point A to ℓ is equal to the distance of the head

$$A' = (1 - 0, 2 - 7) = (1, -5)$$

of the vector $\overrightarrow{OA} - p$ from the line ℓ' which has the same normal vector n, but which passes through the origin $O = (0, 0)$. This parallel translation has simplified the situation since the distance we look for is the length of the projection of $\overrightarrow{OA'}$ on n. Since

$$\mathrm{proj}_n(\overrightarrow{OA'}) = \frac{-4}{2}(1, 1) = (-2, -2),$$

we find the distance as:

$$|\mathrm{proj}_n(\overrightarrow{OA'})| = \sqrt{(-2)^2 + (-2)^2} = \sqrt{8}.$$

2.2. Planes and lines in the space $\mathbb{R}^3$

Assume in $\mathbb{R}^3$ we have a plane $\mathcal{P}$ passing through the origin O (see the left-hand plane $\mathcal{P}$ in Figure 2.3). Fix two non-collinear *direction vectors* d, k of the plane $\mathcal{P}$ (i.e., the heads of d, k belong to $\mathcal{P}$). Take an arbitrary point $A = (x, y, z) \in \mathcal{P}$ defining vector $v = \overrightarrow{OA}$. The vector v can be explained by vectors d, k, as v is coplanar to $\mathcal{P}$: there are $t, s \in \mathbb{R}$ such that $v = td + st$.

In the general case $\mathcal{P}$ is arbitrary plane (see the right-hand plane $\mathcal{P}$ in Figure 2.3). Take any point P on $\mathcal{P}$ and set the *position vector* $p = \overrightarrow{OP}$. For any point $A = (x, y, z)$ on $\mathcal{P}$ the vector $v = \overrightarrow{OA}$ can be presented by the vectors d, k and p:

$$\boldsymbol{v = p + td + sk},$$

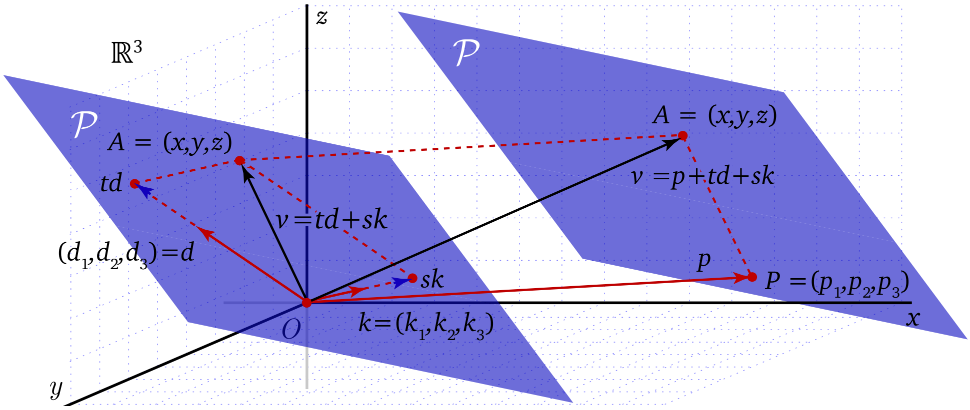


FIGURE 2.3. Constructing the vector form of a plane in $\mathbb{R}^3$.

where $td+sk$ is coplanar to d and k: there are such $t,s \in \mathbb{R}$ that v is the sum of p and $td+sk$. What we obtained is the *vector form* of the plane $\mathcal{P}$ with direction vectors d, k and with the position vector p (with $t,d \in \mathbb{R}$).

We can now get another way to give a plane. If $p = (p_1,p_2,p_3)$, $d = (d_1,d_2,d_3)$ and $k = (k_1,k_2,k_3)$, then

$$(x,y,z) = \vec{v} = \vec{p} + t\vec{d} + s\vec{k} = (p_1,p_2,p_3) + t(d_1,d_2,d_3) + s(k_1,k_2,k_3)$$
$$= (p_1+td_1+sk_1, p_2+td_2+sk_2, p_3+td_3+sk_3).$$

Which is equivalent to the system of three linear equations:

$$\begin{cases} x = p_1 + td_1 + sk_1 \\ y = p_2 + td_2 + sk_2 \\ z = p_3 + td_3 + sk_3. \end{cases}$$

We call this the *parametric form* of the plane $\mathcal{P}$.

Example 2.5. Let us find the vector and parametric forms of the plane $\mathcal{P}$ passing through three points $A = (1,3,2)$, $B = (2,1,0)$, $C = (5,2,-3)$. An easy check shows that they do not belong to the same line.

As a position vector we can take, say, $p = \overrightarrow{OA} = (1,3,2)$. As direction vectors we can choose $d = \overrightarrow{AB} = (1,-2,-2)$ and $k = \overrightarrow{AC} = (4,-1,-5)$, from where the vector form $v = p+td+sk$ is clear. And the parametric form for $\mathcal{P}$ is:

$$\begin{cases} x = 1+t+4s \\ y = 3-2t-s \\ z = 2-2t-5s. \end{cases}$$

Another way to interpret a plane $\mathcal{P}$ in $\mathbb{R}^3$ is to describe it by orthogonality to a fixed vector. Suppose first $\mathcal{P}$ is a plane passing through the origin O (see the left-hand plane $\mathcal{P}$ in Figure 2.4). Fix a non-zero *normal vector* n orthogonal to $\mathcal{P}$. For any $A = (x,y,z) \in \mathcal{P}$ the vector $v = \overrightarrow{OA}$ is orthogonal to n, i.e., $n \cdot v = 0$.

Next consider the general case when $\mathcal{P}$ is any plane (right-hand plane $\mathcal{P}$ in Figure 2.4). Fixing some point $P \in \mathcal{P}$ consider the position vector $p = \overrightarrow{OP}$. Then the difference $v-p$ is orthogonal to n, and we have:

$$\boldsymbol{n \cdot (v-p) = 0} \quad \text{or, equivalently,} \quad \boldsymbol{n \cdot v = n \cdot p},$$

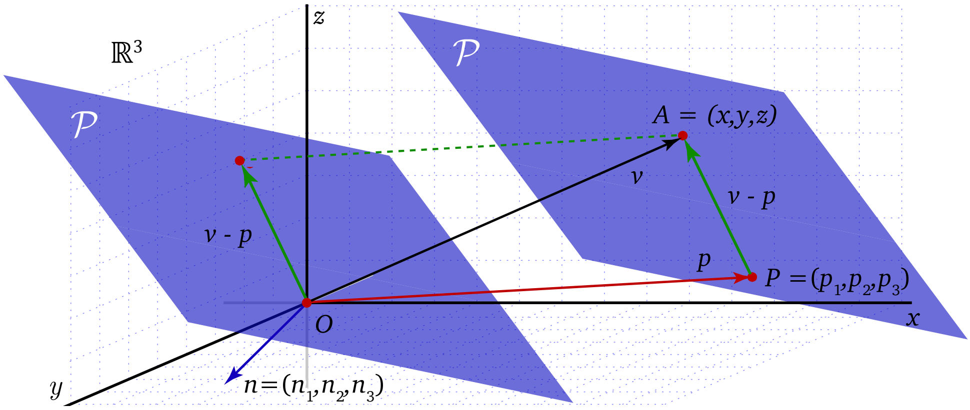


FIGURE 2.4. Constructing the normal form of a plane in $\mathbb{R}^3$.

which is called a *normal form* of the plane $\mathcal{P}$ with normal vector n and position vector p.

If $n = (n_1, n_2, n_3)$, $p = (p_1, p_2, p_3)$ and $v = (x, y, z)$, then we get:

$$(n_1, n_2, n_3) \cdot (x, y, z) = n_1 x + n_2 y + n_3 z$$
$$= (n_1, n_2, n_3) \cdot (p_1, p_2, p_3) = n_1 p_1 + n_2 p_2 + n_3 p_3.$$

Setting $a = n_1$, $b = n_2$, $c = n_3$ and $d = -(n_1 p_1 + n_2 p_2 + n_3 p_3)$ we obtain the *general form* (or *equation*) of the plane $\mathcal{P}$:

$$\boldsymbol{ax + by + cz + d = 0}.$$

Example 2.6. Let us find the normal and general forms of the plane $\mathcal{P}$ which is passing via the point $P = (-3, 1, 2)$, and which is perpendicular to the line ℓ passing through the points $A = (5, 1, 2)$, $B = (2, 3, 0)$.

As a position vector we can take $p = (-3, 1, 2)$, and as a normal vector we may take the vector $n = \overrightarrow{AB} = (-3, 2, -2)$. The normal form $n \cdot v = n \cdot p$ thus is known.

Computing the dot products $n \cdot v = -3x + 2y - 2z$ and $n \cdot p = 9 + 2 - 4 = 7$ we get the general form of $\mathcal{P}$:

$$-3x + 2y - 2z - 7 = 0.$$

In order to find the normal and the general form of a plane $\mathcal{P}$ (for which we already have its vector or parametric form), we basically need be able find a non-zero vector n which is orthogonal to *both* of non-collinear direction vectors d, k of $\mathcal{P}$.

That can be done by the operation of *cross product*:

$$\text{for any } u = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \text{ and } v = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \text{ define } u \times v = \begin{bmatrix} x_2 y_3 - y_2 x_3 \\ x_3 y_1 - y_3 x_1 \\ x_1 y_2 - y_1 x_2 \end{bmatrix}.$$

Figure 2.5 shows how to memorize the cross product composition rule: copy the first two coordinates of u and of v beneath them, draw three crosses to find which coordinates need be multiplied, and which ones of their products occur with plus or minus sign.

One can easily check that $u \times v$ is orthogonal to u and v. For example:

$$u \cdot u \times v = x_1(x_2 y_3 - y_2 x_3) + x_2(x_3 y_1 - y_3 x_1) + x_3(x_1 y_2 - y_1 x_2)$$
$$= x_1 x_2 y_3 - x_1 x_3 y_2 + x_2 x_3 y_1 - x_1 x_2 y_3 + x_1 x_3 y_2 - x_2 x_3 y_1 = 0.$$

$$u \times v = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \times \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_2 y_3 - y_2 x_3 \\ x_3 y_1 - y_3 x_1 \\ x_1 y_2 - y_1 x_2 \end{bmatrix}$$

$$\begin{matrix} x_1 & \quad & y_1 \\ x_2 & \quad & y_2 \end{matrix}$$

FIGURE 2.5. Composing the cross product.

It also is easy to verify that the cross product $u \times v$ of any non-collinear vectors u and v is *non-zero*. Therefore, as a normal vector n for a plane $\mathcal{P}$ with direction vectors d, k we may take their cross product $d \times k$.

Example 2.7. Let us find the general form of the plane $\mathcal{P}$ given by its parametric form

$$\begin{cases} x = -5 + 3t + 4s \\ y = -t \\ z = s. \end{cases}$$

As a position vector take $p = (-5, 0, 0)$. We also have two direction vectors $d = (3, -1, 0)$ and $k = (4, 0, 1)$, the cross product of which is the vector $n = (-1, -3, 4)$. Since the dot product $n \cdot p$ is equal to 5, a general form for $\mathcal{P}$ is:

$$-x - 3y + 4z - 5 = 0.$$

Much later we will compare this example with Example 15.11.

Example 2.8. (Optional) Find the distance from the point $M = (1, -2, 0)$ to the plane $\mathcal{P}$ given by its equation (general form) $2x + y - z + 3 = 0$.

We know a normal vector $n = (2, 1, -1)$ of $\mathcal{P}$. And as a position vector we can take, say, $p = (0, 0, 3)$ which we get after we assign the values $x = y = 0$, and compute the value $z = 3$ from the equation.

Since the parallel translation is not changing the distances between the points, the distance from M to $\mathcal{P}$ is equal to the distance from the head of the vector $w = \overrightarrow{OM} - p = (1, -2, -3)$ to the plane $\mathcal{P}'$, where $\mathcal{P}'$ is parallel to $\mathcal{P}$ (has the same normal vector) and is passing through the origin O. But as we noticed earlier, that distance is equal to the length of the projection

$$w' = \operatorname{proj}_n(w) = \frac{n \cdot w}{n \cdot n} n = \frac{1}{2}(2, 1, -1),$$

i.e., the distance is $w' = \frac{\sqrt{6}}{2}$.

Example 2.9. (Optional) The plane $\mathcal{P}_1$ is given by its points $A = (1, -2, 3)$, $B = (2, 1, 2)$, $C = (1, 0, 3)$, and the plane $\mathcal{P}_2$ is given by its points $D = (0, 1, 1)$, $E = (0, 1, -2)$, $F = (1, 3, 2)$. Find the angle between $\mathcal{P}_1$ and $\mathcal{P}_2$ (the smallest of two angles is assumed).

As direction vectors for the plane $\mathcal{P}_1$ one may take $\overrightarrow{AB} = (1, 3, -1)$ and $\overrightarrow{AC} = (0, 2, 0)$. Their vector product $n_1 = \overrightarrow{AB} \times \overrightarrow{AC} = (2, 0, 2)$ is a normal vector for $\mathcal{P}_1$.

And in the same way as direction vectors for $\mathcal{P}_2$ one may take $\overrightarrow{DE} = (0, 0, -3)$ and $\overrightarrow{DF} = (1, 2, 1)$. Their vector product $n_2 = \overrightarrow{DE} \times \overrightarrow{DF} = (6, 3, 0)$ is a normal vector for $\mathcal{P}_2$.

The angle between $\mathcal{P}_1$ and $\mathcal{P}_2$ actually is the angle α between n_1 and n_2, which we can compute by definition

$$\cos(\alpha) = \frac{n_1 \cdot n_2}{|n_1|\,|n_2|} = \frac{2}{\sqrt{10}}.$$

Let us complete the section by an outline description of *lines* in $\mathbb{R}^3$. The *vector form* of a line ℓ can be constructed by a direction vector $d = (d_1, d_2, d_3)$ and a position vector $p = (p_1, p_2, p_3)$ as in Figure 2.6:

$$\boldsymbol{v = p + t d}.$$

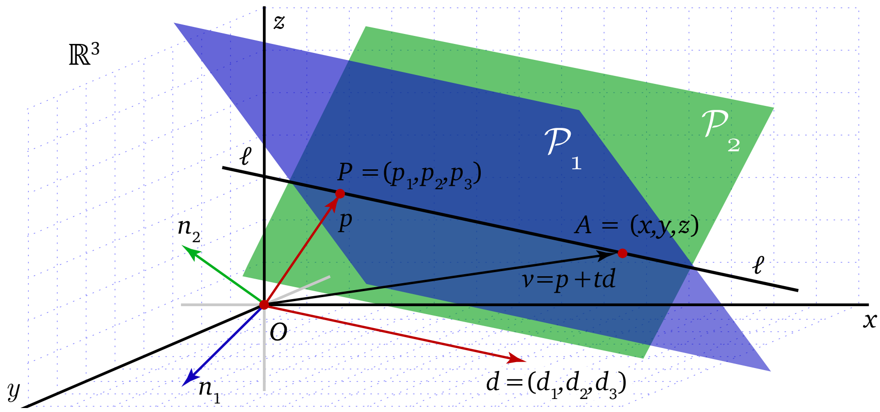


FIGURE 2.6. Constructing the vector and normal forms of a line in $\mathbb{R}^3$.

From this we get the parametric form of ℓ:

$$\begin{cases} x = p_1 + t d_1 \\ y = p_2 + t d_2 \\ z = p_3 + t d_3. \end{cases}$$

The normal form of ℓ can no longer be given by $n \cdot v = n \cdot p$, since there are *infinitely* many lines orthogonal to a single normal vector n, and passing through the given point P. But we still can characterize the line ℓ in $\mathbb{R}^3$ by any two planes $\mathcal{P}_1$ and $\mathcal{P}_2$ that intersect in ℓ (see Figure 2.6). Write a the normal forms of these planes as a system, and call that system a normal form for ℓ:

$$\begin{cases} n_1 \cdot v = n_1 \cdot p_1 \\ n_2 \cdot v = n_2 \cdot p_2. \end{cases}$$

Finally, the normal form of any plane in $\mathbb{R}^3$ can be replaced by the general form. Doing this for both planes $\mathcal{P}_1$ and $\mathcal{P}_2$ we get the *general form* of the ℓ in $\mathbb{R}^3$:

$$\begin{cases} a_1 x + b_1 y + c_1 z + d_1 = 0 \\ a_2 x + b_2 y + c_2 z + d_2 = 0. \end{cases}$$

Example 2.10. Let us find the vector, parametric and the general forms of the line ℓ passing via the points $A = (2, 1, -2)$ and $B = (0, 3, 1)$.

First notice that we can take $d = \overrightarrow{AB} = (-2, 2, 3)$ as a direction vector for ℓ. Taking the position vector $p = (2, 1, -2)$ we find a parametric form for the line ℓ:

$$\begin{cases} x = 2 + 2t \\ y = 1 - 2t \\ z = -2 + 3t. \end{cases}$$

Next we need two normal vectors for ℓ, i.e., two non-collinear vectors n_1 and n_2, both orthogonal to d. To get n_1 just replace one coordinate of d by zero, swap the other two, and negate one of them. Say, take $n_1 = (3, 0, 2)$. Clearly, $d \cdot n_1 = 0$. Similarly, take $n_2 = (2, 2, 0)$. Make sure that n_1 and n_2 are non-collinear, and then compute the normal form:

$$\begin{cases} n_1 \cdot v = n_1 \cdot p \\ n_2 \cdot v = n_2 \cdot p, \end{cases}$$

and the general form:

$$\begin{cases} 3x + 2z - 2 = 0 \\ 2x + 2y - 6 = 0. \end{cases}$$

Example 2.11. (Optional) Find the angle (the smallest angle α is assumed) formed by the line ℓ from previous exercise and by the plane $\mathcal{P}$

given by the parametric form:

$$\begin{cases} x = 1 + t + s \\ y = 2t - 3s \\ z = 2 - t - s. \end{cases}$$

We get a normal vector n for $\mathcal{P}$ using the vector product of the direction vectors of $\mathcal{P}$:

$$n = (1,2,-1) \times (1,-3,-1) = (-5,0,-5).$$

Notice that we can replace $n = (-5,0,-5)$ by slightly simpler vector $n = (1,0,1)$, since it also is a normal vector for $\mathcal{P}$.

If we have the angle β between n and d, then α could be found as $\alpha = \frac{\pi}{2} - \beta$.

To get β just use the definition by dot product $\cos(\beta) = \frac{n \cdot d}{|n|\,|d|} = \frac{1}{\sqrt{34}}$.

Exercises

E.2.1. In $\mathbb{R}^2$ we are given the vector $v = (2,3)$ and two points $A = (-1,3)$, $B = (-2,1)$. **1.** Write the vector and parametric forms of the line ℓ_1 passing via A and B. **2.** Write the normal and general form of the line ℓ_2 passing via the point A and having the normal vector $-2v$. **3.** Find the distance of the point $C = (0,3)$ from the line ℓ_1.

E.2.2. The line ℓ is given in $\mathbb{R}^2$ as graph of the function $y = f(x) = 3x + 1$. **(1)** Write the normal form of the line ℓ_1 which is parallel to ℓ, and is passing via the point $C = (1,2)$. **(2)** Write the general equation of the line ℓ_2 which is perpendicular to l, and is passing via the point $D = (0,3)$.

E.2.3. We are given three points $A = (1,2)$, $B = (-1,1)$, $C = (4,c)$ in $\mathbb{R}^2$. **(1)** Find vector form and the equation of line ℓ_1 passing via A and B. **(2)** Find such a value c that the line ℓ_2 passing via A and C is perpendicular to ℓ_1. **(3)** Write the parametric form and the normal form of the line ℓ_2.

E.2.4. Take two linear functions $f_1(x) = k_1 x + c_1$ and $f_2(x) = k_2 x + c_2$. From Calculus you know that their graphs are lines. Interpreting them in vector language show that: **(1)** these graphs are parallel if and only if $k_1 = k_2$; **(2)** these graphs are perpendicular if and only if $k_1 \cdot k_2 = -1$. *Hint*: Use the fact that, if α_1 and α_2 are the angles formed by these graphs with the OX axis respectively, then $k_1 = \tan(\alpha_1)$ and $k_2 = \tan(\alpha_2)$.

E.2.5. In $\mathbb{R}^2$ we are given the points $A = (4,5)$, $B = (0,3)$, $C = (4,-1)$. **(1)** Find the vector, parametric, normal, general forms of the line ℓ_1 which is passing via the point A, and has the direction vector $-5\overrightarrow{BC}$. **(2)** Find the vector, parametric, normal, general forms of the line ℓ_2 which is passing via the midpoint of the segment AB, and has the normal vector $\overrightarrow{AC}$. **(3)** Write two general equations obtained for ℓ_1 and ℓ_2 above as a system of linear equations in variables x and y. Deduce if that system has a solution (find the number of solutions) just by comparing the direction vectors for two lines. Explain your answers.

E.2.6. In $\mathbb{R}^3$ we are given the points $A = (2,-1,1)$, $B = (1,0,1)$, $C = (2,1,0)$. **(1)** Write the normal and general forms of the plane $\mathcal{P}$ which contains these points. **(2)** Which is the angle α between the vector $v = (-2,0,1)$ and the plane $\mathcal{P}$?

E.2.7. Two planes $\mathcal{P}_1$ and $\mathcal{P}_2$ are given by general equations respectively: $x + 2y - z = 1$ and $x + z = -2$ **(1)** Find out if $\mathcal{P}_1$ and $\mathcal{P}_2$ are perpendicular. **(2)** Find the equation of the plane $\mathcal{P}_3$ that passes through $A = (1,0,-1)$ and is perpendicular to both $\mathcal{P}_1$ and $\mathcal{P}_2$.

E.2.8. In $\mathbb{R}^3$ we are given the points $A = (2,0,3)$, $B = (0,2,1)$, the plane $\mathcal{P}$ with its general form $2x + 3y - z + 1 = 0$, and two vectors $u = (1,3,0)$, $w = (2,0,-1)$. **(1)** Find the vector, parametric, normal, general forms of the plane $\mathcal{Q}$ which is passing via A and is parallel to $\mathcal{P}$. **(2)** Find the vector, parametric, normal, general forms of a plane $\mathcal{R}$ which is passing via B and is parallel to the vectors u, w. **(3)** Write the general equations found for $\mathcal{Q}$ and $\mathcal{R}$ above as a system of linear equations in variables x, y, z. Deduce if that system has a solution (find if the number of solutions is finite or infinite!) just by comparing the normal vectors of two planes.

E.2.9. The points $A = (1,0,2)$, $B = (0,3,-1)$, $C = (2,1,0)$ are given in $\mathbb{R}^3$. **(1)** Find the vector and parametric forms of the plane $\mathcal{P}$ passing by these points. **(2)** Find the normal and general forms of the plane $\mathcal{P}$. *Hint*: use cross product.

E.2.10. A triangle is given in $\mathbb{R}^3$ with its vertices $A = (1,0,2)$, $B = (1,2,2)$, $C = (1,2,-1)$. **(1)** Find the height h of the triangle (distance from C to the base AB). **(2)** Find the area of the triangle.

E.2.11. A parallelogram $ABCD$ is given in $\mathbb{R}^3$ (the vertices are listed in clockwise order). We know three vertices $A = (0,1,2)$, $B = (2,0,2)$, $C = (0,2,-1)$. **(1)** Write the parametric forms of the edges AD and CD. **(2)** Compute the angle $\alpha = \angle ADC$.

E.2.12. Let us go back to the notations of the Exercise E.1.12 about the Great Pyramid of Giza. **(1)** Find the cross product w of the vectors corresponding to edges BM and CB. **(2)** Write the equation of the plane $\mathcal{P}$ which is parallel to the side BCM and contains the midpoint L of the edge MD. **(3)** Write a general from for the line ℓ passing via the vertices D and M.

E.2.13. We are given the points $A = (1,3,1)$, $B = (2,4,3)$, $C = (0,-1,-4)$, $D = (2,1,2)$ in $\mathbb{R}^3$. **(1)** Find the vector and parametric forms of the line ℓ_1 passing by the points A and B, and of the line ℓ_2 passing by the points C and D. **(2)** Find the distance between the lines ℓ_1 and ℓ_2 (i.e., the *minimum* of distances of all possible points of ℓ_1 from points of ℓ_2). *Hint*: consider the vectors $n = \overrightarrow{MN}$, where $M \in \ell_1$ and $N \in \ell_2$. If n is the *shortest* one of all such vectors, then n is orthogonal to ℓ_1 *and* to ℓ_2. **(3)** Find the general forms for ℓ_1 and for ℓ_2. *Hint*: to find normal vectors for ℓ_1 and ℓ_2 you may use the trick from Example 2.10.

CHAPTER 3

The complex space $\mathbb{C}^n$ and modular space $\mathbb{Z}_p^n$

3.1. The complex space $\mathbb{C}^n$

For this section we need some basic facts on complex numbers, and most likely you already are familiar with them. If not, please check appendices C.1, C.2.

Construction of the complex spaces $\mathbb{C}^n$ is very similar to construction of real spaces $\mathbb{R}^n$, and the main changed actor is the *field of scalars* from which we pick the coordinates of the vectors and the scalar multipliers: this time we use the field of scalars $\mathbb{C}$.

Define the complex *n-dimensional space* as the Cartesian product:

$$\mathbb{C}^n = \{(x_1, x_2, \dots, x_n) \,|\, x_i \in \mathbb{C},\ i = 1, \dots, n\}$$

for any natural $n = 1, 2, 3, \dots$, and denote its vectors as $v = (x_1, x_2, \dots, x_n)$. Other alternative notation are $v = [x_1, x_2, \dots, x_n]$ or

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

(just like in the case of real vectors). Operations with complex vectors also are defined in analogy with real vectors: for $v_1 = (x_1, x_2, \dots, x_n)$ and $v_2 = (y_1, y_2, \dots, y_n)$ in $\mathbb{C}^n$ their *sum* is defined by

$$v_1 + v_2 = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n).$$

In column vector notation this looks like:

$$v_1 + v_2 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

For any $v = (x_1, x_2, \dots, x_n) \in \mathbb{C}^n$ and any scalar $a \in \mathbb{C}$ the product av is defined as $av = a(x_1, x_2, \dots, x_n) = (ax_1, ax_2, \dots, ax_n)$, or:

$$a\,v = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix}.$$

Example 3.1. Let us do some vector operations in complex space $\mathbb{C}^3$.

For the vectors $u = (1+i, 3i, 2-4i)$ and $v = (-3i, 1-2i, 5i)$ we have:

$$u + v = (1-2i, 1+i, 2+i).$$

And for the scalar $a = 2+i \in \mathbb{C}$ we can calculate the vectors:

$$au = (2+i)(1+i, 3i, 2-4i)$$

$$= (1+3i, -3+6i, 12-6i).$$

In Section 1.2 we collected the *main algebraic properties* for real spaces $\mathbb{R}^n$ in Proposition 1.1. Their analogs hold for the complex spaces $\mathbb{C}^n$ also. We do not restate the main algebraic properties for complex spaces as a new proposition, since it would be the copy of Proposition 1.1 with one difference only: all occurrences of $\mathbb{R}$ should just be replaced by $\mathbb{C}$. And the proofs of the properties for the complex case also are trivial. Consider some examples only:

Example 3.2. The addition of complex vectors is *commutative* because the addition of complex numbers is commutative. Say:

$$\begin{aligned}&(2+i,\ -i,\ 2+i)+(1+5i,\ 3i,\ 4)\\ &=(2+i\ +\ 1+5i,\ \ -i\ +\ 3i,\ \ 2+i\ +\ 4)\\ &=(1+5i\ +\ 2+i,\ \ 3i\ +\ (-i),\ \ 4\ +\ 2+i)\\ &=(1+5i,\ 3i,\ 4)+(2+i,\ -i,\ 2+i).\end{aligned}$$

As a *zero* vector $\vec{0}$ in $\mathbb{C}^n$ we may take the vector with n zero coordinates

$$\vec{0}=(0,0,\dots,0)$$

since 0 is a complex number also. Existence of opposite vector in $\mathbb{C}^n$ is evident. For, say $v=(5+i,\ -4i,\ -7+i)\in\mathbb{C}^3$ we may take:

$$-v=(-5-i,\ 4i,\ 7-i).$$

Does the analog of Remark 1.2 also hold for complex spaces, i.e., can we *divide* a complex vector $v=(x_1,x_2,\dots,x_n)$ by a non-zero complex number z to get:

$$\frac{1}{z}v=\left(\frac{x_1}{z},\frac{x_2}{z},\dots,\frac{x_n}{z}\right)$$

in $\mathbb{C}^n$? The answer is positive, provided that any complex number x (including the coordinates x_i of v) can be divided by z. To show that first suppose z is *real*. Then for any $x=a+bi$:

$$\frac{x}{z}=\frac{a+bi}{z}=\frac{a}{z}+\frac{b}{z}i\in\mathbb{C},\quad\text{with }\frac{a}{z},\ \frac{b}{z}\in\mathbb{R}.$$

This gives us the hint: compute a fraction $\frac{x}{z}$ of complex numbers x and z by first modifying it so that the denominator becomes a real number. Recall that for any $z\in\mathbb{C}$ the product $z\,\bar{z}$ is a real number (see basic rule **6** in Appendix C.2). Thus, for any $z=c+di\neq 0$ we have:

$$\frac{x}{z}=\frac{a+bi}{c+di}=\frac{a+bi}{c+di}\cdot\frac{c-di}{c-di}$$

$$=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2}=\frac{(ac+bd)+(bc-ad)i}{|z|^2}=\frac{ac+bd}{|z|^2}+\frac{bc-ad}{|z|^2}i=e+fi$$

with both $e=\frac{ac+bd}{|z|^2}$ and $f=\frac{bc-ad}{|z|^2}$ being real numbers.

Example 3.3. Let us do some divisions with complex numbers:

$$\frac{6+5i}{3}=2+\frac{5}{3}i,$$

$$\frac{1+2i}{2+3i}=\frac{1+2i}{2+3i}\cdot\frac{2-3i}{2-3i}$$

$$=\frac{2-6i^2+4i-3i}{2^2+3^2}=\frac{8+i}{13}=\frac{8}{13}+\frac{1}{13}i,$$

$$\frac{3-4i}{2i}=\frac{3-4i}{2i}\cdot\frac{i}{i}$$

$$=\frac{3i-4i^2}{2i^2}=\frac{4+3i}{-2}=-2-\frac{3}{2}i.$$

Notice that for the third division example we multiplied the numerator and the denominator not by $-2i$ but by i, as it already is enough to get a real denominator.

Example 3.4. Assume we are given the vector $u=(1+i,3i,2-4i)$ in $\mathbb{C}^3$ and the scalar $z=1+i$. Then we have:

$$\begin{aligned}\tfrac{1}{z}u&=\tfrac{1}{1+i}(1+i,3i,2-4i)\\ &=\left(1,\ \tfrac{3}{2}+\tfrac{3}{2}i,\ -1-3i\right)\in\mathbb{C}^3.\end{aligned}$$

3.2. The finite modular space $\mathbb{Z}_p^n$

Let us fix a prime p and call it *modulus*. You perhaps have already learned about the set

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$$

with two *modular operations* $+_p$ and $\cdot_p$ on it. If not, see background information in appendices B.1, B.2. In particular, make sure you are familiar with the following main facts and agreements about:

1. Operations of addition and multiplication in $\mathbb{Z}_p$ have the following properties: they are *closed*, *commutative*, *associative* and *distributive* operations. There are additive *zero* 0 and multiplicative *unit* 1 elements in $\mathbb{Z}_p$. See Appendix B.1.

2. There is an *opposite* number $-x$ for every $x \in \mathbb{Z}_p$. And, since p is prime, in $\mathbb{Z}_p$ there is an *inverse* x^{-1} for any non-zero number $x \in \mathbb{Z}_p$. See Theorem B.5 in Appendix B.2.

3. We agree to use the symbol $\mathbb{Z}_p$ with prime modulus p only, even if we do not mention that p is prime. Also for briefness we agree to denote the operations in $\mathbb{Z}_p$ not by $+_p$ and $\cdot_p$ but by just $+$ and $\cdot$ whenever from the context it is clear that we work in $\mathbb{Z}_p$ (see Agreement B.4).

The listed properties make the operations on $\mathbb{Z}_p$ "similar" to operations on $\mathbb{R}$, and we can consider $\mathbb{Z}_p$ as a *field of scalars* to define a new space. In the Cartesian product $\mathbb{Z}_p^n = \{(x_1, x_2, \ldots, x_n) \,|\, x_i \in \mathbb{Z}_p,\ i = 1, \ldots, n\}$ consider the vectors $v = (x_1, x_2, \ldots, x_n)$, or in row- or column vector notation:

$$v = [x_1, x_2, \cdots, x_n] \quad \text{or} \quad v = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

Operations between these vectors can be defined just like we did it for real or complex vectors: for $v_1 = (x_1, x_2, \ldots, x_n)$ and $v_2 = (y_1, y_2, \ldots, y_n)$ their *sum* is defined by $v_1 + v_2 = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$. In, say, column vector notation this looks like:

$$v_1 + v_2 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

Next, for any $v = (x_1, x_2, \ldots, x_n)$ and any scalar $a \in \mathbb{Z}_p$ define the product $a\,v = a(x_1, x_2, \ldots, x_n) = (ax_1, ax_2, \ldots, ax_n)$, or in column vector notation by:

$$a\,v = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix}.$$

Example 3.5. In $\mathbb{Z}_5^4$ for vectors $u = (2, 3, 4, 0)$ and $v = (4, 2, 4, 2)$ we have

$$u + v = (2+4, 3+2, 4+4, 0+2) = (1, 0, 3, 2),$$

and for the scalar $a = 3$ we have

$$au = (3 \cdot 2,\ 3 \cdot 3,\ 3 \cdot 4,\ 3 \cdot 0) = (1, 4, 2, 0).$$

(notice that we no longer used the symbols $+_5$ and $\cdot_5$, as agreed above).

Example 3.6. Let us calculate in $\mathbb{Z}_7^3$ the following expression:

$$w = 3(1, 0, 5) - (5, 1, 2) + 5(2, 2, 6)$$

$$= (3, 0, 1) - (5, 1, 2) + (3, 3, 2) = (1, 2, 1).$$

Example 3.7. In Figure 3.1 we present the modular spaces $\mathbb{Z}_7^2$ and $\mathbb{Z}_5^3$ with some vector operations in them.

$\mathbb{Z}_7^2$ consists of $49 = 7^2$ points. The sum of vectors $u = (4,5)$ and $v = (1,3)$ is the vector $u + v = (5,1)$, i.e., the parallelogram rule no longer seems to work (in fact, it works, but we are no longer able to visualize it).

Then check the scalar multiples of v. The vector $2v = (2,6)$ seems to be on the same line with v. But the vector $3v = (3,2)$ seems not to be collinear with them (in fact, it is collinear, but we are not able *to notice* the modular line in $\mathbb{Z}_7^2$).

The modular space $\mathbb{Z}_5^3$ consists of $125 = 5^3$ points. Notice that for $u = (4,0,3)$ and $v = (3,2,2)$ we have $u + v = (2,2,0)$. Also notice that $2v = 2(3,2,2) = (1,4,4)$, and so the vectors v and $2v$ do not seem to be collinear (in fact, they are, but we do not *see* that).

Earlier we collected the *main algebraic properties* for real spaces $\mathbb{R}^n$ in Proposition 1.1 of Section 1.2. Then in Section 3.1 we noticed that their analogs also hold for the complex spaces $\mathbb{C}^n$.

It is very easy to check that the analogs for these properties also hold for modular spaces $\mathbb{Z}_p^n$. We do not present the main algebraic properties for modular spaces as one more proposition, since that would be the copy of Proposition 1.1 with one difference only: all occurrences of $\mathbb{R}$ should just be replaced by $\mathbb{Z}_p$.

Since the proofs are trivial, we consider some examples only:

Example 3.8. The addition of modular vectors is *commutative* because the modular addition is commutative in $\mathbb{Z}_p$. Consider operations in $\mathbb{Z}_5^3$:

$$\begin{aligned}
&(1,4,3)+(3,2,0)\\
&=(1+3,\ 4+2,\ 3+0)\\
&=(3+1,\ 2+4,\ 0+3)\\
&=(3,2,0)+(1,4,3).
\end{aligned}$$

Existence of *opposite vector* in $\mathbb{Z}_p^n$ is evident. For, say $v = (4,2,1) \in \mathbb{Z}_5^3$ take:

$$-v = (5-4,\ 5-2,\ 5-1) = (1,3,4)$$

(see property **6** about the opposite element in Appendix B.1).

The addition of modular vectors is *associative* because the modular addition is associative in $\mathbb{Z}_p$. Consider example in $\mathbb{Z}_5^3$:

$$\begin{aligned}
&\big((1,4,3)+(3,2,0)\big)+(1,2,3)\\
&=(4,1,3)+(1,2,3)\\
&=(0,3,1)\\
&=(1,4,3)+(4,4,3)\\
&=(1,4,3)+\big((3,2,0)+(1,2,3)\big).
\end{aligned}$$

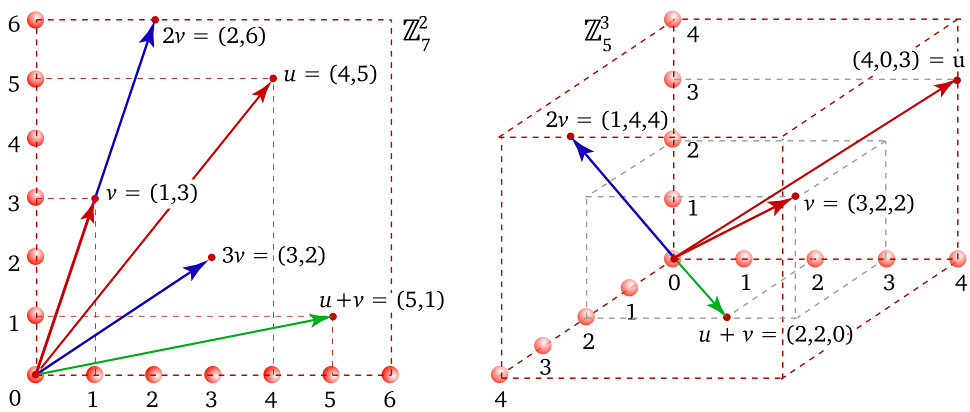


FIGURE 3.1. The finite spaces $\mathbb{Z}_7^2$ and $\mathbb{Z}_5^3$.

And as a *zero* vector $\vec{0}$ in $\mathbb{Z}_p^n$ we may take the vector with n zero coordinates

$$\vec{0} = (0, 0, \ldots, 0),$$

which is possible since the number 0 also is contained in $\mathbb{Z}_p$.

We earlier stressed that the spaces $\mathbb{R}^n$ (see Remark 1.2) and $\mathbb{C}^n$ both have the property of divisibility of vectors by a non-zero scalar. As it follows from Theorem B.5, the modular space $\mathbb{Z}_p^n$ also possesses *divisibility* property: any vector $v = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_p^n$ can be divided by any non-zero scalar c by the formula

$$c^{-1}v = \left(c^{-1} \cdot x_2,\ c^{-1} \cdot x_2, \ldots, c^{-1} \cdot x_n\right)$$

because the inverse c^{-1} does exist in $\mathbb{Z}_p$, and we can multiply all the coordinates by it (in Appendix B.2 we explained how to compute c^{-1} by the Extended Euclid's Algorithm). Notice that we intentionally write not $\frac{1}{c}$ but c^{-1}, since this is the notation normally used in the field $\mathbb{Z}_p$.

Example 3.9. Consider some vector division samples in modular spaces.

Compute the half of the vector $v = (3, 2, 2)$ in $\mathbb{Z}_5^3$. We know the inverse $2^{-1} = 3$ of 2 in $\mathbb{Z}_5$ (see Example B.6). Thus, the half of v is

$$2^{-1}(3, 2, 2) = 3\,(3, 2, 2) = (4, 1, 1).$$

Next find the one-third of the vector $w = (3, 2)$ in $\mathbb{Z}_7^2$. Since $-2 \cdot 7 + 5 \cdot 3 = 1$, we have $3^{-1} = 5$ (see Appendix B.2). Thus the one-third of w is

$$3^{-1}(3, 2) = 5(3, 2) = (1, 3).$$

Now check the Figure 3.1 in which we already have seen that $3\,(1, 3) = (3, 2) = w$.

Example 3.10. In Example B.8 using Euclid's Algorithm we show that $62^{-1} = 95$ in $\mathbb{Z}_{151}$. So for the vector $v = (14, 125, 9) \in \mathbb{Z}_{151}^3$ we have

$$62^{-1}v = 95v = (122, 97, 100).$$

Exercises

E.3.1. Let $a = i - 1$ and $u = (2 - i, 3, -i)$, $v = (2i, 0, -i) \in \mathbb{C}^3$. **(1)** Write $2u - 3v$ as a column vector. **(2)** Write $a(u + v)$ as a row vector. **(3)** Write $a^{-1}u$ as a column vector.

E.3.2. We are given the vectors $u = (2 - i,\ 3i,\ 1 + i)$, $v = (-3i,\ 4 - i,\ 2)$ in $\mathbb{C}^3$, and the complex scalar $c = 2 - i$, $d = 1 + i$. **(1)** (5 points). Compute the vector $w_1 = c^3(u - v)$. **(2)** (5 points). Compute the vector $w_2 = \frac{c}{d}u$. **(3)** (5 points). Compute the vector $w_3 = \frac{(u+v)}{c}$.

E.3.3. We are given the vectors $u = [1 + 3i, 2 - i]$, $v = [5i, 2 - i]$ in $\mathbb{C}^2$, and the complex scalars $c = 1 - i$ and $d = -2 + i$ in $\mathbb{C}$. **(1)** Compute the vector $w = (c^2 + d)(cu + v)$ and write it in *row* vector form. **(2)** Compute the vector $w = (c + d)^{-1}(u + v)$ and write it in *column* vector form.

E.3.4. For a vector $v = (x_1, \ldots, x_n) \in \mathbb{C}^n$ denote $\bar{v} = (\bar{x}_1, \ldots, \bar{x}_n) \in \mathbb{C}^n$ **(1)** Prove that $v + \bar{v} \in \mathbb{R}^n$. **(2)** Find all those vectors $v \in \mathbb{C}^n$ for which $v - \bar{v} \in \mathbb{R}^n$.

E.3.5. **(1)** How many are the 6'th roots of 1? List them all. **(2)** For each t_i of these roots of 1 write the complex vector $u_i = (t_i, t_i^2)$ in space $\mathbb{C}^2$.

E.3.6. Let $u = [2, 1, 0, 1]$, $v = [0, 2, 1, 1] \in \mathbb{Z}_3^4$. **(1)** Find $u + v$ and $2v$. **(2)** Find the half of u. **(3)** Find the opposites $-u$ and $-v$. **(4)** Which is the number of vectors in $\mathbb{Z}_3^4$ (explain)?

E.3.7. We are given the vectors $u = \begin{bmatrix} 3 \\ 0 \\ 2 \end{bmatrix}$ and $v = \begin{bmatrix} 0 \\ 4 \\ 1 \end{bmatrix}$ in $\mathbb{Z}_5^3$. **(1)** Find the vectors $3u + v$ and $-2v$. **(2)** Find the vector $\frac{u-v}{4}$. *Hint*: you actually do not need the Extended Euclid's Algorithm to compute 4^{-1} in $\mathbb{Z}_5$, as it contains only four non-zero elements to choose from.

E.3.8. We are given the vector $v = \left[\begin{smallmatrix} 97 \\ 53 \end{smallmatrix}\right]$ in the modular space $\mathbb{Z}_{151}^2$. **(1)** Find the vector $14v$. **(2)** Find the opposite $-v$ of the vector v. **(3)** Find the vector $\frac{v}{62}$. *Hint*: use Example B.8, i.e, you do not have to apply Euclid's Algorithm for this point. **(4)** Find the vector $\frac{v}{65}$. *Hint*: use the Extended Euclid's Algorithm to find the inverse 65^{-1} of 65 in $\mathbb{Z}_{151}$ (see Appendix B.2).

E.3.9. **(1)** Find three vectors in $\mathbb{Z}_3^3$ which are collinear. **(2)** Find three vectors in $\mathbb{Z}_3^3$ no pair of which is collinear.

E.3.10. Let $u = (0,1,0,1,1)$, $v = (1,0,1,1,1) \in \mathbb{Z}_2^5$ be *binary* vectors. **1.** Find $u+v$. **2.** Find $w = (z_1, z_2, z_3, z_4, z_5) \in \mathbb{Z}_2^5$ if z_i is obtained by logical operation $z_i = x_i \texttt{ XOR } y_i$, where x_i and y_i are the i'th coordinates of u and v respectively. Is w equal to $u+v$?

CHAPTER 4

Introduction to general fields

4.1. Definition and examples of fields

You surely noticed the general plan we followed in previous sections: each time we selected a *field of scalars*, such as $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$, and then based on that field we built the space $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathbb{Z}_p^n$, respectively, using a Cartesian product. The sum of vectors of type $v = (x_1, x_2, \ldots, x_n)$, and the product of a scalar a with v, were defined as coordinate-wise operations.

Could we generalize the approach like this: take an *arbitrary number set* F (or even more generally an *arbitrary set* F with operations of addition $+$ and multiplication $\cdot$), and define a "space" F^n for any $n = 1, 2, \ldots$? In particular, can we define the "spaces", say, $\mathbb{N}^n$, $\mathbb{Z}^n$, $(0,5)^n$, $(-1,1)^n$ for the set of positive integers $\mathbb{N}$, for the set of all integers $\mathbb{Z}$, for the intervals $(0,5)$, $(-1,1)$, etc.?

No, because in such cases the "space" F^n will fail to have some important properties that the real space around us (in which we live!) is expected to have. For example, in $\mathbb{N}^n$ and in $\mathbb{Z}^n$ we not always can divide the vectors to parts: say, the midpoint $\left(\frac{3}{2}, \frac{1}{2}, 1\right)$ of $v = (3,1,2)$ is not in $\mathbb{N}^n$ or in $\mathbb{Z}^n$. Also, the opposite vector $-v = (-3,-1,-2)$ is not in $\mathbb{N}^n$ or in $(0,5)^n$. Further, $\mathbb{N}^n$ and $(0,5)^n$ do not contain the origin $O = (0, \ldots, 0)$. The Cartesian product $(-1,1)^n$ seems to be "better", as it does allow some divisions of its vectors, it does contain the origin $O = (0, \ldots, 0)$, and it does contain the opposite $-v$ of each of its vectors v. But $(-1,1)^n$ has another "defect": we expect that the sum of any two vectors of the space still is inside the space, and this fails to take place in $(-1,1)^n$ because, say, $(0.6, \ldots, 0.6) + (0.7, \ldots, 0.7) = (1.3, \ldots, 1.3) \notin (-1,1)^n$.

This examples show that one should thoroughly select the set F so that its operations $+$ and $\cdot$ satisfy the "natural" properties of the ordinary operations of $+$ and $\cdot$ of real numbers $\mathbb{R}$. I.e., we should select a set F "very similar" to $\mathbb{R}$ (as long as we concern its operations) in order to get a space "rather similar" to the real space $\mathbb{R}^n$, see Remark 1.2. This bring us to one of the key definitions of algebra:

Definition 4.1. Let F be a set with operations of addition $+$ and multiplication $\cdot$ defined on it, i.e., for any $a, b \in F$ the sum $a + b \in F$ and the product $a \cdot b \in F$ are given. Then F is a *field*, if the following axioms hold for any $a, b, c \in F$:

1. $a + b = b + a$; *(commutativity of addition)*
2. $(a + b) + c = a + (b + c)$; *(associativity of addition)*
3. there is a zero element $0 \in F$ such that $a + 0 = a$; *(existence of additive identity)*
4. there is an element $-a \in F$ such that $a + (-a) = 0$; *(existence of opposite element)*
5. $a \cdot b = b \cdot a$; *(commutativity of multiplication)*
6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$; *(associativity of multiplication)*
7. there is a non-zero $1 \in F$ such that $a \cdot 1 = a$; *(existence of multiplicative identity)*

8. if $a \neq 0$, then there is $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$; *(existence of inverse)*
9. $a \cdot (b+c) = a \cdot b + a \cdot c$. *(distributivity)*

After this definition we can just say "F is a field" instead of listing all the necessary properties of F. Examples of fields we so far know are $F = \mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for any prime p.

4.2. The space F^n over the field F

Let F be any field. For any $n = 1, 2, \dots$ consider the Cartesian product:

$$F^n = \{(x_1, x_2, \dots, x_n) \,|\, x_i \in F,\ i = 1, \dots, n\}.$$

Call the elements (ordered sequences) $v = (x_1, x_2, \dots, x_n)$ of F^n *vectors*, and call the elements $a \in F$ *scalars* (so we can refer to F as to the *field of scalars*). We may also use row- or column vector notations:

$$v = [x_1, x_2, \cdots, x_n] \quad \text{or} \quad v = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

The scalars $x_1, x_2, \dots, x_n$ are the *coordinates* of v.

For $v_1 = (x_1, x_2, \dots, x_n)$ and $v_2 = (y_1, y_2, \dots, y_n)$ define their *sum* as

$$v_1 + v_2 = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n),$$

which in column vector notation looks like:

$$v_1 + v_2 = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

For any vector $v = (x_1, x_2, \dots, x_n)$ and any scalar $a \in F$ define:

$$a\,v = a(x_1, x_2, \dots, x_n) = (ax_1, ax_2, \dots, ax_n),$$

or in column vector notation:

$$a\,v = a \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ ax_2 \\ \vdots \\ ax_n \end{bmatrix}.$$

The *main algebraic properties* for F^n are collected in:

Proposition 4.2. *The following properties hold for any vectors $u, v, w \in F^n$ and scalars $a, b \in F$:*

1. $u + v = v + u$; *(commutativity of vector addition)*
2. $(u+v) + w = u + (v+w)$; *(associativity of vector addition)*
3. *there is a vector $0 \in F^n$ such that $v + 0 = v$;* *(existence of additive identity)*
4. *there is a vector $-v \in F^n$ such that $v + (-v) = 0$;* *(existence of opposite vector)*
5. $a(u+v) = au + av$; *(distributivity of vector addition)*
6. $(a+b)v = av + bv$; *(distributivity of multiplication by scalar)*
7. $(a \cdot b)v = a(bv)$; *(homogeneity of multiplication by scalar)*
8. $1v = v$. *(unitarity of multiplication by scalar)*

You may notice that this is the copy of Proposition 1.1 with minor changes only: the character $\mathbb{R}$ here is replaced by F. The proofs of all points of Proposition 4.2 are easy exercises with application of Definition 4.1, and we omit them.

Now we can characterize the so far constructed spaces $\mathbb{R}^n$; $\mathbb{Q}^n$; $\mathbb{C}^n$; $\mathbb{Z}_p^n$ as special cases of the space F^n for specific values of F. In most part of our course all the facts we obtain will concern not a specific space but all spaces, in general (and later we will learn the *abstract* spaces which are even more general than the F^n).

This brings us to the first main step of *abstraction* in our course: after this point not only the spaces but also other mathematical objects will be introduced on general fields F. For example, in the coming chapters we will consider the linear equations $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ over a field F assuming that all a_i and b belong to F. We may consider polynomials $a_0x^n + a_1x^{n-1} + \cdots + a_n$ over a field F assuming that all the coefficients a_i are in F. And we will also discuss matrices $[a_{ij}]$ over a field F assuming all the matrix entries a_{ij} are in F. As we will see later, this more abstract approach not only shortens the notation, but also gives better proofs and quicker computation methods.

Agreement 4.3. Although there are very many fields in mathematics, in this course we are going to mainly use the fileds:

$$\mathbb{R},\ \mathbb{Q},\ \mathbb{C},\ \mathbb{Z}_p$$

we defined earlier. Definition 4.1 is lengthy, and we do not want you to jump back to the nine points of that definition each time you read a phrase like "take a space over a filed F" or "consider an equation over the filed F" in the sequel. Instead, it will be OK if you for now just keep in mind that under F we understand one of the sets $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$ with operations $+$ and $\cdot$ we defined on it. So think of the symbol F as of a shorthand notation for these sets with operations. And in some of the examples below we will mention no field, at all. In all such cases the "most popular" field $F = \mathbb{R}$ will be assumed.

By the way, can you find *other* examples of fields besides $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$?

Exercises

E.4.1. **(1)** Show that the zero element 0 of point 3 in Definition 4.1 is unique in any field. I.e., if for some element $0'$ also holds $a + 0' = a$ for any a, then $0 = 0'$. **(2)** Show that the identity element 1 of point 7 in Definition 4.1 is unique in any field.

E.4.2. Which is the number of vectors in the space F^n, if $F = \mathbb{Z}_p$?

E.4.3. Denote by $\mathbb{Q}(\sqrt{2})$ the set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Clearly, $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$, so we can add and multiply the numbers of $\mathbb{Q}(\sqrt{2})$ as real numbers. Is $\mathbb{Q}(\sqrt{2})$ a field with these operations? *Hint:* notice that for any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ the product $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = r$ is a *rational* number and, therefore, $\frac{a}{r} - \frac{b}{r}\sqrt{2}$ is in $\mathbb{Q}(\sqrt{2})$.

E.4.4. Take $K = \{0, 1, 2, 3\}$ as a *set*. On K define $+_4$ as in $\mathbb{Z}_4$. As multiplication define a new operation $*$. For any $x \in \mathbb{Z}_4$ set $0 * x = x * 0 = 0$ and $1 * x = x * 1 = x$. Further $2 * 2 = 3$, $3 * 3 = 2$ and $2 * 3 = 3 * 2 = 1$. Show that K with $+_4$ and $*$ is a field.

E.4.5. In the field $F = \mathbb{Q}(\sqrt{2})$ of Exercise E.4.3 we are given the scalars $a = 2 + \sqrt{2}$, $b = 3\sqrt{2}$, and in the space $F^2 = \mathbb{Q}(\sqrt{2})^2$ we are given the vectors $u = [3\sqrt{2}, -1]$, $v = [1 - \sqrt{2}, \sqrt{2}]$. **(1)** Compute the vector $w = \frac{u+bv}{a}$. **(2)** Compute the vector $w = -\frac{a^2}{b}u$.

E.4.6. Consider the sets $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ and $B = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}$ with ordinary operations $+$ and $\cdot$ of real numbers. **(1)** Is $\mathbb{Q}(\sqrt{3})$ a field? **(2)** Is B a field?

E.4.7. Form Calculus you may recall the *rational functions* defined as fractions $f(x) = \frac{p(x)}{q(x)}$ where $p(x), q(x)$ are real polynomials, and $q(x)$ is *not* zero. For any such two rational functions $f(x) = \frac{p(x)}{q(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ define the point-wise operations of addition $f + g$ and multiplication $f \cdot g$ as follows: $(f+g)(x) = \frac{p(x)\cdot s(x)+r(x)\cdot q(x)}{q(x)\cdot s(x)}$ and $(f \cdot g)(x) = \frac{p(x)\cdot r(x)}{q(x)\cdot s(x)}$. The set of all real rational functions is denoted $\mathbb{R}(x)$. Checking the points of Definition 4.1 detect if $\mathbb{R}(x)$ is a field with respect to addition and multiplication.

E.4.8. Find a space F^n the cardinality of which is **(1)** 11. **(2)** 1024. **(3)** $\aleph_0$ (countable). **(4)** $\mathfrak{c}$ (continuum). Explain answers.

E.4.9. In 1871 Richard Dedekind wrote: *"By a field we will mean every infinite system of real or complex numbers so closed in itself and perfect that addition, subtraction, multiplication, and division of any two of these numbers again yields a number of the system."* (in original *"Unter einem Körper wollen wir jedes System von unendlich vielen reelen oder complexen Zahlen verstehen, welches in sich so abgeschlossen und vollständig ist, dass die Addition, Subtraction, Multiplication und Division von je zwei dieser Zahlen immer wieder eine Zahl desselben System hervorbringt.*") Is Dedekind's definition the same as the modern one?

Part 2

Systems of Linear Equations

CHAPTER 5

Introduction to linear equations

"What we know is a drop, what we don't know, an ocean."
Isaac Newton

5.1. Systems of linear equations and their geometry

Let F be any field. Consider n *variables* $x_1, x_2, \ldots, x_n$ (any n symbols not in F) and call a *linear equation* over the field F in variables $x_1, x_2, \ldots, x_n$ a formal expression

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{5.1}$$

where $a_1, a_2, \ldots, a_n$ (the *coefficients* of the equation) and b (the *constant term* of the equation) are any elements from F. The variables can also be denoted differently, say, by $y_1, y_2, \ldots, y_n$ or $x, y, z, t, \ldots$, etc. Clearly, an equation is not the same as *equality*.

Example 5.1. The expressions

$$3x_1 + 4x_2 = 2x_3 + 5,$$
$$3x - \cos^2(\tfrac{\pi}{6})\, y = \ln(5)$$

are linear equations over $\mathbb{R}$ (do not get confused by π, by square or trigonometric and logarithmic expressions). But

$$2x^2 + xy + 1 = 0$$

is *not* a linear equation.

Example 5.2. And the expression

$$(2+4i)x - iy + 5iz + 4t = 8i$$

is a linear equations over the complex field $\mathbb{C}$. And, similarly,

$$2x + 3y + 6z = 2$$

is a linear equations over the finite modular field $\mathbb{Z}_7$.

The vector $(x_1', x_2', \ldots, x_n') \in F^n$ is the *solution* of the equation 5.1, if we get an *equality* after we substitute the values $x_i' \in F$ for variables x_i, $i = 1, 2, \ldots, n$, i.e.„ if

$$a_1x_1' + a_2x_2' + \cdots + a_nx_n' = b.$$

Example 5.3. Turning to the equations of the previous two examples it is easy to see that $(1,0,1) \in \mathbb{R}^3$ is a solution for the equation $3x_1 + 4x_2 + 2x_3 = 5$ because $3\cdot 1 + 4\cdot 0 + 2\cdot 1 = 5$. is an equality.

$(0,0,0,2i) \in \mathbb{C}^3$ is a solution for $(2+4i)x - iy + 5iz + 4t = 8i$ because $(2+4i)\cdot 0 - i\cdot 0 + 5i\cdot 0 + 4\cdot 2i = 8i$.

And $(4,3,1) \in \mathbb{Z}_7^3$ is a solution for $2x + 3y + 6z = 2$ because $2 \cdot_7 4 \,+_7\, 3 \cdot_7 3 +_7\, 6 \cdot_7 1 = 2$.

Now consider a *system of m linear equations* over F in variables $x_1, x_2, \ldots, x_n$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{5.2}$$

Notice how we used double indices for coefficients a_{ij}, $i = 1, \cdots, m$; $j = 1, \cdots, n$. The vector $(x'_1, x'_2, \ldots, x'_n) \in F^n$ is called a *solution* of this system of linear equations, if is a solution of each of m equations.

A system of linear equations is called *consistent* system, if it has a solution. If it fails to have a solution, it is called *inconsistent* system. *To solve* a system means to determine if it is consistent and, if yes, to find all the solutions.

Consider illustrative examples of consistent or inconsistent systems, and in the same time notice some connections of systems of linear equations with some *geometric* objects.

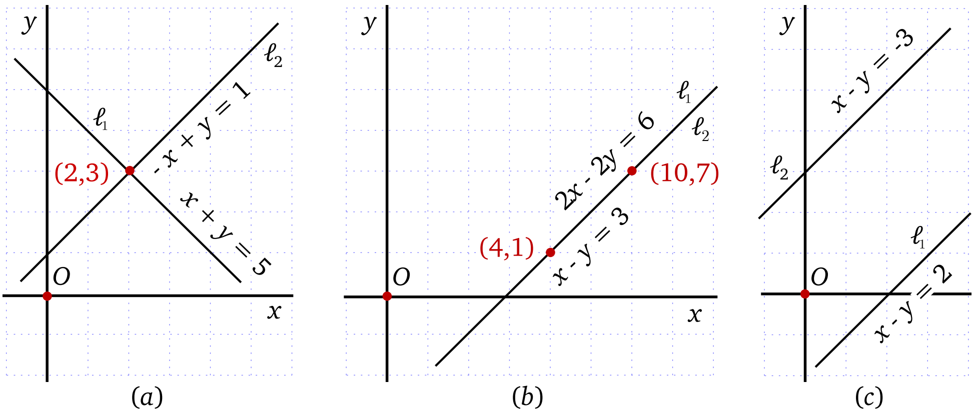


FIGURE 5.1. Three systems and their geometry on $\mathbb{R}^2$.

Example 5.4. Consider the system:

$$\begin{cases} x + y = 5 \\ -x + y = 1. \end{cases}$$

Adding equations we get $0 + 2y = 6$. The only option for y' is $y' = 6/2 = 3$. Then from $x + y = 5$ we get $x' = 5 - y' = 5 - 3 = 2$. And $(x', y') = (2, 3)$ clearly is the (*only*) solution of the system.

On the other hand, these equations define lines ℓ_1 and ℓ_2 in $\mathbb{R}^2$. A point (x', y') is a solution of the system only if it belongs to $\ell_1 \cap \ell_2$. As Figure 5.1 (*a*) shows, those lines actually have just *one* common point.

Example 5.5. Consider the system

$$\begin{cases} x - y = 3 \\ 2x - 2y = 6. \end{cases}$$

The second equation is the same as the first equation, just multiplied by 2. So if some (x', y') is a solution of one of the equations, it is a solution for the second also. Some of the solutions of $x - y = 3$ are $(4, 1)$, $(10, 7)$, $(103, 100)$, and any couple of type $(a+3, a)$. So this system has *infinitely* many solutions.

As Figure 5.1 (*b*) shows, these equations define *coinciding* lines ℓ_1 and ℓ_2 in $\mathbb{R}^2$. So each point of ℓ_1 belongs to ℓ_2, and so it is a solution of the system.

Example 5.6. Consider the third system

$$\begin{cases} x - y = 2 \\ x - y = -3. \end{cases}$$

It has no solution because for *no* couple (x', y') may we have $x' - y' = 2$ and $x' - y' = -3$ simultaneously.

These equations define two *parallel* lines ℓ_1 and ℓ_2 with no intersection $\mathbb{R}^2$, as seen in Figure 5.1 (*c*). No point of $\mathbb{R}^2$ may belong to ℓ_1 and ℓ_2 simultaneously.

Situation is more complicated when the system is in three variables:

$$\begin{cases} a_{11}x + a_{12}y + a_{13}z = b_1 \\ a_{21}x + a_{22}y + a_{23}z = b_2 \\ a_{31}x + a_{32}y + a_{33}z = b_3. \end{cases}$$

Each of the equations determines a plane in $\mathbb{R}^3$. Denote them by $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, and see how their placement may affect the solutions of the system in some cases:

Case 1. The planes $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ may be *parallel*, and the system may have no solution (see Figure 5.2 (a)).

Case 2. $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ may *not* be parallel, but the system still has no solution. Each pair of planes intersects by a different line (see Figure 5.2 (b)).

Case 3. $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ intersect by a *single line* ℓ, and the system has *infinitely many solutions* (see Figure 5.2 (c)).

Case 4. $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ intersect by a *single point* A, and the system has a *single solution* $A=(x',y',z')$ (see Figure 5.2 (d)).

And the situation may be even more mixed if the number of equations or the number of variables is more then 3. The task of full description of all the solutions will be completed in sections 7.1, 7.2, 15.2.

5.2. Elementary operations and first examples of elimination

Call two systems of linear equations in the *same* variables (such as, variables $x_1,\dots,x_n$, or $x,y,z,\dots$, etc.) *equivalent*, if either they both are consistent and the sets of their solutions coincide, or they both are inconsistent. Clearly, this is an *equivalence relation*: it is *reflexive*, *symmetric* and *transitive*.

The method by which we solve a system is going to consist of certain steps, in each of which we replace a system by an equivalent system. If we eventually end up with a system all the solutions of which are known, then they are the solution for our initial system also. Else, if we end up with an inconsistent system, then our initial system also has no solutions. Each of those steps will be one of three main *elementary operations* which transfer the given system to an equivalent one.

Define the following three types of elementary operations on a system of linear equations over a field F:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases}$$

EO1. *Elementary operation of the* 1'*st type*: swap any two rows of the system.

EO2. *Elementary operation of the* 2'*nd type*: multiply a row of the system by a *non-zero* scalar from F.

EO3. *Elementary operation of the* 3'*rd type*: add to a row of the system the scalar multiple of any *other* row.

Example 5.7. Consider the real system:

$$\begin{cases} \quad\;\; y+z=1 \\ 2x-y+z=9 \\ \;\; x-y-z=2 \end{cases}$$

of linear equations, and practice each of elementary operations above. Also notice how we record the elementary operations by special symbols below.

By an elementary operation of the 1'st type swap, say, the 1'st and 3'rd rows:

$$\begin{cases} \;\; x-y-z=2 \\ 2x-y+z=9 \\ \quad\;\; y+z=1. \end{cases}$$

This has a shorthand notation $\boldsymbol{R1} \longleftrightarrow \boldsymbol{R3}$.

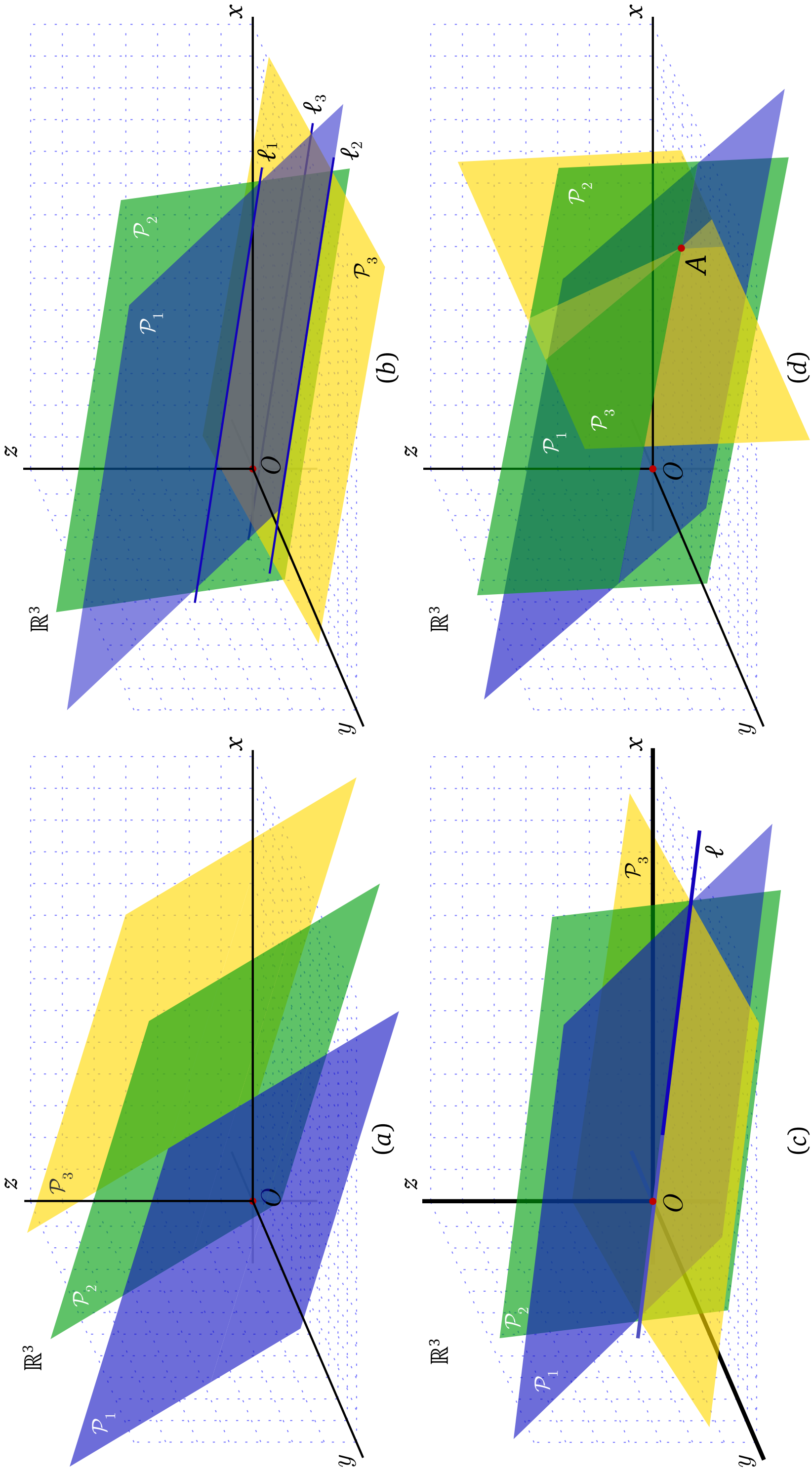


FIGURE 5.2. Three planes in $\mathbb{R}^3$ and the possible options for solutions of system of three equations in three variables.

Next, using an elementary operation of the 2'nd type multiply, say, the 1'st row by 5:

$$\begin{cases} 5x - 5y - 5z = 10 \\ 2x - \ \ y + \ \ z = 9 \\ \qquad\ \ y + \ \ z = 1. \end{cases}$$

This step can be recorded as $\boldsymbol{5 \cdot R1}$.

Finally, using an elementary operation of the 3'rd type add, say, to the 2'nd row the 3'rd row times 7:

$$\begin{cases} 5x - 5y - 5z = 10 \\ 2x + 6y + 8z = 16 \\ \qquad\ \ y + \ \ z = 1. \end{cases}$$

This can be recorded as $\boldsymbol{R2 + 7R3}$.

Clearly, each elementary operation is *reversible*: if we by any of them transform a system to a new system, we can get the old system from the new one. Indeed:

Reversibility is evident for elementary operation of the 1'st type.

Concerning the 2'nd type, recall that all our operations are over a *field* F. So if we multiply a row by a non-zero constant c, we can "undo" the change by multiplying the same row by $c^{-1} \in F$.

Finally, if we by an operation of the 3'rd type add to the i'th row the k't row multiplied by $c \in F$, we can reverse by adding to the i'th row (of the new system) the k't row multiplied by $-c \in F$.

Lemma 5.8. *Each elementary operation transforms a system of linear equations to an equivalent system of linear equations.*

***Proof*.** Since each of elementary operations is reversible, it is sufficient to show that if we apply it to a system, then the solutions of the initial system will also be solutions of the new system. This will complete the proof, since we can come back from the new system to the initial system with all solutions preserved.

If $(x'_1, x'_2, \ldots, x'_n) \in F^n$ is a solution, it will clearly remain a solution for the new system after we swap two rows, or if we multiply a row by a non-zero scalar.

Next, assume we add to the i'th row of the system the k't row times $c \in F$. The new i'th row is:

$$(a_{i1} + c a_{k1})x_1 + (a_{i2} + c a_{k2})x_2 + \cdots + (a_{in} + c a_{kn})x_n = b_i + c b_k.$$

$(x'_1, x'_2, \ldots, x'_n)$ is a solution of for this equation because from the old system we have:

$$a_{i1}x'_1 + a_{i2}x'_2 + \cdots + a_{in}x'_1 = b_i,$$

$$c\, a_{k1}x'_1 + c\, a_{k2}x'_2 + \cdots + c\, a_{kn}x'_1 = c\, b_k,$$

and it remains to just add these equalities. □

There is a special kind of application for elementary operation of the 3'rd type. Assume the coefficient a_{11} is non-zero. If we add to the 2'nd row the 1'st row times $-\frac{a_{21}}{a_{11}}$, then the 1'st summand in the new 2'nd row will be

$$a_{21}x_1 - \frac{a_{21}}{a_{11}} \cdot a_{11}x_1 = a_{21}x_1 - a_{21}x_1 = 0$$

(we can use $\frac{1}{a_{11}}$ since F is a *field*, and the inverse of $a_{11} \neq 0$ exists). Thus, if $a_{11} \neq 0$, we can *turn to* 0 *any of other coefficients in* 1*'st column*.

Let us apply the elementary operations (including the trick above) to three specific examples. Notice how we use the $\Leftrightarrow$ symbol to denote equivalence of systems, and how we use the above mentioned shortcuts

$$\boldsymbol{Ri \longleftrightarrow Rk}, \quad \boldsymbol{c \cdot Ri}, \quad \boldsymbol{Ri + cRk}$$

on the right-hand sides of the formulas in order to highlight which elementary operation we use.

Example 5.9. Consider the system of three linear equations over three variables:

$$\begin{cases} y+z=1 \\ 2x-y+z=9 \\ x-y-z=2 \end{cases}$$

$$\Leftrightarrow \begin{cases} x-y-z=2 \\ 2x-y+z=9 \\ y+z=1 \end{cases} \quad {\scriptstyle R1 \leftrightarrow R3}$$

$$\Leftrightarrow \begin{cases} x-y-\ \ z=2 \\ \quad\ y+3z=5 \\ \quad\ y+\ \ z=1 \end{cases} \quad {\scriptstyle R2+(-2)R1}$$

$$\Leftrightarrow \begin{cases} x-y-\ \ z=\ \ 2 \\ \quad\ y+3z=\ \ 5 \\ \quad\ \ -2z=-4. \end{cases} \quad {\scriptstyle R3+(-1)R2}$$

Thus, $z' = 2$, and $y' = 5-3\cdot 2 = -1$, then $x' = 2-1+2 = 3$. So we have a *single* solution $(3,-1,2)$.

Example 5.10. Next consider the system:

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

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \\ 3x\qquad +3z=4 \end{cases} \quad {\scriptstyle R2+(-2)R1}$$

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \\ \quad 3y-3z=1 \end{cases} \quad {\scriptstyle R3+(-3)R1}$$

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \\ \qquad\quad 0=1. \end{cases} \quad {\scriptstyle R3+(-1)R2}$$

And the third equation seems to have no solution, since $0 \neq 1$. Thus the entire system has *no* solution and is *inconsistent*.

Example 5.11. Finally, consider the system:

$$\begin{cases} x-y+2z=1 \\ 2x+y+\ \ z=2 \\ 3x\qquad +3z=3 \end{cases}$$

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \\ \quad 3y-3z=0 \end{cases} \quad {\scriptstyle R2+(-2)R1;\ R3+(-3)R1}$$

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \\ \qquad\quad 0=0 \end{cases} \quad {\scriptstyle R3+(-1)R2}$$

$$\Leftrightarrow \begin{cases} x-\ \ y+2z=1 \\ \quad 3y-3z=0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x-y+2z=1 \\ \quad\ y-\ \ z=0. \end{cases} \quad {\scriptstyle \frac{1}{3}\cdot R2}$$

If we now take, say, $z' = 1$, we will have a smaller system on just two variables:

$$\begin{cases} x-y+2\cdot 1=1 \\ \quad\ y-\ \ 1\ \ =0 \end{cases}$$

$$\Leftrightarrow \begin{cases} x-y=-1 \\ \quad\ y=\ \ 1 \end{cases} \Leftrightarrow \begin{cases} x=\ \ 0 \\ y=1. \end{cases}$$

The solution is $(0,1,1)$. And if we take *any* value $z' = \alpha \in \mathbb{R}$, we get

$$\begin{cases} x-\ \ y+2\alpha=1 \\ \quad 3y-3\alpha=0 \end{cases} \Leftrightarrow \begin{cases} x-y=1-2\alpha \\ \quad\ y=\alpha \end{cases}$$

$$\Leftrightarrow \begin{cases} x-\alpha=1-2\alpha \\ \qquad y=\alpha \end{cases} \Leftrightarrow \begin{cases} x=1-\alpha \\ y=\alpha. \end{cases}$$

So the solution is $(1-\alpha,\ \alpha,\ \alpha)$ for any $\alpha \in \mathbb{R}$. Say, when $\alpha = 5$ we get the solution $(-4,5,5)$.

Let us summarize these examples to see what we already know and which problems we still face. We know that a system may have one solution, finitely many solutions (any consistent system on a finite field), infinitely many solutions (like Example 5.11), or no solution at all.

We have three types of elementary operations which we used in elimination examples above. But we do *not* know if such an elimination process may output *the same* solutions, if we use other choices of elementary operations. We found infinitely many solutions for the system of Example 5.11. But are these *all* the solutions of this system? What if we apply elementary operations in a different order (or even us a completely different solution method) to find new solutions not covered in Example 5.11?

Also, we do not know what will happen if a system is *inconsistent*. In Example 5.10 we deduced that fact from an evidently wrong statement $0 = 1$. But which output will occur for other inconsistent systems?

To answer these questions we need some technique with *matrices* to which we are about to turn in the next section.

Exercises

E.5.1. **(1)** On $\mathbb{R}^2$ choose poins A, B, C, D so that the line ℓ_1 passing via A and B is parallel to the line ℓ_2 passing via C and D. **(2)** Write the general equations of the lines ℓ_1 and ℓ_2 as a system of linear equations. Then using elementary operations find out if that system is consistent.

E.5.2. **(1)** To system of Example 5.9 apply the following elementary operations: $R1 \longleftrightarrow R2$, $R3 + (-\frac{1}{2})R1$, $R3 + \frac{1}{2}R2$. Which is the solution found after that? **(2)** Find out the fact that the system of Example 5.10 is inconsistent using other elementary operations, such that the final row you get is *not* $0=1$.

E.5.3. In $\mathbb{R}^3$ choose three planes $\mathcal{P}_1$, $\mathcal{P}_2$ and $\mathcal{P}_3$ such that: **(1)** $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ have no intersection. Deduce that the system of linear equations consisting of the equations of these planes is inconsistent. **(2)** $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ have *only one point* in their intersection. Deduce that the system consisting of the equations of these planes is consistent, and has only one solution. **(3)** $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$ have *only one line* in their intersection. Deduce that the system consisting of the equations of these planes is consistent, and has more than one solution.

E.5.4. In $\mathbb{R}^3$ choose three non-zero vectors $n_1,\ n_2,\ n_3$, and write general forms of some planes $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ with normal vectors $n_1,\ n_2,\ n_3$, respectively, such that: **(1)** The corresponding system of linear equations consisting of the general equations of these planes is inconsistent. **(2)** The corresponding system is consistent, and has only one solution. **(3)** The corresponding system is consistent, and has more than one solutions.

E.5.5. Apply the following sequence of the elementary operations to the system you obtained in the first point of Exercise E.5.3: $R1 + 5R2$, $R2 + 5R1$, $R1 + R3$, $R1 \longleftrightarrow R3$, $3 \cdot R2$. Is the resulting system consistent? How can you explain those operations geometrically?

E.5.6. **(1)** Using Exercise E.5.3 or Figure 5.1 and Figure 5.2 show geometrically that if a *real* system of equations in two or three variables has more then one solution, then it also has *infinitely* many solutions. **(2)** Does the statement of the previous point true for any field? I.e., can there be a system of linear equations (over some field F, other then $\mathbb{R}$) which has more than one, but still *finitely* many solutions?

E.5.7. Write a system of linear equations of three variables over *some* field F such that it is consistent and has *exactly two* solutions.

CHAPTER 6

Introduction to matrices

6.1. Matrices over fields

Let a field F be given. Fix two natural numbers m and n and select any $m \cdot n$ elements $a_{ij} \in F$ ($i = 1, \dots, m$ and $j = 1, \dots, n$). Put these $m \cdot n$ elements in a table with m rows and n columns:

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

Call this a *matrix* over the field F with m rows and n columns (or an $m \times n$ matrix, or m-by-n matrix). If $m = n$, then A is called a *square* matrix. The elements a_{ij} are the *entries* or *elements* of the matrix A, and a_{ij} is called the (i, j)'th entry of A. The entries $a_{i1}, \dots, a_{in}$ form the *i'th row* of A. The entries $a_{1j}, \dots, a_{mj}$ form the *j'th column* of A. And $a_{11}, a_{22}, a_{33}, \dots$ form the *diagonal* of A. We can write the matrix shorter:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix},$$

and in the literature there also are other notations of matrices:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \quad \begin{Vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{Vmatrix}, \quad [a_{ij}]_{m,n}, \quad \|a_{ij}\|_{m,n}.$$

The set of all $m \times n$ matrices over F is denoted by $M_{m,n}(F)$, and we can use the short notation $A \in M_{m,n}(F)$ to say *"Let us take an $m \times n$ matrix over the field F"*.

Example 6.1. Here are some matrix examples of different sizes and on different fields:

$$\begin{bmatrix} 3/2 & \pi & 3 \\ 1 & -1 & 0 \\ 0.5 & 1 & \sqrt{2} \\ 0 & -3 & 0 \end{bmatrix} \in M_{4,3}(\mathbb{R}),$$

$$\begin{bmatrix} 3 & 1 \\ 1 & 4 \\ 2 & 0 \end{bmatrix} \in M_{3,2}(\mathbb{Z}_5),$$

$$\begin{bmatrix} i & 2i & 3 \\ 1 & i & 1 \\ 0 & 0 & i \end{bmatrix} \in M_{3,3}(\mathbb{C}).$$

A matrix may also consist of one row or one column only:

$$\begin{bmatrix} 5 & \frac{1}{3} & 4 & -1 & 2 & 0 \end{bmatrix} \in M_{1,6}(\mathbb{Q}),$$

$$\begin{bmatrix} 1 \\ 4 \\ -2 \\ 0 \\ -\frac{1}{2} \end{bmatrix} \in M_{5,1}(\mathbb{R})$$

(we call such matrices a *row matrix* or a *column matrix*).

6.2. Writing elimination process by matrices and the row-equivalence

The first application of matrices is to use them as means to write the elimination process in shorter way. For a given system of linear equations over a field F

$$\begin{cases} a_{11}x_1 & +a_{12}x_2 & +\cdots+a_{1n}x_n & =b_1 \\ a_{21}x_1 & +a_{22}x_2 & +\cdots+a_{2n}x_n & =b_2 \\ \multicolumn{4}{c}{\dotfill} \\ a_{m1}x_1 & +a_{m2}x_2 & +\cdots+a_{mn}x_n & =b_m \end{cases}$$

we form two matrices consisting of coefficients and constants of the system: the *matrix* A of the system (sometimes also called the *coefficient matrix* of the system), and the *augmented matrix* $\bar{A}$ of the system (sometimes also denoted by $[A\,|\,B]$):

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \qquad \bar{A}=\left[\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}\right].$$

Example 6.2. For the system of linear equations in Example 5.9

$$\begin{cases} \quad y+z=1 \\ 2x-y+z=9 \\ x \quad -y-z=2 \end{cases}$$

we have the matrix and the augmented matrix respectively:

$$A=\begin{bmatrix} 0 & 1 & 1 \\ 2 & -1 & 1 \\ 1 & -1 & -1 \end{bmatrix}, \quad \bar{A}=\left[\begin{array}{ccc|c} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{array}\right].$$

These matrices are shorter means to hold information for the system. $\bar{A}$ already is enough to restore the system: the symbols "x", "y", "x_i", "$+$", "$=$" hold no essential information, and they can be dropped.

Recall that in elimination process we actually manipulate with the coefficients a_{ij} and constants b_i only. This brings us to a useful idea: what if we define the analogs of three elementary operations of the system for the matrices, and do the elimination process using *matrices only*?

For a matrix $A \in M_{m,n}(F)$ define three *elementary matrix operations*:

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

EO1. *Elementary matrix operation of the* 1'*st type*: swap any two rows of A.
EO2. *Elementary matrix operation of the* 2'*nd type*: multiply a row of A by a non-zero scalar from F.
EO3. *Elementary matrix operation of the* 3'*rd type*: add to a row of A the multiple of any *other* row. Say, if we add to i'th row the k't row times $c \in F$, the new i'th row is:

$$\begin{bmatrix} a_{i1}+ca_{k1} & a_{i2}+ca_{k2} & \cdots & a_{in}+ca_{kn} \end{bmatrix}.$$

Example 6.3. Consequently apply operations of three types, starting by $A \in M_{3,3}(\mathbb{R})$:

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

$$\begin{bmatrix} 3 & 1 & 0 \\ 2 & 1 & 3 \\ 1 & -2 & 1 \end{bmatrix} \quad R1 \leftrightarrow R3.$$

$$\begin{bmatrix} 15 & 5 & 0 \\ 2 & 1 & 3 \\ 1 & -2 & 1 \end{bmatrix} \; 5 \cdot R1. \qquad\qquad \begin{bmatrix} 15 & 5 & 0 \\ 4 & -1 & 5 \\ 1 & -2 & 1 \end{bmatrix} \; R2 + 2R3$$

(also notice the shorthand notations on the right-hand side).

Example 6.4. Let us redo the steps of Example 5.9 displaying the same process for system of linear equation and for matrices side by side:

The elementary operations written in systems of linear equations:	The same elementary operations written by matrices:
$\begin{cases} y+z=1 \\ 2x-y+z=9 \\ x-y-z=2 \end{cases}$	$\left[\begin{array}{ccc\|c} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{array}\right]$
$\begin{cases} x-y-z=2 \\ 2x-y+z=9 \\ y+z=1 \end{cases}$	$\left[\begin{array}{ccc\|c} 1 & -1 & -1 & 2 \\ 2 & -1 & 1 & 9 \\ 0 & 1 & 1 & 1 \end{array}\right]$ $R1 \leftrightarrow R3$
$\begin{cases} x-y-z=2 \\ y+3z=5 \\ y+z=1 \end{cases}$	$\left[\begin{array}{ccc\|c} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 1 & 1 & 1 \end{array}\right]$ $R2 + (-2)\,R1$
$\begin{cases} x-y-z=2 \\ y+3z=5 \\ -2z=-4 \end{cases}$	$\left[\begin{array}{ccc\|c} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & -2 & -4 \end{array}\right]$ $R3 + (-1)\,R2$

Each of three elementary operations for matrices is *reversible*: if we by any of them transform a matrix to a new matrix, we can reconstruct the old matrix from the new matrix by an elementary operation.

That is evident for elementary operation of the 1'st type.

For the 2'nd type, recall that all our scalars are in a *field* F. So, if we multiply a row by a non-zero constant c, we can reverse to old matrix by multiplying the row by c^{-1} which does exist in F.

If we by an operation of the 3'rd type add to the i'th row of the matrix the k't row multiplied by $c \in F$, we can reverse by adding to the i'th row (of the new matrix) the k'th row multiplied by $-c \in F$ which also does exist in F.

Definition 6.5. The matrix $B \in M_{m,n}(F)$ is called *row-equivalent* to the matrix $A \in M_{m,n}(F)$, if B can be obtained from A by a series of elementary operations.

Row-equivalence of A and B is denoted by:

$$\boldsymbol{A \sim B},$$

and it clearly is a *relation* on the set $M_{m,n}(F)$ of all $m \times n$ matrices over the field F. Moreover, $\sim$ also is an *equivalence relation* on $M_{m,n}(F)$, i.e., it is *reflexive*, *symmetric* and *transitive*. Reflexivity is evident: $A \sim A$ since A can be obtained from A by multiplying any of its rows by $1 \in F$. Symmetry follows from reversibility proved above. Transitivity also is evident: if $A \sim B$ and $B \sim C$, then we can arrive to C, if we first apply to A the series of elementary operations corresponding to $A \sim B$, and then apply the elementary operations corresponding to $B \sim C$.

Since $\sim$ is equivalence, it defines a *partition* on $M_{m,n}(F)$, each equivalence class (or part) consisting of mutually row-equivalent matrices. For each $A \in M_{m,n}(F)$ denote by

$$\mathcal{R}_A = [A] = \{X \in M_{m,n}(F) \mid X \sim A\}$$

the class consisting of all matrices X in $M_{m,n}(F)$ which are row-equivalent to A. Conversely, for any class $\mathcal{R}$ of this partition we can choose any matrix $A = A_{\mathcal{R}} \in \mathcal{R}$. Then we will have $\mathcal{R} = \mathcal{R}_A$. We are going to give description of such equivalence classes much later in Section 14.2.

Recall that when two systems of linear equations are obtained from each other by elementary operations, then they are equivalent (they have the same solution). Thus, if A and B are row-equivalent augmented matrices of two systems, then those systems have the same solutions. So solving a system of linear equation we are free to replace A by any matrix $B \sim A$.

6.3. The row-echelon form of matrices

Roughly speaking the row-echelon form of a matrix is a form in which lower left-hand "half" is filled-in by zeros (the formal definition yet to follow). Suppose we are given a matrix A over the field F, and let the i'th column of A contains a non-zero element $\boldsymbol{a}_{i1}$ which we stress it by bold font (please read the steps below parallelly comparing them with Example 6.11 and Example 6.12):

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a}_{i1} & \cdots & a_{in} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

Using an elementary operation of the 1'st type we can swap the i'th row with the 1'st row, so that (after a *renumeration* of rows) the first entry $\boldsymbol{a}_{11}$ of our matrix is non-zero:

$$\begin{bmatrix} \boldsymbol{a}_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

Notice that, this step might be skipped, if the first element in the 1'st row of A were non-zero from the beginning.

We are going to use elementary operations of the 3'rd type to turn to 0 all the elements below $\boldsymbol{a}_{11}$ in the 1'st column. If $a_{21} \neq 0$, add to the 2'nd row the 1'st row multiplied by the scalar $-\frac{a_{21}}{\boldsymbol{a}_{11}}$ (we *can* use this fraction since $\boldsymbol{a}_{11}$ is non-zero, and its inverse does exist in F). Clearly, $a_{21} - \frac{a_{21}}{\boldsymbol{a}_{11}} a_{11} = a_{21} - a_{21} = 0$, and the first entry in the 2'nd row of the new matrix will be 0. The other $n-1$ entries in that row may get other values, and to keep the notations simple denote them by the previously used symbols $a_{22}, \dots, a_{2n}$. Repeating this step for all non-zero elements below $\boldsymbol{a}_{11}$ we get:

$$\begin{bmatrix} \boldsymbol{a}_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Consider the entries $\begin{bmatrix} a_{22} \\ \vdots \\ a_{m2} \end{bmatrix}$ below a_{12}. We have two main options:

Case 1. One of those entries is non-zero. Then by an elementary operation of the 1'st type bring it to the 2'nd line, and use a series of elementary operations to turn all the entries below it to 0 as in previous step. The zeros in the 1'st column are not affected. We get a matrix of the form:

$$\begin{bmatrix} \boldsymbol{a}_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & \boldsymbol{a}_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \multicolumn{5}{c}{\dotfill} \\ 0 & 0 & a_{m3} & \cdots & a_{mn} \end{bmatrix}.$$

Case 2. All those entries below a_{12} are 0. Then we leave the 2'nd column, and consider the 3'rd, 4'th, etc. columns, till we find the *first* column which has a non-zero entry (below the 1'st row). Repeat steps of Case 1 for this column to get a matrix of the form:

$$\begin{bmatrix} \boldsymbol{a}_{11} & a_{12} & \cdots & a_{1j} & a_{1j+1} & \cdots & a_{1n} \\ 0 & 0 & \cdots & \boldsymbol{a}_{2j} & a_{2j+1} & \cdots & a_{2n} \\ 0 & 0 & \cdots & 0 & a_{3j+1} & \cdots & a_{3n} \\ \multicolumn{7}{c}{\dotfill} \\ 0 & 0 & \cdots & 0 & a_{mj+1} & \cdots & a_{mn} \end{bmatrix}.$$

Continuing this process for the 3'rd, 4'th rows, etc., we get matrices of the following general type:

$$\begin{bmatrix} \boldsymbol{a}_{11} & \multicolumn{5}{c}{\dotfill} & a_{1n} \\ 0 & \cdots & 0 & \boldsymbol{a}_{2j_2} & \multicolumn{2}{c}{\dotfill} & a_{2n} \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \multicolumn{2}{c}{\dotfill} & 0 & \boldsymbol{a}_{rj_r} & \cdots & a_{rn} \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \multicolumn{2}{c}{\dotfill} & 0 & \boldsymbol{a}_{mj_r} & \cdots & a_{mn} \end{bmatrix},$$

When may this process eventually end? It will end either when there are *no more* non-zero elements at the bottom of the matrix, i.e., we arrive to the form:

$$\begin{bmatrix} \boldsymbol{a}_{11} & \multicolumn{5}{c}{\dotfill} & a_{1n} \\ 0 & \cdots & 0 & \boldsymbol{a}_{2j_2} & \multicolumn{2}{c}{\dotfill} & a_{2n} \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \multicolumn{2}{c}{\dotfill} & 0 & \boldsymbol{a}_{rj_r} & \cdots & a_{rn} \\ 0 & \multicolumn{5}{c}{\dotfill} & 0 \\ \multicolumn{7}{c}{\dotfill} \\ 0 & \multicolumn{5}{c}{\dotfill} & 0 \end{bmatrix},$$

or when the process reaches the last row, i.e., if in the above matrix we have $r = m$.

We started by assuming that the 1'st column contains a non-zero element, but if not so, we will have the same matrix as above, just with some entirely zero columns in the beginning:

$$\begin{bmatrix} 0 & \cdots & 0 & \boldsymbol{a}_{1j_1} & \multicolumn{4}{c}{\dotfill} & a_{1n} \\ 0 & \multicolumn{3}{c}{\dotfill} & 0 & \boldsymbol{a}_{2j_2} & \multicolumn{2}{c}{\dotfill} & a_{2n} \\ \multicolumn{9}{c}{\dotfill} \\ 0 & \multicolumn{5}{c}{\dotfill} & 0 & \boldsymbol{a}_{rj_r} \cdots & a_{rn} \\ 0 & \multicolumn{7}{c}{\dotfill} & 0 \\ \multicolumn{9}{c}{\dotfill} \\ 0 & \multicolumn{7}{c}{\dotfill} & 0 \end{bmatrix}.$$

In our coming considrations we are going to mostly ignore the cases with such entirely zero starting columns.

Remark 6.6. Let us stress that for simplicity of notation we always used the symbol a_{ij} for the (i, j)-th entry of the *current* matrix A. I.e., we assume that after each elementary operation the matrix elements are renamed. E.g., if $a_{21} = 3$, then after swapping the 1'st and 2'nd rows we have $a_{11} = 3$.

A row of a matrix A is called a *zero row*, if all its entries are zero, and it is *non-zero row*, if it contains at least one non-zero entry. For each non-zero row of A call the first non-zero entry of the row the *pivot* or the *leading element* of that row. Call the column holding a pivot a *pivot column*.

Definition 6.7. A matrix A is in *row-echelon form*, if:

1. any zero row of A is below all the non-zero rows,
2. any pivot of A is strictly to the left of any pivots below it.

Example 6.8. The following matrix is in row-echelon form:

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

with three non-zero rows and one zero row. It has three pivots $a_{11} = 3,\ a_{23} = 2,\ a_{34} = 6$. The 1'st, 3'rd, 4'th columns are pivot columns, and the 2'nd column is a not pivot.

While the following matrix:

$$\begin{bmatrix} \mathbf{3} & 1 & 0 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{2} & 5 \\ 0 & 0 & \mathbf{7} & 6 \end{bmatrix}$$

is *not* in row-echelon form because the 2'nd row is zero, and it is above some non-zero rows, and because the pivot 2 in the 3'rd row is *not* to the left of the pivot 7 in the 4'rd row below it.

What we constructed earlier in this section is the proof of the following important:

Theorem 6.9. *Any matrix A over a field F is row-equivalent to a matrix in row-echelon form. I.e., applying a series of elementary operations we can bring A to row-echelon form.*

How to bring a matrix to a row-echelon form. Theorem 6.9 establishes the following algorithm of *Gaussian elimination* for any matrix. By Remark 6.6 we assume that in each step a_{ij} denotes the (i, j)-th entry of the *current* matrix.

Algorithm 6.10 (Bringing a matrix to a row-echelon form). We are given a matrix A over a field F:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

► Find a row-echelon form R of A.

1. Set $i = 1$ and $j = 1$.
2. If $i = m$, output the current matrix as R. End of the process.
3. If $a_{ij} \neq 0$, i.e., a_{ij} is a pivot, go to Step 5.
4. Else, if the j'th column contains a non-zero entry below a_{ij}, i.e., if $a_{ik} \neq 0$ for a $k = i + 1, \ldots, m$, then swap the i'th and k'th rows to create a non-zero pivot a_{ij},
   else set $j = j + 1$, and go to Step 3.
5. Eliminate all non-zero entries below the pivot a_{ij}: if $a_{kj} \neq 0$ for some $k = i+1, \ldots, m$, then add to k'th row the i'th row times $-\frac{a_{kn}}{a_{ij}}$.
6. If $j = n$, output the current matrix as R. End of the process.
7. Else set $i = i + 1,\ j = j + 1$, and go to Step 2.

Example 6.11. The following matrix will be repeatedly used later:

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

$$\sim \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \\ -1 & -1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 & 1 \end{bmatrix} \quad R2-2R1$$

$$\sim \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 & 1 \end{bmatrix} \quad R3+R1$$

$$\sim \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 2 & -1 & 2 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \end{bmatrix} \quad R4-R1$$

$$\sim \begin{bmatrix} 1 & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & -7 & 2 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \end{bmatrix} \quad R3-2R2$$

$$\sim \begin{bmatrix} \mathbf{1} & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 3 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{-7} & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad R4-R2$$

The pivots are marked in bold.

Example 6.12. Earlier in Example 6.4 we already constructed the row-echelon form of a matrix over $\mathbb{R}$. Here is that process without indication of the vertical line of the augmented matrix:

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{bmatrix} \overset{R1 \leftrightarrow R3}{\sim} \begin{bmatrix} 1 & -1 & -1 & 2 \\ 2 & -1 & 1 & 9 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\overset{R2-2\,R1}{\sim} \begin{bmatrix} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\overset{R3-R2}{\sim} \begin{bmatrix} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & -2 & -4 \end{bmatrix}.$$

Notice the different placement of the elementary operation shorthand notations *above* the $\sim$ signs. You are free to use this notation wherever needed.

And for briefness one could also rather informally write

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{bmatrix} \overset{\substack{R1 \leftrightarrow R3 \\ R2-2\,R1 \\ R3-R2}}{\sim} \begin{bmatrix} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & -2 & -4 \end{bmatrix}$$

in cases when only the first and last matrices are relevant.

Example 6.13. Consider elementary operations with the following matrix over $\mathbb{C}$:

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

$$\sim \begin{bmatrix} i & 1 & 0 \\ 0 & 2i & i \\ 2+i & 1 & i \end{bmatrix} \quad R2+2i\,R1 \text{ since } -2/i = 2i$$

$$\sim \begin{bmatrix} i & 1 & 0 \\ 0 & 2i & i \\ 0 & 2i & i \end{bmatrix} \quad R3{+}(-1+2i)\,R1 \text{ since } -\frac{2+i}{i} = -1+2i$$

$$\sim \begin{bmatrix} i & 1 & 0 \\ 0 & 2i & i \\ 0 & 0 & 0 \end{bmatrix} \quad R3-R1 \text{ since } -\frac{2i}{2i} = -1$$

Example 6.14. Consider some elementary operations with the following matrix over the finite field $\mathbb{Z}_3$:

$$\begin{bmatrix} 1 & 1 & 2 \\ 2 & 0 & 2 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad R2{-}2\,R1 \text{ and } R4{-}R1$$

$$\sim \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{bmatrix} \quad R3-2\,R2$$

$$\sim \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \quad R4-2\,R3$$

It is important to stress that *the results of the elimination process may be different depending on the choice of the elementary operations we use*. Let us apply other operations to the matrix of Example 6.12 to see what happens:

Example 6.15. For the above considered matrix we have:

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{bmatrix}$$

$$\sim \begin{bmatrix} 2 & -1 & 1 & 9 \\ 0 & 1 & 1 & 1 \\ 1 & -1 & -1 & 2 \end{bmatrix} \quad R1 \leftrightarrow R2$$

$$\sim \begin{bmatrix} 2 & -1 & 1 & 9 \\ 0 & 1 & 1 & 1 \\ 0 & -\frac{1}{2} & -\frac{3}{2} & -\frac{5}{2} \end{bmatrix} \quad R3 - \frac{1}{2}R1$$

$$\sim \begin{bmatrix} 2 & -1 & 1 & 9 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & -1 & -2 \end{bmatrix} \quad R3 + \frac{1}{2}R2.$$

That is, not only the results of two elimination processes are *different matrices*, but even the *pivots are distinct*.

Exercises

E.6.1. Write a matrix A such that: **(1)** $A \in M_{4,4}(\mathbb{R})$ and $a_{i,j} = a_{j,i}$ for each $i, j = 1,2,3$. **(2)** $A \in M_{3,4}(\mathbb{C})$ and $\mathrm{Im}(a_{1,j}) = \mathrm{Re}(a_{3,j})$, $a_{2,j} = \bar{a}_{2,j}$ for each $j = 1,2,3$. **(3)** $A \in M_{4,3}(\mathbb{Q})$, $a_{i,j} > 0$ for all $i > j$, $a_{i,j} < 0$ for all $i < j$, and all the diagonal elements of A are zero. **(4)** $A \in M_{3,3}(\mathbb{Z}_5)$ and the columns of A are distinct, collinear vectors in $\mathbb{Z}_5^3$.

E.6.2. Write elimination process in Example 5.10 by matrices (in analogy to Example 6.4).

E.6.3. **(1)** Write the matrix A and the augmented matrix $\bar{A}$ for the system of linear equations of the Example 5.11. **(2)** Restore the system of linear equations, if we know that its augmented matrix is the last matrix of Example 6.15.

E.6.4. We are given the matrices $A = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 0 & 4 & 0 \end{smallmatrix}\right] \in M_{2,3}(\mathbb{R})$, $B = \left[\begin{smallmatrix} 1+i & 2i \\ -2 & 5i \end{smallmatrix}\right] \in M_{2,2}(\mathbb{C})$, and $C = \left[\begin{smallmatrix} 3 & 2 \\ 1 & 4 \\ 4 & 3 \end{smallmatrix}\right] \in M_{3,2}(\mathbb{Z}_7)$. **(1)** Write down the 1'st column, the 2'nd row, and the diagonal of each of the matrices A, B, C. **(2)** Apply the sequence of elementary operatios $R1 + 2R2$, $R2 + 5R1$, $R1 \leftrightarrow R2$, $3 \cdot R2$ to each of the matrices A, B, C. *Hint*: Remember that over each of the fields $\mathbb{R}, \mathbb{C}, \mathbb{Z}_7$ you should use respective operations $+$ and $\cdot$.

E.6.5. Write the matrix $A = \left[\begin{smallmatrix} 0 & 2 & 3 & 0 \\ 3 & 0 & k & 1 \\ 1 & 0 & 1 & 2 \\ -\frac{2}{9} & \frac{1}{9} & 0 & 0 \end{smallmatrix}\right] \in M_{4,4}(\mathbb{R})$ where k is your birth day (e.g., if you are born on May 9'th, then $k = 9$). **(1)** Consecutively apply to A the following sequence of elementary operations: $[R1 \leftrightarrow R3]$, $[9 \cdot R4]$, $[R2 - 3R1]$, $[R4 + 2R1]$. What is the first column of the matrix after these steps? **(2)** Bring the obtained matrix to a row-echelon form.

E.6.6. Bring to a row-echelon form the following matrices. Indicate the pivots and the pivot columns. Indicate all the elementary operations you use.

$$A = \begin{bmatrix} 0 & 1 & -2 & 0 \\ 1 & 0 & 0 & 1 \\ 2 & 2 & -4 & 0 \end{bmatrix} \in M_{3,4}(\mathbb{R}), \quad B = \begin{bmatrix} 0 & i \\ i & 3 \\ 2i & 0 \end{bmatrix} \in M_{3,2}(\mathbb{C}), \quad C = \begin{bmatrix} 0 & 3 & 2 \\ 1 & 2 & 4 \\ 3 & 1 & 0 \end{bmatrix} \in M_{3,3}(\mathbb{Z}_5).$$

E.6.7. Bring to row-echelon form each of five matrices in Example 6.1 over fields $\mathbb{R}, \mathbb{Z}_5, \mathbb{C}, \mathbb{Q}$.

E.6.8. Find a matrix $A \in M_{3,4}(\mathbb{R})$ which is *not* in row-echelon form because: **(1)** point 1 of Definition 6.7 holds for A, but point 2 does *not* hold for it. **(2)** point 1 of Definition 6.7 does *not* hold for A, but point 2 holds for it.

E.6.9. **(1)** List two matrices from the equivalence class $\mathcal{R}_A = [A]$, if A is the last matrix of Example 6.15. **(2)** Find a matrix in $M_{3,4}(\mathbb{R})$ which is *not* row-equivalent to A.

E.6.10. **(1)** To some matrix A we applied the elementary operations $R2 + R1$, $R1 - R2$, $R2 + R1$, $(-1) \cdot R1$. Which is the final effect of these operations? Could we achieve the same result by *one* elementary operation only? **(2)** Prove that if $A \sim B$, then we can get one of the matrices from the other using elementary operations of the 2'nd and 3'rd types only. I.e., elementary operation of the 1'st type in fact *is not necessary*.

CHAPTER 7

Solving systems by Gaussian elimination

7.1. Solving the system of linear equations, the basic method

We are given any system of linear equations

$$\left\{\begin{array}{l} a_{11}x_1 \ + \cdots + a_{1n}x_n \ = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{array}\right. \tag{7.1}$$

over a field F, and our objective *to solve it:* to detect if it is consistent or inconsistent (weather it has solution or not), and to find the *general* solution of this system, in case it is consistent. For the system we have introduced its augmented matrix

$$\bar{A} = \left[\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right],$$

and by Theorem 6.9 we know that using three types of elementary operations $\bar{A}$ can be brought to a row-echelon form:

$$R = \left[\begin{array}{cccccccc|c} \boldsymbol{a}_{11} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & a_{1n} & b_1 \\ 0 & \cdots & 0 & \boldsymbol{a}_{2j_2} & \cdots & \cdots & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & 0 & \boldsymbol{a}_{rj_r} & \cdots & a_{rn} & b_r \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_{r+1} \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \end{array}\right],$$

where $r \le m$ (for simplicity we agreed to use in R the same symbols a_{ij} and b_i, although they may have been changed after elementary operations).

Inversely, for this R we can reconstruct the respective system of linear equations equivalent to the system (7.1): we just use the elements a_{ij} of the first n columns as coefficients, and the elements b_i of last column as constants.

There are two options for the last column in R:

Case 1. If it *is* a pivot column, then $b_{r+1} \ne 0$, and the $(r+1)$'th row of R consists of n zeros followed by a non-zero b_{r+1}. Then the system of linear equations respective to R has the following $(r+1)$'th row:

$$0x_1 + \cdots + 0x_n = b_{r+1}$$

which has no solution, since $0 \ne b_{r+1}$. Thus, (7.1) also has no solutions (compare this with Example 5.10).

Case 2. If the last column of R is *not* a pivot column, then $b_{r+1} = 0$, i.e., either R has $m-r$ zero rows at the bottom, or R has no zero rows, at all (this happens when $r = m$). Let us show that this time (7.1) has solution(s) (please read the proof below comparing it with Example 7.2).

Call *pivot variables* (or *leading variables*) the variables $x_{j_1}, \dots, x_{j_r}$ standing in pivot columns. Call the rest of variables *free variables* and denote them $x_{t_1} \dots, x_{t_d}$, where, clearly, $d = n-r$ (in Example 7.2 we have $n = 5$, $r = 3$, $n-r = 2$, x_1, x_3, x_5 are the pivot variables, x_2, x_4 are the free variables).

In R drop the zero rows if any. Then consider the respective system of linear equations, and move all its terms with free variables to the right-hand side:

$$\left\{\begin{array}{rl} a_{1j_1}x_{j_1} + a_{1j_2}x_{j_2} + \cdots + a_{1j_r}x_{j_r} &= b_1 - a_{1t_1}x_{t_1} - \cdots - a_{1t_d}x_{t_d} \\ a_{2j_2}x_{j_2} + \cdots + a_{2j_r}x_{j_r} &= b_2 - a_{2t_1}x_{t_1} - \cdots - a_{2t_d}x_{t_d} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{rj_r}x_{j_r} &= b_r - a_{rt_1}x_{t_1} - \cdots - a_{rt_d}x_{t_d} \end{array}\right. \tag{7.2}$$

(we suppose $1 = j_1$). Choose *any* fixed values $x'_{t_1}, \dots, x'_{t_d} \in F$ for the free variables (in Example 7.2 we set $x'_2 = x'_5 = 1$), and using them compute the values:

$$c_i = b_i - a_{it_1}x'_{t_1} - \cdots - a_{it_d}x'_{t_d}, \quad i = 1, \dots, d. \tag{7.3}$$

We get a system of r equations in r variables:

$$\left\{\begin{array}{rl} a_{1j_1}x_{j_1} + a_{1j_2}x_{j_2} + \cdots + a_{1j_r}x_{j_r} &= c_1 \\ a_{2j_2}x_{j_2} + \cdots + a_{2j_r}x_{j_r} &= c_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \cdots \\ a_{rj_r}x_{j_r} &= c_r\,. \end{array}\right. \tag{7.4}$$

Now we start the *inverse substitution* process. From the r'th (last) row we get the *unique* value $x'_{j_r} = c_r / a_{rj_r}$. Having the x'_{j_r} we from the $(r-1)$'th row

$$a_{r-1\,j_{r-1}}x_{j_{r-1}} + a_{r-1\,j_r}x_{j_r} = c_{r-1}$$

get the *unique* value of $x'_{j_{r-1}}$. Continuing the process we get a *unique* (for the given choice of free variables) solution $(x'_1, \dots, x'_n)$ for the system (7.2) and also for our initial system (7.1).

A specific subcase is the situation where $r = n$, that is, there are *no* free variables (compare with Example 7.3). Then we have to move nothing to the right-hand side. After we drop the zero rows if any, we get the following analog of (7.4):

$$\left\{\begin{array}{rl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots & \cdots \\ a_{nn}x_n &= b_n\,. \end{array}\right. \tag{7.5}$$

By inverse substitution process we then compute the *single* solution $(x'_1, \dots, x'_n)$ of (7.5) and for our initial system (7.1).

Summarizing these cases we see that:

1. Either the system (7.1) is inconsistent if and only if the last column of R is a pivot column (i.e., the $(r+1)$'th row of R consists of n zeros followed by one non-zero element, like in Example 5.10).
2. Or the system (7.1) is consistent if and only if the last column of R is *not* a pivot column (i.e., the last non-zero row of R is not of the above mentioned type). Then we have two options:

a) either $r = n$, and the system has a single solution, like in Example 7.3;

b) or $r < n$, and it has multiple solutions – one for each choice of $d = n - r$ free variables (infinitely many solutions, if F is infinite), like in Example 7.2.

We found a method to find some solutions for (7.1), but do the found solutions cover *all possible solutions* of our system? Or there may still be a solution $(x''_1, \dots, x''_n)$ which could *not* be covered by the process above? This question has negative answer, i.e., the solutions built above in fact form the *general solution* of (7.1).

Indeed, assume $(x''_1, \dots, x''_n)$ is an arbitrary solution of (7.1). Remember that for a given choice of free variables $x_{t_1} \dots, x_{t_d}$ the inverse substitution process in (7.2) provides the values for pivot variables $x_{j_1}, \dots, x_{j_r}$ *uniquely*. Thus, if we chose $x_{t_1} = x''_{t_1}, \dots, x_{t_d} = x''_{t_d}$, we will get a solution of (7.1) coinciding with $(x''_1, \dots, x''_n)$ not only in free variables, but also in pivot variables.

How to solve a system of linear equations, basic method. We get the following very basic method of solving any system of linear equation over any field:

Algorithm 7.1 (Solving a system of linear equations, basic method)**.** We are given a system (7.1) of m linear equations in n variables over a field F.

► Solve the system. If it is consistent, describe the general solution.

1. Write down the augmented matrix $\bar{A}$ of the system (7.1).
2. Bring $\bar{A}$ to a row-echelon form R by elementary row-operations of Algorithm 6.10.
3. If the last column of R is a pivot column or, equivalently, if $(r+1)$'th row of R consists of n zeros followed by one non-zero element, output: the system (7.1) is inconsistent. End of the process.
4. Else, if R has zero rows, drop them.
5. If $r < n$, go to Step 7.
6. The respective system corresponding to our matrix is (7.5). Using inverse substitution process output its *single solution* $(x'_1, \dots, x'_n)$. End of the process.
7. Denote the pivot variables by $x_{j_1}, \dots, x_{j_r}$, and denote the free variables by $x_{t_1}, \dots, x_{t_d}$, where $d = n - r$.
8. Construct the corresponding system of linear equations (7.2) by moving the free variables to the right-hand side.
9. Output the *general solution* of our system (7.1) by assigning any values $x'_{t_1}, \dots, x'_{t_d} \in F$ to free variables, computing the constants $c_1, \dots, c_r$ by (7.3), and then computing the corresponding values for pivot variables by inverse substitution in the system (7.4).

Example 7.2. Consider the system:

$$\begin{cases} x_1 + x_2 + x_3 - x_4 + x_5 = 1 \\ 2x_1 + 2x_2 + 3x_3 + x_4 + 2x_5 = 2 \\ -x_1 - x_2 + x_3 + x_5 = 0 \\ x_1 + x_2 + 2x_3 + 2x_4 + x_5 = 1. \end{cases}$$

The augmented matrix $\bar{A}$ and a row-echelon form (see Example 6.11) for $\bar{A}$ are:

$$\bar{A} = \left[\begin{array}{ccccc|c} 1 & 1 & 1 & -1 & 1 & 1 \\ 2 & 2 & 3 & 1 & 2 & 2 \\ -1 & -1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 & 1 \end{array}\right],$$

$$R = \left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 3 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{-7} & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

The pivots are $a_{11} = 1$, $a_{23} = 1$, $a_{34} = -7$. Evidently, the last column is not pivot, thus, the system is consistent.

Drop 4'th row and construct the corresponding system:

$$\begin{cases} x_1 + x_2 + x_3 - x_4 + x_5 = 1 \\ x_3 + 3x_4 = 0 \\ -7x_4 + 2x_5 = 1 \end{cases}.$$

There are $d = n - r = 5 - 3 = 2$ free variables x_2, x_5. Move the free variables to right-hand side:

$$\begin{cases} x_1 + x_3 - \quad x_4 = 1 - x_2 - x_5 \\ \qquad x_3 + \ 3x_4 = 0 \\ \qquad\quad -7x_4 = 1 \qquad -2x_5 \end{cases}.$$

If we assign the values, say, $x_2' = x_5' = 1$ to the free variables, we get the system:

$$\begin{cases} x_1 + x_3 - \quad x_4 = -1 \\ \qquad x_3 + \ 3x_4 = \ \ 0 \\ \qquad\quad -7x_4 = -1 \end{cases},$$

from where $x_4' = \frac{1}{7}$, $x_3' = -\frac{3}{7}$ and $x_1' = -1 + \frac{4}{7} = -\frac{3}{7}$. So *one* of the solutions of our system is:

$$(-\tfrac{3}{7},\ 1,\ -\tfrac{3}{7},\ \tfrac{1}{7},\ 1).$$

More generally, assigning *arbitrary* values $x_2' = \alpha$ and $x_5' = \beta$ we get the system

$$\begin{cases} x_1 + x_3 - \quad x_4 = 1 - \alpha - \beta \\ \qquad x_3 + \ 3x_4 = 0 \\ \qquad\quad -7x_4 = 1 \qquad -2\beta \end{cases}.$$

Then the general solution of the system is:

$$\left(\tfrac{3}{7} - \alpha + \tfrac{1}{7}\beta,\ \ \alpha,\ \ \tfrac{3}{7} - \tfrac{6}{7}\beta,\ \ -\tfrac{1}{7} + \tfrac{2}{7}\beta,\ \ \beta\right)$$

with any $\alpha, \beta \in \mathbb{R}$. We could also write the solution *as a set*:

$$\left\{\left(\tfrac{3}{7}-\alpha+\tfrac{1}{7}\beta,\ \alpha,\ \tfrac{3}{7}-\tfrac{6}{7}\beta,\ -\tfrac{1}{7}+\tfrac{2}{7}\beta,\ \beta\right) \mid \alpha, \beta \in \mathbb{R}\right\}$$

Example 7.3. Consider the system of Example 5.9 and Example 6.4.

$$\begin{cases} \qquad\ \ y + z = 1 \\ 2x - y + z = 9 \\ x \ \ - y - z = 2 \end{cases}$$

The augmented matrix and a row-echelon form for it are the matrices:

$$\bar{A} = \left[\begin{array}{rrr|r} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{array}\right],$$

$$R = \left[\begin{array}{rrr|r} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 1 & 2 \end{array}\right].$$

The last column is not pivot. Since $r = 3$, the number of free variables is $d = n - r = 0$. So we move no variables to the right-hand side. From the 3'rd row we get $z' = 2$. Then from the 2'nd row we get $y' = -1$. And from the 1'st row we get $x' = 3$. The final *only* solution is $(3, -1, 2)$.

Example 7.4. Let us consider and example over finite field $\mathbb{Z}_5$:

$$\begin{cases} \ \ x + y = 3 \\ 3x \qquad = 2 \\ 4x + y = 0 \\ 2x + y = 2\,. \end{cases}$$

The augmented matrix is:

$$\bar{A} = \left[\begin{array}{rr|r} 1 & 1 & 3 \\ 3 & 0 & 2 \\ 4 & 1 & 0 \\ 2 & 1 & 2 \end{array}\right].$$

Its row-echelon form are is easy to compute by two elementary operations:

$$\left[\begin{array}{rr|r} 1 & 1 & 3 \\ 0 & 2 & 3 \\ 0 & 2 & 3 \\ 0 & 4 & 1 \end{array}\right] \sim \left[\begin{array}{rr|r} 1 & 1 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] = R.$$

The last column is not pivot, so the system is consistent. Drop the last two rows and write the system:

$$\begin{cases} x + \ \ y = 3 \\ \qquad 2y = 3 \end{cases}.$$

From $2y = 3$ we get $y' = 4$. Then $x' = 3 - 1 \cdot 4 = 4$. The *only* solution is $(4, 4)$.

There is a specific case to stress. A system of linear equations is *homogeneous*, if its constant terms are zero:

$$\begin{cases} a_{11}x_1 \ + \cdots + a_{1n}x_n \ = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0. \end{cases} \tag{7.6}$$

Such systems are going to play important role later, and for now just state some of their properties easily following from previous facts:

The last column of the augmented matrix $\bar{A}$ of the system (7.6) consists of zeros only. No elementary operation may change these zeros, and the last column of any row-echelon form R is not a pivot. I.e., (7.6) is consistent for any choice of coefficients.

One of the solutions of (7.6) evidently is the zero solution $(0,\dots,0)$. In case $r=n$ this is the *only* solution of the system. In case $r<n$ the system (7.6) has more then one solutions (one for each choice of free variables).

7.2. The reduced row-echelon form and the Gauss-Jordan method

The first aim of this section is to introduce a very important tool of linear algebra: the *reduced row-echelon form* $\operatorname{rref}(A)$ of matrix A.

By Theorem 6.9 each matrix can be brought to a row-echelon form:

$$\begin{bmatrix}
\boldsymbol{a}_{11} & \dots\dots & a_{1j_2} & \cdots & a_{1j_3} & \cdots & a_{1j_r} & \cdots & a_{1n}\\
0 \;\cdots\; 0 & & \boldsymbol{a}_{2j_2} & \cdots & a_{2j_3} & \cdots & a_{2j_r} & \cdots & a_{2n}\\
0 & \dots\dots\dots\dots & 0 & & \boldsymbol{a}_{3j_3} & \cdots & a_{3j_r} & \cdots & a_{3n}\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & \dots\dots\dots\dots\dots\dots & & & & 0 & \boldsymbol{a}_{rj_r} & \cdots & a_{rn}\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0
\end{bmatrix}$$

(we intentionally wrote the entries above the pivots, since we are going to operate with them shortly). By elementary operations of 2'nd type we can replace all the pivots by 1:

$$\begin{bmatrix}
\mathbf{1} & \dots\dots & a_{1j_2} & \cdots & a_{1j_3} & \cdots & a_{1j_r} & \cdots & a_{1n}\\
0 \;\cdots\; 0 & & \mathbf{1} & \cdots & a_{2j_3} & \cdots & a_{2j_r} & \cdots & a_{2n}\\
0 & \dots\dots\dots\dots & 0 & & \mathbf{1} & \cdots & a_{3j_r} & \cdots & a_{3n}\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & \dots\dots\dots\dots\dots\dots & & & & 0 & \mathbf{1} & \cdots & a_{rn}\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0\\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots\\
0 & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & & & & & & 0
\end{bmatrix}.$$

Then by elementary operations of the 3'rd type we can replace all elements above the pivots by zeros (say, after $R2-a_{2j_3}R3$ we have $a_{2j_3}=0$):

$$\operatorname{rref}(A)=\begin{array}{c}
\begin{bmatrix}
\mathbf{1} & * & 0 & * & 0 & * & \cdots & * & 0 & * & \cdots & *\\
 & & \mathbf{1} & * & 0 & * & \cdots & * & 0 & * & \cdots & *\\
 & & & & \mathbf{1} & * & \cdots & * & 0 & * & \cdots & *\\
 & & & & & & & & \dots & \dots & \dots & \dots\\
 & & & & & & & & \mathbf{1} & * & \cdots & *\\
 & & & & & & & & & & & \\
\mathbf{0} & & & & & & & & & & &
\end{bmatrix}\\
\begin{matrix} j_1 & & j_2 & & j_3 & & & & j_r & & & \end{matrix}
\end{array}. \tag{7.7}$$

Notice the following about notation: we added some asterisks $*$ to denote the elements between the pivot columns (because otherwise the notation $1\cdots0\cdots0\cdots0$ could mean that *all* entries in between are zeros); also, we put the first pivot in 1'st column assuming $j_1=1$ (our matrix may have initial zero column, but we ignore them for simplicity of notation).

Definition 7.5. A matrix A is in *reduced row-echelon form*, if:

1. A is in row-echelon form;
2. all pivots of A are 1, and all other elements in pivot columns are zero.

Above we have just proved the following:

Theorem 7.6. *Any matrix A over any field F is row-equivalent to a matrix in reduced row-echelon form. That is, applying a series of elementary operations we can bring A to reduced row-echelon form* rref(A).

How to bring a matrix to the reduced row-echelon form. Theorem 7.6 and the construction above suggest the following algorithm often called after C.F. Gauss and W. Jordan.

Algorithm 7.7 (Bringing a matrix to the reduced reduced row-echelon form)**.** We are given a matrix over a field F

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

► Find the reduced row-echelon form rref(A) of A.

1. Bring A to a row-echelon form R by Algorithm 6.10.
2. Set r to be the total number of non-zero rows in R, and $j_1, \dots, j_r$ to be the numbers of pivot columns in R.
3. If $r = 0$, output R (a zero matrix) as rref(A). End of the process.
4. Else, set $s = r$.
5. Turn the pivot a_{sj_s} to 1 by multiplying the s'th row of R by $a_{sj_s}^{-1}$.
6. Eliminate all non-zero entries above the pivot $a_{sj_s} = 1$: if $a_{kj_s} \neq 0$ for some $k = 1, \dots, s-1$, then add to k'th row of R the s'th row times $-a_{kj_s}$.
7. If $s = 1$, output the current matrix R as rref(A). End of the process.
8. Else set $s = s - 1$, and go to Step 5.

Notice that we started elimination from the right-hand side by setting $s = r$. We could arrive to the same result starting from the left-hand side, but our approach requires less computations. Examples of application of this algorithm will come shortly.

A straightforward application of reduced row-echelon form allows us to simplify the solution of a system of linear equations. Namely, let us bring the augmented matrix $\bar{A}$ of a *consistent* system (7.1) to reduced row-echelon form:

$$\left[\begin{array}{cccccccccccc|c} \mathbf{1} & * & 0 & * & 0 & * & \cdots & * & 0 & * & \cdots & * & b_1 \\ & & \mathbf{1} & * & 0 & * & \cdots & * & 0 & * & \cdots & * & b_2 \\ & & & & \mathbf{1} & * & \cdots & * & 0 & * & \cdots & * & b_3 \\ & & & & & & & & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & & & & & \mathbf{1} & * & \cdots & * & b_r \\ & & & & & & & & & & & & \\ \mathbf{0} & & & & & & & & & & & & \end{array}\right].$$

Since the last column is not a pivot, all entries below b_r are zero and, like above, we assume the pivot column numbers are $j_1, \dots, j_r$, while the other column numbers are $t_1, \dots, t_d$, where $d = n - r$.

In the respective system of linear equations dropping the zero rows and moving the free variables to the right-hand side we get:

$$\begin{cases} x_{j_1} \qquad = b_1 - a_{1t_1}x_{t_1} - \cdots - a_{1t_d}x_{t_d} \\ \quad x_{j_2} \quad = b_2 - a_{2t_1}x_{t_1} - \cdots - a_{2t_d}x_{t_d} \\ \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \qquad x_{j_r} = b_r - a_{rt_1}x_{t_1} - \cdots - a_{rt_d}x_{t_d}\,. \end{cases}$$

Arbitrarily choose *any* fixed values $x'_{t_1}, \ldots, x'_{t_d} \in F$ for the free variables, and set: $c_i = b_i - a_{it_1}x'_{t_1} - \cdots - a_{it_d}x'_{t_d}$, for $i = 1, \ldots, r$. We get a system of r very simple equations in r variables:

$$\begin{cases} x_{j_1} = c_1 \\ x_{j_2} = c_2 \\ \cdots\cdots \\ x_{j_r} = c_r \end{cases} \tag{7.8}$$

in which *no inverse substitution process is needed*, as the unique values of pivot variables are given explicitly.

A specific case is when $r = n$, i.e., when the system has no free variable, and we have nothing to move to the right-hand side. Then we just have:

$$\begin{cases} x_1 = b_1 \\ x_2 = b_2 \\ \cdots\cdots \\ x_n = b_n \end{cases} \tag{7.9}$$

and the single solution of the system is $(b_1, \ldots, b_n)$.

How to solve a system of linear equations, the Gauss-Jordan method.

Algorithm 7.8 (Solving a system of linear equations, the Gauss-Jordan method)**.** We are given a system (7.1) of m linear equations in n variables over a field F.

► Solve the system by the Gauss-Jordan method.

1. Write the augmented matrix $\bar{A}$ of the system (7.1).
2. Bring $\bar{A}$ to a row-echelon form R by elementary row-operations.
3. If the last column of R is a pivot column (equivalently, if $(r+1)$'th row of R consists of n zeros followed by one non-zero element), output: the system (7.1) is inconsistent. End of the process.
4. Else, bring R to the reduced row-echelon form rref(A) by Algorithm 7.7.
5. If $r < n$, go to Step 7.
6. The respective system corresponding to our matrix is (7.9). Output its *single solution* $(b_1, \ldots, b_n)$. End of the process.
7. Denote the pivot variables by $x_{j_1}, \ldots, x_{j_r}$, and denote the free variables by $x_{t_1}, \ldots, x_{t_d}$, where $d = n - r$.
8. Construct the corresponding system of linear equations (7.8) by moving the free variables to the right-hand side.
9. Output the *general solution* of our system (7.1) as the following set: assign any values $x'_{t_1}, \ldots, x'_{t_d} \in F$ to free variables, compute the constants $c_1, \ldots, c_r$ by (7.3), and then get the corresponding values for pivot variables from (7.8).

Here are some applications of the Gauss-Jordan method:

Example 7.9. Turn back to the system considered in Example 7.2

$$\begin{cases} x_1 + \ x_2 + \ x_3 - \ x_4 + \ x_5 = 1 \\ 2x_1 + 2x_2 + 3x_3 + \ x_4 + 2x_5 = 2 \\ -x_1 - \ x_2 + \ x_3 \qquad + \ x_5 = 0 \\ x_1 + \ x_2 + 2x_3 + 2x_4 + \ x_5 = 1. \end{cases}$$

A row-echelon form of the augmented matrix $\bar{A}$ is already computed above:

$$R = \left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 3 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{-7} & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right],$$

and we can construct reduced row-echelon form as:

$$R \sim \left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & \mathbf{1} & 3 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & -\frac{2}{7} & -\frac{1}{7} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \ -\tfrac{1}{7}R3$$

$$\sim \left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 1 & 0 & \frac{5}{7} & \frac{6}{7} \\ 0 & 0 & \mathbf{1} & 0 & \frac{6}{7} & \frac{3}{7} \\ 0 & 0 & 0 & \mathbf{1} & -\frac{2}{7} & -\frac{1}{7} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \ R2{-}3R3;\ R1{+}R3$$

$$\sim \left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 0 & 0 & -\frac{1}{7} & \frac{3}{7} \\ 0 & 0 & \mathbf{1} & 0 & \frac{6}{7} & \frac{3}{7} \\ 0 & 0 & 0 & \mathbf{1} & -\frac{2}{7} & -\frac{1}{7} \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \ R1{-}R2.$$

The pivots are $a_{11} = a_{23} = a_{34} = 1$. There are $d = n - r = 5 - 3 = 2$ free variables. Dropping the 4'th row and moving the free variables x_2, x_5 to right-hand side we get the new system:

$$\begin{cases} x_1 = \frac{3}{7} - x_2 + \frac{1}{7}x_5 \\ x_3 = \frac{3}{7} - \frac{6}{7}x_5 \\ x_4 = -\frac{1}{7} + \frac{2}{7}x_5. \end{cases}$$

Assigning arbitrary values $x_2' = \alpha$ and $x_5' = \beta$ we get the same general solution as in Example 7.2:

$$\left(\tfrac{3}{7} - \alpha + \tfrac{1}{7}\beta,\ \alpha,\ \tfrac{3}{7} - \tfrac{6}{7}\beta,\ -\tfrac{1}{7} + \tfrac{2}{7}\beta,\ \beta\right)$$

for any $\alpha, \beta \in \mathbb{R}$.

Example 7.10. For the system of Example 7.3

$$\begin{cases} \qquad y + z = 1 \\ 2x - y + z = 9 \\ x \ \ - y - z = 2 \end{cases}$$

we already know a row-echelon form of its augmented matrix:

$$R = \left[\begin{array}{ccc|c} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & -2 & -4 \end{array}\right].$$

The reduced row-echelon form also is easy to find:

$$R \sim \left[\begin{array}{ccc|c} 1 & -1 & -1 & 2 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 1 & 2 \end{array}\right] \ -\tfrac{1}{2}\cdot R3$$

$$\sim \left[\begin{array}{ccc|c} 1 & -1 & -1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right] \ R2 + (-3)\cdot R3$$

$$\sim \left[\begin{array}{ccc|c} 1 & -1 & 0 & 4 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right] \ R1 + R3$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{array}\right] \ R1 + R2.$$

The last matrix is in reduced row-echelon form, and it immediately gives the single solution $(3, -1, 2)$, which actually stands in the 4'th column.

Example 7.11. Turn back to the system of Example 7.4 over the finite field $\mathbb{Z}_5$:

$$\begin{cases} x + y = 3 \\ 3x \qquad = 2 \\ 4x + y = 0 \\ 2x + y = 2. \end{cases}$$

We have already computed a row-echelon form of the augmented matrix of this system:

$$R = \left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right].$$

Reduced row-echelon form can be computed via operations on $\mathbb{Z}_5$:

$$R \sim \left[\begin{array}{cc|c} 1 & 1 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \ 3\cdot R2$$

(because in $\mathbb{Z}_5$ we have $2^{-1} = 3$, and so $3 \cdot 3 = 4$)

$$\sim \left[\begin{array}{cc|c} 1 & 0 & 4 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \ R1 - R2$$

(because in $\mathbb{Z}_5$ we have $3 - 4 = 4$). Dropping the last two rows we get the system:

$$\begin{cases} x = 4 \\ y = 4 \end{cases},$$

which has the single solution $(4, 4)$.

Notice that in these examples we drew the vertical line before the last column to stress that we discuss *augmented* matrices for some systems. However, that line brings nothing new to the row-echelon and reduced row-echelon forms of matrices, and we will in general drop that line in the sequel.

7.3. Uniqueness of the reduced row-echelon form, the rank of a matrix

As we have seen, a matrix A may have different row-echelon forms (see Example 6.15 and Example 6.12). A remarkable and helpful property of *the reduced row-echelon form* rref(A) *is that it is unique for any matrix A.*

Assume H and S are some *distinct* reduced row-echelon forms of a matrix A, i.e., we obtained them from A by some elementary row-operations. Select the first column in which H and S differ. Then erase in H and S all the columns except the selected columns and the columns containing pivots to the left of it. Denote the new matrices by H' and S' respectively. They clearly are row-equivalent, since H and S are row-equivalent.

Example 7.12. Assume we have:

$$H=\begin{bmatrix} \mathbf{1} & 3 & 0 & 1 & 0 & 2\\ 0 & 0 & \mathbf{1} & 2 & 0 & 1\\ 0 & 0 & 0 & 0 & \mathbf{1} & 4\\ 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix},\quad S=\begin{bmatrix} \mathbf{1} & 3 & 0 & 4 & 0 & 5\\ 0 & 0 & \mathbf{1} & 3 & 0 & 4\\ 0 & 0 & 0 & 0 & \mathbf{1} & 2\\ 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}.$$

The selected column is the 4'th column. And after we erase the 5'th, 6' and 2'nd columns, we get respectively:

$$H'=\left[\begin{array}{cc:c} \mathbf{1} & 0 & 1\\ 0 & \mathbf{1} & 2\\ \hdashline 0 & 0 & 0\\ 0 & 0 & 0\end{array}\right],\quad S'=\left[\begin{array}{cc:c} \mathbf{1} & 0 & 4\\ 0 & \mathbf{1} & 3\\ \hdashline 0 & 0 & 0\\ 0 & 0 & 0\end{array}\right].$$

We intentionally wrote the parts of H' and S' by dashed lines to stress: the top left-hand part is I, the bottom left-hand part is a zero block, the bottom right-hand part is zero column, and top right-hand part is a column containing the element in which H and S differ.

Alternatively, if the 4'th column of, say, S contained a pivot, then we would get:

$$S'=\left[\begin{array}{cc:c} \mathbf{1} & 0 & 0\\ 0 & \mathbf{1} & 0\\ \hdashline 0 & 0 & \mathbf{1}\\ 0 & 0 & 0\end{array}\right],$$

i.e. top right-hand part is a zero column, and the bottom right-hand part is the column vector $\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$.

In general case we, clearly, have two alternative forms for each of R' and S':

$$(7.10)\quad H'=\left[\begin{array}{c:c} I & u\\ \hdashline \mathbf{0} & \mathbf{0}\end{array}\right] \text{ or } H'=\left[\begin{array}{c:c} I & \mathbf{0}\\ \hdashline \mathbf{0} & \begin{bmatrix}1\\0\\ \vdots\\0\end{bmatrix}\end{array}\right];\quad S'=\left[\begin{array}{c:c} I & w\\ \hdashline \mathbf{0} & \mathbf{0}\end{array}\right] \text{ or } S'=\left[\begin{array}{c:c} I & \mathbf{0}\\ \hdashline \mathbf{0} & \begin{bmatrix}1\\0\\ \vdots\\0\end{bmatrix}\end{array}\right].$$

H' and S' are augmented matrices of some sytems of linear equations. These systems are equivalent, since H' and S' are row-equivalent.

If H' is in second form in (7.10), then its system is inconsistent, and the system of S' need also be inconsistent, i.e., S' need also be in second form, and so $H' = S'$. Contradiction with selection of H' and S'.

Next, assume H' is in first form, and the column vector u is $\left[\begin{smallmatrix}a_1\\ \cdots\\ a_r\end{smallmatrix}\right]$. Since the top left-hand side of H' is I, the system has a unique solution $(x_1,\dots,x_r) = (a_1,\dots,a_r)$. Thus, the system of S' also is consistent and has the same solution. This only is possible when S' is in first form, and $w=\left[\begin{smallmatrix}a_1\\ \cdots\\ a_r\end{smallmatrix}\right]=u$. We again get a contradiction.

We proved the following important theorem:

Theorem 7.13. *The reduced row-echelon form* $\mathrm{rref}(A)$ *of any matrix* $A \in M_{m,n}(F)$ *is unique.*

Corollary 7.14. *Any two matrices* $A, B \in M_{m,n}(F)$ *are row-equivalent if and only if they have the same reduced row-echelon form. I.e.,* $A \sim B$ *if and only if* $\mathrm{rref}(A) = \mathrm{rref}(B)$.

***Proof*.** If $A \sim B$, we can by a sequence of elementary operations go from A to B, and then by another sequence go from B to $\mathrm{rref}(B)$. Combining this two sequences we see that $\mathrm{rref}(B)$ is a reduced row-echelon form for A, and so $\mathrm{rref}(A) = \mathrm{rref}(B)$ by Theorem 7.13.

If $\mathrm{rref}(A) = \mathrm{rref}(B)$, then we can by a sequence of elementary operations go from A to $\mathrm{rref}(A)$. Then go from $\mathrm{rref}(B)$ (whcih is $\mathrm{rref}(A)$) to B, and combine these sequences to get $A \sim B$. □

How to detect if two matrices are row-equivalent. Using Theorem 7.13 we can detect if two matrices $A, B \in M_{m,n}(F)$ are row-equivalent. Compute the matrices $\mathrm{rref}(A)$ and $\mathrm{rref}(B)$ by Algorithm 7.7. Then $A \sim B$ if and only if $\mathrm{rref}(A) = \mathrm{rref}(B)$.

Example 7.15. In Examples 6.15 and 6.12 we found two distinct row-echelon forms for a matrix. They clearly are row-equivalent. And these matrices both have the same reduced row-echelon form which we calculated in Example 7.10.

Two row-echelon forms of a matrix may be distinct. But since the reduced row-echelon form may be obtained from *any* row-echelon form (by turning all pivots to 1 and by eliminating the entries above the pivots), we get:

Corollary 7.16. *For any matrix* $A \in M_{m,n}(F)$*:*

1. *any two row-echelon forms of* A *have the same number of non-zero rows, and*

2. *any two row-echelon forms of* A *have the same number of pivots standing in columns with the same numbers.*

Turning back to Example 6.15 and Example 6.12 we notice that although the row-echelon forms in these examples are distinct, and they have distinct pivots (namely, $1, 1, -2$ and $2, 1, -1$), in both cases we have three pivots, and in both cases the pivots are in the 1'st, 2'nd and 3'rd columns.

Definition 7.17. The number of non-zero rows in a row-echelon form of a matrix $A \in M_{m,n}(F)$ is called the *rank* of the matrix A, and it is denoted by $\mathrm{rank}(A)$.

How to compute the rank of a matrix by row-elimination. Corollary 7.16 is a simple tool to find $\mathrm{rank}(A)$ for the given matrix A: bring the matrix to a row-echelon form and count the number of non-zero rows (or of the pivots, or of the pivot columns).

Example 7.18. Turning back to the earlier examples notice that for the augmented matrix $\bar{A}$ of Example 7.2 we have $\mathrm{rank}(\bar{A}) = 3$.

For the augmented matrix $\bar{A}$ over the field $\mathbb{Z}_p$ of Example 7.4 we get $\mathrm{rank}(\bar{A}) = 2$.

For the real matrix of Example 6.12 we have:

$$\mathrm{rank}\begin{bmatrix} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{bmatrix} = 3.$$

For the complex matrix of Example 6.13 we get

$$\mathrm{rank}\begin{bmatrix} i & 1 & 0 \\ 2 & 0 & i \\ 2+i & 1 & i \end{bmatrix} = 2.$$

For the matrix over $\mathbb{Z}_p$ of Example 6.14 we have

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

The matrix rank allows to reformulate the condition of consistence for a system of linear equations. In Section 7.1 we saw that a system (7.1) is *not* consistent if and only if the last column of the row-eachelon form R of the augmented matrix $\bar{A}$ is a *pivot* column. It is clear that in this case $\operatorname{rank}(\bar{A}) = r+1$ and $\operatorname{rank}(A) = r$ (where A is the matrix of the coefficients of the system – see Section 6.2). Otherwise, the system is consistent, and $\operatorname{rank}(\bar{A}) = \operatorname{rank}(A) = r$. We get a well known theorem often attributed to L. Kronecker and A. Capelli (also called by the names of E. Rouché, G. Fontené or F.G. Frobenius):

Theorem 7.19. *A system of linear equations with a coefficient matrix A and an augmented matrix $\bar{A}$ is consistent if and only if*

$$\mathbf{rank}(A) = \mathbf{rank}(\bar{A}).$$

7.4. *Applications*: Controlling structures by linear equations

Let us discuss a topic which not only uses systems of linear equations for real-life problems, but also displays an unexpected application of algebra over finite fields.

Assume we have an organized structure, such as company performing some actions. Its managers can order, say, to send some funds from one department to the other, or to relocate some equipment from old building to a new building. They can give commands of any kind they want, but *each command has a consequence:* if they, say, send some amount from one department to the other, then the first department may no longer be able to perform some actions. Or if they bring some equipment to a new building, some operations will no longer be possible in the old building. How to bring our company to the best desirable condition taking into account the consequences of the commands?

This can be modeled by the following simple means. Assume we have a structure with 5 lights that can be either on or off. We can switch any of the lights (to turn it on, when it is off; or to turn it off, when it is on) but each of our actions has a *consequence:* some of other lights may also be switched simultaneously, so our commands actually concern a group of lights. For example, assume we can send the following commands A, B, C, D, E, F to the structure (imagine this is a "control panel" in Figure 7.1):

the command A switches the lights 1 and 2;
the command B switches the lights 1 and 3;
the command C switches the lights 3 and 4;
the command D switches the last four lights 2–5;
the command E switches the first and last lights;
the command F switches the last two lights.

For example, starting from the structure condition with all lights off, we by commands BDF can arrive to the condition shown in Figure 7.1.

Problem 7.20. *Starting from any structure condition can we by a series of commands A, B, C, D, E, F arrive to a condition with any pre-given desired values for lights? Are there conditions that may never occur? Can we list all possible ways to achieve the desired condition, and choose the shortest possible ways?*

Finding the shortest way is useful for the situations when our company competes with another company in an environment where only certain commands are allowed, and we want to win the competition.

For example, starting with a system with only light 3 on can we arrive to a system with only lights 3 and 5 on? Can we arrive to a system with only lights 1, 3 and 5 on Figure 7.1?

To solve this represent the condition of each light by boolean variables 0 (if it is off) and 1 (if it is on) which we can consider to be elements of the finite field $F = \mathbb{Z}_2 = \{0, 1\}$ (e.g., $0+1=1$ and $1+1=0$). Switching a 0 light to 1 (or vise versa) is the same as adding 1 to 0 (or to 1) in the field $\mathbb{Z}_2$. And leaving a 0 or 1 light unchanged is the same as adding 0 to it.

The conditions of the structure can be represented by vectors $(x_1, x_2, x_3, x_4, x_5)$ in the space $\mathbb{Z}_2^5$. For example, $u = (0,0,0,0,0)$ means the system with all lights off. $w = (0,0,1,0,0)$ means the system with only light 3 on.

Sending commands A, B, C, D, E, F to our system is the same as adding the following vectors to the current vector $v = (x_1, x_2, x_3, x_4, x_5)$:

the command A means adding the vector $v_1 = (1,1,0,0,0)$ to v;
the command B means adding the vector $v_2 = (1,0,1,0,0)$ to v;
the command C means adding the vector $v_3 = (0,0,1,1,0)$ to v;
the command D means adding the vector $v_4 = (0,1,1,1,1)$ to v;
the command E means adding the vector $v_5 = (1,0,0,0,1)$ to v;
the command F means adding the vector $v_6 = (0,0,0,1,1)$ to v.

In particular, the sequence of commands BDF sent to $u = (0,0,0,0,0)$ can be represented as:

$$u + v_2 + v_4 + v_6 = \begin{bmatrix} 0\\0\\0\\0\\0 \end{bmatrix} + \begin{bmatrix} 1\\0\\1\\0\\0 \end{bmatrix} + \begin{bmatrix} 0\\1\\1\\1\\1 \end{bmatrix} + \begin{bmatrix} 0\\0\\0\\1\\1 \end{bmatrix} = \begin{bmatrix} 1\\1\\0\\0\\0 \end{bmatrix}.$$

And the question we formulated above is: *can we arrive to any pre-given vector of $\mathbb{Z}_2^5$ by starting from any vector of $\mathbb{Z}_2^5$ and by adding a series of vectors $v_1, \ldots, v_6$* (as many times as we wish, in any order)? In particular, can we start from $w = (0,0,1,0,0)$ and arrive to the vector $b_1 = (0,0,1,0,1)$ or to $b_2 = (1,0,1,0,1)$.

Firstly, notice that vector addition in $\mathbb{Z}_2^5$ is *commutative*. So any sum $v_i + v_j$ can be replaced to $v_j + v_i$. That is, in any sum of any number of vectors $v_1, \ldots, v_6$ we can interchange vectors to group them by v_i's. We have:

$$w + x_1 v_1 + x_2 v_2 + x_3 v_3 + x_4 v_4 + x_5 v_5 + x_6 v_6 = b_1,$$

where $x_i = 0, 1, 2, 3 \ldots$, and $i = 1, \ldots, 6$.

Secondly, notice that in $\mathbb{Z}_2^5$ for any vector v we have

$$2v = 4v = \cdots = (2s)v = \cdots = \vec{0}.$$

So in the sum above the actual values of x_i are 0 or 1 only: each command either is not needed, or is needed *once only* (and x_i is a number of the field $\mathbb{Z}_2$ actually)! Bring the sum to the form:

$$x_1 v_1 + x_2 v_2 + x_3 v_3 + x_4 v_4 + x_5 v_5 + x_6 v_6 = b_1 - w = (0,0,0,0,0,1).$$

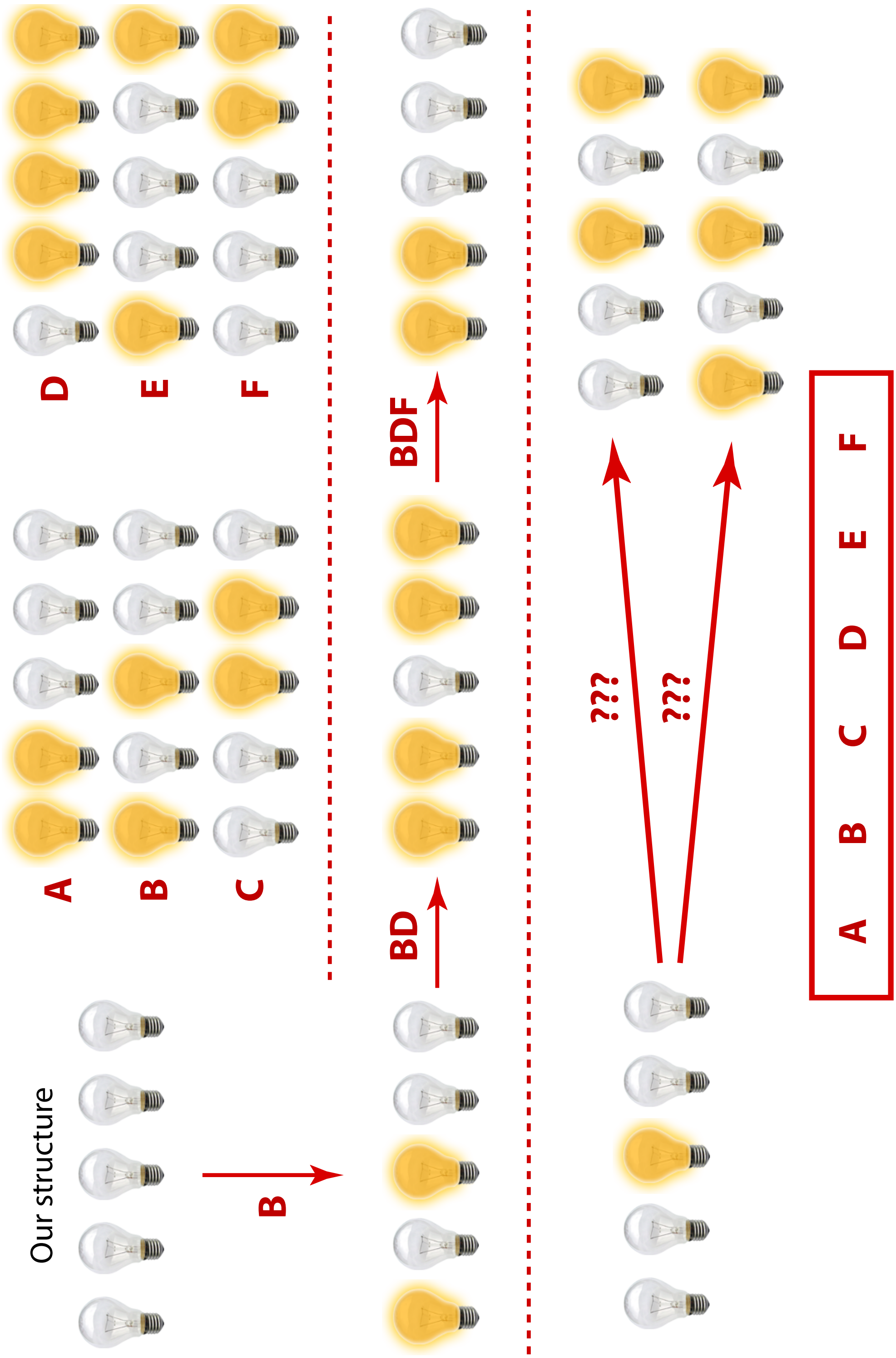


FIGURE 7.1. Controlling the structures by linear equations over $\mathbb{Z}_2$.

These steps bring us to a system of 5 linear equations in variables $x_1, \dots, x_6$ over the field $\mathbb{Z}_2$:

$$\begin{cases} 1x_1 + 1x_2 + 0x_3 + 0x_4 + 1x_5 + 0x_6 = 0 \\ 1x_1 + 0x_2 + 0x_3 + 1x_4 + 0x_5 + 0x_6 = 0 \\ 0x_1 + 1x_2 + 1x_3 + 1x_4 + 0x_5 + 0x_6 = 0 \\ 0x_1 + 0x_2 + 1x_3 + 1x_4 + 0x_5 + 1x_6 = 0 \\ 0x_1 + 0x_2 + 0x_3 + 1x_4 + 1x_5 + 1x_6 = 1 \end{cases}$$

(we intentionally write the zero coefficients also). The augmented matrix of the system and its row-echelon form are:

$$\bar{A} = \left[\begin{array}{cccccc|c} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right], \quad R = \left[\begin{array}{cccccc|c} \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{array}\right].$$

Thus, the system has no solution because the last column of R is pivot, or by Theorem 7.19, since $6 = \text{rank}\big(\bar{A}\big) > \text{rank}(A) = 5$. So we will *never* get the vector (structure condition) b_1 by the commands A, B, C, D, E, F.

Turning to vector $b_2 = (1, 0, 1, 0, 1)$ we get the vector equation:

$$x_1 v_1 + x_2 v_2 + x_3 v_3 + x_4 v_4 + x_5 v_5 + x_6 v_6 = b_2 - w = (1, 0, 0, 0, 0, 1)$$

which gives the system:

$$\begin{cases} 1x_1 + 1x_2 + 0x_3 + 0x_4 + 1x_5 + 0x_6 = 1 \\ 1x_1 + 0x_2 + 0x_3 + 1x_4 + 0x_5 + 0x_6 = 0 \\ 0x_1 + 1x_2 + 1x_3 + 1x_4 + 0x_5 + 0x_6 = 0 \\ 0x_1 + 0x_2 + 1x_3 + 1x_4 + 0x_5 + 1x_6 = 0 \\ 0x_1 + 0x_2 + 0x_3 + 1x_4 + 1x_5 + 1x_6 = 1 \end{cases}.$$

The augmented matrix of this system and its row-echelon form are:

$$\bar{A} = \left[\begin{array}{cccccc|c} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right], \quad R = \left[\begin{array}{cccccc|c} \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & \mathbf{1} & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

This time the system has solution. We can compute the reduced row-echelon form:

$$\left[\begin{array}{cccccc|c} \mathbf{1} & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

and the respective system of linear equations:

$$\begin{cases} x_1 = 1 - x_5 - x_6 \\ x_2 = -x_6 \\ x_3 = 1 - x_5 \\ x_4 = 1 - x_5 - x_6 \end{cases} \quad \text{or} \quad \begin{cases} x_1 = 1 + x_5 + x_6 \\ x_2 = x_6 \\ x_3 = 1 + x_5 \\ x_4 = 1 + x_5 + x_6 \end{cases}$$

(we replaced the coefficients -1 by 1, since in $\mathbb{Z}_2$ we have $-1 = 1$). It remains to assign all four possible choices to couples of free variables x_5, x_6:

Assigning the values $x_5 = x_6 = 0$ we get the solution $(1,0,1,1,0,0)$. That is, starting from w we arrive to b_2 by adding v_1, v_3, v_4, or by the commands ACD.

Assigning the values $x_5 = x_6 = 1$ we get the solution $(1,1,0,1,1,1)$ or the commands ABDEF.

Assigning the values $x_5 = 0$, $x_6 = 1$ we get the solution $(0,1,1,0,0,1)$ or the commands BCF.

Assigning the values $x_5 = 1$, $x_6 = 0$ we get the solution $(0,0,0,0,1,0)$ or the single command E (attention, the shortest solution!), and there are *no other solutions* (excluding repetitions).

Exercises

E.7.1. We are given two real systems of linear equations:

$$\begin{cases} x_1 + 2x_2 \qquad + 2x_4 + x_5 = 1 \\ \qquad 2x_2 + 2x_3 \qquad + 4x_5 = 0 \\ 2x_1 + x_2 \qquad\qquad\qquad = 2 \\ x_1 + 3x_2 + x_3 + 2x_4 + 3x_5 = 1 \end{cases} \qquad \begin{cases} -x_4 + 3x_1 = 1 \\ 3x_4 + x_1 + x_2 = 0 \\ 2x_3 = -2 \\ x_1 + 3x_4 = 0. \end{cases}$$

(1) Find if the first system is consistent by bringing its augmented matrix $\bar{A}$ to row-echelon form and checking if its last column holds a pivot. **(2)** Perform the same steps for the second system. Warning: notice that its variables need be re-ordered first. **(3)** If the first system is consistent, find the general solution by the basic Gaussian elimination and backwards substitution process. **(4)** If the second system is consistent, find its general solution by the same process.

E.7.2. We are given the system of linear equations:

$$\begin{cases} x_1 + 2x_2 + x_3 + x_4 + x_5 + x_6 = 2 \\ \qquad\qquad -2x_4 - 2x_5 + x_6 = -5 \\ 2x_1 + 4x_2 + 2x_3 \qquad\qquad = 2 \\ \qquad\qquad 2x_4 + 2x_5 \qquad = 4 \end{cases}$$

(1) Write the matrix and the augmented matrix of this system. Bring the augmented matrix to a row-echelon form. **(2)** Restore the system of linear equations corresponding to that row-echelon form. Indicate the pivot columns in the matrix, and the pivot and free variables in the system. **(3)** Move the free variables to the right-hand side, and obtain one solution of the system by assigning the 0 value to all free variables. **(4)** Write the general solution by assigning parametric values to free variables.

E.7.3. Solve each of two systems of Exercise E.7.1 by the Gauss-Jordan method (you may use computations already done for Exercise E.7.1).

E.7.4. We are given the system of Exercise **E.7.2** above. **(1)** Bring the augmented matrix $\bar{A}$ to the reduced row-echelon form. *Hint*: if you have already found the row-echelon form, you can use it to shorten your work. **(2)** Restore the system of linear equations corresponding to the reduced row-echelon form, and write the general solution by the Gauss-Jordan method. **(3)** Find rank$(\bar{A})$. Explain by using the non-zero rows *and* by the number of pivots. **(4)** Apply Theorem 7.19 to this sytem.

E.7.5. We have a systems of linear equation on $\mathbb{C}$, and a system on finite field $\mathbb{Z}_3$:

$$\begin{cases} ix + y + z = -1 \\ \qquad y + 2z = 0 \\ 2ix \qquad + (1+i)z = 1 \end{cases} \qquad \begin{cases} \qquad y + z = 1 \\ x + 2y + 2z = 0 \\ x + y \qquad = 2. \end{cases}$$

Solve these systems by the Gauss-Jordan method.

E.7.6. For the augmented matrix $\bar{A}$ of each of the systems in Exercise E.7.5, using Theorem 7.13 about uniqueness of the reduced row-echelon form, find a matrix which is *not* row-equivalent to $\bar{A}$. Compare this to Exercise E.6.3 (2).

E.7.7. Find a matrix $A \in M_{3,4}(\mathbb{R})$ which is *not* in reduced row-echelon form because: **(1)** point 1 of Definition 7.5 holds for A, but point 2 does *not* hold for it. **(2)** point 1 of Definition 7.5 does *not* hold for A. Compare this to Exercise E.6.8.

E.7.8. Write a matrix A such that: **(1)** A is in $M_{3,5}(\mathbb{R})$. A is in row-echelon form but *not* in reduced row-echelon form. All pivots of A are equal to 1, and A has two non-pivot columns. **(2)** A is in $M_{3,3}(\mathbb{Z}_3)$. A is in reduced row-echelon form, and contains four non-zero entries. A has two pivot columns. **(3)** A is in $M_{4,3}(\mathbb{C})$. A is in row-echelon form but *not* in reduced row-echelon form. A has no real entries, and A has just two pivots which are conjugates of each other.

E.7.9. Indicate the ranks for each of four augmented matrices in exercises E.7.1 and E.7.5 (you do not need to compute the ranks again, just use the row-reduction computations already done for exercises E.7.1 and E.7.5).

E.7.10. Apply Theorem 7.19 to each of four systems of in exercises E.7.1 and E.7.5. I.e., indicate if each of them is consistent based on fact if the equality $\operatorname{rank}(A) = \operatorname{rank}(\bar{A})$ holds for it.

E.7.11. **(1)** Write a matrix of rank 2 in $M_{4,3}(\mathbb{R})$. **(2)** Write a square matrix of rank 3 and of degree 4 over $\mathbb{Z}_7$.

E.7.12. We are given the real matrices:

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

(1) Find which pairs of these matrices are row-equivalent. *Hint*: you may use uniqueness of the reduced row-echelon form. **(2)** Find the ranks of these real matrices. *Hint*: use calculations done for the previous point. Explain your answers.

Part 3

Matrix Algebra

CHAPTER 8

Elements of matrix algebra

"L'algèbre est généreuse: elle donne souvent plus que ce qu'on lui demande."
Jean D'Alembert

8.1. Matrix addition and multiplication

Fix a field F and consider any two $m \times n$ matrices $A, B \in M_{m,n}(F)$:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \dots & \dots & \dots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix}.$$

We can define their *sum* by the rule:

$$A + B \overset{\text{def}}{=} \begin{bmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \dots & \dots & \dots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{bmatrix}.$$

Also, for any scalar $c \in F$ the *product* cA is defined as

$$cA \overset{\text{def}}{=} \begin{bmatrix} ca_{11} & \cdots & ca_{1n} \\ \dots & \dots & \dots \\ ca_{m1} & \cdots & ca_{mn} \end{bmatrix}.$$

By shorter notation we mentioned earlier this could also be given as:

$$A + B = \left[a_{ij}\right]_{m,n} + \left[b_{ij}\right]_{m,n} \overset{\text{def}}{=} \left[a_{ij} + b_{ij}\right]_{m,n},$$

$$cA = c\left[a_{ij}\right]_{m,n} \overset{\text{def}}{=} \left[ca_{ij}\right]_{m,n}.$$

Example 8.1. Here is a real example:

$$\begin{bmatrix} 2 & 1 & 0 \\ 3 & 0 & 2 \\ \frac{1}{2} & -1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & \pi & 2 \\ -1 & 0 & 2 \\ 1 & 3 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1+\pi & 2 \\ 2 & 0 & 4 \\ \frac{3}{2} & 2 & 1 \end{bmatrix},$$

and a complex example:

$$3i \begin{bmatrix} 2 & -1 & i \\ 1-i & \frac{1}{3} & 1 \\ 1 & i & i \end{bmatrix} = \begin{bmatrix} 6i & -3i & -3 \\ 3+3i & i & 3i \\ 3i & -3 & -3 \end{bmatrix}.$$

Example 8.2. And here are examples of operations with matrices in $M_{2,3}(\mathbb{Z}_3)$ over the finite field $\mathbb{Z}_3$:

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

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

For any matrix A we introduce the *opposite* matrix

$$-A \overset{\text{def}}{=} (-1)A = \left[-a_{ij}\right]_{m,n}.$$

Using it we can also consider the *difference* of matrices as $A-B=A+(-B)$, such as:

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

This is not a new operation defined on matrices, but is a shorthand notation for $A+(-B)$.

It is important to notice that for matrices the operation of addition and multiplication by scalar satisfy the analogs of the *main algebraic properties* that we stressed for real spaces:

Proposition 8.3. *Let $A, B, C \in M_{m,n}(F)$ be any matrices over the field F, and $c, d \in F$ be any scalars. Then:*

1. $A+B=B+A$, *(commutativity of matrix addition)*
2. $(A+B)+C=A+(B+C)$, *(associativity of matrix addition)*
3. *there is zero matrix O such that $A+O=A$,* *(existence of additive identity)*
4. *there is a matrix $-A$ such that $A+(-A)=O$,* *(existence of opposite matrix)*
5. $c(A+B)=cA+cB$, *(distributivity of matrix addition)*
6. $(c+d)A=cA+dA$, *(distributivity of multiplication by scalar)*
7. $(c\cdot d)A=c(dA)$, *(homogeneity of multiplication by scalar)*
8. $1A=A$. *(unitarity of multiplication by scalar)*

Proves of all points are trivial exercises. In particular, as a zero matrix O one may take a matrix with all entries zero. The reason why we call these points actually are the axioms of abstract space definition.

Consider two matrices $A \in M_{m,n}(F)$ and $B \in M_{n,k}(F)$ where the *number of columns* in A is equal to the *number of rows* in B:

$$A=\begin{bmatrix}a_{11}&\cdots&a_{1n}\\ \multicolumn{3}{c}{\dotfill}\\ \boldsymbol{a_{i1}}&\cdots&\boldsymbol{a_{in}}\\ \multicolumn{3}{c}{\dotfill}\\ a_{m1}&\cdots&a_{mn}\end{bmatrix},\quad B=\begin{bmatrix}b_{11}&\cdots&\boldsymbol{b_{1j}}&\cdots&b_{1k}\\ \multicolumn{5}{c}{\dotfill}\\ b_{n1}&\cdots&\boldsymbol{b_{nj}}&\cdots&b_{nk}\end{bmatrix}.$$

Take i'th row in A, the j'th column in B, and form the sum:

$$\boldsymbol{c_{ij}=a_{i1}\cdot b_{1j}+\cdots+a_{in}\cdot b_{nj}}.$$

Define the *product AB* of matrices A and B as the $m\times k$ matrix consisting of all such c_{ij}:

$$AB=\begin{bmatrix}c_{11}&\cdots&c_{1k}\\ \multicolumn{3}{c}{\dotfill}\\ c_{m1}&\cdots&c_{mk}\end{bmatrix}\in M_{m,k}(F).$$

If A is a square matrix, we can define the square $A^2=AA$ and the k'th power $\boldsymbol{A^k=\underbrace{A\cdots A}_{k}}$ for any positive integer k.

Example 8.4. Consider an example of products of two square matrices:

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

And here are products of matrices of different sizes:

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

$$\begin{bmatrix} 0\\ 1\\ -1\\ 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0\\ 0 & -1 & 0 & 2\\ 0 & 1 & 0 & -2\\ 0 & -2 & 0 & 4 \end{bmatrix}.$$

Example 8.5. Let $A \in M_{m,n}(F)$ be a matrix and $v \in F^n$ is a vector in a space over the same field F. Writing v as a *column vector* we get an $n \times 1$ matrix, so that the matrix product Av is possible. For, say, $A = \left[\begin{smallmatrix} 2 & 3 & 1\\ 2 & 1 & 2\\ 4 & 0 & 1 \end{smallmatrix}\right]$ and $v = (2,1,0) \in \mathbb{R}^3$ we have:

$$Av = \begin{bmatrix} 2 & 3 & 1\\ 2 & 1 & 2\\ 4 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2\\ 1\\ 0 \end{bmatrix} = \begin{bmatrix} 5\\ 6\\ 5 \end{bmatrix} \in \mathbb{R}^3.$$

Example 8.6. The dot products of vectors can also be interpreted by matrices Compare:

$$(2,3,1) \cdot (2,1,0) = 2 \cdot 2 + 3 \cdot 1 + 1 \cdot 0 = 7,$$

$$\begin{bmatrix} 2 & 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2\\ 1\\ 0 \end{bmatrix} = \begin{bmatrix} 7 \end{bmatrix}.$$

Did you also notice some similarity with the previous example? If we rewrite the vector $u = (2,3,1)$ as a row vector $u = [2,3,1] \in \mathbb{R}^3$, then we have a special case of Example 8.5, when $A = u$.

So we enjoy the freedom of multiplication of a matrix-by-vector, vector-by-vector or vector-by-matrix, if their sizes permit such multiplication.

Consider some examples over other fields:

Example 8.7. Example with complex matrices:

$$\begin{bmatrix} i & 1+i & 0\\ 0 & 1 & 2\\ 2 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2i & 2\\ 0 & 3\\ 2 & 1 \end{bmatrix} = \begin{bmatrix} -2 & 3+5i\\ 4 & 5\\ 4i & 7 \end{bmatrix}.$$

Example 8.8. Example on finite field $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 2\\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 & 0 & 1\\ 1 & 3 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2\\ 3 & 3 & 1 \end{bmatrix}.$$

Example 8.9. On any field F we may define a specific square matrix called *identity* or *trivial* matrix of degree n:

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

(here 1 is the multiplicative identity of F). Evidently, $AI = IA = A$ holds for any matrix A as long as the size of A permits the multiplications. For instance:

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

Operation of matrix multiplication also satisfies the following properties:

Proposition 8.10. *Let A, B, C be any matrices over the field F. If the matrices are of appropriate sizes allowing addition and multiplication, then:*

1. $A(BC) = (AB)C$, *(associativity)*
2. $A(B+C) = AB + AC$, *(left distributivity)*
3. $(A+B)C = AC + BC$, *(right distributivity)*
4. *there is a matrix I such that $AI = A = IA$ for any A.* *(identity matrix)*

Before we prove them notice that for *square matrices* of the same size these properties together with the first four of the main properties of matrix addition in Proposition 8.3 mean that $M_{n,n}(F)$ is a *ring* by matrix addition and multiplication.

Proof of Proposition 8.10. First prove property (2). Let the i'th row of A be:

$$\begin{bmatrix} a_{i1} & \cdots & a_{in} \end{bmatrix}$$

and the j'th columns of B, of C and of the sum $B+C$ be:

$$\begin{bmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{bmatrix}, \quad \begin{bmatrix} c_{1j} \\ \vdots \\ c_{nj} \end{bmatrix}, \quad \begin{bmatrix} b_{1j}+c_{1j} \\ \vdots \\ b_{nj}+c_{nj} \end{bmatrix}.$$

Then the (i,j)'th entry in $A(B+C)$ is:

$$a_{i1}(b_{1j}+c_{1j})+\cdots+a_{in}(b_{nj}+c_{nj}),$$

whereas the (i,j)'th entry in $AB+AC$ is:

$$(a_{i1}b_{1j}+\cdots+a_{in}b_{nj})+(a_{i1}c_{1j}+\cdots+a_{in}c_{nj}).$$

The above sums evidently are equal.

Property (3) is similar to property (2), and can be proved in the same way.

Property (4) is already discussed in Example 8.9.

To prove property (1) suppose that the products AB and BC both are possible, that is, A is an $m \times n$ matrix, B is an $n \times k$ matrix, C is a $k \times s$ matrix:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}, \ B = \begin{bmatrix} b_{11} & \cdots & b_{1k} \\ \ldots & \ldots & \ldots \\ b_{n1} & \cdots & b_{nk} \end{bmatrix}, \ C = \begin{bmatrix} c_{11} & \cdots & c_{1s} \\ \ldots & \ldots & \ldots \\ c_{k1} & \cdots & c_{ks} \end{bmatrix}.$$

The j't column of BC is:

$$\begin{bmatrix} b_{11}c_{1j}+\cdots+b_{1n}c_{nj} \\ \vdots \\ b_{11}c_{1j}+\cdots+b_{1n}c_{nj} \end{bmatrix}.$$

Multiplying the i'th row of A with the above column we get:

$$a_{i1}(b_{11}c_{1j}+\cdots+b_{1n}c_{nj})+\cdots+a_{in}(b_{11}c_{1j}+\cdots+b_{1n}c_{nj}) = \sum_{r=1}^{k}\sum_{s=1}^{n} a_{is}b_{sr}c_{rj}.$$

Doing the same for $A(BC)$ we get the same values for each i,j. □

The matrix multiplication is *not* a commutative operation, in general:

Example 8.11. Consider the products:

$$AB = \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 2 \\ 0 & -2 & 0 \\ 2 & 1 & 0 \end{bmatrix},$$

$$BA = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & -1 & 6 \\ 1 & -2 & 0 \\ 1 & 0 & 0 \end{bmatrix} \neq BA.$$

While on the other hand:

$$AC = \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 6 \\ 0 & -3 & 3 \\ 3 & 0 & 0 \end{bmatrix},$$

$$CA = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 0 & 6 \\ 0 & -3 & 3 \\ 3 & 0 & 0 \end{bmatrix} = AC.$$

It sometimes is useful to visually divide the matrices to *blocks* to better describe the matrix structure. We indicate the blocks by "virtual" dashed lines and call the matrix a *block matrix*. This does not change the matrix or its entries actually.

$$\left[\begin{array}{ccc:ccc:ccc} a_{11} & \cdots & * & * & \cdots & * & * & \cdots & a_{1n} \\ * & \cdots & * & * & \cdots & * & * & \cdots & * \\ \hdashline * & \cdots & * & * & \cdots & * & * & \cdots & * \\ a_{m1} & \cdots & * & * & \cdots & * & * & \cdots & a_{mn} \end{array}\right].$$

Example 8.12. Consider the matrix sum:

$$\left[\begin{array}{ccc:cc} 1 & 2 & 1 & 1 & 2 \\ 2 & 1 & 3 & 0 & 1 \\ \hdashline 1 & 1 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 & 1 \end{array}\right] + \left[\begin{array}{ccc:cc} 1 & 2 & 1 & 0 & 0 \\ 2 & 1 & 3 & 3 & 1 \\ \hdashline 0 & 3 & 0 & 2 & 4 \\ 1 & 0 & 1 & 0 & 2 \end{array}\right] = \left[\begin{array}{ccc:cc} 2 & 4 & 2 & 1 & 2 \\ 4 & 2 & 6 & 3 & 2 \\ \hdashline 1 & 4 & 0 & 3 & 6 \\ 3 & 0 & 2 & 0 & 3 \end{array}\right].$$

The entries in respective blocks are added to each other. Denote:

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

Then the same sum can be presented as:

$$\begin{bmatrix} A & B \\ C & B \end{bmatrix} + \begin{bmatrix} A & D \\ E & 2B \end{bmatrix} = \left[\begin{array}{c:c} 2A & B+D \\ \hdashline C+E & 3B \end{array}\right],$$

which gives clearer picture for the matrices structure.

8.2. The transpose and the inverse matrix

For any $m \times n$ matrix A its *transpose* is the $n \times m$ matrix A^T constructed by interchanging the rows and columns of A. Namely, the i'th row of A^T is the i'th column of A:

$$\text{if } A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}, \quad \text{then } A^T = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}.$$

Transpose can also be obtained by reflection of A over its diagonal $a_{11}, a_{22}, \ldots$ The (i, j)'th entry of A^T is the (j, i)'th entry a_{ji} of A.

A is called a *symmetric* matix, if $A^T = A$, i.e., if reflection of A over its diagonal does not alter it. A symmetric matrix clearly has to be square.

Example 8.13. Here are examples of matrix transposes:

$$\begin{bmatrix} 3 & 2 & 1 & 1 \\ 2 & 1 & 5 & 0 \\ 2 & 0 & 1 & 1 \end{bmatrix}^T = \begin{bmatrix} 3 & 2 & 2 \\ 2 & 1 & 0 \\ 1 & 5 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 7 \end{bmatrix}^T = \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix}^T = \begin{bmatrix} 1 & 2 & 7 \end{bmatrix}.$$

Example 8.14. Consider the following square matrix

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

This is a symmetric matrix, and equality $A = A^T$ does hold.

Here are some basic properties of matrix transposes:

Proposition 8.15. *Let A, B be any matrices over the field F, and $c \in F$ be any scalar. If the matrices are of appropriate sizes allowing addition or multiplication, then:*

1. $(A^T)^T = A$,
2. $(A+B)^T = A^T + B^T$,
3. $(cA)^T = c(A^T)$,
4. $(AB)^T = B^T A^T$,
5. $(A^k)^T = (A^T)^k$ *for any positive integer* k.

Proof. The only point that is not evident and requires a proof is (4).

The product AB is correctly defined, if A is an $m \times n$ matrix and B is an $n \times k$ matrix. Clearly, A^T is an $n \times m$ matrix, and B is a $k \times n$ matrix, so the product $B^T A^T$ is correctly defined (and it is an $k \times m$ matrix).

By definition the (i, j)'t element of AB is $a_{i1}b_{1j} + \cdots + a_{in}b_{nj}$. The j't row of B^T and the i'th column of A^T respectively are:

$$\begin{bmatrix} b_{1j} & \cdots & b_{nj} \end{bmatrix}, \qquad \begin{bmatrix} a_{i1} \\ \vdots \\ a_{in} \end{bmatrix}.$$

Thus, the (j, i)'th element of $B^T A^T$ is $b_{1j}a_{i1} + \cdots + b_{nj}a_{in}$. □

You can easily find examples to show that the more "naturally" looking condition $(AB)^T = A^T B^T$ in general does *not* hold.

The proposition above can be used to prove:

Corollary 8.16.

1. *For any matrix* A *the products* AA^T *and* $A^T A$ *are correctly defined and are symmetric matrices.*
2. *For any square matrix* A *the sum* $A + A^T$ *is a symmetric matrix.*

Proof. Let us use the properties established earlier:

$$(AA^T)^T = (A^T)^T A^T = AA^T$$

(clearly, the product AA^T is defined). And for a square matrix A we have:

$$(A + A^T)^T = A^T + (A^T)^T = A^T + A = A + A^T.$$

□

A square matrix $A \in M_{n,n}(F)$ is called *invertible* (or *nonsingular*) matrix, if there is such a matrix $A^{-1} \in M_{n,n}(F)$ for which:

$$\boldsymbol{AA^{-1} = A^{-1}A = I.}$$

Then A^{-1} is called *inverse* of A. Not every matrix has an inverse:

Example 8.17. A zero matrix O has no inverse because the product of O with *any* matrix (of appropriate size) is equal to O, not to I.

Example 8.18. (Optional) $A = \begin{bmatrix} 2 & 1 \\ 6 & 3 \end{bmatrix}$ has no inverse. If for whatever matrix $B = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ the equality $AB = I$ holds, then from

$$\begin{bmatrix} 2 & 1 \\ 6 & 3 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

we have $1 = 2 \cdot x + 1 \cdot z$ and $0 = 6 \cdot x + 3 \cdot z = 3(2x + z) = 3$. Contradiction.

Example 8.19. Take any non-zero $a, b \in F$ and consider the matrix $A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. Then a direct verification shows that

$$\begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix},$$

is the inverse A^{-1}, and so A is an invertible matrix.

Example 8.20. (Optional) More generally, a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2,2}(F)$ is invertible if and only if $ad - bc \neq 0$.

We omit the proof, as this is just a particular case of a more general Corollary 19.3 to be proved later. The above expression $ad - bc$ is the *determinant* of A. It will be studied in Part 6.

In Section 8.1 we defined the powers $A^k = A \cdots A$ for any square matrix A and for any *positive* k. Also set $\boldsymbol{A^0 = I}$. In case A is invertible, we can for any *negative* integer k define the negative powers of A as $\boldsymbol{A^k = (A^{-1})^{-k}}$ using the *positive* $-k$. That is, for an invertible matrix A its power A^k is defined for *any integer* $k \in \mathbb{Z}$.

Proposition 8.21. *Assume $A, B \in M_{n,n}(F)$ are any invertible matrices, $c \in F$ is any non-zero scalar. Then:*

1. *the inverse matrix A^{-1} is unique,*
2. $\left(A^{-1}\right)^{-1} = A$,
3. $(cA)^{-1} = c^{-1}A^{-1}$,
4. $(AB)^{-1} = B^{-1}A^{-1}$,
5. $\left(A^k\right)^{-1} = \left(A^{-1}\right)^k$ *and* $A^{-k} = \left(A^k\right)^{-1}$ *for any power* $k \in \mathbb{Z}$,
6. $\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$.

Clearly, these points also mean that the respective matrix mentioned in each step *is invertible*. Say, point (4) means that AB is invertible *and* its inverse is $B^{-1}A^{-1}$. The proofs of points in Proposition 8.21 are simple, and we leave them as easy exercises. Notice that the very "naturally" looking condition $(AB)^{-1} = A^{-1}B^{-1}$ may fail.

Invertible matrices allow the *cancellation* feature: if C is an invertible matrix, and the equality

$$AC = BC \tag{8.1}$$

holds for some matrices A, B, then also $A = B$. So to say, we can *cancel* C in (8.1). This simple fact is easy to prove by multiplying both sides of (8.1) by C^{-1} from the right. The analog of this no longer is true, if C is *not* invertible, as this simple example shows:

$$\begin{bmatrix} 2 & 1 \\ 0 & 9 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 8 \\ 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 7 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 8 \\ 0 & 0 \end{bmatrix}.$$

However, for a special case a variation of cancellation is possible. If A is an $m \times n$ matrix, and the vector $v \in F^n$ is written as a column vector, i.e., as an $n \times 1$ matrix, then we can interpret Av as a correctly defined $m \times 1$ product matrix. In these terms:

Lemma 8.22. *If for the matrices $A, B \in M_{m,n}(F)$ the equality $Av = Bv$ holds for arbitrary column vector $v \in F^n$, then $A = B$.*

Notice that equality $A = B$ may not follow from a *single* equality $Av = Bv$. But if the equality $Av = Bv$ holds for *arbitrary* v, then $A = B$ according to this lemma.

Proof. If $A \neq B$, then $a_{ij} \neq b_{ij}$ for some i, j. If $Av = Bv$ for *any* v, then also

$$Av = \begin{bmatrix} a_{11} \cdots a_{1j} \cdots a_{1n} \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots \boldsymbol{a_{ij}} \cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ a_{m1} \cdots a_{mj} \cdots a_{mn} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ \boldsymbol{1} \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} a_{1j} \\ \vdots \\ \boldsymbol{a_{ij}} \\ \vdots \\ a_{mj} \end{bmatrix} = Bv = \begin{bmatrix} b_{11} \cdots b_{ij} \cdots b_{in} \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots \boldsymbol{b_{ij}} \cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ b_{m1} \cdots b_{mj} \cdots b_{mn} \end{bmatrix} \begin{bmatrix} 0 \\ \vdots \\ \boldsymbol{1} \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} b_{ij} \\ \vdots \\ \boldsymbol{b_{ij}} \\ \vdots \\ b_{mj} \end{bmatrix}$$

for the vector v in which all coordinates are zero except the j'th coordinate 1. But this clearly is impossible as $a_{ij} \neq b_{ij}$. $\square$

Later we will use this lemma repeatedly.

So far we learned some properties of invertible matrices and built some examples of matrices which *are* or *are not* invertible. We still need:

1. a criterion to detect if the given matrix A is invertible;

2. a method to compute A^{-1}, *if* A is invertible.

We will return to this task in Section 9.3.

Exercises

E.8.1. We are given the real matrices:

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

Consider *all* possible pairs of above matrices, such as A,B, or B,A, etc., and for each pair indicate if their sum or product is possible. Compute such two sums and two products.

E.8.2. Present the matrices A and B of Exercise E.8.1 as block matrices of type $\left[\begin{array}{c:c} X & Y \\ \hdashline Z & W \end{array}\right]$ for suitable 2×2 matrices X, Y, Z, W for each. Then write the product $A\cdot B$ using the block matrix form.

E.8.3. We are given the real matrices

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

Explain which of the following operations are possible (and calculate the results): **(1)** $(A^T + C)^T + B$; **(2)** $(A^T + 2C)\cdot A$; **(3)** $D\cdot C + D\cdot A^T$; **(4)** $B^2 - A\cdot C$.

E.8.4. Prove point 5 of Proposition 8.3.

E.8.5. Prove point 3 of Proposition 8.10. *Hint*: use the proof of point 2 of Proposition 8.10.

E.8.6. Write the transposes of the matrices A, C, D of Exercise E.8.1.

E.8.7. We are given the real matrices $M=\begin{bmatrix}3&-1\\-2&1\end{bmatrix}$, $N=\begin{bmatrix}-1&2\\1&-1\end{bmatrix}$, $O=\begin{bmatrix}0&0\\0&0\end{bmatrix}$. Compose the matrix $G=\left[\begin{array}{c:c} M & O \\ \hdashline O & N \end{array}\right]$, and detect if G is the inverse of a matrix in Exercise E.8.1.

CHAPTER 9

Systems of linear equations and the elementary matrices

9.1. Interpreting systems and elementary operations by matrices

Suppose we are given a system of linear equations over a field F:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{9.1}$$

Write down its matrix A, a column-matrix X consisting of variables $x_1, \ldots, x_n$, and the column-matrix of constant terms B:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad B = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

It is easy to notice that our system (9.1) can be interpreted as the matrix equation

$$\boldsymbol{AX = B}$$

because

$$AX = \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{bmatrix},$$

and this product matrix is equal to the matrix B if and only if $a_{i1}x_1 + \cdots + a_{in}x_n = b_i$ for all $i = 1, \ldots, m$.

Example 9.1. Consider the system used earlier:

$$\begin{cases} \quad\;\; y + z = 1 \\ 2x - y + z = 9 \\ x \;\; - y - z = 2 \end{cases}$$

It is equivalent to matrix equation $AX = B$, where

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 2 & -1 & 1 \\ 1 & -1 & -1 \end{bmatrix}, X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, B = \begin{bmatrix} 1 \\ 9 \\ 2 \end{bmatrix}.$$

Agreement 9.2. For the future let us use the handy notation $AX = B$ to indicate not only a matrix equation, but the system of linear equations like (9.1) also. So instead of writing down the big system (9.1), we can just note: "Assume we are given a system of linear equations $AX = B$". This helps to reduce routine in writing.

In literature $AX = B$ is sometimes denoted by $A\boldsymbol{x} = \boldsymbol{b}$ or by by $A\mathbf{x} = \mathbf{b}$, i.e., bold symbols $\boldsymbol{x}$, $\boldsymbol{b}$ or $\mathbf{x}$, $\mathbf{b}$ are used to denote the matrices X and B.

Relations between systems of linear equations and matrices are even deeper: *we can replace the elementary operations by matrix multiplication*. Let us start by examples:

Example 9.3. Multiply a matrix A from the left by the matrix E where

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

We then have:

$$EA=\begin{bmatrix}1&1&0&2\\0&3&4&1\\3&0&2&0\end{bmatrix}\ {\scriptstyle R2\leftrightarrow R3.}$$

So multiplication by E is equivalent to swapping the 2'nd row with the 3'rd row.

Example 9.4. Multiply the matrix A of previous example from the left by another matrix

$$E=\begin{bmatrix}1&0&0\\0&1&0\\0&0&5\end{bmatrix}.$$

We easily get:

$$EA=\begin{bmatrix}1&1&0&2\\3&0&2&0\\0&15&20&5\end{bmatrix}\ {\scriptstyle 5\cdot R3.}$$

I.e., multiplication of A by this E is equivalent to multiplication of its 3'rd row by 5.

Example 9.5. Now take another matrix

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

Then we have:

$$EA=\begin{bmatrix}1&1&0&2\\6&3&2&6\\0&3&4&1\end{bmatrix}\ {\scriptstyle R2+3R1.}$$

So multiplication by E is equivalent to addition to the 2'nd row of A the 1'st row times 3.

Here are three matrices of the previous three examples:

$$\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},\quad \begin{bmatrix}1&0&0\\0&1&0\\0&0&5\end{bmatrix},\quad \begin{bmatrix}1&0&0\\3&1&0\\0&0&1\end{bmatrix}. \tag{9.2}$$

Multiplication of A (from the left) by each of the matrices (9.2) is equivalent to one of elementary operations with A. Also, each of these matrices can be obtained from the identity matrix $I=\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right]$ by the *respective* elementary operation.

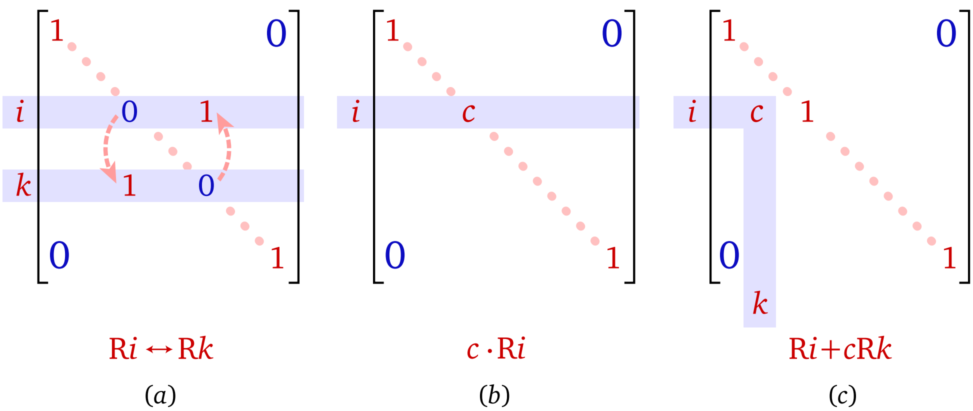


FIGURE 9.1. Elementary matrices of the 1'st, 2'nd and 3'rd types.

Call a matrix E an *elementary matrix of* 1*'st type*, if it can be obtained from the identity matrix by an elementary operation of the 1'st type. Say, if we apply $Ri \longleftrightarrow Rk$ to I_n, then to get E we just move in I_n the i'th diagonal entry 1 to the k'th row, and move the k'th diagonal entry 1 to the i'th row. See Figure 9.1 (a).

Call E an *elementary matrix of* 2*'nd type*, if it can be obtained from the identity matrix by an elementary operation of the 2'nd type. Say, if we apply $c\cdot Ri$ to I_n, then to get E we just replace in I_n the i'th diagonal entry 1 by c. See Figure 9.1 (b).

Call E an *elementary matrix of* 3'rd *type*, if it can be obtained from the identity matrix by an elementary operation of the 3'rd type. Say, if we apply $Ri + cRk$ to I_n, then to get E we just replace in I_n the entry 0 in i'th row and k'th column by c (recall that $i \neq k$). See Figure 9.1 (c).

Using elementary matrices we can introduce an extremely useful computational feature that allows us to magically replace a whole sequence of elementary operations (needed to bring a matrix to a row-echelon form or for other purposes) by a *single* matrix multiplication. Suppose we apply a sequence of elementary operations to a matrix A to get the matrix B. Let $E_1, \dots, E_t$ be the elementary matrices corresponding to the elementary operations we applied. What will then be the following matrix product?

$$E_t \cdots E_1 \cdot A. \tag{9.3}$$

We can rewrite it as $E_t\big(\cdots\big(E_2\,(E_1 A)\big)\cdots\big)$, and understand it so that we first multiply A by E_1 (i.e., we do the first of our elementary operations), next we multiply the result by E_2 (i.e., we do the second operation), etc... and finally we multiply the obtained matrix by E_t (i.e., we do the last operation). So the product (9.3) is nothing but the matrix B.

Next, denote $N = E_t \cdots E_1$ to be the product of our elementary matrices (notice the order in which they stand). We have:

$$N \cdot A = (E_t \cdots E_1)\,A = B,$$

i.e., multiplication of A from the left by t matrices $E_1, \dots, E_t$ (that is, application to A a sequence of t elementary operations) can be replaced by *just one* matrix multiplication.

Example 9.6. Now let us turn back to the system of Example 7.3:

$$\begin{cases} \quad\ \ y + z = 1 \\ 2x - y + z = 9 \\ x \ \ - y - z = 2 \end{cases}$$

The step-by-step Gauss-Jordan elimination process for this system was given in Example 6.4 and Example 7.10. Let us list all seven elementary operations used in those examples, and for each of them indicate the elementary matrix:

$$R1 \longleftrightarrow R3, \quad \text{matrix } E_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$R2 + (-2)R1, \quad \text{matrix } E_2 = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$R3 + (-1)R2, \quad \text{matrix } E_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix},$$

$$-\tfrac{1}{2} \cdot R3, \quad \text{matrix } E_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{2} \end{bmatrix},$$

$$R2 + (-3)R3, \quad \text{matrix } E_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix},$$

$$R1 + R3, \quad \text{matrix } E_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$R1 + R2, \quad \text{matrix } E_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The product $N = E_7E_6E_5E_4E_3E_2E_1$ of these seven matrices is equal to

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

It is easy to check that

$$\begin{bmatrix} 1 & 0 & 1 \\ \frac{3}{2} & -\frac{1}{2} & 1 \\ -\frac{1}{2} & \frac{1}{2} & -1 \end{bmatrix} \left[\begin{array}{ccc|c} 0 & 1 & 1 & 1 \\ 2 & -1 & 1 & 9 \\ 1 & -1 & -1 & 2 \end{array}\right]$$

$$= \left[\begin{array}{ccc|c} \mathbf{1} & 0 & 0 & 3 \\ 0 & \mathbf{1} & 0 & -1 \\ 0 & 0 & \mathbf{1} & 2 \end{array}\right],$$

or in other notation:

$$N \cdot \bar{A} = \operatorname{rref}\big(\bar{A}\big).$$

I.e., the seven steps of row-reduction of A to $\operatorname{rref}\big(\bar{A}\big)$ can be written as multiplication by some elementary matrices, and then the entire process can be replaced by multiplication by a *single* matrix N which alone "holds" all the steps of elimination.

Using row-elimination steps we can bring any matrix A to its reduced row-echelon form rref(A), and in analogy with the above example and with (9.3) we can write the result of this process as:

$$E_t \cdots E_1 \cdot A = \mathrm{rref}(A). \tag{9.4}$$

The obtained formula will be used later repeatedly.

Another fact that will be repeatedly used later is that each elementary matrix is *invertible*. Moreover, the inverse of an elementary matrix is the matrix corresponding to the *reverse of the respective elementary operation*. Let us display this simple fact for matrices (9.2) used above:

$\begin{bmatrix} 1&0&0\\ 0&0&1\\ 0&1&0 \end{bmatrix}^{-1} = \begin{bmatrix} 1&0&0\\ 0&0&1\\ 0&1&0 \end{bmatrix}$. We can check this either by direct multiplication, or by observing that swapping two rows twice changes nothing in a matrix.

$\begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&5 \end{bmatrix}^{-1} = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&\frac{1}{5} \end{bmatrix}$. One may verify this by direct multiplication, or by just noticing that multiplying a row by 5 and then by $\frac{1}{5}$ changes nothing.

$\begin{bmatrix} 1&0&0\\ 3&1&0\\ 0&0&1 \end{bmatrix}^{-1} = \begin{bmatrix} 1&0&0\\ -3&1&0\\ 0&0&1 \end{bmatrix}$. We can check this by direct multiplication, or by noticing that adding to a row another row times 3 and then again the same row times -3 changes nothing in the matrix.

9.2. Invertible matrices and square systems of linear equations

As a starting point fix any *invertible* matrix

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \in M_{n,n}(F).$$

Choose any *square* systems of linear equations over a field F with coefficient matrix A, and with any constants $b_1, \dots, b_n$:

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

As we saw in previous section, this system can be given by matrix equation $AX = B$, where B is the matrix of constant terms, and X is the variables matrix. We have a new method of solution for this system:

Lemma 9.7. *If the coefficient matrix A of the system $AX = B$ is invertible, then the system is consistent. It has a unique solution which can be obtained as a matrix product $A^{-1}B$.*

Proof. Multiplying both sides of $AX = B$ by A^{-1} from the left we get:

$$A^{-1} \cdot AX = A^{-1} \cdot B \quad \text{and so} \quad X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = A^{-1}B.$$

$A^{-1}B$ is a column matrix, and the above equality gives the unique values for variables $x_1, \dots, x_n$ as entries of the column $A^{-1}B$. □

Example 9.8. Consider the system discussed in above examples:

$$\begin{cases} \quad\;\; y+z=1\\ 2x-y+z=9\\ x\;\;-y-z=2. \end{cases}$$

Its matrix is:

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

which is invertible, and has the inverse:

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

(for now leave aside the questions why A is invertible, how did we compute the inverse A^{-1}, and why it is equal to the matrix N in recent Example 9.6).

By Lemma 9.7 the single solution of our system can be given by:

$$A^{-1}B=\begin{bmatrix}1&0&1\\\frac{3}{2}&-\frac{1}{2}&1\\-\frac{1}{2}&\frac{1}{2}&-1\end{bmatrix}\cdot\begin{bmatrix}1\\9\\2\end{bmatrix}=\begin{bmatrix}3\\-1\\2\end{bmatrix}.$$

This is exactly the same solution that we found earlier in Example 7.10 using elimination steps of the Gauss-Jordan method.

A special case of the above lemma concerns the *homogeneous* systems, i.e., systems in which all constant terms b_i are zero. The matrix B in this case is the zero matrix $O=\begin{bmatrix}0\\\vdots\\0\end{bmatrix}$, and the matrix form of a homogeneous system is $AX=O$. Since any homogeneous system has at least one solution (consisting of zero coordinates), we by Lemma 9.7 get: *if A is invertible, then the only solution of the system $AX=O$ is the zero solution.*

Now let us apply the steps of the Gauss-Jordan method to the system $AX=O$. During this process we typically get $r=\operatorname{rank}(A)$ pivot variables and $d=n-r$ free variables, which we should move to the right-hand side (to assign them some values). If there were *at least one* such free variable, we would get *more than one* solutions. But since $AX=O$ has just *one* solution, we have $d=0$ and $n=r=\operatorname{rank}(A)$. Therefore, $r=n$ rows of the reduced row-echelon form of A are non-zero, i.e., $\operatorname{rref}(A)$ actually is equal to I_n. We arrive to the next milestone:

Lemma 9.9. *If for a square matrix A of degree n the system $AX=O$ has a single solution only, then* $\operatorname{rank}(A)=n$*, and the reduced row-echelon form of A is the identity matrix I_n.*

As we saw in (9.4), the reduced row-echelon form of any matrix A can be obtained by multiplying A by some elementary matrices. And since in our case $\operatorname{rref}(A)=I_n$, the equality (9.4) yields:

$$\boldsymbol{E_t\cdots E_1\cdot A=I_n}. \tag{9.5}$$

Since elementary matrices are invertible, we can multiply both sides of the above equality from the left by the inverses $E_1^{-1},\ldots,E_t^{-1}$:

$$E_1^{-1}\cdots E_t^{-1}\cdot E_t\cdots E_1\cdot A \;=\; E_1^{-1}\cdots E_t^{-1}\cdot I_n,$$

i.e.,

$$A\;=\;E_1^{-1}\cdots E_t^{-1}.$$

The inverse of any elementary matrix is an elementary matrix. So denoting E_i^{-1} by F_i for ll $i=1,\ldots,t$ we have the presentation of A as a *product of elementary matrices*:

$$\boldsymbol{A=F_1\cdots F_t}.$$

A product of invertible matrices F_i is invertible by Proposition 8.21. Thus, A is *invertible* and, moreover, we know its inverse is $A^{-1}=\left(E_1^{-1}\cdots E_t^{-1}\right)^{-1}$, i.e.,

$$\boldsymbol{A^{-1}=E_t\cdots E_1}. \tag{9.6}$$

Do you remember that *invertability* of A was the starting point from which we departured at the beginning this section? The circular chain of the obtained statements can summarized as:

Theorem 9.10. *Let A be a square matrix of degree n over a field F. Then the following conditions are equivalent:*

1. *A is an invertible matrix;*
2. *the system $AX = B$ has a single solution for any B;*
3. *the homogeneous system $AX = O$ has zero solution only;*
4. $\mathrm{rank}(A) = n$*;*
5. $\mathrm{rref}(A) = I_n$*;*
6. *A is a product of some elementary matrices.*

Example 9.11. Let us continue calculations of Example 9.6 to obtain presentation of matrix

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

as a product of elementary matrices. We have already computed seven elementary matrices $E_1, \ldots, E_7$ for the equality

$$E_7E_6E_5E_4E_3E_2E_1 \cdot A = \mathrm{rref}(A).$$

In previous section we saw how to compute the inverses of elementary matrices of each ot three types. We have:

$$F_1 = E_1^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$F_2 = E_2^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$F_3 = E_3^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

$$F_4 = E_4^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix},$$

$$F_5 = E_5^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix},$$

$$F_6 = E_6^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$F_7 = E_7^{-1} = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

From where $A = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \cdot F_5 \cdot F_6 \cdot F_7$.

9.3. Computing the inverse matrix

We are given a square matrix $A \in M_{n,n}(F)$. We want to detect *if A is invertible* and if yes, *calculate the inverse A^{-1}*.

By Theorem 9.10 we know that A is invertible if and only if $\mathrm{rank}(A) = n$. So start by bringing A to a row-echelon form to find its rank. If $\mathrm{rank}(A) \neq n$, then A is not invertible.

If $\mathrm{rank}(A) = n$, then proceed to calculation of $\mathrm{rref}(A)$ which in this case will be I_n by Theorem 9.10. According to (9.4) that process is equivalent to multiplication of A by some elementary matrices:

$$E_t \cdots E_1 \cdot A = \mathrm{rref}(A) = I_n. \tag{9.7}$$

Multiplying this equality from the right by A^{-1} we get:

$$E_t \cdots E_1 \cdot A \cdot A^{-1} = I_n \cdot A^{-1},$$

$$\boldsymbol{E_t \cdots E_1 \cdot I_n = A^{-1}}. \tag{9.8}$$

Comparing the equalities (9.7) and (9.8) we see that, if a series of elementary operations (corresponding to $E_1, \ldots, E_t$) brings the matrix A to reduced row-echelon form $\mathrm{rref}(A) = I_n$, then *the same series of elementary operations brings the matrix I_n to A^{-1}*. All we need is to bring A to reduced row-echelon form by some elementary operations, and then to apply each of those elementary operations to I_n to get A^{-1}.

There is a handy method to perform these two processes *simultaneously*. Merge the matrices A and I_n into a block matrix $\left[A \,\vdots\, I_n\right]$. Then do the necessary operations to bring it to reduced row-echelon form. That is, we construct the product

$$E_t \cdots E_1 \cdot \left[A \,\vdots\, I_n\right].$$

Evidently, each elementary operation changes the right-hand side of our block matrix in the *same* way as it changes the left hand side: if, say, E_i swaps two rows in the left-hand side, it has to swap the same rows in the right-hand side, etc... Thus, if the left-hand side of $\left[A \,\vdots\, I_n\right]$ becomes I_n, in the right-hand side we discover the inverse matrix A^{-1}, i.e., we have the row-equivalence:

$$\boldsymbol{\left[A \,\vdots\, I_n\right] \sim \left[I_n \,\vdots\, A^{-1}\right]}.$$

How to compute the inverse matrix. The method can be presented as:

Algorithm 9.12 (Inverse matrix computation)**.** We are given a square matrix A of degree n over a field F:

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

► Detect, if A is an invertible matrix. If, yes, compute the inverse matrix A^{-1}.

1. Form the block matrix $\left[A \,\vdots\, I_n\right]$ using A and the identity matrix I_n.

2. Bring $\left[A \,\vdots\, I_n\right]$ to a row-echelon form R by elementary row-operations.

3. If R has a zero row, i.e., if $\operatorname{rank}(A) < n$, then output: the matrix A is not invertible. End of the process.

4. Else bring R to the reduced row-echelon form $\operatorname{rref}(R) = \operatorname{rref}\left[A \,\vdots\, I_n\right]$ by elementary row-operations.

5. Output the right-hand side n columns of the matrix $\operatorname{rref}\left[A \,\vdots\, I_n\right] = \left[I_n \,\vdots\, A^{-1}\right]$ as the inverse matrix A^{-1}.

Could we get a "better" algorithm by directly bringing $\left[A \,\vdots\, I_n\right]$ to the reduced row-echelon form, without discussing the matrix R in step 3? No, because when A is *not* invertible, we no longer need to calculate the reduced row-echelon form $\operatorname{rref}\left[A \,\vdots\, I_n\right]$.

Example 9.13. Consider the matrix already used in previous examples:

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

$$\left[A \,\vdots\, I_3\right] = \left[\begin{array}{rrr|rrr} 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & -1 & 1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 0 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{rrr|rrr} 1 & -1 & -1 & 0 & 0 & 1 \\ 2 & -1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{rrr|rrr} 1 & -1 & -1 & 0 & 0 & 1 \\ 0 & 1 & 3 & 0 & 1 & -2 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{rrr|rrr} 1 & -1 & -1 & 0 & 0 & 1 \\ 0 & 1 & 3 & 0 & 1 & -2 \\ 0 & 0 & -2 & 1 & -1 & 2 \end{array}\right] = R.$$

The row-echelon form R is found. Since $\operatorname{rank}(R) = \operatorname{rank}(A) = 3$, we get that the matrix is invertible. Proceed to reduced row-echelon form:

$$R \sim \left[\begin{array}{rrr|rrr} 1 & -1 & -1 & 0 & 0 & 1 \\ 0 & 1 & 3 & 0 & 1 & -2 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & -1 & -1 & 0 & 0 & 1 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{1}{2} & 1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & -1 & 0 & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{1}{2} & 1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & \frac{3}{2} & -\frac{1}{2} & 1 \\ 0 & 0 & 1 & -\frac{1}{2} & \frac{1}{2} & -1 \end{array}\right] = \left[I_3 \,\vdots\, A^{-1}\right].$$

In the right-hand half we find the matrix A^{-1}:

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

Notice that is it the matrix used in Example 9.8.

Example 9.14. Compute the inverse of the matrix over $\mathbb{Z}_3$ (do not forget that the operations in matrices are being done in the finite field $\mathbb{Z}_3$):

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

$$\left[A \,\vdots\, I_3\right] = \left[\begin{array}{ccc:ccc} 0 & 2 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 & 2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{array}\right] = R.$$

We already get that A is invertible, since R has no zero rows.

Proceed the steps:

$$R \sim \left[\begin{array}{ccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{array}\right] = \left[I_3 \,\vdots\, A^{-1}\right].$$

Thus we obtain the inverse matrix:

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

Exercises

E.9.1. Write the system of linear equations in Example 7.9 in the matrix form $AX = B$.

E.9.2. Write the elementary matrices corresponding to each of the following seven operations applied to a 3×4 matrix: **(1)** operation $R3 - 2R1$. **(2)** $R1 + (-3)R2$. **(3)** $4 \cdot R2$. **(4)** $R3 \leftrightarrow R2$. **(5)** operation of adding the first row to the second row. **(6)** operation of adding to the second row the first row. **(7)** operation of swapping the first and last rows.

E.9.3. The elementary matrices E_1, E_2, E_3 are those given in (9.2). **(1)** *Without using the row-by-column rule of matrix multiplication* compute the matrix powers E_1^{10}, E_1^{11}, E_2^{3}, E_3^{10}. **(2)** Find the inverses E_1^{-1}, E_2^{-1}, E_3^{-1} using the fact that they are inverses of some matrices corresponding to elementary operations. **(3)** Find the inverse of the block matrix $B = \left[\begin{array}{c:c} E_2 & O \\ \hdashline O & E_3 \end{array}\right]$. *Hint:* present B as a product of elementary matrices.

E.9.4. In Example 7.9 we bring the row-echelon matrix R to reduced row-echelon form using four elementary operations. **(1)** For these elementary operations write the respective elementary matrices E_1, E_2, E_3, E_4. **(2)** Compute the product $N = E_4E_3E_2E_1$ and the product NR. If you are right, NR is the reduced row-echelon form found in Example 7.9.

E.9.5. In Example 7.4 we bring the augmented matrix $\bar{A}$ to a row-echelon form R using two elementary operations. Write the respective elementary matrices E_1, E_2. Compute the product $N = E_2E_1$ and check if $N\bar{A} = R$.

E.9.6. We are given the real matrices.

$$M = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad N = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & -1 \\ 0 & 0 & 1 \end{bmatrix}.$$

(1) Compute the ranks, and based on ranks deduce if each matrix is invertible. **(2)** Without any other row-operations deduce if each of the matrices above is a product of elementary matrices, and find their reduced row-echelon forms. **(3)** Compute the inverses of the matrices above, if you find they are invertible. **(4)** Explain how many solutions will have the homogeneous system of linear equations the matrix of which is M, N or MN.

E.9.7. We are given the real matrices $A = \left[\begin{smallmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 2 & 3 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 3 & 3 \end{smallmatrix}\right]$. **(1)** By reducing these matrices to row-echelon form compute rank(A) and rank(B), then using Theorem 9.10 argument that A is invertible and B is *not* invertible. **(2)** At this step *without any new elementary operations* find rref(A), and indicate that rref$(B) \neq I$. **(3)** Using Theorem 9.10 argument that A can be presented as a product of elementary matrices. **(4)** Compute the presentation of A as a product of elementary matrices.

E.9.8. We are given the matrices $A = \left[\begin{smallmatrix} 2 & 0 & 1 \\ 2 & 3 & 2 \\ 1 & 1 & 1 \end{smallmatrix}\right] \in M_{3,3}(\mathbb{R})$, $B = \left[\begin{smallmatrix} i & 0 \\ 2 & -i \end{smallmatrix}\right] \in M_{2,2}(\mathbb{C})$, $C = \left[\begin{smallmatrix} 2 & 1 \\ 1 & 0 \end{smallmatrix}\right] \in M_{2,2}(\mathbb{Z}_3)$. By Gauss-Jordan Algorithm 6.10 detect if each of them is invertible and, if so, compute respective inverses.

E.9.9. We are given three real matrices:

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

(1) For each matrix detect if it is invertible using some point of Theorem 9.10. **(2)** If the matrix is invertible, write for it the formula $E_t \cdots E_1 \cdot M = \mathrm{rref}(M) = I$ (explain why $\mathrm{rref}(M) = I$). *Hint*: find the elementary matrices E_i using the elementary operations needed to bring the matrix to the reduced row-echelon form.

Part 4

Abstract Vector Spaces

CHAPTER 10

Abstract vector spaces, main examples, subspaces

"Tous les effets de la nature ne sont que les résultats mathématiques d'un petit nombre de lois immuables."
Pierre S. Laplace

10.1. Motivation to abstract vector spaces, main examples

In our course we had an important milestone where we allowed some more *abstraction* into our constructions, and it made our arguments more natural and even simpler. Namely, we started the course by considering the spaces $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathbb{Z}_p^n$ separately. Then we allowed the abstraction of *field* F, and considered the previous spaces as particular cases of F^n. After that milestone all further objects such as the systems of linear equations, matrices, row-echelon forms, elementary operations, etc., were introduced not individually over $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$, but over any *abstract field* F, in general. This really simplified the things because we would have many unnecessary and routine repetitions, if we had learned, say, how to solve systems of linear equations for real numbers using real matrices, then had repeated everything for complex numbers with complex matrices, then for $\mathbb{Z}_p$ with modular matrices, etc.

Now we are at the next milestone to introduce another step of *abstraction*: the *vector space*. Let us start by examples of structures which are not the spaces F^n, but which have "behaviour" very similar to them.

Assume we are given the polynomials

$$\begin{aligned}
f_1(x) &= 3 + x^2 + 2x^3,\\
f_2(x) &= -1 + x + x^3,\\
f_3(x) &= 5 + 2x^2 + 2x^3,\\
f_4(x) &= 3 + 2x - 5x^2 + 6x^3,\\
g(x) &= 2 + x + 3x^2 + 4x^3,
\end{aligned}$$

and we want to find out if there are numbers $a_1, a_2, a_3, a_4 \in \mathbb{R}$ (and if yes, how many) such that $g(x)$ can be expressed as:

$$g(x) = a_1 f_1(x) + a_2 f_2(x) + a_3 f_3(x) + a_4 f_4(x). \tag{10.1}$$

Write the coefficients of our polynomials as row vectors:

$$f_1 = (3, 0, 1, 2),\;\; f_2 = (-1, 1, 0, 1),\;\; f_3 = (5, 0, 2, 2),\;\; f_4 = (3, 2, -5, 6),\;\; g = (2, 1, 3, 4).$$

It is intuitively clear to understand (strict explanation will follow in Section 12.1) that (10.1) holds if and only if

$$g = a_1 f_1 + a_2 f_2 + a_3 f_3 + a_4 f_4 \tag{10.2}$$

holds. But this vector equation is equivalent to the system of linear equations

$$\left\{\begin{array}{rcrcrcrcl} 3x_1 & - & x_2 & + & 5x_3 & + & 3x_4 & = & 2 \\ & & x_2 & & & + & 2x_4 & = & 1 \\ x_1 & & & + & 2x_3 & - & 5x_4 & = & 3 \\ 2x_1 & + & x_2 & + & 2x_3 & + & 6x_4 & = & 4, \end{array}\right. \tag{10.3}$$

which we can handle by more than one methods to get the single solution

$$\left(\tfrac{81}{26}, \tfrac{22}{13}, -\tfrac{12}{13}, -\tfrac{9}{26}\right). \tag{10.4}$$

So we have a *unique* presentation

$$g(x) = \tfrac{81}{26} f_1(x) + \tfrac{22}{13} f_2(x) - \tfrac{12}{13} f_3(x) - \tfrac{9}{26} f_4(x)$$

of polynomial $g(x)$ by polynomials $f_1(x)$, $f_2(x)$, $f_3(x)$, $f_4(x)$ of type (10.1).

Next coniser a very differently looking question. Suppose we have matrices

$$M_1 = \begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}, \; M_2 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \; M_3 = \begin{bmatrix} 5 & 0 \\ 2 & 2 \end{bmatrix}, \; M_4 = \begin{bmatrix} 3 & 2 \\ -5 & 6 \end{bmatrix}, \; N = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix},$$

and we want to know if there are numbers $a_1, a_2, a_3, a_4 \in \mathbb{R}$ such that:

$$N = a_1 M_1 + a_2 M_2 + a_3 M_3 + a_4 M_4. \tag{10.5}$$

Do you notice any *similarity* between these matrices and the above polynomials? "Slicing" each matrix to two rows, and putting these rows side-by-side we get five row vectors with four coordinates each:

$$m_1 = (3,0,1,2), \;\; m_2 = (-1,1,0,1), \;\; m_3 = (5,0,2,2), \;\; m_4 = (3,2,-5,6), \;\; n = (2,1,3,4)$$

(say, from M_1 we get the vector $(3,0,1,2)$). Clearly, (10.5) holds if and only if

$$n = a_1 m_1 + a_2 m_2 + a_3 m_3 + a_4 m_4.$$

But this vector equation is the *same* as (10.2), and it also is equivalent to the *same* system (10.3). Since we know it has the unique solution (10.4), we get the *unique* presentation

$$N = \tfrac{81}{26} M_1 + \tfrac{22}{13} M_2 - \tfrac{12}{13} M_3 - \tfrac{9}{26} M_4.$$

The moral of the fable is that there are structures which consist of objects *different* from vectors $\vec{v} = (x_1, \ldots, x_n)$ of the spaces F^n, but which are *very similar* to F^n in many aspects. The polynomial $3 + x^2 + 2x^3$, the matrix $\begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}$, and the vector $(3,0,1,2)$ turned out to have important similarities, although they are very different mathematical objects (for instance, a polynomial $f(x)$ has a derivative $f'(x)$ which a vector v does not possess, and a matrix A has a rank which is not defined for a polynomial).

The *big advantage* of noticing this fact is that after we have established a problem solving method or a theorem for F^n, we may generalize it for other *very similar* structures, just like we above used the solution of system of linear equations to handle a problem about polynomials and a problem about matrices.

Hopefully, you now are prepared to meet the abstract definition of vector space:

Definition 10.1. Let V be a non-empty set and F be a field. An operation of *addition* $+$ is defined on V: for any $u, v \in V$ the sum $u + v \in V$ is given. Also, an operation of *multiplication by a scalar* is defined: for any $a \in F$ and any $v \in V$ the product $av \in V$ is given. The following axioms hold for any $u, v, w \in V$, $a, b \in F$:

1. $u + v = v + u$; *(commutativity of vector addition)*
2. $(u + v) + w = u + (v + w)$; *(associativity of vector addition)*

3. there is an element $0 \in V$ such that $v + 0 = v$; *(existence of additive identity)*
4. there is an element $-v \in V$ such that $v + (-v) = 0$; *(existence of opposite vector)*
5. $a(u + v) = au + av$; *(distributivity of vector addition)*
6. $(a + b)v = av + bv$; *(distributivity of multiplication by scalar)*
7. $(a \cdot b)v = a(bv)$; *(homogeneity of multiplication by scalar)*
8. $1v = v$. *(unitarity of multiplication by scalar)*

Then V together with the defined operations is called a *vector space over the field F*. The elements of V are called *vectors* and the elements of F are called *scalars*.

The vector spaces also are called *linear spaces*. For briefness we may mostly call them just *spaces*. To distinguish the vectors they sometimes are denoted as $\vec{v}$. We will use such notation with arrow, only if it is necessary to stress that the given object is a vector (say, we may denote the identity vector by $\vec{0}$ to distinguish it from the zero element 0 in the field F). In literature you may also find notations $\vec{\mathbf{v}}$, $\vec{\boldsymbol{v}}$, $\mathbf{v}$, $\boldsymbol{v}$.

Let us list some widely used examples of vector spaces that will be repeatedly used later (please learn and remember them properly!). Some of them are new, while others already were considered before, and we have already displayed the points of the vector space definition as *"main algebraic properties"* in Part 1 and in Part 3.

Example 10.2. The first natural examples of vector spaces are the Euclidean one-, two- or three-dimensional spaces containing arrow-like vectors with "head to tail" addition and with multiplication with real scalars by "vector length scaling". The points of Definition 10.1 are easy to check.

Example 10.3. Next examples of spaces are $\mathbb{R}^n$, $\mathbb{Q}^n$, $\mathbb{C}^n$, $\mathbb{Z}_p^n$ for the fields $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$. Moreover for any field F the set of vectors

$$V = F^n = \{(x_1, \dots, x_n) \mid x_i \in F,\ i = 1, \dots, n\}$$

is a vector space over F with operations defined as follows: if $u = (x_1, \dots, x_n)$, $v = (y_1, \dots, y_n)$ and $c \in F$, then

$$u + v \overset{\text{def}}{=} (x_1 + y_1, \dots, x_n + y_n)$$

$$c(x_1, \dots, x_n) \overset{\text{def}}{=} (cx_1, \dots, cx_n).$$

The points of Definition 10.1 hold in F^n by Proposition 4.2. In particular:

$$\vec{0} = (0, \dots, 0), \quad -u = (-x_1, \dots, -x_n).$$

And $u + v = v + u$ because $x_i + y_i = y_i + x_i$ in F for any of the indices $i = 1, \dots, n$.

As the coming examples show, vector spaces are not limited to spaces F^n of sequences over fields only. Let us find spaces in some less evident places also.

Example 10.4. Consider the set of all $m \times n$ matrices $M_{m,n}(F)$ over any fixed field F. For matrices we have already defined the operations of addition and of multiplications by a scalar in Section 8.1.

And we have also stressed the main algebraic properties of these operations in Proposition 8.3. Comparing them with Definition 10.1 we see they actually state that $M_{m,n}(F)$ is a vector space. As we agreed, if $F = \mathbb{R}$, we may just write $M_{m,n}$.

We may consider matrix vectors and their combinations, such as:

$$\vec{u} = A = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}, \quad \vec{v} = B = \begin{bmatrix} 2 & -3 \\ \frac{1}{2} & 0 \end{bmatrix},$$

$$2\vec{u} + 3\vec{v} = \begin{bmatrix} 8 & -5 \\ \frac{3}{2} & -2 \end{bmatrix}.$$

(we intentionally used the arrows in $\vec{u}$, $\vec{v}$ to stress that we consider the matrices as vectors). It would be easy to build examples of matrix vectors on other fields also.

When the field F already is known from the context, or when $F = \mathbb{R}$, we may for briefness denote this space by $M_{m,n}$.

Example 10.5. Fix a field F and consider the set $F[x]$ of all *polynomials $f(x)$ over the field F*, i.e., the set of all *formal sums*:

$$f(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + a_n x^n$$

where $n \in \mathbb{N} \cup \{0\}$, $a_i \in F$, and $a_n \neq 0$ for $n \neq 0$.

Each such polynomial $f(x)$ is a formal expression defined by its *coefficients* $a_i \in F$, and by a new object: the *variable* x with its *formal powers* x^i (see also Appendix C.2).

Addition and multiplication by a scalar are defined in natural way by respective powers. It is easy to verify that $F[x]$ is a vector space. The zero polynomial $f(x) = 0$ is the zero vector of the space $F[x]$.

Say, in the real space $\mathbb{R}[x]$ we have:

$$\begin{aligned}(2 + x - 4x^2 + 2x^3) \;+\; (7 + 3x + 3x^2)\\ = 9 + 4x - x^2 + 2x^3,\end{aligned}$$

$$4(2 + x - 4x^2 + 2x^3) = (8 + 4x - 16x^2 + 8x^3).$$

Whereas in the space $\mathbb{Z}_5[x]$ we have:

$$(4+4x^2+3x^3)+(1+4x+2x^2)=4x+x^2+3x^3$$

$$4(4 + 4x^2 + 3x^3) = 1 + x^2 + 2x^3.$$

Example 10.6. For the above polynomial $f(x) = a_0 + \cdots + a_n x^n$ $(a_n \neq 0)$ the number n is called the *degree* of $f(x)$, and is denoted by $n = \deg(f(x))$. No degree is defined for the *zero* polynomial $f(x) = 0$.

Define a subset $\mathcal{P}_n(F)$ of $F[x]$ consisting of all polynomials $f(x) \in F[x]$ with degrees not more than n (and the zero polynomial).

It is easy to check that all the points of Definition 10.1 are satisfied, and $\mathcal{P}_n(F)$ also is a vector space.

So we have examples of "nested" spaces: the space $\mathcal{P}_n(F)$ is inside the space $\mathcal{P}_m(F)$ for any $m \geq n$. Also, any space $\mathcal{P}_n(F)$ is inside the space $F[x]$.

When we do not want to stress the field F, we will for briefness denote this space by $\mathcal{P}_n$. In most cases we are going to consider the polynomial space $\mathcal{P}_n = \mathcal{P}_n(\mathbb{R})$ on real field $F = \mathbb{R}$.

The next example displays a space even larger than $F[x]$:

Example 10.7. Let $\mathcal{F}(\mathbb{R})$ or $\mathcal{F}$ denote the set of all real functions over $\mathbb{R}$. Define the addition and multiplications by a scalar for functions $f, g \in \mathcal{F}$ *point-wise*:

$$(f + g)(x) = f(x) + g(x)$$
$$(af)(x) = a \cdot f(x) \quad (a \in \mathbb{R}).$$

The points of Definition 10.1 are easy to verify. Say, as a zero vector of $\mathcal{F}$ we take the constant zero function $f(x) = 0$. So $\mathcal{F}$ is another example of vector space. It evidently contains the space of polynomials $\mathbb{R}[x]$.

We may get other spaces $\mathcal{F}^1, \mathcal{F}^2, \ldots$ defining $\mathcal{F}^n$ to be the set of n times differentiable function. Clearly, $\mathcal{F}^n$ is a space as the sums of scalar multiples of any n times differentiable functions are n times differentiable.

Another direction to generalize $\mathcal{F}$ is to consider the space $\mathcal{F}(F)$ of functions over any abstract field F.

Example 10.8. Take a homogeneous system of linear equations $AX = O$ over any field F:

$$\begin{cases} a_{11}x_1 \;+\cdots+ a_{1n}x_n \;= 0\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0. \end{cases}$$

Let $v = (x_1', \ldots, x_n')$ and $u = (x_1'', \ldots, x_n'')$ be any two solutions of $AX = O$ and $a \in F$ be any scalar. It is easy to verify that $v + u$ and av also are solutions: for any $i = 1, \ldots, m$:

$$\begin{aligned} a_{i1}(x_1' + x_1'') + \cdots + a_{in}(x_n' + x_n'')\\ = \left[a_{i1}x_1' + \cdots + a_{in}x_n'\right]\\ + \left[a_{i1}x_1'' + \cdots + a_{in}x_n''\right]\\ = 0 + 0 = 0,\end{aligned}$$

and we also is easy to check the equalities:

$$\begin{aligned} a_{i1}(a \cdot x_1') + \cdots + a_{in}(a \cdot x_n')\\ = a\left[a_{i1}x_1' + \cdots + a_{in}x_n'\right] = a \cdot 0 = 0.\end{aligned}$$

The points of Definition 10.1 are very easy to check.

So we got the *the space of solutions* of the given homogeneous system of linear equations. Clearly, this space lies inside F^n, since each solution $(x_1', \ldots, x_n')$ is a vector in F^n.

Agreement 10.9. Since we are going to often present polynomial vectors $f(x)$ via the vectors $1,\ x,\ \ldots\ , x^n$, we agree to write polynomials *in ascending order* of terms:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

whenever we consider them *vectors* in polynomial spaces $\mathcal{P}_n(F)$ or $F[x]$. In all other cases we prefer to write polynomials in conventional way, starting by the leading term with the highest degree.

Let us denote $u-v=u+(-v)$. This is not a new operation defined on V but just a shorthand notation.

Proposition 10.10. *Let V be a vector space over a field F. Then for any $u,v\in V$ and $a\in F$ the following properties hold:*

1. *The trivial vector $\vec{0}$ is unique,*
2. *The opposite vector $-v$ is unique,*
3. *$-\vec{0}=\vec{0}$ and $-(-v)=v$,*
4. *$0v=\vec{0}$ and $a\vec{0}=\vec{0}$,*
5. *$-(av)=(-a)v=a(-v)$, in particular, $-v=(-1)v$.*
6. *$-(u+v)=-u-v$,*
7. *$a(u-v)=au-av$,*

The proofs of these basic properties are easy to deduce (see Exercise E.10.8).

10.2. Subspaces in spaces

Consider a few subsets in $V=\mathbb{R}^3$: the cube $\mathcal{C}$, the ball $\mathcal{B}$, the plain $\mathcal{P}$, the line ℓ, the subset $\{\vec{0}\}$, and the entire space $\mathbb{R}^3$ as a subset of itself (see Figure 10.1). Let us check which of these subsets also are spaces according to operations already defined on V? $\mathcal{B}$ is not a space because it does not contain the zero vector $\vec{0}$. The cube $\mathcal{C}$ does contain $\vec{0}$, but it still is not a space because the sums and scalar multiples of its vectors may not belong to $\mathcal{C}$. The plain $\mathcal{P}$ and the line ℓ actually are spaces, and they seem to be "the same" as the spaces $\mathbb{R}^2$ and $\mathbb{R}$. Finally, $\{\vec{0}\}$ and the entire $\mathbb{R}^3$ also are spaces. We see that some of the subsets of V also are spaces, and we even have spaces nested into each other:

$$\{\vec{0}\}\subseteq\mathcal{P}\subseteq\mathbb{R}^3=V,\quad \{\vec{0}\}\subseteq\ell\subseteq\mathbb{R}^3=V,$$

whereas other subsets such as $\mathcal{C},\mathcal{B}$ do not "inherit" the space structure from V.

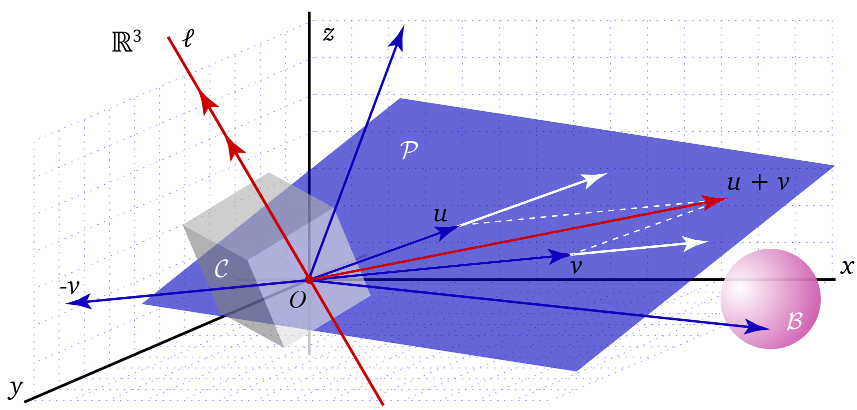


FIGURE 10.1. Subspaces and non-subspaces in $\mathbb{R}^3$

Definition 10.11. Let V be a vector space over a field F. The subset $U\subseteq V$ is a *subspace* of V, if it is a vector space with operations of addition and multiplication by scalar defined on V.

The following equivalent definition makes it easy to detect the subspaces:

Definition 10.12. The non-empty subset U of a vector space V over a field F is a *subspace* of V if and only if:

1. for any $u, v \in U$ we have $u + v \in U$, and
2. for any $v \in U$ and $a \in F$ we have $av \in U$.

It is clear that, if U is a subspace by the first definition, then both points of the second definition are satisfied (they are included in space definition). So the advantage of second definition is that instead of testing all the points of Definition 10.1, we can check two conditions *only*.

Proof of equivalence of Definition 10.11 and Definition 10.12. Assume the subset $U \subseteq V$ satisfies both points of Definition 10.12. This also means that vector sums and scalar multiples are defined in U.

$\vec{0}$ is in U because $\vec{0} = 0u \in U$ for any $u \in U$.

For any $u \in U$ there is a $-u$ in U because $-u = (-1)u \in U$.

All the remaining points of Definition 10.1 hold for U because they hold for all vectors of V in general. □

The simplest examples of subspace in any space V are the trivial zero subspace $U = \{\vec{0}\}$ and the subspace $U = V$ coinciding with V. These subspaces are called *improper* subspaces to distinguish them from all other subspaces, which are called *proper* subspaces.

Example 10.13. Some subspaces in real spaces are displayed in Figure 10.1. Points of Definition 10.12 are very easy to check. The only subspaces of $\mathbb{R}^3$ are the improper subspaces $\{\vec{0}\}$ and $\mathbb{R}^3$, plus the proper subspaces: the lines and planes passing via O.

Example 10.14. For any $n \in \mathbb{N}$ the polynomial space $\mathcal{P}_n(F)$ is a subspace of $F[x]$. For, if $\deg(f(x)), \deg(g(x)) \le n$, $a \in F$, $a \ne 0$, then $\deg(f(x) + g(x)) \le n$ and $\deg(a \cdot f(x)) \le n$. Also, for any $m \le n$ the space $\mathcal{P}_m(F)$ is a subspace of $\mathcal{P}_n(F)$.

Example 10.15. $\mathbb{R}^2$ is *not* a subspace in $\mathbb{R}^3$. And, in general, F^m is *not* a subspace in F^n for any $m < n$. This may sound unexpectedly, but actually $\mathbb{R}^2$ is not even a *subset* in $\mathbb{R}^3$ ($\mathbb{R}^3$ consists of triples, not couples). But if we consider the subset $U = \{(x_1, x_2, 0) \,|\, x_1, x_2 \in \mathbb{R}\} \subseteq \mathbb{R}^3$, then U is a subspace of V. Similar examples can be built for F^n.

Example 10.16. Consider any homogeneous system of linear equations $AX = O$ on, say, n variables. We already knew that the set of its solutions is a space, and now we can see that it is a *subspace* of F^n.

In particular, when F^n is just $\mathbb{R}^3$, we see that the solutions of $AX = O$ have to be either zero, or form a line, or a plane or the entire $\mathbb{R}^3$. This is not new information for us if the number of equations is just 2. But the news is that this fact does not change if we add any number of new equations.

Let U and W be any subspaces of the vector space V. It is easy to verify by Definition 10.12 that their *intersection* $U \cap W$ also is a subspace of V. This can easily be generalized to intersection $\bigcap_{i=1}^{k} U_i = U_1 \cap \cdots \cap U_k$ for any subspaces $U_1, \ldots, U_k$ of V.

We may expect to see the dual definition of *union* of subspaces U and W. However, as the example of lines Ox and Oy in $\mathbb{R}^2$ shows, a union of subspaces may *not* be a subspace. Yet another construction comes to let us to construct larger subspaces from the given subspaces in V:

Definition 10.17. Let U and W be any subspaces of the vector space V. The set

$$\{u + w \mid u \in U,\ w \in W\}$$

is called the *sum* of subspaces U and W, and is denoted by $U + W$.

It is easy to apply Definition 10.12 to check that $U + W$ is a subspace of V. We will be particularly interested in the cases when $V = U + W$. Definition of the sum of spaces for any collection $U_1, \dots, U_k$ of subspaces in V is similar:

$$U_1 + \cdots + U_k = \{u_1 + \cdots + u_k \mid u_i \in U_i,\ i = 1, \dots, k\}.$$

This sum also is denoted by $\sum_{i=1}^{k} U_i$.

Example 10.18. The sum of plane xOy and line Oz in $\mathbb{R}^3$ is equal to $\mathbb{R}^3$. In general, the sum of any plane $\mathcal{P}$ (passing via O) and any line ℓ (passing via O and not lying in $\mathcal{P}$) is $\mathbb{R}^3$. Also, the sum of any three non-coplanar lines ℓ_1, ℓ_2, ℓ_3 (passing via O) is $\mathbb{R}^3$.

Example 10.19. Consider the subspace $\mathcal{P}_3$ of the real polynomial space $\mathcal{P}_5$, and take $U = \{ax^2 + bx^4 + cx^5 \mid a, b, c \in \mathbb{R}\}$. It is easy to verify that U is a subspace in $\mathcal{P}_5$, and $\mathcal{P}_3 + U = \mathcal{P}_5$.

Example 10.20. In $M_{2,2}(F)$ take

$$E_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad E_{1,2} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$E_{2,1} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad E_{1,2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

and define four subsets $U_1 = \{aE_{1,1} \mid a \in F\}$, $U_2 = \{aE_{1,2} \mid a \in F\}$, $U_3 = \{aE_{2,1} \mid a \in F\}$, $U_4 = \{aE_{2,2} \mid a \in F\}$. It is easy to check that each of these subsets is a subspace and

$$U_1 + U_2 + U_3 + U_4 = M_{2,2}(F).$$

It is clear that adding brackets to the sum does not change the result. For instance, $U_1 + U_2 + U_3 = (U_1 + U_2) + U_3 = U_1 + (U_2 + U_3)$. In other words, working with sums of subspaces we can write (or omit) the brackets wherever needed.

In Section 16.2 we will return to study of sums and intersections of subspaces after we build the auxiliary tools needed.

Exercises

E.10.1. Consider the set $V = \{(x, y) \mid x, y \in \mathbb{R}\}$ with operations $(x, y) + (x', y') = (x + x', 0)$ and $c(x, y) = (cx, 0)$ for any scalar $c \in \mathbb{R}$. Is V a vector space with these operations?

E.10.2. V is a set of vectors from $\mathbb{R}^3$, in which addition and multiplication by scalar are defined in the same way as in $\mathbb{R}^3$. Find out if or not V is a vector space, when **(1)** $V = \{(x - y,\ y - z,\ z - x) \mid x,\ y,\ z \in \mathbb{R}\}$. **(2)** $V = (x,\ x^2,\ x^3) \mid x \in \mathbb{R}\}$. **(3)** $V = \big\{\big(x\sin(\frac{\pi}{2}),\ x\sin^2(\frac{\pi}{4}),\ x\sin^3(\frac{\pi}{6})\big) \mid x \in \mathbb{R}\big\}$.

E.10.3. V is a set of real matrices, in which addition and multiplication by scalar are defined in the same way as in $M_{2,2}(\mathbb{R})$. Find out if or not V is a vector space, when **(1)** $V = \left\{\left[\begin{smallmatrix} x & x+y \\ 0 & y \end{smallmatrix}\right] \mid x, y \in \mathbb{R}\right\}$. **(2)** $V = \left\{\left[\begin{smallmatrix} 11x & 12x \\ 13x & 14x \end{smallmatrix}\right] \mid x \in \mathbb{R}\right\}$. **(3)** $V = \left\{\left[\begin{smallmatrix} x & x-1 \\ 0 & x \end{smallmatrix}\right] \mid x \in \mathbb{R}\right\}$.

E.10.4. Let $V = \{\alpha + \beta x + \gamma x^3 \mid \alpha, \beta, \gamma \in \mathbb{Q}\} \subseteq \mathbb{Q}[x]$ be a set of polynomials. **(1)** Is V a vector space with respect to addition of polynomials and multiplication of polynomials by scalars from the field $\mathbb{Q}$? **(2)** Is the *same* set V a vector space over the field $\mathbb{R}$?

E.10.5. Consider the set $V = \mathbb{C}$ with operations of complex numbers addition, and multiplication of complex numbers by *real* numbers: $(a+bi)+(a'+b'i) = (a+a')+(b+b')i$, $c(a+bi) = (ca)+(cb)i$ for any $c \in \mathbb{R}$. Is V a vector space over the field $F = \mathbb{R}$?

E.10.6. Determine weather U is a subspace in the space $\mathbb{R}^3$, if **(1)** $U = \{(x, y, z) \mid x, y, z > 0\}$. **(2)** $U = \{(x, y, z) \mid x + y = z\}$. **(3)** $U = \{(x, y, z) \mid x^2 = z\}$.

E.10.7. Find out if U is a subspace in the real polynomial space $\mathcal{P}_3$, when **(1)** $U = \{\alpha(5-2x^2)+\beta(3+x) \mid \alpha, \beta \in \mathbb{R}\}$. **(2)** $U = \{f(x) \mid \deg(f(x)) \geq 3\}$. **(3)** $U = \{f(x) \mid \deg(f(x)) \geq 3\} \cup \{f(x) = 0\}$.

E.10.8. From axiom 1 of Definition 10.1 it is clear that $\vec{0} + v = v$ (compare with the equality $v + \vec{0} = v$ in axiom 3), and $-v + v = \vec{0}$ (compare with $v + (-v) = \vec{0}$ in axiom 4). Show that these two equalities also follow from axioms 2–4 of Definition 10.1 *without* using axiom 1.

E.10.9. Prove all points of Proposition 10.10. Optional, more complicated task: do it *without* using the commutativity axiom 1 of Definition 10.1. *Hint*: you can use Exercise E.10.8.

E.10.10. Show that axiom 1 in Definition 10.1 is *redundant*, i.e., it can be deduced from the remaining seven axioms 2–8. *Hint*: you can use Exercise E.10.8.

E.10.11. Prove that axiom 8 in Definition 10.1 is *necessary*, i.e., removing the last axiom we may get a system which is *not* an abstract vector space in the sense of Definition 10.1.

CHAPTER 11

Linear dependence, spanning sets and bases

11.1. Linear dependence and independence of vectors

For any vectors $v_1, \dots, v_n$ in a vector space V over F, and for any scalars $a_1, \dots, a_n \in F$ call the sum

$$a_1 v_1 + \cdots + a_n v_n \tag{11.1}$$

the *linear combinations* of vectors $v_1, \dots, v_n$ by coefficients $a_1, \dots, a_n$. Notice that our notation allows repeated vectors, i.e., some of v_i and v_j may be equal vectors, but we distinguish them by their indices $i \neq j$.

Call the linear combination (11.1) a *non-trivial* combination, if at least one of its coefficients a_i is non-zero. Otherwise the combination is *trivial*, i.e., all the coefficients are zero, and then the combination is equal to zero vector.

Example 11.1. Here are examples of linear combinations in different spaces:

a. in real space $\mathbb{R}^3$:

$$2\begin{bmatrix}1\\ \frac{1}{2}\\ 2\end{bmatrix} - \begin{bmatrix}0\\3\\0\end{bmatrix} + \begin{bmatrix}2\\1\\0\end{bmatrix} + 3\begin{bmatrix}1\\-1\\3\end{bmatrix} = \begin{bmatrix}7\\-4\\13\end{bmatrix},$$

b. in modular space $\mathbb{Z}_7^2$ over the field $\mathbb{Z}_7$ we have the equality:

$$3\begin{bmatrix}1\\2\end{bmatrix} + \begin{bmatrix}2\\0\end{bmatrix} + 2\begin{bmatrix}1\\3\end{bmatrix} = \begin{bmatrix}0\\5\end{bmatrix},$$

c. in matrix space $M_{3,3}(\mathbb{R})$:

$$2\begin{bmatrix}1&2&0\\0&2&3\\1&0&1\end{bmatrix} + 4\begin{bmatrix}0&\frac{1}{2}&2\\1&0&2\\1&1&2\end{bmatrix} + 0\begin{bmatrix}2&3&\frac{1}{7}\\4&0&0\\1&\pi&2\end{bmatrix} = \begin{bmatrix}2&6&8\\4&4&14\\6&4&10\end{bmatrix},$$

d. in polynomial space $\mathbb{Z}_5[x]$:

$$3(1+x^3) + 2(x+4x^2+2x^3) = 3 + 2x + 3x^2 + 2x^3.$$

Linear combinations are abundant in of mathematics. Let us recall two situations when you used them, without mentioning the word “linear combination” though.

First consider two non-collinear vectors v_1, v_2 in a plane $\mathcal{P}$ shown in Figure 11.1. It is clear that $\mathcal{P}$ consists of all vectors $u = a_1 v_1 + a_2 v_2$, so the plane $\mathcal{P}$ is nothing but the set of all linear combinations of v_1, v_2. Similarly, the line ℓ_1 is the set of all linear combinations $a_1 v_1$ of v_1. But if we take any vector w *outside* the plane, then w cannot be presented as a linear combination of vectors v_1, v_2. So to say, the vector u is “dependent” on v_1, v_2, whereas w is not.

Next consider any system of linear equations over any field F:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{11.2}$$

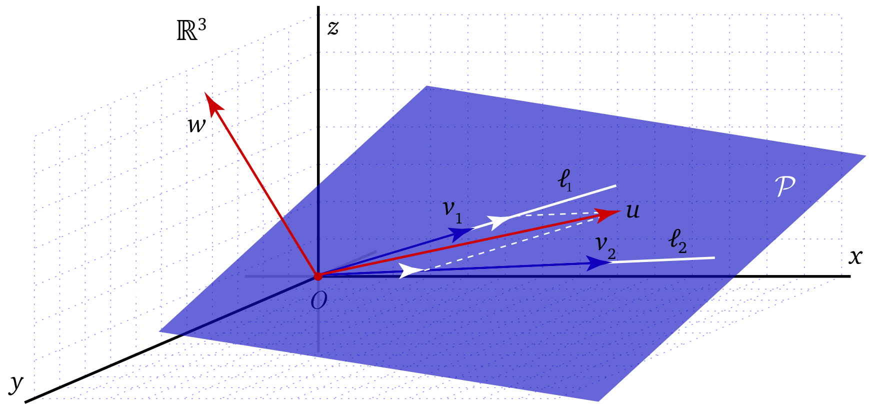


FIGURE 11.1. Linearly dependent and independent vectors in $\mathbb{R}^3$.

So far we only worked with its rows. What if we take a look at the same system *"vertically"*, and analyse it by columns? Namely, take the column vectors

$$\vec{v}_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \dots, \ \vec{v}_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}, \quad \vec{u} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}, \tag{11.3}$$

and interpret the system (11.2) and its consistency in a new way: $(x'_1, \dots, x'_n)$ is a solution for this system if and only if the vector equality

$$x'_1\vec{v}_1 + \cdots + x'_n\vec{v}_n = \vec{u}.$$

holds for the coefficients $x'_1, \dots, x'_n \in F$. That is, the system (11.2) is consistent if and only if $\vec{u}$ is a linear combination of vectors $\vec{v}_1, \dots, \vec{v}_n$. So to say, the vector u is "dependent" on $\vec{v}_1, \dots, \vec{v}_n$, whenever (11.2) has a solution.

As these two illustrations show, the fact if the vectors u, w belong to the plane $\mathcal{P}$, and the fact if the system (11.2) is consistent, although they look differently, both are two implementations of the *same* property of linear combinations. Now it is time to give two equivalent definitions of linear dependence:

Definition 11.2. Let V be a vector space over a field F. The set $S = \{v_1, \dots, v_n\}$ of vectors of V is *linearly dependent*, if one of its vectors is a linear combination of others, i.e., for a $v_k \in S$ there are scalars $a_i \in F$ such that:

$$\boldsymbol{v_k = a_1 v_1 + \cdots + a_{k-1} v_{k-1} \ + \ a_{k+1} v_{k+1} + \cdots + a_n v_n}. \tag{11.4}$$

Definition 11.3. Let V be a vector space over a field F. The set $S = \{v_1, \dots, v_n\}$ of vectors of V is *linearly dependent*, if there are some scalars $b_1, \dots, b_n \in F$, not *all* equal to zero (i.e., $b_k \neq 0$ for some index k) such that:

$$\boldsymbol{b_1 v_1 + \cdots + b_n v_n = \vec{0}}. \tag{11.5}$$

(In other words, a non-trivial linear combination of the vectors $v_1, \dots, v_n$ is zero.)

The above two definitions of linear dependence are equivalent:

Proof of equivalence of Definition 11.2 and Definition 11.3. Assume the set $S = \{v_1, \dots, v_n\}$ is linearly dependent by Definition 11.2, i.e., (11.4) holds for it. Then the linear combination with a non-zero $b_k = -1$ mentioned in Definition 11.3 is:

$$a_1v_1 + \cdots + a_{k-1}v_{k-1} \boldsymbol{-1v_k} + a_{k+1}v_{k+1} + \cdots + a_nv_n = \vec{0}.$$

Next, assume S is linearly dependent by Definition 11.3:

$$b_1v_1 + \cdots + \boldsymbol{b_kv_k} + \cdots + b_nv_n = \vec{0},$$

and $b_k \neq 0$ for some index k. Then:

$$\boldsymbol{v_k} = -\tfrac{b_1}{b_k}v_1 - \cdots - \tfrac{b_{k-1}}{b_k}v_{k-1} - \tfrac{b_{k+1}}{b_k}v_{k+1} - \cdots - \tfrac{b_n}{a_k}v_n,$$

i.e., S is linearly dependent by Definition 11.2 for coefficients $a_i = \frac{b_i}{b_k}$ (we can divide by b_k, since it is a non-zero element in the field F). ☐

A set of vectors S is called *linearly independent*, if it is not linearly dependent.

So far we considered linear dependence for *finite* sets. Call *any* (finite or infinite) set $S = \{v_i \mid i \in \mathcal{I}\}$ of vectors in V linearly dependent, if it has a *finite* linearly dependent subset. Call S linearly independent, if it fails to have such a finite subset (see Example 11.8 below).

Example 11.4. Any couple v_1, v_2 of non-zero vectors is dependent if and only if the vectors are *collinear*. For, Definition 11.2 in this case means that either $v_2 = a_1v_1$, or $v_1 = a_2v_2$, i. e., it just means collinearity of v_1 and v_2.

Example 11.5. Any tipple $v_1, v_2, v_3 \in \mathbb{R}^3$ of vectors is dependent if and only if the vectors are coplanar. For, the equality $v_i = a_1v_j + a_2v_k$ implies coplanarity, and from coplanarity it follows that one of the vectors is the linear combination of the others.

Example 11.6. In the space F^n consider the vectors:

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

They are linearly independent because for any choice of scalars $a_1, a_2, \ldots, a_n \in F$ the equality

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n = \begin{bmatrix}a_1\\a_2\\\vdots\\a_n\end{bmatrix} = \vec{0} = \begin{bmatrix}0\\0\\\vdots\\0\end{bmatrix}$$

holds if and only if $a_1, a_2, \ldots, a_n = 0$.

It is easy to figure out that in this example in column vectors instead of 1 we could take any non-zero scalars $c_1, \ldots, c_n \in F$.

Example 11.7. Consider the set $S = \{E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}\}$ of matrices in $M_{2,2}(F)$ from Example 10.20:

$$E_{1,1} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix},\quad E_{1,2} = \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix},$$

$$E_{2,1} = \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix},\quad E_{2,2} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}.$$

The set S is linearly independent because for any $a_1, a_2, a_3, a_4 \in F$ we have

$$a_1E_{1,1} + a_2E_{1,2} + a_3E_{2,1} + a_4E_{2,2} = \begin{bmatrix}a_1 & a_2\\a_3 & a_4\end{bmatrix}$$

which is zero if and only if $a_1, a_2, a_3, a_4 = 0$.

More generally, denote by

$$E_{i,j} = \begin{bmatrix}0 & \cdots & 0 & \cdots & 0\\ \dots & \dots & \dots & \dots & \dots\\ 0 & \cdots & \mathbf{1} & \cdots & 0\\ \dots & \dots & \dots & \dots & \dots\\ 0 & \cdots & 0 & \cdots & 0\end{bmatrix}$$

the matrix in $M_{m,n}(F)$ defined as follows: the (i,j)-th term of $E_{i,j}$ is 1, and all other terms of $E_{i,j}$ are zero. Then the set of matrices

$$E = \{E_{i,j} \mid i = 1, \ldots, m;\ j = 1, \ldots, n\}$$

is linearly independent.

Example 11.8. Consider the polynomials

$$e_0(x) = 1 = x^0,$$
$$e_1(x) = x = x^1,$$
$$e_2(x) = x^2,$$
$$\cdots\cdots\cdots$$
$$e_n(x) = x^n.$$

Let us check that they are linearly independent. For arbitrary choice of the coefficients

$a_0, a_1, \ldots, a_n \in F$ denote

$$g(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$= a_0 e_0(x) + a_1 e_1(x) + \cdots + a_n e_n(x).$$

Now we have to show that $g(x) = \vec{0}$ holds if and only if all of its coefficients are zero.

Notice that under $g(x) = \vec{0}$ we mean point-wise *equality* of $g(x)$ to zero for *any* $x \in \mathbb{R}$ (*not* finding some solutions for the *equation* $g(x) = 0$). A polynomial of non-zero degree n may not have more then n roots, so if $g(x)$ is zero for all $x \in \mathbb{R}$, then it is the constant zero function.

We can extend this concept to an *infinite* set of linearly independent polynomials:

$$e_0(x) = 1,\ e_1(x) = x,\ \ldots,\ e_n(x) = x^n,\ \ldots$$

The proof of linear independence is an easy adaptation of the above idea.

So far this is our first example of an *infinite* linearly independent set.

Here are some of the basic properties of linear dependence and independence:

Proposition 11.9. *Let $S = \{v_i \mid i \in \mathcal{I}\}$ be any set of vectors of the space V. Then:*

1. *if S contains a zero vector, then it is linearly dependent;*
2. *if S contains two equal vectors, then it is linearly dependent;*
3. *if one of the vectors of S is a linear combination of some other vectors of S, then S is linearly dependent;*
4. *if S contains a linearly dependent subset, then it is linearly dependent;*
5. *if S is linearly independent, then any of its subsets also is linearly independent.*

***Proof*.** Let us prove the proposition for finite sets $S = \{v_1, \ldots, v_n\}$ only, as the proofs for infinite cases can be easily reduced to the respective finite cases.

1. If one of the vectors, say $v_k \in S$ is zero, then S is linearly dependent by Definition 11.3:

$$0v_1 + \cdots + 0v_{k-1} + 1v_k + 0v_{k+1} + \cdots + 0v_n = \vec{0}.$$

2. If $v_k = v_m$ for some $k \neq m$, then we can take a combination, where the coefficient of v_k is 1, the coefficient of v_m is -1, and all other coefficients are zero. By the way, by definition a *set* may never contain equal elements, but as we agreed in the beginning of this section, we may consider indexed sets of vectors: v_k and v_m may be equal as vectors, but we include them in S distinguishing them by indices $k \neq m$.

3. If $v_k = b_1 v_{m_1} + \cdots + b_s v_{m_s}$, we can take the combination, $-v_k + b_1 v_{m_1} + \cdots + b_s v_{m_s} = 0$, and add all the remaining vectors of S with 0 coefficients.

4. This follows from the 3'rd point.

5. This follows from the 4'th point. □

11.2. Spans and space bases

Let $S = \{v_1, \ldots, v_n\}$ be a set of vectors in a vector space V over F. The *span* of this set is defined to be the set of all linear combinations of these vectors by coefficients from F:

$$\mathbf{span}(S) = \{a_1 v_1 + \cdots + a_n v_n \mid a_1, \ldots, a_n \in F\}.$$

By Definition 10.12 it is easy to check that span(S) is a *subspace* of V.

If span$(S) = U$, then S is called a *spanning set* of the subspace U. In particular, if span$(S) = V$ holds, then S is a *spanning set* of the entire space V.

Example 11.10. Let V is the space $\mathbb{R}^3$, and $v_1 = (1,0,0)$, $v_2 = (0,1,0)$, $v_3 = (0,0,1)$. Then $\operatorname{span}(v_1, v_2, v_3) = V$.

Notice that to simplify the notation we wrote not $\operatorname{span}(\{v_1, v_2, v_3\})$ but $\operatorname{span}(v_1, v_2, v_3)$. Moreover, if $u_1 = (a,0,0)$, $u_2 = (0,b,0)$, $u_3 = (0,0,c)$ are any non-zero vectors, then $\operatorname{span}(u_1, u_2, u_3) = V$.

We will soon see that *arbitrary* three linearly independent vectors u_1, u_2, u_3 form a spanning set in $\mathbb{R}^3$.

Example 11.11. In $V = \mathbb{R}^3$ the span of any non-trivial vector v is the line passing via O with direction vector v. And the span of any two non-collinear vectors u, v is the plane passing via O with direction vectors u, v.

Example 11.12. Turning back to the matrices $E_{i,j}$ in Example 11.7 it is easy to check that

$$\operatorname{span}\big(E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}\big) = M_{2,2}(F),$$

and more generally:

$$\operatorname{span}\big(E_{i,j} \mid i = 1, \dots, m;\ j = 1, \dots, n\big) = M_{m,n}(F).$$

The notion of span can be generalized for *infinite* sets also. If S is an infinite subset of V, then $\operatorname{span}(S)$ is the set of all linear combinations of all *finite* subsets of S. In this case also $\operatorname{span}(S)$ is a subspace of V.

Using polynomials we can construct both finite and infinite spanning sets:

Example 11.13. The polynomial space $\mathcal{P}_n(F)$ evidently has a finite spanning set:

$$\operatorname{span}(1, x, \dots, x^n) = \mathcal{P}_n(F),$$

as each polynomial is a linear combination of powers of x.

Example 11.14. The polynomial space $F[X]$ has no finite spanning set. See Exercise E.11.8 and its solution below.

But $F[X]$ has an infinite spanning set:

$$\operatorname{span}(1, x, \dots, x^n, \dots) = F[x].$$

The *key advantage* of finding a spanning set S for a subspace $U = \operatorname{span}(S)$ is that knowing S we already know U, for, we can by linear combinations of vectors from S *construct* all the other vectors of U. The drawback, however, is that this construction *is not unique*: if we for, say, $S = \{v_1, \dots, v_n\}$ have two combinations

$$a_1 v_1 + \cdots + a_n v_n \quad \text{and} \quad b_1 v_1 + \cdots + b_n v_n,$$

we are not yet aware, if these are the *same* vector u or not.

Example 11.15. In $V = \mathbb{R}^2$ fix the vectors $v_1 = (-2,1)$, $v_2 = (4,3)$, $v_3 = (3,1)$ (see Figure 11.2). $u = (8,6)$ can in different ways be presented as their linear combination. Say:

$$u = 2v_1 + 0v_2 + 4v_3,$$
$$u = 0v_1 + 2v_2 + 0v_3,$$
$$u = \tfrac{110}{273} v_1 + \tfrac{436}{273} v_2 + \tfrac{220}{273} v_3.$$

The first two presentations are geometrically clear from Figure 11.2, and the third "unexpected" presentation can be verified directly.

If you remember how we solved systems of linear equations with a free variable, you may figure out how we obtained those presentations. Can you find infinitely many presentations of u as linear combinations of v_1, v_2, v_3?

In this example although $S = \{v_1, v_2, v_3\}$ is a spanning set for $\mathbb{R}^2$, and we are able to present any $u \in V$ as linear combinations of v_1, v_2, v_3, the process is not a satisfying one, as we still have the burden to do computations to discover that $2v_1 + 0v_2 + 4v_3$ and $\frac{110}{273} v_1 + \frac{436}{273} v_2 + \frac{220}{273} v_3$ actually present the *same* vector u (despite, they have very differently looking coefficients).

Wouldn't it be good to have such an "advanced" spanning set that each vector has a *unique* linear combination by its vectors? Then, having two linear combinations, we can immediately detect, if or not they present the same vector by simply comparing the coefficients. We arrive to a very important:

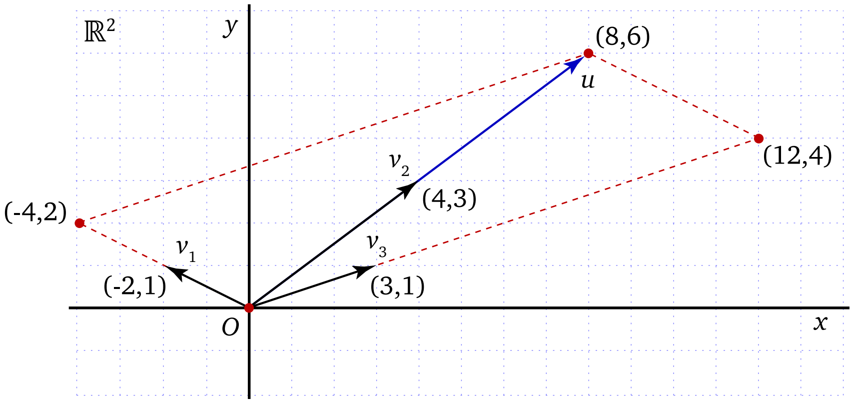


FIGURE 11.2. Two linear presentations of u by spanning vectors v_1, v_2, v_3.

Definition 11.16. A set E of vectors of the space V is a *basis* of V, if it is a linearly independent spanning set for V.

Example 11.17. The set

$$\begin{aligned} e_1 &= (1, 0, \dots, 0) \\ e_2 &= (0, 1, \dots, 0) \\ &\dots\dots\dots\dots\dots\dots \\ e_n &= (0, 0, \dots, 1) \end{aligned}$$

is a basis for F^n. This basis is called *standard basis* of F^n.

Example 11.18. The matrix set

$$E = \{E_{i,j} \,|\, i = 1, \dots, m;\; j = 1, \dots, n\}$$

is a basis for the matrix space $V = M_{m,n}(F)$. The linear independence is shown in Example 11.7, and E is a spanning set by Example 11.12.

Example 11.19. The polynomial vectors

$$e_0(x) = 1,\; e_1(x) = x,\; \dots, e_n(x) = x^n$$

form a basis for the polynomial space $V = \mathcal{P}_n(F)$. The linear independence is given in Example 11.8, and this set spans V by Example 11.13. Denote this basis by E. It is also often called "the $\{1, x, x^2, \dots\}$ basis".

We can write:

$$\begin{aligned} f(x) &= 1 + 2x + 7x^2 + 8x^3 \\ &= 1e_0(x) + 2e_1(x) + 7e_2(x) + 8e_3(x) \end{aligned}$$

(or, just briefly)

$$= 1e_0 + 2e_1 + 7e_2 + 8e_3.$$

Notice how we wrote $f(x)$ in ascending order of terms by Agreement 10.9.

Example 11.20. Furthermore, we get an example of an *infinite* basis E. If $V = F[x]$, then

$$e_0(x) = 1,\; e_1(x) = x,\; \dots, e_n(x) = x^n,\; \dots$$

is a basis for V (see Example 11.8 and Example 11.14).

Other examples of spaces with infinite bases are the functional spaces $\mathcal{F}, \mathcal{F}^1, \mathcal{F}^2, \dots$ in Example 10.7.

Due to special importance of bases, we denote their elements not by characters generally used for vectors (such as $u, v, w, \dots$), but we reserve special characters $e, g, h\dots$ for them. Say, $E = \{e_1, \dots, e_n\}$, $E = \{e_i \,|\, i \in \mathcal{I}\}$, $G = \{g_1, \dots, g_n\}$, etc...

Here is the property we we alluded earlier:

Theorem 11.21. *Assume the space V has the basis $E = \{e_i \,|\, i \in \mathcal{I}\}$ and v is any vector in V. Then the presentation of v as a linear combination of vectors of E is unique.*

***Proof*.** Assume some vector $v \in V$ has two presentations:

$$v = a_1 e_1 + \cdots + a_m e_m, \qquad v = b_1 e_1 + \cdots + b_m e_m, \tag{11.6}$$

for some $e_1, \dots, e_m \in E$. In both presentations we used the *same* basis vectors, although they *could* actually use different vectors from E. This, however, is not an obstacle, since in any of presentations (11.6) we can add the "missing" vectors by zero coefficients.

Subtracting the second presentation from the first we get:

$$\vec{0} = v - v = (a_1 - b_1)e_1 + \cdots + (a_m - b_m)e_m.$$

Since E is linearly independent, $a_i - b_i = 0$, and $a_i = b_i$ for all $i = 1, \dots, m$. □

The flowing simple lemma, which will be often used below, shows that removing a linearly dependent vector from a spanning set we still get a spanning set.

Lemma 11.22. *If S spans the space V, and if a vector $u \in S$ is a linear combinations of some other vectors of S, then the set $S \backslash \{u\}$ also spans V.*

***Proof*.** Assume $u = a_1u_1 + \cdots + a_ku_k$ is the linear combination mentioned in lemma's hypothesis for some $u_1, \dots, u_k \in S$. Since S spans V, any vector $v \in V$ has a presentation as a linear combination of some vectors from S. If u is one of the vectors in that linear combination, just replace it by $a_1u_1 + \cdots + a_ku_k$. We get a presentation of v as a linear combination of vectors from $S \backslash \{u\}$. □

Theorem 11.23. *Any two bases of a vector space V have the same cardinality (in particular, they consist of the same number of vectors in the case if bases are finite).*

The proof will be given for finite bases only, since the infinite case requires transfinite induction *not* included in our course. In the sequel we will use the finite case only.

***Proof of Theorem 11.23*.** Let us start by a preliminary step to use it later. Assume a set $\{v_1, \dots, v_n\}$ of vectors is linearly dependent. By Definition 11.2 one of its vectors v_k is a linear combination of the others:

$$v_k = b_1v_1 + \cdots + b_{k-1}v_{k-1} \;+\; b_{k+1}v_{k+1} + \cdots + b_nv_n. \tag{11.7}$$

This presentation may be possible for some of the indices $1, \dots, n$, and we can choose k to be the *largest* index for which (11.7) is possible. Then the coefficients $b_{k+1}, \dots, b_n$ all are zero because, if say $b_{k+1} \neq 0$, we can move $b_{k+1}v_{k+1}$ to the left hand side of (11.7), then move v_k to the right hand side, and then divide both sides of the obtained equality by $-b_{k+1}$. We get a presentation of v_{k+1} by the remaining vectors which contradicts to *maximality* of k.

We obtained a modification of Definition 11.2: the vectors $v_1, \dots, v_n$ are linearly dependent if and only if one of them is a linear combination of *previous vectors*, i.e., there is a $k \leq n$ such that:

$$v_k = b_1v_1 + \cdots + b_{k-1}v_{k-1}.$$

Now take any two bases $E = \{e_1, \dots, e_n\}$ and $G = \{g_1, \dots, g_m\}$ of the space V, and assume $n < m$. Adding g_1 from the left to vectors of E we get the vectors

$$g_1, e_1, \dots, e_n,$$

which are linearly dependent, since $g_1 \in V = \text{span}(E)$. By the above modification of Definition 11.2 one of these vectors is a linear combination of the *previous* vectors. Since it cannot be g_1 (no vector proceeds it), the dependent vector is among $e_1, \dots, e_n$. For simplicity of notation assume it is the last vector e_n. Removing it we still have a spanning set

$$g_1, e_1, \dots, e_{n-1}$$

by Lemma 11.22. Adding g_2 from the left to them we get linearly dependent vectors:

$$g_2, g_1, e_1, \ldots, e_{n-1}.$$

Again, one of these vectors is a linear combinations of the *previous* vectors, and it is not g_2 or g_1 because G is a basis. For simplicity assume it is the last vector e_{n-1}. Removing it we get the spanning set

$$g_2, g_1, e_1, \ldots, e_{n-2}.$$

Repeating these steps not more than n times we get the spanning set

$$g_n, \ldots, g_2, g_1.$$

Thus, g_m (like any other vector of V) is a linear combination of the above spanning set. So G is linearly dependent. Contradiction. □

Since all bases of a space V have the same cardinality, we can define:

Definition 11.24. The *dimension* $\dim(V) = |E|$ of the vector space V is the cardinality of any basis E of V (the number of elements in E for the finite case).

If a basis E of V has n elements, we write this as $\dim(V) = n$, and call V a *finite-dimensional* space. If the basis is infinite, we write $\dim(V) = \infty$, and call V an *infinite-dimensional* space.

Example 11.25. Based on the examples above, we have:

1. $\dim(\mathbb{R}^2) = 2$, $\dim(\mathbb{R}^3) = 3$, $\dim(\mathbb{R}^n) = n$;
2. and, in general, $\dim(F^n) = n$;
3. $\dim(F[x]) = \infty$;
4. $\dim(\mathcal{P}_n(F)) = n + 1$;
5. $\dim(\mathcal{F}) = \infty$;
6. $\dim\big(M_{m,n}(F)\big) = m \cdot n$.

Since below we are going to deal with finite-dimensional spaces mainly, let us make an important agreement:

Agreement 11.26. In the sequel under a vector space we will usually understand a *finite-dimensional* space. The infinite-dimensional case, if it is needed, will be specially stressed. So we will write "Consider a space V with the basis E" assuming a finite basis $E = \{e_1, \ldots, e_n\}$. We will not concern the infinite-dimensional case unless it is directly required by the context.

According to the above agreement we consider the following properties for finite-dimensional spaces only (although their analogs are true for any dimension):

Proposition 11.27. *In statements below let S be a set of vectors in a non-trivial space V.*

1. *If S is a linearly independent, then one can get a basis of V by adding some new vectors to S. In particular, any non-trivial space has a basis.*
2. *If S is a spanning set, then one can get a basis of V by excluding some vectors from S.*
3. *If $\dim(V) = n$, and $m > n$, then no set of m vectors is linearly independent.*
4. *If $\dim(V) = n$, and $m < n$, then no set of m vectors can span V.*
5. *If $\dim(V) = n$, then any set of n linearly independent vectors forms a basis of V.*
6. *If $\dim(V) = n$, then any spanning set of n vectors forms a basis of V.*
7. *If U is a subspace of V, then $\dim(U) \le \dim(V)$; the equality holds if and only if $U = V$.*

***Proof*.** **1.** If the independent set S also is a spanning set, it already is a bases, and we are done. If not, there is a vector $u \in V$ which is *not* a linear combination of S. Then $S \cup \{u\}$ is independent (order S in any way, consider u as the *last* vector of $S \cup \{u\}$, and apply the criterion about the *previous vectors* from the proof of Theorem 11.23). If this new independent set is a spanning set, we are done. If not, add one more vector. Since this process cannot run infinitely long, we at some step get a basis.

2. If the spanning set S also is linearly independent, it already is a bases. If not, one of its vectors u is the linear combination of the others. Removing it from S we still get a spanning set $S \backslash \{u\}$ by Lemma 11.22. If this new spanning set is independent, we are done. If not, remove a vector again. Continuing the process we arrive to a basis.

3. If $m > n$, and a set of m vectors is linearly independent, then by point 1 we could obtain a basis from it by adding new vectors to it. But by Theorem 11.23 a basis of V cannot consist of more than n vectors.

4. This can be proved in analogy with point 3, using point 2 and Theorem 11.23.

5. If a set of n linearly independent vectors is not already a basis, we by point 1 can obtain a basis by adding some new vectors to it. But then the basis will have more then n vectors, whcih is impossible.

6. This can be proved in analogy with point 5.

7. Assume $\dim(U) > \dim(V) = n$. Any basis of U is a linearly independent set in V, and by point 1 we can add new vectors to it to get a basis for V. This new basis contains more then n vectors, whcih is impossible. □

Exercises

E.11.1. Find out if the vector $v = [3,2,1]$ is linear combination of the vectors $u_1 = [0,1,1]$, $u_2 = [1,0,1]$, $u_3 = [1,1,0]$, $u_4 = [0,1,0]$ in $\mathbb{R}^3$. If yes, find a combination. Is it unique?

E.11.2. Are the following vectors linearly dependent in $\mathbb{R}^4$? **(1)** $v_1 = (1,2,1,1)$, $v_2 = (0,1,2,1)$, $v_3 = (0,0,1,2)$. **(2)** $u_1 = (1,2,0,0)$, $u_2 = (2,1,0,0)$, $u_3 = (0,0,1,2)$, $u_4 = (0,0,2,1)$. **(3)** $w_1 = (1,2,1,1)$, $w_2 = (0,0,0,2)$, $w_3 = (1,2,1,6)$, $w_4 = (1,0,0,3)$. *Hint*: you may reduce the questions to a systems of linear equations.

E.11.3. Is Definition 11.2 equivalent to the following definition? Let V be a vector space over a field F. The set $S = \{v_1, \ldots, v_n\}$ of vectors of V is *linearly dependent*, if *each* of its vectors is a linear combination of others.

E.11.4. **(1)** In $\mathbb{R}^3$ find a set of four vectors $\{u_1, u_2, u_3, u_4\}$ which is linearly dependent, but a subset of *any* three of its vectors is independent. **(2)** In $\mathbb{Z}_5^3$ find three vectors which are linearly dependent, but no two of them are collinear. **(3)** In $\mathbb{Z}_5^3$ find three vectors which are linearly independent.

E.11.5. Is the following system linearly dependent in $M_{3,4}(\mathbb{R})$? *Hint*: compare the columns.

$$M_1 = \begin{bmatrix} 2 & 0 & 1 & -7 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 2 & 1 & 1 & -7 \\ 1 & 2 & 0 & 0 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 2 & 0 & 3 & 0 \\ 1 & 2 & 0 & 0 \\ 3 & 1 & 1 & -7 \end{bmatrix}.$$

E.11.6. **(1)** In $\mathbb{R}^3$ geometrically describe the span of the set $S = \{v_1, v_2\}$, where $v_1 = (2,2,0)$, $v_2 = (0,0,-\pi^2)$. **(2)** Show that $\mathbb{R}^3 = \operatorname{span}(S)$, where the set S consists of vectors $w_1 = [1,1,1]$, $w_2 = [0,2,2]$, $w_3 = [0,0,3]$. **(3)** In polynomial space $\mathcal{P}_4$ describe $\operatorname{span}(f_1, f_2, f_3)$, if $f_1(x) = 2x$, $f_2(x) = 2 + 2x^2$, $f_3(x) = -1 + x$.

E.11.7. Let U be a subspace of a space V. Find $\operatorname{span}(U)$ and $\operatorname{span}(V)$.

E.11.8. Prove that the polynomial space $F[X]$ has no finite spanning set. *Hint*: assume the contrary, and compare the degrees of the spanning polynomials.

E.11.9. Find out if the given vectors form a basis in $\mathbb{R}^3$ (indicate why). **(1)** $u_1 = (1,1,0)$, $u_2 = (1,-1,0)$, $u_3 = (0,0,2)$. **(2)** $v_1 = (2,2,0)$, $v_2 = (2,-2,0)$. **(3)** $w_1 = (1,1,0)$, $w_2 = (-1,1,0)$, $w_3 = (0,0,3)$, $w_4 = (2,2,2)$.

E.11.10. The vectors $u_1,\ldots,u_m \in V$ have the property that any vector $v \in V$ has a *unique* presentation as a linear combination of $u_1,\ldots,u_m$. Do they form a basis for V? *Hint:* consider the case $v = \vec{0}$.

E.11.11. **(1)** We are given the vectors $u_1 = [1,1,0]$, $u_2 = [0,1,1]$, $u_3 = [1,1,1]$, $u_4 = [1,2,1]$, $u_5 = [1,3,1]$. Exclude some vectors to get a basis for $\mathbb{R}^3$. **(2)** Add some new vectors to the vector $v = (1,3i,0)$ to get a basis for $\mathbb{C}^3$.

E.11.12. Find the dimension by giving a basis for the space V, if **(1)** V is the plane in $\mathbb{R}^3$ passing via the points $A = (1,2,0)$, $B = (0,-2,-1)$, $C = (0,2,1)$. **(2)** $V = \text{span}(M_1,\, M_1 + M_2,\, M_1 - M_2)$ in where are the matrices given in Example 10.20. **(3)** $V = \mathbb{C}$ is that of Exercise E.10.5.

E.11.13. Testing *both points* of the basis definition (independence *and* spanning) detect: **(1)** if the matrices $M_1 = \left[\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right]$, $M_2 = \left[\begin{smallmatrix}2&2\\0&0\end{smallmatrix}\right]$, $M_3 = \left[\begin{smallmatrix}3&3\\0&3\end{smallmatrix}\right]$, $M_4 = \left[\begin{smallmatrix}4&5\\0&6\end{smallmatrix}\right]$ form a basis for $M_{2,2}(\mathbb{R})$. Find $\dim\big(\text{span}(M_1, M_2, M_3, M_4)\big)$. **(2)** if the polynomials $f_1(x) = 3x^2 + 1$, $f_2(x) = x^2 + x$, $f_3(x) = 5x$, form a basis for $\mathcal{P}_3(\mathbb{R})$. Find $\dim(\text{span}(f_1, f_2, f_3))$.

CHAPTER 12

Coordinate systems

12.1. Setting up coordinate systems

One of the widely used features of school mathematics is that we can identify an arrow-like vector $\vec{v}$ of the Euclidean plane to a pair of coordinates (x, y) (see Figure 12.1). It is easier to do calculations with such pairs rather than with arrow-like vectors. This feature can be generalized on abstract vector spaces.

Let V be a *finite-dimensional* vector space over a field F with a basis $E = \{e_1, \dots, e_n\}$. Any vector $v \in V$ has a *unique* linear presentation:

$$v = a_1 e_1 + \cdots + a_n e_n. \tag{12.1}$$

Write down its coefficients $a_1, \dots, a_n$ as a tuple $(a_1, \dots, a_n)$ in the same order as they appear in (12.1). Does this tuple determine the vector v *uniquely*? Not *yet*, because it depends on the *order* of the basis vectors. If we write the same basis E, say, in inverse order $E = \{e_n, \dots, e_1\}$, then we have $v = a_n e_n + \cdots + a_1 e_1$, which gives a different tuple $(a_n, \dots, a_1)$. Since a basis E is defined as a *set*, not as an ordered sequence, its vectors may be written in any order.

But if we *fix some order* of the basis vectors, say $e_1, \dots, e_n$, then the tuple of coefficients $(a_1, \dots, a_n)$ is a vector of F^n which determines v *uniquely*. Then the coefficients $a_1, \dots, a_n$ are called the *coordinates* of v relative to the basis E. Their tuple $(a_1, \dots, a_n)$ is called the *coordinates vector* of v, and is denoten by $[v]_E$. When we do not want to stress the basis E, we may write the coordinates vector just as $[v]$.

We *identify* v with its coordinates vector $[v]_E$, and write $v = [v]_E$. Since a vector can be written both vertically or horizontally (with parentheses or square brackets), we may use any of the notations:

$$\boldsymbol{v = [v]_E = (a_1, \dots, a_n), \qquad v = [v]_E = [a_1, \dots, a_n],}$$

or in vertical vector notation:

$$\boldsymbol{v = [v]_E = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.}$$

Example 12.1. In $\mathbb{R}^2$ fix the standard basis E with vectors $e_1 = (1,0)$, $e_2 = (0,1)$ ordered in the way we listed them.

Then for the vectors $v, u \in \mathbb{R}^2$ in Figure 12.1 (a) any of the following notations is appropriate: $v = (5,2)$, $[v]_E = [5,2]$, $u = [u] = [u]_E = (2,4)$, $u = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$, $v = \begin{bmatrix} 5 \\ 2 \end{bmatrix}$. And we can write:

$$u + v = [u]_E + [v]_E = \begin{bmatrix} 2 \\ 4 \end{bmatrix} + \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 7 \\ 6 \end{bmatrix}.$$

Example 12.2. If we in previous example take the basis $G = \{e_2, e_1\}$, i.e., the same basis written in reverse order, then $v = [v]_G = (2,5)$ and $u = [u]_G = (4,2)$.

Example 12.3. The suggested flexibility in horizontal/vertical notations of $[v]_E$ (for the same vector v) often is very comfortable.

Let v be the vector of Example 12.1, and let M be the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 4 \end{bmatrix}$. Then the notations $[v]_E \cdot M$ or $[v] \cdot M$ stand for the matrix product

$$[5,2]\begin{bmatrix} 2 & 1 \\ 0 & 4 \end{bmatrix} = [10,9],$$

whereas $M \cdot [v]_E$ or $M \cdot [v]$ stand for the product

$$\begin{bmatrix} 2 & 1 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \end{bmatrix}.$$

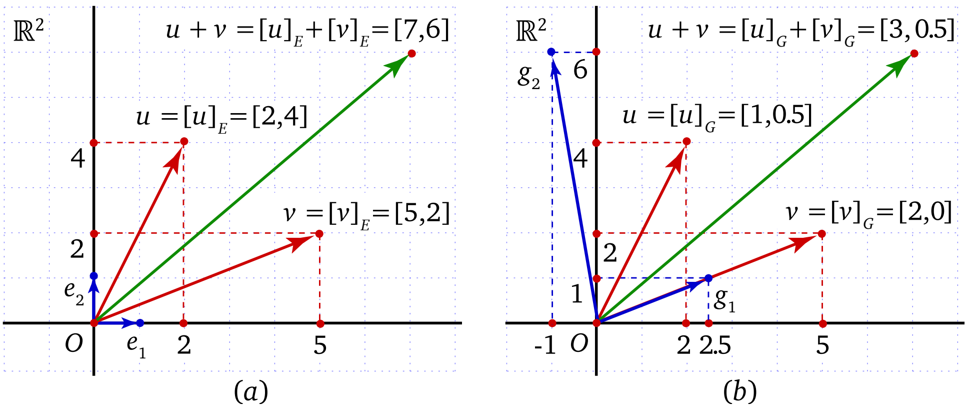


FIGURE 12.1. Two coordinate systems in $\mathbb{R}^2$.

The case of *infinite-dimensional* spaces is analogous. Take an infinite basis $E = \{e_i \mid i \in \mathcal{I}\}$, and order E in some way. Any vector $v \in V$ is a linear combination of *finitely many* vectors form E:

$$v = a_{i_1} e_{i_1} + \cdots + a_{i_n} e_{i_n}. \tag{12.2}$$

If we write down these coordinates $a_{i_1}, \ldots, a_{i_n}$, and add 0's for all those vectors of E which are not evolved in (12.2) (respective to the order of E), we will get an infinite sequence of ordered coefficients. For countable E this will be an infinite sequence $[v]_E = (\ldots, 0, a_{i_1}, 0, \ldots, 0, a_{i_n}, 0, \ldots)$, see Example 12.7 below.

We say that a *coordinate system* is given in the vector space V, if a basis E with some order is fixed in V, and a sequence of coefficients $[v]_E$ corresponds to each vector $v \in V$. Denote this correspondence or map by $\phi_E : V \to F^n$, i.e., $\phi_E(v) = [v]_E$.

Roughly speaking, the space F^n is the "simplest" of all n-dimensional vector spaces V over F, and a coordinate system uses a basis E to set up a correspondence $\phi_E : V \to F^n$ allowing *to treat* vectors $v \in V$ as sequences $[v]_E \in F^n$.

Agreement 12.4. We have to stress that v is a vector of the abstract space V (it may be an arrow-like vector, a polynomial, a matrix, etc.) whereas $[v]_E$ is a sequence in F^n. So v and $[v]_E$ may *not* be *equal* mathematical objects. But if a coordinate system is fixed, the handy notation $v = [v]_E$ is used to state that $[v]_E$ corresponds to v (consists of the coordinates of v in E). We identify v with $[v]_E$ in the same manner as every arrow-like vector $\vec{v}$ of the Euclidean plane is identified to an (x, y).

Example 12.5. If we in the space of Example 12.1 take basis G of vectors $g_1 = (\frac{5}{2}, 1)$, $g_2 = (-1, 6)$ (see Figure 12.1 (*b*)), then we have

$$v = 2g_1 + 0g_2 \text{ and } u = 1g_1 + \tfrac{1}{2}g_2,$$

and we can write

$$v = [v]_G = \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \quad u = [u]_G = \begin{bmatrix} 1 \\ \frac{1}{2} \end{bmatrix}.$$

Here we have the *same* vectors v, u in the *same* space as in Example 12.1, but since the bases E and G are different, we have *different* coordinates for the same vectors since we have different coordinate systems.

Example 12.6. Take the polynomial $f(x) = 5 - x^2 + 4x^3$ in the 4-dimensional space $\mathcal{P}_3(\mathbb{R})$ with the basis $E = \{1, x, x^2, x^3\}$. We can write, say, $f(x) = [f]_E = (5, 0, -1, 4)$ or, when vertical notation is preferred:

$$f(x) = [f]_E = \begin{bmatrix} 5 \\ 0 \\ -1 \\ 4 \end{bmatrix}.$$

When there is no need to stress the basis, we can simply use the common notation $f(x) = [f(x)] = (4, -1, 0, 5)$.

Example 12.7. Consider the same polynomial $f(x) = 5 - x^2 + 4x^3$ in the infinite-dimensional space of all polynomials $\mathbb{R}[x]$ with the basis $E = \{1, x, x^2, \ldots, x^n, \ldots\}$. Using infinite Cartesian power $\mathbb{R}^\infty$ we could write, say,

$$f(x) = [f]_E = (5, 0, -1, 4, 0, 0, \ldots, 0, \ldots) \in \mathbb{R}^\infty.$$

Example 12.8. The 4-dimensional space $M_{2,2}$ of 2×2 matrices has a basis E of vectors:

$$e_1 = E_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_2 = E_{1,2} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$e_3 = E_{2,1} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad e_4 = E_{2,2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

In these coordinate system the matrix

$$M = \begin{bmatrix} 5 & 7 \\ -9 & 14 \end{bmatrix}$$

may be written as:

$$M = [M]_E = [5, 7, -9, 14].$$

Clearly, using a standard basis (where possible) is preferable, since the coordinates are especially easy to find. In Example 12.1 we have $u = [u]_E = (2, 4)$ in standard basis E, but in Example 12.5 we for the same vector have $u = [u]_G = (1, \frac{1}{2})$.

12.2. Basic properties of coordinate systems

Since the facts of this section have simple proofs, they will be given for *finite-dimensional* spaces only, leaving the analogs for infinite-dimensional case as optional exercises.

Let V be an n-dimensional space over a field F, and let some coordinate system be selected: an ordered basis $E = \{e_1, \ldots, e_n\}$ is fixed, and the map $\phi_E : V \to F^n$ with $\phi_E(v) = [v]_E$ is given.

Lemma 12.9. *Under the above circumstances the map $\phi_E : V \to F^n$ is bijective, i.e.:*

1. *coordinates of any two distinct vectors are distinct: if $u \neq v$, then $[u]_E \neq [v]_E$,*
2. *for any sequence $(a_1, \ldots, a_n) \in F^n$ there is a vector $v \in V$ which it corresponds to, i.e., $[v]_E = (a_1, \ldots, a_n)$.*

***Proof*.** The first point follows from Theorem 11.21 and from the fact that E is ordered. To prove the second point take any $(a_1, \ldots, a_n) \in F^n$, and consider the vector $v = a_1e_1 + \cdots + a_ne_n \in V$. Then $[v]_E = (a_1, \ldots, a_n)$. □

Lemma 12.10. *Under the above circumstances the map $\phi_E : V \to F^n$ is linear, i.e.:*

1. *for any $u, v \in V$ we have $[u + v]_E = [u]_E + [v]_E$,*
2. *for any $v \in V$ and $a \in F$ we have $[av]_E = a[v]_E$,*
3. *more generally, for any linear combination $w = a_1v_1 + \cdots + a_kv_k$ we have*

$$[w]_E = a_1[v_1]_E + \cdots + a_k[v_k]_E.$$

Proof. If $u = [u]_E$, then $u = a_1 e_1 + \cdots + a_n e_n$ for some scalars $a_1, \ldots, a_n \in F$. Similarly, $v = [v]_E$ means that $v = b_1 e_1 + \cdots + b_n e_n$ for some $b_1, \ldots, b_n \in F$. Then by commutativity and distributivity axioms:

$$\begin{aligned} u + v &= (a_1 e_1 + \cdots + a_n e_n) + (b_1 e_1 + \cdots + b_n e_n) \\ &= (a_1 + b_1)e_1 + \cdots + (a_n + b_n)e_n \to [a_1 + b_1, \ldots, a_n + b_n]_E \\ &= [u]_E + [v]_E. \end{aligned}$$

The point (2) can be proved similarly. And (3) is a consequence of (1) and (2). □

Lemma 12.11. *Under the above circumstances:*

1. *a set of vectors $v_1, \ldots, v_k$ spans V if and only if the corresponding set $[v_1]_E, \ldots, [v_k]_E$ spans F^n,*
2. *a set of vectors $v_1, \ldots, v_k$ is linearly independent in V if and only if the corresponding set $[v_1]_E, \ldots, [v_k]_E$ is linearly independent in F^n,*
3. *a set of vectors $v_1, \ldots, v_k$ is a basis of V if and only if the corresponding set $[v_1]_E, \ldots, [v_k]_E$ is a basis of F^n.*

Proof. The first point easily follows from previous two lemmas.

To prove the second point suppose a linear combination of our vectors is zero:

$$a_1 v_1 + \cdots + a_k v_k = 0. \tag{12.3}$$

Present each vector v_i as a linear combination of vectors of E and as $[v_i]_E$:

$$\begin{aligned} v_1 &= c_{11} e_1 + \cdots + c_{1n} e_n = [v_1]_E = [c_{11}, \ldots, c_{1n}], \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ v_k &= c_{k1} e_1 + \cdots + c_{kn} e_n = [v_k]_E = [c_{k1}, \ldots, c_{kn}], \end{aligned}$$

where $c_{ij} \in F$, $i = 1, \ldots, k$; $j = 1, \ldots, n$. Substituting these sums in (12.3) we get:

$$\begin{aligned} [0]_E = 0 &= a_1(c_{11} e_1 + \cdots + c_{1n} e_n) + \cdots + a_k(c_{k1} e_1 + \cdots + c_{kn} e_n) \\ &= a_1[c_{11}, \ldots, c_{1n}] + \cdots + a_k[c_{k1}, \ldots, c_{kn}] \\ &= a_1[v_1]_E + \cdots + a_k[v_k]_E. \end{aligned}$$

So a linear combination of vectors $v_1, \ldots, v_k \in V$ and a linear combination of coordinate vectors $[v_1]_E, \ldots, [v_k]_E \in F^n$ with the same coefficients are equal to zero simultaneously. I.e., these systems simultaneously are linearly dependent or independent.

The point (3) follows from the first two points of the lemma. □

Example 12.12. Consider polynomials:

$$\begin{aligned} f_1(x) &= 2 + x + 3x^2 + 2x^3 \\ f_2(x) &= x + 3x^3 \\ f_3(x) &= 1 + x^2 + x^3. \end{aligned}$$

Can we find out if or not each of the following polynomials:

$$\begin{aligned} g(x) &= 19 - 4x + 31x^2 - 14x^3 \\ h(x) &= 19 - 4x + 31x^2 - 15x^3 \end{aligned}$$

is a linear combination of $f_1(x)$, $f_2(x)$, $f_3(x)$? Assuming $E = \{1, x, x^2, x^3\}$ write

$$[f_1]_E = \begin{bmatrix} 2 \\ 1 \\ 3 \\ 2 \end{bmatrix}, \ [f_2]_E = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 3 \end{bmatrix}, \ [f_3]_E = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix},$$

$$[g]_E = \begin{bmatrix} 19 \\ -4 \\ 31 \\ -14 \end{bmatrix}, \ [h]_E = \begin{bmatrix} 19 \\ -4 \\ 31 \\ -15 \end{bmatrix}.$$

If there exist values of variables x_1, x_2, x_3 for which

$$x_1[f_1]_E + x_2[f_2]_E + x_3[f_3]_E = [g]_E,$$

then those values form a solution of the system of linear equations:

$$\begin{cases} 2x_1 \quad\quad\quad +x_3 = 19 \\ x_1 \quad +x_2 \quad\quad = -4 \\ 3x_1 \quad\quad\quad +x_3 = 31 \\ 2x_1 \; +3x_2 \; +x_3 = -14 \end{cases}$$

Its augmented matrix has the following row-echelon form:

$$\left[\begin{array}{ccc|c} 1 & 0 & \frac{1}{2} & \frac{19}{2} \\ 0 & 1 & -\frac{1}{2} & -\frac{27}{2} \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \end{array}\right],$$

i.e., the system has a solution, which can uniquely be computed as $(7,-11,5)$, if needed. So we have:

$$g(x) = 7f_1(x) - 11f_2(x) + 5f_3(x).$$

Doing the same steps for the polynomial $h(x)$, we get the following row-echelon form

$$\left[\begin{array}{ccc|c} 1 & 0 & \frac{1}{2} & \frac{19}{2} \\ 0 & 1 & -\frac{1}{2} & -\frac{27}{2} \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & -1 \end{array}\right],$$

which means that $h(x)$ is *not* a linear combination of $f_1(x)$, $f_2(x)$, $f_3(x)$.

The above lemmas and this example show that any coordinate system *preserves* the "linear properties" of vectors: the correspondence is a *bijective*, it maps a *spanning set* to a spanning set of coordinate vectors, it maps a *linearly independent* set (and a *basis*) to a linearly independent set (and a basis) of coordinate vectors. And for any subspace U of V we can consider the respective subspace $\phi_E(U)$ in F^n, if a coordinate map $\phi_E : V \to F^n$ is given.

This not only allows to replace abstract vectors by simpler objects (finite sequences), but also makes it possible to apply methods of matrix calculus, row-echelon methods, systems of linear equations to abstract vector spaces. You will have beautiful applications of this approach in Part 5.

Exercises

E.12.1. In $\mathbb{R}^2$ we are given a basis of vectors $g_1 = (2,0)$, $g_2 = (0,3)$. Find the coordinates of the vectors $u = (2,3)$, $v = (0,9)$, $w = (1,1)$ in this basis.

E.12.2. In $\mathbb{C}^2$ we are given a basis E by vectors $e_1 = (3i,0)$, $e_2 = (0,-i)$. Find the coordinates of the vector $u = (6,3i)$ in this basis.

E.12.3. In the space $\mathbb{R}^3$ find a basis $G = \{g_1, g_2, g_3\}$ in which the vector $v = (3,4,-5)$ has the coordinates $[v]_G = (1,1,1)$.

E.12.4. In the polynomial space $\mathcal{P}_3$ we are given the basis $E = \{1, x, x^2, x^3\}$. Find $[f(x)]_E$ and $[g(x)]_E$, if $f(x) = x + 5 - 3x^3$ and $g(x) = 7x^3 + (x-2)^2$.

E.12.5. In $\mathcal{P}_3$ we are given the basis $E = \{2,\ 2x,\ 2x^2,\ 2x^3\}$. Find $[f(x)]_E$ for $f(x) = 10 + 12x^3 - 6x^2$, $f(x) = 4x^3 - 1$, $f(x) = 3(x^2 + 2)$.

E.12.6. Let the matrices $E_{i,j}$, $i = 1,2$, $j = 1,2,3,4$ given in Example 11.18 form the basis for the matrix space $V = M_{2,4}(F)$. Find the coordinates of the following matrices in this basis: $A = \left[\begin{smallmatrix} 1 & 2 & 5 & 0 \\ 0 & 3 & 1 & 3 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{smallmatrix}\right]$.

CHAPTER 13

Change of basis in space

13.1. Change of basis matrices

We have already had examples when the same vector has distinct coordinates in different bases (see examples 12.1, 12.2, 12.5). Let us find relationship between them, i.e., find how the vector coordinates change when we change the coordinate system. Within this chapter all spaces are finite-dimensional by Agreement 11.26.

Assume we have a space V over a field F, and two bases of V:

$$E = \{e_1, \dots, e_n\}, \quad G = \{g_1, \dots, g_n\}.$$

Each vector $g_i \in G$ can be presented as a linear combination of vectors of E

$$\begin{aligned} g_1 &= p_{11}e_1 + \cdots + p_{n1}e_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ g_n &= p_{1n}e_1 + \cdots + p_{nn}e_n \end{aligned} \tag{13.1}$$

by some coefficients $p_{ij} \in F$, $i, j = 1, \dots, n$. Construct a matrix P by placing these coefficients by *columns*:

$$P = \Big[[g_1]_E \;\vdots\; \cdots \;\vdots\; [g_n]_E \Big] = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix}. \tag{13.2}$$

Call this *change of basis matrix* from the basis E to the basis G (notice how we indexed the coefficients in (13.1) to match entries indexation in (13.2)).

Often, in order to stress the bases, we may denote the matrix P by P_{EG}. Also, we may call E the *old* basis, and G the *new* basis.

Take any vector $v \in V$ and assume its coordinates in these bases are:

$$v = [v]_E = [a_1, \dots, a_n], \quad v = [v]_G = [b_1, \dots, b_n].$$

Then:

$$\begin{aligned} v = [v]_G &= b_1 g_1 + \cdots + b_n g_n \\ &= b_1(p_{11}e_1 + \cdots + p_{n1}e_n) + \cdots + b_n(p_{1n}e_1 + \cdots + p_{nn}e_n) \\ &= (b_1p_{11} + \cdots + b_np_{1n})e_1 + \cdots + (b_1p_{n1} + \cdots + b_np_{nn})e_n. \end{aligned}$$

Since also $v = [v]_E = a_1e_1 + \cdots + a_ne_n$, we get that

$$a_i = b_1p_{i1} + \cdots + b_np_{in}, \quad i = 1, \dots, n,$$

i.e., the i'th coordinate a_i is equal to the product of the i'th row of P by the column vector $[v]_G$. That is:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \dots & \dots & \dots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \tag{13.3}$$

or, in other words:

$$\boldsymbol{[v]_E = P_{EG} \cdot [v]_G}. \tag{13.4}$$

Let us consider an example that displays the above formula for some simple cases. This example is for illustrative purposes only, later we will learn more efficient methods to compute change of basis matrices.

Example 13.1. Consider the plane $\mathbb{R}^2$ with two bases of Example 12.1 and Example 12.5:

$$E = \{e_1, e_2\} = \{(1,0), (0,1)\},$$
$$G = \{g_1, g_2\} = \{(\tfrac{5}{2}, 1), (-1, 6)\}.$$

To compute P_{EG} by the above definition we need find the linear combinations

$$g_1 = p_{11}e_1 + p_{21}e_2$$
$$g_2 = p_{12}e_1 + p_{22}e_2.$$

Since the basis E is standard, the values of variables p_{ij} coincide with coordinates of g_1, g_2, and we have:

$$P_{EG} = \begin{bmatrix} \frac{5}{2} & -1 \\ 1 & 6 \end{bmatrix}.$$

So for $P = P_{EG}$ the formula (13.4) implies:

$$[v]_E = P_{EG}\,[v]_G = \begin{bmatrix} \frac{5}{2} & -1 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \end{bmatrix},$$

$$[u]_E = P_{EG}\,[u]_G = \begin{bmatrix} \frac{5}{2} & -1 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 1 \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \end{bmatrix}.$$

Less trivial part is finding the coordinates in basis G, if we have the coordinates in basis E. This can be done with change of basis matrix P_{GE}. Form new linear combinations

$$e_1 = p_{11}g_1 + p_{21}g_2$$
$$e_2 = p_{12}g_1 + p_{22}g_2,$$

from where the values p_{ij} can be found by solving two systems in variables p_{ij}:

$$\begin{cases} \frac{5}{2}p_{11} & -p_{21} = 1 \\ p_{11} & +6p_{21} = 0, \end{cases}$$

$$\begin{cases} \frac{5}{2}p_{12} & -p_{22} = 0 \\ p_{12} & +6p_{22} = 1. \end{cases}$$

Solving them we get $p_{11} = \frac{3}{8}$, $p_{21} = -\frac{1}{16}$, $p_{12} = \frac{1}{16}$, $p_{22} = \frac{5}{32}$, i.e.:

$$P_{GE} = \begin{bmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{16} & \frac{5}{32} \end{bmatrix}.$$

In Exercise 12.5 we found the coordinates of vectors $v = (5,2)$ and $u = (2,4)$ in basis G:

$$[v]_G = \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \quad [v]_G = \begin{bmatrix} 1 \\ \frac{1}{2} \end{bmatrix}.$$

Now we can compute the same vectors differently, using change of basis matrix $P = P_{GE}$:

$$[v]_G = P_{GE}\,[v]_E = \begin{bmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{16} & \frac{5}{32} \end{bmatrix} \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix},$$

$$[u]_G = P_{GE}\,[u]_E = \begin{bmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{16} & \frac{5}{32} \end{bmatrix} \begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \\ \frac{1}{2} \end{bmatrix}$$

(compare this with Figure 12.1 (b)).

We stress again: if we have the coordinates $[v]_E$ of a vector v in the *old* basis E, and want to find its coordinates $[v]_G$ in the *new* basis G, then we multiply $[v]_E$ by the matrix $P = P_{GE}$ (by the change of basis matrix from the *new* basis G to the *old* basis E, *not* by P_{EG}).

Under the above circumstances P_{EG} is *the only* matrix, for which (13.4) holds for any $v \in V$. Indeed, if there is another matrix Q for which the analog of (13.4) is satisfied, i.e., if $[v]_E = Q\,[v]_G$ for any v, then $Q\,[v]_G = P\,[v]_G$ for any $[v]_G$, and so $P = Q$ by Lemma 8.22. We have proved:

Theorem 13.2. *Let E and G be any bases of the space V, and let P_{EG} be the change of basis matrix from E to G. Then:*

1. *for any vector $v \in V$ the equality $[v]_E = P_{EG} \cdot [v]_G$ holds;*
2. *P_{EG} is the only matrix for which the above equality holds for all $v \in V$.*

The following fact displays a relation between three change of basis matrices:

Theorem 13.3. *Let E, H and G be any bases in the space V, and let P_{EH}, P_{HG} and P_{EG} be the respective change of basis matrices. Then:*

$$P_{EG} = P_{EH} P_{HG}. \tag{13.5}$$

***Proof*.** Let $[v]_E$, $[v]_H$ and $[v]_G$ be the coordinates of a vector $v \in V$ in bases E, H and G. By the above theorem $[v]_E = P_{EH}\,[v]_H$ and $[v]_H = P_{HG}\,[v]_G$. Then:

$$[v]_E = P_{EH}\,[v]_H = P_{EH}\,\left(P_{HG}\,[v]_G\right) = \left(P_{EH}\,P_{HG}\right)\,[v]_G.$$

But on the other hand $[v]_E = P_{EG}\,[v]_G$, and since the change of basis matrix is unique, we get that $P_{EG} = P_{EH}P_{HG}$. □

From this we deduce:

Theorem 13.4. *Let E and G be any bases of the space V, and let P_{EG} be the change of basis matrix from E to G. Then the matrix P_{EG} is invertible and*

$$P_{EG}^{-1} = P_{GE}. \tag{13.6}$$

***Proof*.** If we change basis from E to G by P_{EG}, and then change back from G to E by P_{GE}, then the change of basis matrix by Theorem 13.3 is $P_{EG}P_{GE}$. On the other hand, after these two changes we stay in basis E or, in other words, go from E to E by the identity change of basis matrix $P_{EE} = I$. So $P_{EG}P_{GE} = I$ and $P_{EG}^{-1} = P_{GE}$. □

Example 13.5. Let us compare this theorem with Example 13.1, and compute the (mutual) inverses of the change of basis matrices P_{EG} and P_{GE} computed in that example.

They can obtained either by the above theorem or by:

$$P_{EG}^{-1} = \begin{bmatrix} \frac{5}{2} & -1 \\ 1 & 6 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{16} & \frac{5}{32} \end{bmatrix} = P_{GE}.$$

It turns out that the statement in some sense opposite to Theorem 13.4 also is true: *any* invertible matrix is a change of basis for some bases:

Theorem 13.6. *Let P be any invertible matrix of degree n over F, and let E be any basis in an n-dimensional space V over F. Then there is a (unique) basis G such that P is the change of basis matrix P_{EG} from E to G.*

***Proof*.** In V fix a coordinate system with the basis E. Define the vectors

$$g_i = p_{1i}e_1 + \cdots + p_{ni}e_n, \tag{13.7}$$

$i = 1, \ldots, n$, i.e., each g_i is taken to be a linear combination of vectors of E with coefficients from the i'th column of P. In the coordinate system with the basis E the vectors g_i have the coordinates:

$$[g_1]_E = \begin{bmatrix} p_{11} \\ \vdots \\ p_{n1} \end{bmatrix}, \ \ldots\ , [g_n]_E = \begin{bmatrix} p_{1n} \\ \vdots \\ p_{nn} \end{bmatrix}. \tag{13.8}$$

Since (13.7) is the same as (13.1), P will be the change of basis matrix P_{EG}, provided that the set $G = \{g_1, \ldots, g_n\}$ actually *is a basis* in V. To prove this we just need to check that the vectors $g_1, \dots, g_n$ are linearly independent, for, in an n-dimensional space V every n independent vectors form a basis by point 5 of Proposition 11.27. So suppose

$$c_1 g_1 + \cdots + c_n g_n = 0, \tag{13.9}$$

and deduce that $c_i = 0,\ i = 1, \dots, n$.

By point 3 in Lemma 12.10 equality (13.9) translates to $c_1[g_1]_E + \cdots + c_n[g_n]_E = [0]_E$ which by (13.8) means that $(c_1, \dots, c_n)$ is a solution of the homogeneous system $PX = O$ (compare to the "motivational" example we gave with (11.2) and (11.3)). Since P is invertible, $c_i = 0,\ i = 1, \dots, n$ by point 3 of Theorem 9.10. □

As you will see later, linear independence of the columns of P is a particular case of Corollary 14.14.

Now we can add one more equivalent condition for invertible matrices:

Corollary 13.7 (Amendment to Theorem 9.10)**.** *A matrix $A \in M_{n,n}(F)$ is invertible if and only if it is a change of basis matrix $A = P_{EG}$ (from the given basis E to a basis G).*

13.2. Computation of change of basis matrices

There is a surprisingly straightforward way to compute the change of basis matrix from a basis E to a basis G:

How to compute the change of basis matrix.

Algorithm 13.8 (Computation of change of basis matrix)**.** We are given two bases $E = \{e_1, \dots, e_n\}$ and $G = \{g_1, \dots, g_n\}$ in an n-dimensional space V over a field F. A coordinate system is fixed, and we can present vectors of V by their coordinates in that system.

► Find the change of basis matrix P_{EG}.

1. Using the coordinate system present the vectors of E and G as sequences in F^n:

$$\begin{array}{ll} e_1 = (a_{11}, \dots, a_{n1}) & g_1 = (b_{11}, \dots, b_{n1}) \\ \dots\dots\dots\dots\dots\dots, & \dots\dots\dots\dots\dots\dots \\ e_n = (a_{1n}, \dots, a_{nn}) & g_n = (b_{1n}, \dots, b_{nn}) \end{array} \tag{13.10}$$

2. Form a block matrix by placing coordinates of these vectors by *columns:*

$$A = \left[\begin{array}{c|c} a_{11} \cdots a_{1n} & b_{11} \cdots b_{1n} \\ \dots\dots\dots\dots & \dots\dots\dots\dots \\ a_{n1} \cdots a_{nn} & b_{n1} \cdots b_{nn} \end{array}\right]. \tag{13.11}$$

3. Bring A to reduced row-echelon form rref(A) by elementary row-operations:

$$\text{rref}(A) = \left[\begin{array}{ccc|c} 1 & \cdots & 0 & p_{11} \cdots p_{1n} \\ \dots & \dots & \dots & \dots\dots\dots\dots \\ 0 & \cdots & 1 & p_{n1} \cdots p_{nn} \end{array}\right] = \left[\, I \;\vdots\; P_{EG} \,\right].$$

4. Output the right-hand side n column of rref(A) as the change of basis matrix P_{EG}.

To shorten notation we may sometimes as "mathematical slang" write the matrix (13.11) as $A = \left[\, E \;\vdots\; G \,\right]$, assuming that the vectors of bases E and G already are presented as sequences. In these notations we have established the row-equivalence:

$$\left[\, \boldsymbol{E} \;\vdots\; \boldsymbol{G} \,\right] \sim \left[\, \boldsymbol{I} \;\vdots\; \boldsymbol{P_{EG}} \,\right].$$

Proof of Algorithm 13.8. Suppose H is the basis according to which the initial coordinates (13.10) of vectors of E and G are given. By Theorem 13.3 and then by Theorem 13.4 we have $P_{EG} = P_{EH}P_{HG} = P_{HE}^{-1}\,P_{HG}$.

Both matrices P_{HG} and P_{HE} are known: their entries are the coordinates (13.10) of vectors of E and of G written by columns. Thus, the product $P_{HE}^{-1}\,P_{HG}$ also is known, and the method we suggested in the algorithm *simultaneously* computes P_{HE}^{-1} and multiplies it with P_{HG} as follows. Since P_{HE} is invertible, we by (9.6) have $E_t\cdots E_1\cdot P_{HE} = I$ and, thus, $E_t\cdots E_1 = P_{HE}^{-1}$ for some elementary matrices E_i. Thus,

$$E_t\cdots E_1\cdot P_{HG} = P_{HE}^{-1}\,P_{HG},$$

and to achieve this we use the block matrix (13.11). Doing any elementary operation with its left-hand half, we do the same operation with the right-hand half (i.e. multiply it by the same elementary matrix E_i).

Since the matrix P_{HE} is invertible, its reduced row-echelon form is I. Hence, the left-hand half of rref(A) will actually be I, as mentioned in the algorithm. □

To get the inverse matrix P_{GE} we can either use the same method, just putting in (13.11) the entries a_{ij} in the right-hand half, and the entries b_{ij} in the left-hand half, or we can compute the inverse $P_{EG}^{-1} = P_{GE}$.

Example 13.9. Let us compute the matrices P_{EG} and P_{GE} for the bases

$$E = \{e_1, e_2\} = \{(1,0),(0,1)\},$$
$$G = \{g_1, g_2\} = \{(\tfrac{5}{2},1),(-1,6)\}$$

of Example 13.1 by this algorithm. The first augmented matrix is

$$\left[\begin{array}{cc|cc} 1 & 0 & \frac{5}{2} & -1 \\ 0 & 1 & 1 & 6 \end{array}\right].$$

Since this already is in reduced raw-echelon form, we have

$$P_{EG} = \begin{bmatrix} \frac{5}{2} & -1 \\ 1 & 6 \end{bmatrix}.$$

Write the second augmented matrix, and bring it to reduced raw-echelon form:

$$\left[\begin{array}{cc|cc} \frac{5}{2} & -1 & 1 & 0 \\ 1 & 6 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{cc|cc} 1 & -\frac{5}{2} & \frac{5}{2} & 0 \\ 0 & 1 & -\frac{1}{16} & \frac{5}{32} \end{array}\right]$$

$$\sim \left[\begin{array}{cc|cc} 1 & 0 & \frac{3}{8} & \frac{1}{16} \\ 0 & 1 & -\frac{1}{16} & \frac{5}{32} \end{array}\right] = \left[\, I \;\vdots\; P_{GE} \,\right],$$

i.e.:

$$P_{GE} = \begin{bmatrix} \frac{3}{8} & \frac{1}{16} \\ -\frac{1}{16} & \frac{5}{32} \end{bmatrix}.$$

Example 13.10. Consider two bases in $\mathbb{R}^3$:

$$E = \{e_1, e_2, e_3\} = \{(0,1,2),(1,1,-1),(2,-1,0)\},$$
$$G = \{g_1, g_2, g_3\} = \{(-1,1,1),(2,0,2),(0,3,2)\}.$$

Then we have:

$$A = \left[\, E \;\vdots\; G \,\right] = \left[\begin{array}{ccc|ccc} 0 & 1 & 2 & -1 & 2 & 0 \\ 1 & 1 & -1 & 1 & 0 & 3 \\ 2 & -1 & 0 & 1 & 2 & 2 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 1 & -1 & 1 & 0 & 3 \\ 0 & 1 & 2 & -1 & 2 & 0 \\ 0 & 0 & 1 & -\frac{1}{2} & 1 & -\frac{1}{2} \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{2} & 1 & \frac{3}{2} \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -\frac{1}{2} & 1 & -\frac{1}{2} \end{array}\right],$$

$$P_{EG} = \begin{bmatrix} \frac{1}{2} & 1 & \frac{3}{2} \\ 0 & 0 & 1 \\ -\frac{1}{2} & 1 & -\frac{1}{2} \end{bmatrix}.$$

Example 13.11. The polynomials

$$f_1(x) = 2 + x + 3x^2 + 2x^3$$
$$f_2(x) = x + 3x^3$$
$$f_3(x) = 1 + 2x^2 + x^3$$
$$f_4(x) = 19 - 4x + 31x^2 - 15x^3$$

are linearly independent in $\mathcal{P}_3$ (we have shown this in Example 12.12, where we put $f_4(x) = h(x)$). Since $\mathcal{P}_3$ is 4-dimensional, these polynomials form a basis G for this space. Take any polynomial, say, $g(x) = 2 + x + 3x^2 + x^3$, and use change of basis matrix to find the linear presentation

$$g(x) = c_1 f_1(x) + c_2 f_2(x) + c_3 f_3(x) + c_4 f_4(x),$$

i.e., the coordinates $[g]_G = (c_1, c_2, c_3, c_4)$. The coordinates of $g(x)$ in the basis $E = \{1, x, x^2, x^3\}$ are known: $[g]_E = (2,1,3,1)$. If we find P_{GE}, then we will have $[g]_G = P_{GE}\,[g]_E$. The block matrix constructed by the rule

$$\left[\,G \;\vdots\; E\,\right]$$

is the matrix:

$$A = \left[\begin{array}{cccc|cccc} 2 & 0 & 1 & 19 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & -4 & 0 & 1 & 0 & 0 \\ 3 & 0 & 2 & 31 & 0 & 0 & 1 & 0 \\ 2 & 3 & 1 & -15 & 0 & 0 & 0 & 1 \end{array}\right],$$

and its reduced raw-echelon form is:

$$\left[\,I \;\vdots\; P_{GE}\,\right] = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 37 & -21 & -22 & 7 \\ 0 & 1 & 0 & 0 & -57 & 34 & 34 & -11 \\ 0 & 0 & 1 & 0 & 22 & -15 & -13 & 5 \\ 0 & 0 & 0 & 1 & -5 & 3 & 3 & -1 \end{array}\right].$$

We get that $P_{GE}\,[g]_E$ is equal to

$$\begin{bmatrix} 37 & -21 & -22 & 7 \\ -57 & 34 & 34 & -11 \\ 22 & -15 & -13 & 5 \\ -5 & 3 & 3 & -1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 3 \\ 1 \end{bmatrix} = \begin{bmatrix} -6 \\ 11 \\ -5 \\ 1 \end{bmatrix} = [g]_G.$$

Exercises

E. 13.1. In the space $\mathbb{R}^3$ we are given the standard basis $E = \{e_1, e_2, e_3\}$ and the basis $G = \{g_1, g_2, g_3\}$, where $g_1 = (1,3,1)$, $g_2 = (0,2,1)$, $g_3 = (0,1,1)$. Find the change of bases matrices P_{EG} and P_{GE}.

E. 13.2. For matrices obtained in Exercise E.13.1 compute the product matrices $P_{EG} \cdot P_{GE}$ and $P_{GE} \cdot P_{EG}$. Explain the results obtained.

E. 13.3. In $\mathbb{R}^3$ we are given two bases E and G mentioned in Exercise E.13.1. Compute the coordinates of the vectors $u = [u]_E = (1,3,0)$ and $v = [v]_E = (2,0,1)$ in the basis G.

E.13.4. In the space $\mathbb{Z}_5^2$ we are given two bases $E = \{e_1, e_2\}$ and $G = \{g_1, g_2\}$, where $e_1 = (2,3)$, $e_2 = (0,4)$ and $g_1 = (1,4)$, $g_2 = (2,2)$. Compute the change of bases matrices P_{EG} and P_{GE} (notice that none of the bases is standard).

E. 13.5. In the space $\mathbb{R}^3$ we are given three bases. The frist basis E is the standard basis. The second basis G and the third basis H consist of vectors, respectively:

$$g_1 = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix},\ g_2 = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix},\ g_3 = \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}; \qquad h_1 = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix},\ h_2 = \begin{bmatrix} 0 \\ 1 \\ 3 \end{bmatrix},\ h_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}.$$

(1) Can you without any row-elimination operations write the change of basis matrices P_{EG} and P_{EH}? **(2)** Compute the change of basis matrix P_{GE}. **(3)** Let the vectors $u = (3,1,2)$ and $v = (1,0,3)$ be given in the basis E. Find their coordinates $[u]_G$ and $[v]_G$ in the basis G using the appropriate change of basis matrix. **(4)** Let the vector w be given by its coordinates $[w]_G = (1,2,3)$ in the basis G. Find its coordinates $[w]_E$ in basis E using the appropriate change of basis matrix. **(5)** Find the change of basis matrix P_{GH}. Detect the equality $P_{EH} = P_{EG}P_{GH}$ for the matrices you found. Explain your answers.

Part 5

Matrix Computations in Spaces

CHAPTER 14

Matrices and vector spaces

"It is my experience that proofs involving matrices can be shortened by 50% if one throws the matrices out."
Emil Artin

14.1. Row spaces and column spaces

You perhaps noticed that the material of previous parts was separated to two streams: in Part 2 and Part 3 we havily used *matrix-related* notions, such as: elementary operations, row-echelon form, reduced row-echelon form, pivots, rank, etc..., and in Part 4 we mostly used *space-related* notions, such as: vectors, dependence, bases, dimension, etc... So far these two streams were mainly separated, but now it is time for their confluence.

Emil Artin is right about matrices in *proofs*, but when it comes to *computations*, matrices turn out to be extremely helpful tools, as we will see soon...

Let us start by initial simple preparations. Assume we have any vectors $v_1, \dots, v_m$ in an n-dimensional space V over a field F. If $V = F^n$, we can present the vectors as

$$\begin{aligned} v_1 &= (a_{11}, \dots, a_{1n}),\\ &\dots\dots\dots\dots\dots\dots\\ v_m &= (a_{m1}, \dots, a_{mn}), \end{aligned}$$

and we can build matrices placing these coordinates a_{ij} either as *rows* or as *columns*:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}, \quad \begin{bmatrix} a_{11} & \cdots & a_{m1} \\ \dots & \dots & \dots \\ a_{1n} & \cdots & a_{mn} \end{bmatrix}.$$

And if the vectors $v_1, \dots, v_m$ are *not* in F^n, but are in some other n-dimensional space V over F, we can first choose a coordinate system with an ordered basis $E = \{e_1, \dots, e_n\}$ of V, find the coordinate vectors $[v_1]_E, \dots, [v_m]_E$, and then build the respective matrices.

Example 14.1. In $\mathbb{R}^4$ take the following three vectors: $v_1 = (1,5,3,1)$, $v_2 = (7,2,0,3)$, $v_3 = (1,3,0,6)$. Using their coordinates we can build two matrices:

$$\begin{bmatrix} 1 & 5 & 3 & 1 \\ 7 & 2 & 0 & 3 \\ 1 & 3 & 0 & 6 \end{bmatrix} = \begin{bmatrix} v_1 \\ \hdashline v_2 \\ \hdashline v_3 \end{bmatrix}$$

(coordinates of v_1, v_2, v_3 are placed by raws),

$$\begin{bmatrix} 1 & 7 & 1 \\ 5 & 2 & 3 \\ 3 & 0 & 0 \\ 1 & 3 & 6 \end{bmatrix} = \left[\begin{array}{c:c:c} v_1 & v_2 & v_3 \end{array}\right]$$

(coordinates of v_1, v_2, v_3 are placed by columns).

Example 14.2. Assume $v_1 = f_1(x) = 1 + 2x + 3x^2$ and $v_2 = f_2(x) = 3 + 5x^2$ are vectors in $V = \mathcal{P}_2(\mathbb{R})$. Then in the coordinate system with the basis $\{1, x, x^2\}$ these vectors have coordinates $v_1 = [v_1]_E = (1,2,3)$ and $v_2 = [v_2]_E = (3,0,5)$. We build the matrices:

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 0 & 5 \end{bmatrix} = \begin{bmatrix} v_1 \\ \hdashline v_2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 3 \\ 2 & 0 \\ 3 & 5 \end{bmatrix} = \left[\begin{array}{c:c} v_1 & v_2 \end{array}\right].$$

Example 14.3. We can use this approach even when the initial vectors already are matrices themselves. Consider the following vectors in $V = M_{2,2}(\mathbb{Z}_7)$:

$$v_1 = B_1 = \begin{bmatrix} 2 & 2 \\ 3 & 0 \end{bmatrix},\ v_2 = B_2 = \begin{bmatrix} 1 & 5 \\ 4 & 3 \end{bmatrix},\ v_3 = B_3 = \begin{bmatrix} 4 & 5 \\ 4 & 6 \end{bmatrix}.$$

We know that V has a basis:

$$e_1 = E_{1,1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},\ e_2 = E_{1,2} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$e_3 = E_{2,1} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},\ e_4 = E_{2,2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

In this basis the coordinates of our vectors are the following:

$$v_1 = [B_1]_E = (2,2,3,0),$$
$$v_2 = [B_2]_E = (1,5,4,3),$$
$$v_3 = [B_3]_E = (4,5,4,6).$$

Using these coordinates we can build matrices:

$$\begin{bmatrix} 2 & 2 & 3 & 0 \\ 1 & 5 & 4 & 3 \\ 4 & 5 & 4 & 6 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 2 & 1 & 4 \\ 2 & 5 & 5 \\ 3 & 4 & 4 \\ 0 & 3 & 6 \end{bmatrix}.$$

So whenever a finite system of vectors in a finite-dimensional space is given, we can consider them as rows or columns of an appropriate matrix.

The reverse procedure also is possible: we can "brake down" any matrix to row- and column vectors. Namely for any matrix in $M_{m,n}(F)$:

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

we can consider its rows or columns as some of vectors in F^n or in F^m respectively:

$$v_1 = [a_{11}, \ldots, a_{1n}],$$
$$\ldots\ldots\ldots\ldots$$
$$v_m = [a_{m1}, \ldots, a_{mn}]$$

and

$$u_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \ldots, u_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix}.$$

The space spanned by the row vectors $v_1, \ldots, v_m$ is called *row space* of the matrix A, and is denoted by $\mathrm{row}(A)$; the space spanned by the column vectors $u_1, \ldots, u_n$ is called *column space* of A, and is denoted by $\mathrm{col}(A)$. Clearly, $\mathrm{row}(A)$ is a subspace in F^n while $\mathrm{col}(A)$ is a subspace in F^m.

Importantly, since each subspace U of F^n is at most n-dimensional, U is a row space $\mathrm{row}(A)$ for some matrix $A \in M_{n,n}(F)$. This allows to reduce consideration of any subspaces of F^n to row spaces of some matrices only. Further, if V is any n-dimensional abstract space other than F^n, then taking a coordinate map $\phi_E : V \to F^n$ we get a bijective correspondence between the subspaces of V and of F^n. I.e., row spaces of matrices are means to uniquely describe all the subspaces of V. Similar observations can be made for column spaces also.

Example 14.4. Let us consider the following real matrix:

$$A = \begin{bmatrix} 2 & 5 & 1 & 4 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 \end{bmatrix}.$$

It can be presented as

$$A = \begin{bmatrix} v_1 \\ \hdashline v_2 \\ \hdashline v_3 \end{bmatrix}$$

where $v_1 = (2,5,1,4)$, $v_2 = (0,1,2,0)$, $v_3 = (0,0,3,1)$. The row space $\mathrm{row}(A)$ is the subspace $\mathrm{span}(v_1, v_2, v_3)$. It is easy to see that

v_1, v_2, v_3 are linearly independent, so row(A) is a 3-dimensional proper subspace inside the 4-dimensional space $\mathbb{R}^4$.

The matrix A can also be presented as:

$$A = \left[\ u_1 \ \vdots\ u_2\ \vdots\ u_3\ \vdots\ u_4\ \right]$$

where

$$u_1 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}, u_2 = \begin{bmatrix} 5 \\ 1 \\ 0 \end{bmatrix}, u_3 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, u_4 = \begin{bmatrix} 4 \\ 0 \\ 1 \end{bmatrix}.$$

The column vectors u_1, u_2, u_3, u_4 are linearly dependent, since any four vectors of 3-dimensional space $\mathbb{R}^3$ are dependent by point 3 of Proposition 11.27.

On the other hand, three vectors u_1, u_2, u_3 evidently are linearly independent, and they form a basis of $\mathbb{R}^3$.

So we have:

$$\text{col}(A) = \mathbb{R}^3.$$

The following two "paired" lemmas will have have many applications below:

Lemma 14.5. *Elementary row-operations of any matrix $A \in M_{m,n}(F)$ do not alter*

1. *the row space* row(A) *of A, and*
2. *the linear dependence (or independence) of any subset of columns of A.*

***Proof*.** Let the matrix B be obtained from A by an elementary operation. Clearly, any new row that we obtain in B still is in row(A), and so row$(B) \subseteq$ row(A). Since each elementary operation is reversible, we can obtain A from B, and so row$(A) \subseteq$ row(B).

To prove the second point assume $u_{j_1}, \ldots, u_{j_s}$ are any s columns of A. Suppose they are linearly dependent, i.e., for some scalars $b_1, \ldots, b_s \in F$:

$$\vec{0} = b_1 u_{j_1} + \cdots + b_s u_{j_s} = b_1 \begin{bmatrix} a_{1j_1} \\ \vdots \\ a_{mj_1} \end{bmatrix} + \cdots + b_s \begin{bmatrix} a_{1j_s} \\ \vdots \\ a_{mj_s} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{14.1}$$

and $b_k \neq 0$ for a certain k. Clearly, swapping the i'th and j'th rows of A just swaps the i'th and j'th coordinates in all column vectors in (14.1) without altering that equality. The same for multiplying the i'th row of A by some non-zero scalar c, or for adding to the i'th row of A another j'th row multiplied by any scalar. So the columns with numbers $j_1, \ldots, j_s$ are linearly dependent in B also. And since each elementary operation is invertible, the columns $u_{j_1}, \ldots, u_{j_s}$ are dependent provided that the columns with the same numbers are dependent in B. □

Lemma 14.6. *If the matrix $R \in M_{m,n}(F)$ is in row-echelon form, then:*

1. *the non-zero rows of R form a basis for* row(R)*;*
2. *the pivot columns of R form a basis for* col(R)*.*

***Proof*.** Assume R is in row echelon form schematically presented as

$$R = \begin{array}{c} \begin{bmatrix} \boldsymbol{a_{1j_1}} & * & a_{1j_2} & * & a_{1j_3} & * \cdots * & a_{1j_r} & * \cdots * \\ & & \boldsymbol{a_{2j_2}} & * & a_{2j_3} & * \cdots * & a_{2j_r} & * \cdots * \\ & & & & \boldsymbol{a_{3j_3}} & * \cdots * & a_{3j_r} & * \cdots * \\ & & & & & & \cdots\cdots & \cdots\cdots \\ & & & & & & \boldsymbol{a_{rj_r}} & * \cdots * \\ & & & & & & & \\ \boldsymbol{0} & & & & & & & \end{bmatrix} \\ \begin{array}{cccccccc} j_1 & & j_2 & & j_3 & & j_r & \end{array} \end{array}, \tag{14.2}$$

where the $*$'s stand for blocks of any elements (for simplicity we may assume that the 1'st column is non-zero, i.e., $j_1 = 1$). Denote the first r non-zero rows by $v_1, \ldots, v_r$. Since the other $m - r$ rows of R are zero, row(R) is at most r-dimensional, so it will be enough to show that $v_1, \ldots, v_r$ are linearly independent. Assume for some $b_1, \ldots, b_r \in F$ we have $b_1v_1+\cdots+b_rv_r=0$. The j_1'st coordinate of this sum is $b_1a_{1j_1}+b_20+\cdots+b_r0=0$. Thus $b_1=0$, so we can ignore the summand b_1v_1, and get $b_2v_2+\cdots+b_rv_r=0$. Then j_2'nd coordinate of this new sum is $b_2a_{2j_2}+b_30+\cdots+b_r0=0$, and so $b_2=0$. Repeating these steps we get $b_1,\dots,b_r=0$.

Turning to the point **(2)** first notice that in each of the columns of (14.2) all the coordinates after the r'th coordinate are zero. Thus, $\mathrm{col}(R)$ is at most r-dimensional, and it will be enough to show that the r pivot columns are linearly independent. The pivot columns of R evidently are independent, which is easy to show by arguments similar to proof of the first point (applied to columns). □

The first applications of these lemmas are the methods of computations for row- and column spaces. Before we bring them let us first clear what we mean under *finding* row space, column space of a matrix A or, in general, *finding a space or subspace* V. This is a tricky question, since a space may contain *infinitely many* vectors, so to find a space we cannot write down its vectors one-by-one. The solution is *to find a basis* $E=\{e_1,\dots,e_n\}$ for V. This will allow to output the vectors of V as unique combinations $a_1e_1+\cdots+a_ne_n$ with coefficients a_i from the field.

How to find the row space of a matrix.

Algorithm 14.7 (Finding a basis for row space)**.** We are given a matrix $A\in M_{m,n}(F)$ over a field F.

► Find basis for the row space $\mathrm{row}(A)$.

1. Bring A to a row-echelon form R by elementary row-operations.

2. Output the set of all non-zero rows of R as a basis for $\mathrm{row}(A)$.

Example 14.8. Consider the following matrix A and its row-echelon form R:

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

$$R=\begin{bmatrix}\mathbf{1}&1&1&-1&1\\0&0&\mathbf{1}&3&0\\0&0&0&-\mathbf{7}&2\\0&0&0&0&0\end{bmatrix}.$$

We see that a basis for $\mathrm{row}(A)$ is formed by three vectors $e_1=(1,1,1,-1,1)$, $e_2=(0,0,1,3,0)$, $e_3=(0,0,0,-7,2)$.

Example 14.9. Take a matrix A over the finite field $\mathbb{Z}_7$:

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

(see Example 14.3). A row-echelon form of A is:

$$R=\begin{bmatrix}\mathbf{2}&2&3&0\\0&\mathbf{4}&6&3\\0&0&0&0\end{bmatrix},$$

which means that as a basis for $\mathrm{row}(A)$ we may take two vectors $e_1=(2,2,3,0)$, $e_2=(0,4,6,3)$.

How to find the column space of a matrix.

Algorithm 14.10 (Finding a basis for column space)**.** We are given a matrix $A\in M_{m,n}(F)$ over a field F.

► Find a basis for the column space $\mathrm{col}(A)$.

1. Bring A to a row-echelon form R by elementary row-operations.

2. If the pivots in R stand in columns with numbers $j_1,\dots,j_r$, then output the columns with numbers $j_1,\dots,j_r$ of A as a basis for $\mathrm{col}(A)$.

Proof. By Lemma 14.6 the pivot columns of R form a basis for $\mathrm{col}(R)$. And by Lemma 14.5 the columns with the same numbers form a basis in A. □

Example 14.11. A row-echelon form of the matrix A of Example 14.8 is

$$R = \begin{bmatrix} \mathbf{1} & 1 & 1 & -1 & 1 \\ 0 & 0 & \mathbf{1} & 3 & 0 \\ 0 & 0 & 0 & \mathbf{-7} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Thus, as a basis for $\operatorname{col}(A)$ we may take the 1'st, 3'rd and 4'th columns of A:

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

Example 14.12. For the matrix A of Example 14.9 we have computed the following row-echelon form:

$$R = \begin{bmatrix} \mathbf{2} & 2 & 3 & 0 \\ 0 & \mathbf{4} & 6 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

So as a basis for $\operatorname{col}(A)$ we can take the 1'st and 2'th columns of A:

$$\begin{bmatrix} 2 \\ 1 \\ 4 \end{bmatrix}, \quad \begin{bmatrix} 2 \\ 5 \\ 5 \end{bmatrix}.$$

Notice that both Algorithm 14.7 and Algorithm 14.10 also are methods for matrix rank calculation.

14.2. Subspaces and the matrix operations

This section collects some key facts connecting subspaces, linear independence, row-equivalence and the reduced row-echelon form.

Theorem 14.13. *The rank of any matrix $A \in M_{m,n}(F)$ is:*

1. *the maximal number of linearly independent rows of A;*
2. *the dimension of* $\operatorname{row}(A)$*;*
3. *the maximal number of linearly independent columns of A;*
4. *the dimension of* $\operatorname{col}(A)$*.*

Proof. $\operatorname{rank}(A)$ is equal to the number r of non-zero rows in any row-echelon form R of A. By Lemma 14.6 the non-zero rows of R form a basis for $\operatorname{row}(R)$, and by Lemma 14.5 $\operatorname{row}(R) = \operatorname{row}(A)$. So $r = \dim(\operatorname{row}(A))$.

Since each non-zero row of R holds one pivot, R has exactly r pivot columns. By Lemma 14.6 they form a basis for $\operatorname{col}(R)$, so $r = \dim(\operatorname{col}(R))$. But $\operatorname{col}(R)$ and $\operatorname{col}(A)$ have the same dimension, since elementary row-operations do not change linear dependence of columns by Lemma 14.5. □

Now we can add the following to Theorem 9.10 about equivalent conditions for invertible matrices, and to Corollary 13.7:

Corollary 14.14 (Amendment to Theorem 9.10). *A matrix $A \in M_{n,n}(F)$ is invertible if and only if:*

1. *the row vectors of A are linearly independent, or*
2. *the column vectors of A are linearly independent.*

Proof. By Theorem 9.10 the matrix A is invertible if and only if $A \sim \operatorname{rref}(A) = I_n$. The rows and columns of I_n always are linearly independent (as they form a standard basis) so for a square matrix $A \in M_{n,n}(F)$ the fact of having linearly independent rows and columns is equivalent to the condition $A \sim I_n$. □

Reduced row-echelon forms allow to prove the following classification theorem strengthening Theorem 7.13 and its Corollary 7.14:

Theorem 14.15. *Let $A, B \in M_{m,n}(F)$ be any matrices. Then the following conditions are equivalent:*

1. *A and B have the same row space:* $\mathrm{row}(A) = \mathrm{row}(B)$*;*
2. *A and B are row-equivalent: $A \sim B$;*
3. *A and B have the same reduced row-echelon form:* $\mathrm{rref}(A) = \mathrm{rref}(B)$*.*

***Proof*.** The theorem need be proved for non-zero matrices only. Since we by Corollary 7.14 already know that $A \sim B$ if and only if $\mathrm{rref}(A) = \mathrm{rref}(B)$, it is enough to show that $\mathrm{row}(A) = \mathrm{row}(B)$ if and only if $A \sim B$.

Moreover, by Lemma 14.5 from $A \sim B$ it follows that $\mathrm{row}(A) = \mathrm{row}(B)$. So the only tedious part is to suppose $\mathrm{row}(A) = \mathrm{row}(B)$, and to deduce $A \sim B$. Let R and S be some row-echelon forms of A and B respectively. It is enough to show that $R \sim S$.

By Theorem 14.13 and Lemma 14.5 we may denote $r = \mathrm{rank}(A) = \mathrm{rank}(B) = \mathrm{rank}(R) = \mathrm{rank}(S)$, and write:

$$R = \begin{bmatrix} u_1 \\ \hdashline \vdots \\ \hdashline u_m \end{bmatrix}, \quad S = \begin{bmatrix} v_1 \\ \hdashline \vdots \\ \hdashline v_m \end{bmatrix},$$

where only the first r rows are non-zero in R and in S. Since $v_1 \in U$, we can write $v_1 = a_1 u_1 + \cdots + a_r u_r$. We may require $a_1 \neq 0$ because, if not, we can (by elementary operations of the 2'nd type) reorder the rows $v_1, \ldots, v_r$ so that for the new row v_1 we get $a_1 \neq 0$ (this can be done because if *each* of $v_1, \ldots, v_r$ is a linear combination of $u_2, \ldots, u_r$, then $\mathrm{span}(v_1, \ldots, v_r)$ is *less* than U). Since $a_1 \neq 0$, we can apply to R the elementary operations $a_1 R1, \; R1 + a_2 R2, \; \ldots, \; R1 + a_r Rr$, and get a new matrix R in which the *first* row is v_1, and other rows are unchanged.

Since $\mathrm{row}(U)$ did not change, we can write v_2 as a linear combination of new rows of U: $v_2 = b_1 v_1 + b_2 u_2 + \cdots + a_r u_r$. We may require $b_2 \neq 0$ because, if not, we can reorder the rows $v_2, \ldots, v_r$ so that for the new row v_2 we have $b_2 \neq 0$ (if *each* of $v_2, \ldots, v_r$ is a linear combination of $v_1, u_3, \ldots, u_r$, then $\mathrm{span}(v_1, \ldots, v_r)$ is *less* than U). Since $b_2 \neq 0$, we can apply to R the elementary operations $b_2 R2, \; R2 + b_1 R1, \; R2 + b_3 R3, \; \ldots, \; R2 + b_r Rr$, and get a new R in which the *second* row also is replaced by v_2.

Continuing the procedure we by elementary operations bring R to S. □

Remark 14.16. An interesting outcome of this proof is that building new vectors *by any linear combination* of the vectors $u_1, \ldots, u_m$ in some sense is not a "stronger" operation than just *doing elementary row-operations* with $u_1, \ldots, u_m$ (as rows of some matrix). Elementary operations are simple *constructive bricks* by means of which all linear combinations can be "imitated" like in proof above.

Recall that for a given matrix $A \in M_{m,n}(F)$ we in Section 6.2 denoted by

$$\mathcal{R}_A = \{X \in M_{m,n}(F) \mid X \sim A\}$$

the class of all matrices of $M_{m,n}(F)$ row-equivalent to A. If it immaterial to mention the actual matrix A, we denote the class just $\mathcal{R}$ supposing that $\mathcal{R} = \mathcal{R}_A$ for an arbitrary $A \in \mathcal{R}$. By Theorem 14.15 each class $\mathcal{R}$ contains a unique matrix $A_{\mathcal{R}}$ in reduced row-echelon form.

In these notation let us again stress the three-fold "indicator" role of the reduced row-echelon form. In $M_{m,n}(F)$ there is a bijective correspondence between the classes $\mathcal{R}$ of row-equivalent matrices and the matrices in reduced row-echelon form: each such class $\mathcal{R}$ contains one matrix $A_{\mathcal{R}}$ which is the reduced row-echelon form $\mathrm{rref}(X)$ for any

$X \in \mathcal{R}$. Inversely, we can obtain any $X \in \mathcal{R}$ from $A_{\mathcal{R}}$ by some elementary operations. All matrices of $X \in \mathcal{R}$ have the same row space $\text{row}(X) = \text{row}(A_{\mathcal{R}})$, and the non-zero rows of $A_{\mathcal{R}}$ from a basis for it.

Moreover, since each subspace U of F^n is a row space for some matrix in $M_{m,n}(F)$ for certain $m \le n$, we get a bijective correspondence between the matrices $A \in M_{n,n}(F)$ in reduced row-echelon form and the subspaces U of F^n. More precisely, to an r-dimensional subspace of F^n corresponds a reduced row-echelon matrix with exactly r non-zero rows. Finally, if V is an n-dimensional space other than F^n, then fixing a coordinate system in V we again get a bijective correspondence between the subspaces U of V and the $n \times n$ matrices in reduced row-echelon form.

Example 14.17. In $\mathbb{R}^3$ all the 1-dimensional subspaces are lines ℓ passing via the origin O.

All the reduced row-echelon matrices in $M_{3,3}(\mathbb{R})$ with only one non-zero row are of the following three types:

$$\begin{bmatrix} \mathbf{1} & a_{12} & a_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \mathbf{1} & a_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Clearly the vectors $(1, a_{12}, a_{13})$, $(0, 1, a_{13})$, $(0, 0, 1)$ (for all $a_{12}, a_{13} \in \mathbb{R}$) do cover all possible directions for ℓ.

Adding three more matrix types:

$$\begin{bmatrix} \mathbf{1} & 0 & a_{13} \\ 0 & \mathbf{1} & a_{23} \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} \mathbf{1} & a_{12} & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix}$$

we get all the 2-dimensional subspaces of $\mathbb{R}^3$.

To cover all the remaining subspaces of $\mathbb{R}^3$ we just need add two more matrices: the only reduced row-echelon matrix of rank 3, i.e., the identity matrix I_3, and the zero matrix corresponding to the zero subspace.

Example 14.18. Especially simple is the situation for spaces of finite fields, since in this case the number of reduced row-echelon matrices is finite only. Say, if $F = \mathbb{Z}_p$, then in previous example we get $p^2 + p$ options for matrices with one non-zero row, and again $p^2 + p$ options for matrices with two non-zero rows. Therefore, $\mathbb{Z}_p^3$ has $2(p^2 + p) + 2 = 2(p^2 + p + 1)$ subspaces in total.

14.3. Matrix computation methods in spaces

The results we obtained above allow us to build methods based on row- and column space technique, using row-echelon and reduced row-echelon forms. As agreed above, under finding a space we understand finding a *basis* for it.

How to find a basis for a subspace (span of vectors), first method. A slight adaptation of Algorithm 14.7 allows to find a subspace given as a span of vectors:

Algorithm 14.19 (Finding a basis for a subspace (span of vectors), first method)**.** We are given a set of vectors $v_1, \ldots, v_m$ in an n-dimensional space V over a field F.

► Find a basis for the subspace $U = \text{span}(v_1, \ldots, v_m)$.

1. If $V = F^n$, then the vectors $v_1, \ldots, v_m$ are sequences of length n, and we form a matrix by their coordinates, putting them by *rows*:

$$A = \begin{bmatrix} v_1 \\ \cdots \\ v_m \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}. \tag{14.3}$$

2. Else, if V is another space, fix any coordinate system in V with a basis E and a coordinate map $\phi_E : V \to F^n$, and build the matrix A putting the respective coordinate vectors $[v_1]_E, \ldots, [v_m]_E$ by *rows*.

3. Bring A to a row-echelon form R by elementary row-operations.
4. If $V = F^n$, then output the set $[w_1], \ldots, [w_r]$ of all non-zero rows of R as a basis for the subspace U.
5. Else, if V is another space, output as a basis for U the unique vectors $w_1, \ldots, w_r \in V$ corresponding to $[w_1], \ldots, [w_r]$, i.e., $w_i = \phi_E^{-1}([w_i])$ for $i = 1, \ldots, r$.

Example 14.20. Consider the vectors $v_1 = (1,1,1,-1,1)$, $v_2 = (2,2,3,1,2)$, $v_3 = (1,1,2,2,1)$, $v_4 = (-1,-1,1,0,1)$ in $\mathbb{R}^5$. Using these vectors in Algorithm 14.19 we can form a matrix A. To save space we have taken the vectors so that we get the matrix A of the above Example 14.8. Its row-echelon form R is computed in Example 14.8, and it has three non-zero rows $w_1 = (1,1,1,-1,1)$, $w_2 = (0,0,1,3,0)$, $w_3 = (0,0,0,-7,2)$ forming a basis for $U = \operatorname{span}\big(v_1, v_2, v_3, v_4\big)$.

We also get that $\{v_1, v_2, v_3, v_4\}$ contains a subset of three linearly independent vectors, since $\dim(U) = 3$. We do not yet know *which* three vectors they are.

Example 14.21. The polynomials

$$f_1(x) = 1 + 2x + 3x^2,$$
$$f_2(x) = 3 + 5x^2$$

from Example 14.2 can be presented as row vectors with respect to the basis $\{1, x, x^2\}$ to construct the matrix

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

Since the latter has a row-echelon form

$$R = \begin{bmatrix} \mathbf{1} & 2 & 3 \\ 0 & \mathbf{-6} & -4 \end{bmatrix},$$

the polynomials $1 + 2x + 3x^2$ (this actually is $f_1(x)$) and $-6x - 4x^2$ form a basis of the space $U = \operatorname{span}(f_1, f_2)$. And as U is 2-dimensional, *any* spanning set with two vectors already is a basis for it (see point 6 in Proposition 11.27). That is, $f_1(x)$ and $f_2(x)$ also form a basis for the span U.

Example 14.22. For the matrices B_1, B_2, $B_3 \in M_{2,2}(\mathbb{Z}_7)$ in Example 14.3 we have already built the matrix

$$A = \begin{bmatrix} [B_1]_E \\ \hdashline [B_2]_E \\ \hdashline [B_3]_E \end{bmatrix} = \begin{bmatrix} 2 & 2 & 3 & 0 \\ 1 & 5 & 4 & 3 \\ 4 & 5 & 4 & 6 \end{bmatrix}$$

with respect to the basis $E_{1,1}$, $E_{1,2}$, $E_{2,1}$, $E_{2,2}$ of the space $M_{2,2}(\mathbb{Z}_7)$. A row-echelon form of A is:

$$R = \begin{bmatrix} \mathbf{2} & 2 & 3 & 0 \\ 0 & \mathbf{4} & 6 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which means that a basis for the span $U = \operatorname{span}(B_1, B_2, B_3)$ may consist of two matrices

$$E_1 = \begin{bmatrix} 2 & 2 \\ 3 & 0 \end{bmatrix} = \phi_E^{-1}(2,2,3,0),$$

$$E_2 = \begin{bmatrix} 0 & 4 \\ 6 & 3 \end{bmatrix} = \phi_E^{-1}(0,4,6,3).$$

Since $\{E_1, E_2\}$ is a basis for U, the vectors B_1, B_2, B_3 contain a subset of $2 = \dim(U)$ linearly independent vectors. But we do not yet know *which* two matrices they are.

How to detect linear dependence.

Algorithm 14.23 (Linear dependence detection)**.** We are given a set of vectors $v_1, \ldots, v_m$ in an n-dimensional space V over a field F.

► Detect if or not the vectors $v_1, \ldots, v_m$ are linearly dependent.

1. If $V = F^n$, form the matrix A of (14.3) by the coordinates of the vectors $v_1, \ldots, v_m$.
2. Else, if V is another space, fix any coordinate system in V with a basis E, and build the matrix (14.3) using the respective coordinate vectors $[v_1]_E, \ldots, [v_m]_E$.
3. Bring A to a row-echelon form R by elementary row-operations.
4. If the last row of R is zero, then $v_1, \ldots, v_m$ are linearly dependent, else they are linearly independent.

Proof. The vectors $v_1, \ldots, v_m$ are linearly independent if and only if they form a basis for $U = \operatorname{span}(v_1, \ldots, v_m)$, i.e., if $\dim(U) = m$. By Lemma 14.6 the non-zero rows of R form a basis for row(A). Since row(A) = row(R), we just need check if the last row in R is non-zero. □

Checking the above examples we see that the vectors $v_1, v_2, v_3, v_4 \in \mathbb{R}^5$ of Example 14.20 and the vectors (matrices) B_1, B_2, $B_3 \in M_{2,2}(\mathbb{Z}_7)$ of Example 14.22 are linearly dependent, whereas the vectors (polynomials) $f_1(x), f_2(x) \in \mathcal{P}_2(\mathbb{R})$ of Example 14.21 are linearly independent.

For the given $v_1, \ldots, v_m$ we are able to build a basis the span $U = \operatorname{span}(v_1, \ldots, v_m)$, and to find its dimension $r = \dim(U)$. In particular, we know that $v_1, \ldots, v_m$ contains *a maximal subset of exactly r linearly independent vectors*. However, we were not yet able to find *which* r vectors of $v_1, \ldots, v_m$ do actually form that subset (see examples 14.20 and 14.22 above). We answer this question using column spaces technique (see Algorithm 14.10):

How to find a maximal linearly independent subset.

Algorithm 14.24 (Finding a maximal linearly independent subset)**.** We are given a set of vectors $\{v_1, \ldots, v_m\}$ in an n-dimensional space V over a field F.

► Find a maximal linearly independent subset of $\{v_1, \ldots, v_m\}$.

1. If $V = F^n$, then the vectors are the sequences:

$$\begin{aligned} v_1 &= (a_{11}, \ldots, a_{1n}), \\ &\ldots\ldots\ldots\ldots \\ v_m &= (a_{m1}, \ldots, a_{mn}), \end{aligned}$$

and we form a matrix putting their coordinates by *columns*:

$$A = \left[\, v_1 \;\vdots\; \cdots \;\vdots\; v_m \,\right] = \begin{bmatrix} a_{11} & \cdots & a_{m1} \\ \ldots & \ldots & \ldots \\ a_{1n} & \cdots & a_{mn} \end{bmatrix}. \tag{14.4}$$

2. If V is another space, fix any coordinate system with a basis E, and build the matrix (14.4) putting the respective coordinate vectors $[v_1]_E, \ldots, [v_m]_E$ by *columns*.

3. Bring A to a row-echelon form R by elementary row-operations.

4. If the pivots in R stand in columns with numbers $j_1, \ldots, j_r$, then output as a maximal linearly independent subset the set $\{v_{j_1}, \ldots, v_{j_r}\}$.

Proof. Directly follows from the previous Algorithm 14.10. □

Example 14.25. Turn back to the vectors v_1, v_2, v_3, v_4 of examples 14.20 and 14.8. We already know their span is 3-dimensional.

Put the coordinates of these vectors by columns in a matrix A and compute any of its row-echelon forms.

I.e, consider the matrix:

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

and compute the row-echelon form:

$$R = \begin{bmatrix} \mathbf{1} & 2 & 1 & -1 \\ 0 & \mathbf{1} & 1 & 2 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since the pivots stand in 1'st, 2'nd and 4'th columns, the maximal linearly independent subset we look for is v_1, v_2, v_4.

Comparing these with Example 14.20 we also get that v_1, v_2, v_4 and w_1, w_2, w_3 both are bases for the $\operatorname{span}\big(v_1, v_2, v_3, v_4\big) = \operatorname{col}(A)$.

Notice that the vectors v_1, v_2, v_3 are *not* linearly independent.

Also notice that in Example 14.11 we placed the coordinates of the same vectors by rows, and arrived to other results.

Example 14.26. Let us find a maximal linearly independent subset for matrix-vectors over $\mathbb{Z}_7$ of Example 14.3.

$$B_1 = \begin{bmatrix} 2 & 2 \\ 3 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 & 5 \\ 4 & 3 \end{bmatrix}, \quad B_3 = \begin{bmatrix} 4 & 5 \\ 4 & 6 \end{bmatrix}$$

(in Example 14.22 we have already found that their number is two).

Using the coordinate system with basis $E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}$ we have already presented the matrices as

$$[B_1]_E = (2,2,3,0)$$
$$[B_2]_E = (1,5,4,3)$$
$$[B_3]_E = (4,5,4,6).$$

Putting the coordinates by columns we get a matrix A and its row-echelon form R:

$$A = \begin{bmatrix} 2 & 1 & 4 \\ 2 & 5 & 5 \\ 3 & 4 & 4 \\ 0 & 3 & 6 \end{bmatrix}, \quad R = \begin{bmatrix} \mathbf{2} & 1 & 4 \\ 0 & \mathbf{4} & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

In R the pivots stand in columns number $1, 2$. The maximal linearly independent subset we look for is B_1, B_2.

Of course, the maximal linearly independent subset $\{v_{j_1}, \dots, v_{j_r}\}$ provided by Algorithm 14.24 is *not* the only such maximal subset possible, and $\{v_1, \dots, v_m\}$ may also possess other maximal linearly independent subsets. Say, for Example 14.25 it can be directly verified that the vectors v_1, v_3, v_4 also are linearly independent.

How to find a basis for a subspace (span of vectors), second method. The previous algorithm also suggests another method to find a basis for a subspace given by its spanning vectors.

Algorithm 14.27 (Finding a basis for a subspace (span of vectors), second method)**.** We are given a set of vectors $v_1, \dots, v_m$ in an n-dimensional space V over a field F.

► Choose a basis for the subspace $U = \text{span}(v_1, \dots, v_m)$ among the vectors $v_1, \dots, v_m$.

1. Using the vectors $v_1, \dots, v_m$ as input for Algorithm 14.24 find a maximal linearly independent subset $\{v_{j_1}, \dots, v_{j_r}\}$ of $\{v_1, \dots, v_m\}$.

2. Output $\{v_{j_1}, \dots, v_{j_r}\}$ as a basis for U.

As examples for application of this algorithm we may adapt Example 14.25 where we found a basis $\{v_1, v_2, v_4\}$ for $\text{span}\big(v_1, v_2, v_3, v_4\big)$ in $V = \mathbb{R}^5$, and Example 14.26 where we got a basis $\{B_1, B_2\}$ for $\text{span}(B_1, B_2, B_3)$ in $V = M_{2,2}(\mathbb{Z}_7)$.

Remark 14.28. Let us compare the weak and strong sides of two generic processes we suggested. Going by the first processes (Algorithm 14.19) we build a matrix A by putting the vector coordinates by *rows*, then bring A to a row-echelon form R, and then take the non-zero row vectors $w_1, \dots, w_r$ of R as a basis for the row space. Since a row-echelon form typically contains many zeros, we get a relatively uncomplicated basis with some coordinates zero. However, although this process preserves the subspace $\text{span}(v_1, \dots, v_m) = \text{span}(w_1, \dots, w_r)$ or $\text{row}(A)$, it "forgets" which are the linearly independent vectors among $v_1, \dots, v_m$ (even if we do not use the row swapping elementary operation at all).

Going by the second processes (Algorithm 14.27) we build a matrix A by putting the vector coordinates by *columns*, then bring A to a row-echelon form R. If the pivot columns have numbers $j_1, \dots, j_r$, then the basis we are looking for is $\{v_{j_1}, \dots, v_{j_r}\}$. Although this process preserves the numbers $j_1, \dots, j_r$ of linearly independent vectors, it "forgets" the subspace $\text{span}(v_1, \dots, v_m)$: the pivot columns of R may no longer span it. All we know is: $\text{span}(v_1, \dots, v_m) = \text{span}\big(v_{j_1}, \dots, v_{j_r}\big)$. We now know which of the vectors $v_1, \dots, v_m$ to pick, but this time we loose the chance to get vectors with many zero coordinates.

How to present a vector as a linear combination. Earlier we handled this solving a system of linear equations. We can shorten this process also:

Algorithm 14.29 (Presenting a vector as a linear combination)**.** We are given vectors u, $v_1, \ldots, v_m$ in an n-dimensional space V over a field F.

► Detect if or not u can be presented as a linear combination of $v_1, \ldots, v_m$. If yes, find the coefficients of the presentation.

1. If $V = F^n$, then our vectors are the sequences:

$$\begin{aligned} u \; &= (b_1, \ldots, b_n), \\ v_1 &= (a_{11}, \ldots, a_{1n}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ v_m &= (a_{m1}, \ldots, a_{mn}), \end{aligned}$$

and we form a matrix putting their coordinates by *columns*:

$$A = \left[\; v_1 \;\vdots\; \cdots \;\vdots\; v_m \;\vdots\; u \;\right] = \begin{bmatrix} a_{11} & \cdots & a_{m1} & b_1 \\ \ldots & \ldots & \ldots & \ldots \\ a_{1n} & \cdots & a_{mn} & b_n \end{bmatrix}. \tag{14.5}$$

2. If V is another space, fix a coordinate system with $E = \{e_1, \cdots, e_n\}$, and build the matrix (14.5) by putting the coordinate vectors $[v_1]_E, \ldots, [v_m]_E, [u]_E$ by *columns*.

3. Bring A to a row-echelon form R by elementary row-operations.

4. If the last column of R is a pivot column, then u cannot be presented as a linear combination of $v_1, \ldots, v_m$. End of the process.

5. Else bring R to the reduced row-echelon form $\mathrm{rref}(A)$ by elementary row-operations.

6. If the pivots in $\mathrm{rref}(A)$ stand in columns with numbers $j_1, \ldots, j_r$, then output the linear combination $u = c_1 v_{j_1} + \cdots + c_r v_{j_r}$, where the coefficients $c_1, \ldots, c_r$ are the first r entries in the last column of $\mathrm{rref}(A)$. If needed, we can add the remaining vectors with zero coefficients.

***Proof*.** u is a linear combination of $v_1, \ldots, v_m$ if and only if the system of linear equations $AX = [u]$ is consistent. Solving it by the Gauss-Jordan method, after we find the pivot columns, we move the free variables to the right hand side, and assign them any values to get a solution of $AX = [u]$. As a possible choice for them we can take zero values. This outputs the combination of point 6 above. □

Example 14.30. Let us find if $u = (5, 2, 2, 5)$ is a linear combination of vectors $v_1 = (3, 0, 6, 9)$, $v_2 = (3, 1, 2, 4)$, $v_3 = (8, 4, 0, 4)$. The matrix A and R are:

$$A = \begin{bmatrix} 3 & 3 & 8 & 5 \\ 0 & 1 & 4 & 2 \\ 6 & 2 & 0 & 2 \\ 9 & 4 & 4 & 5 \end{bmatrix},$$

$$R = \begin{bmatrix} \mathbf{1} & 1 & \frac{8}{3} & \frac{5}{3} \\ 0 & \mathbf{1} & 4 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since the last column of $\mathrm{rref}(A)$ is not pivot, the linear combination is possible, and we calculate:

$$\mathrm{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & -\frac{4}{3} & -\frac{1}{3} \\ 0 & \mathbf{1} & 4 & \mathbf{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

As the coefficients of the linear combination we can take two first elements of the last column. Namely:

$$u = -\tfrac{1}{3} v_1 + 2 v_2.$$

If needed, we can add v_3, too:

$$u = -\tfrac{1}{3} v_1 + 2 v_2 + 0 v_3.$$

If we in this example change u to $u' = (5,2,2,6)$ (only the last coordinate is changed), then the respective R' will be:

$$R' = \begin{bmatrix} \mathbf{1} & 1 & \frac{8}{3} & \frac{5}{3} \\ 0 & \mathbf{1} & 4 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

The last column holds a pivot, so u' is *not* a linear combination of v_1, v_2, v_3.

Example 14.31. Let us detect if the polynomial $g(x) = 6 + 4x + 3x^2$ is the linear combination of $f_1(x) = -3 - x - 2x^2$, $f_2(x) = 2 + 4x + 2x^2$, $f_3(x) = 6 + 3x$ (all polynomials are in $\mathcal{P}_2(\mathbb{R})$). Take the coordinate system with the ordered basis $\{1, x, x^2\}$. Then

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

$$\text{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & 0 & -1 \\ 0 & \mathbf{1} & 0 & \frac{1}{2} \\ 0 & 0 & \mathbf{1} & \frac{1}{3} \end{bmatrix}.$$

We, thus, have:

$$g(x) = -f_1(x) + \tfrac{1}{2} f_2(x) + \tfrac{1}{3} f_3(x).$$

And we also know that this is the *only* possible presentation of $g(x)$ as a linear combination of $f_1(x)$, $f_2(x)$, $f_3(x)$.

Exercises

E.14.1. We are given the matrices:

$$A = \begin{bmatrix} 0 & 2 & 4 & 0 \\ 2 & 1 & 3 & 1 \\ 2 & 0 & 1 & 1 \\ 4 & 2 & 6 & 2 \end{bmatrix} \in M_{4,4}(\mathbb{R}), \quad B = \begin{bmatrix} 1 & 2 & 1 & 1 & 1 \\ 3 & 1 & 0 & 1 & 1 \\ 1 & 3 & 0 & 0 & 1 \end{bmatrix} \in M_{3,5}(\mathbb{R}), \quad C = \begin{bmatrix} 1 & 2 & 4 \\ 2 & 4 & 3 \\ 0 & 1 & 2 \\ 0 & 3 & 1 \end{bmatrix} \in M_{4,3}(\mathbb{Z}_5).$$

Using Algorithm 14.7 compute the row space of each matrix by finding a basis for it.

E.14.2. By Algorithm 14.19 find the subspace $U = \text{span}(S)$ spanned by the vectors set S of the space V, and indicate if $U = V$ provided that **(1)** S consists of vectors $u_1 = [0,2,4,0]$, $u_2 = [2,1,3,1]$, $u_3 = [2,0,1,1]$, $u_4 = [4,2,6,2]$ in $\mathbb{R}^4$. **(2)** S consists of vectors $v_1 = [1,2,1,1,1]$, $v_2 = [3,1,0,1,1]$, $v_3 = [1,3,0,0,1]$ in $\mathbb{R}^5$. **(3)** S consists of vectors $w_1 = [1,2,4]$, $w_2 = [2,4,3]$, $w_3 = [0,1,2]$, $w_4 = [0,3,1]$ in $\mathbb{Z}_5^3$. *Hint*: you may use your computations already done for Exercise 14.1.

E.14.3. Compute the subspace $U = \text{span}(f_1(x), f_2(x), f_3(x))$ in $\mathcal{P}_3(\mathbb{R})$, if $f_1(x) = 1 + 2x - x^2$, $f_2(x) = x + x^2$, $f_3(x) = -1 + x$. *Hint*: you may use the coordinate map $\phi_E : \mathcal{P}_3(\mathbb{R}) \to \mathbb{R}^4$ to represent the polynomials by sequences (see step 2 in Algorithm 14.19).

E.14.4. Using Algorithm 14.23 detect if the following vectors form a linearly independent set: **(1)** $u_1 = [2,4,4]$, $u_2 = [0,-3,-2]$, $u_3 = [1,5,4]$, $u_4 = [3,12,10]$ in $\mathbb{R}^3$. **(2)** $v_1 = \left[\begin{smallmatrix} 1 & 0 \\ 2 & 2 \end{smallmatrix}\right]$, $v_2 = \left[\begin{smallmatrix} 0 & 2 \\ 2 & 4 \end{smallmatrix}\right]$, $v_3 = \left[\begin{smallmatrix} 1 & 1 \\ 3 & 4 \end{smallmatrix}\right]$ in $M_{2,2}(\mathbb{R})$.

E.14.5. Earlier you may have solved Exercise 11.2 by composing systems of linear equations. Compare those solutions with the method of Algorithm 14.23. Solve the exercise Exercise 11.2 (1) using this algorithm.

E.14.6. Find the column spaces of matrices A, B, C of Exercise E.14.1 using Algorithm 14.10.

E.14.7. Using Algorithm 14.24 find a maximal subset of linearly independent vectors for each of two vectors sets in Exercise E.14.4.

E.14.8. Let $U = \text{span}(f_1(x), f_2(x), f_3(x))$ be the subspace given in Exercise E.14.3. By Algorithm 14.27 choose among the vectors $f_1(x), f_2(x), f_3(x)$ a basis for U.

E.14.9. Using Algorithm 14.29 present the vector $u = (1,1,5,0)$ as a linear combination of vectors $v_1 = (1,0,2,0)$, $v_2 = (1,2,1,1)$, $v_3 = (2,1,0,1)$.

E.14.10. We are given the vectors $v_1 = (2,-1,1)$, $v_2 = (-4,2,-2)$, $v_3 = (1,0,2)$, $v_4 = (0,-2,1)$ in $V = \mathbb{R}^3$. **(1)** Find a basis for the subspace spanned by v_1, v_2, v_3, v_4 using Algorithm 14.19. **(2)** From the result of the first point can you deduce that $\text{span}(v_1, v_2, v_3, v_4) = V$? **(3)** From the result of the first and second points can you deduce that the basis for $\text{span}(v_1, v_2, v_3, v_4)$ is $\{v_1, v_2, v_3\}$? **(4)** Using Algorithm 14.23 detect if the vectors v_1, v_2, v_3 are linearly independent. **(5)** Find a maximal linearly independed subset among the vectors v_1, v_2, v_3, v_4 by Algorithm 14.24 Do these vectors span the same subspace as the basis found in point 1? **(6)** Present the vector $u = (7,7,7)$ as a linear combination of vectors v_1, v_2, v_3, v_4 by Algorithm 14.29.

E.14.11. In the 4-dimensional space $V = \mathbb{R}^4$ we have the vectors $u_1 = (1,0,2,1)$, $u_2 = (0,1,2,0)$, $u_3 = (1,1,4,1)$, $u_4 = (1,0,1,2)$ which span the subspace $U = \text{span}(u_1, u_2, u_3, u_4)$. **(1)** Using Algorithm 14.19 find $\dim(U)$, and construct a basis for U. Deduce from here if or not $U = V$. **(2)** Using Algorithm 14.23 detect if the vectors u_1, u_2, u_3 are linearly independent. Deduce from here if or not $\text{span}(u_1, u_2, u_3) = U$. **(3)** Using Algorithm 14.24 find a maximal linearly independed set of vectors u_1, u_2, u_3, u_4. Do they span the same subspace as the basis found in point **1** above?

E.14.12. In the real space $V = \mathbb{R}^3$ we are given three vectors $e_1 = (2,1,0)$, $e_2 = (0,1,2)$, $e_3 = (1,0,1)$, **(1)** By any method show that $E = \{e_1, e_2, e_3\}$ is a basis in V. **(2)** By Algorithm 14.29 find the coordinates $[w]_E$ of the vector $w = (4,3,6)$ in the basis E.

E.14.13. Show that the points of Lemm. 14.5 cannot be generalized for the column space and for the linear dependence of rows. Namely: **(1)** Find a matrix A such that its column space *can* be changed by an elementary operation. **(2)** Find a matrix B in which on some rows number $i_1, \ldots, i_s$ we have linearly independent vectors, but after an elementary operation we get dependent vectors on the rows with *same* numbers.

E.14.14. We are given the real vectors $u_1 = (1,0,2)$, $u_2 = (-1,1,1)$, $v_1 = (-1,3,7)$, $v_2 = (3,-2,0)$ and the matrices $A = \left[\begin{smallmatrix} u_1 \\ u_2 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right]$ composed by them. **(1)** Using Algorithm 14.24 detect if v_1 and v_2 can be presented as linear combinations of u_1 and u_2. **(2)** Using the previous point compare $\text{row}(A)$ and $\text{row}(B)$. **(3)** Then using Theorem 14.15 deduce *without any calculations* if A and B can be obtained from each other by elementary row-operations. **(4)** (Optional) using the steps of the proof for Theorem 14.15 obtain B from A by elementary operations. **(5)** Without any new calculations deduce by Theorem 14.15 if $\text{rref}(A) = \text{rref}(B)$. **(6)** Using the previous point obtain B from A in one more way: bring both A and B to their reduced row-echelon forms, compare them. *Hint*: you may use reverse elementary operations at some step.

CHAPTER 15

The null space and solutions of systems of linear equations

15.1. The null space of a matrix

Another important subspace related to a matrix $A \in M_{m,n}(F)$ is its *null space*: the space null(A) of all solutions of the homogeneous system of linear equations $AX = O$ for the matrix A. In Example 10.8 and Example 10.16 we have shown that null(A) actually is a space, and it is a subspace of F^n. Its dimension dim(null(A)) is called *nullity* of A, and is denoted by nullity(A).

The following theorem (often called *"rank-nullity theorem"*) and its proof technique allow us to find a basis for null(A) and the dimension nullity(A).

Theorem 15.1. *For any matrix $A \in M_{m,n}(F)$ the sum of its rank and nullity is equal to n:*

$$\mathbf{rank}(A) + \mathbf{nullity}(A) = n.$$

***Proof*.** Let us solve the homogeneous system of linear equations $AX = O$ using the Gauss-Jordan method by bringing A to the reduced row-echelon form rref(A). Assume its rank is r, i.e., rref(A) has r non-zero rows and r pivots. For simplicity of notation assume the pivots are in the first r columns:

$$\text{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & 0 & \cdots & 0 & a_{1r+1} & \cdots & a_{1n} \\ & \mathbf{1} & 0 & \cdots & 0 & a_{2r+1} & \cdots & a_{2n} \\ & & & & \cdots & \cdots & \cdots & \cdots \\ & & & & \mathbf{1} & a_{rr+1} & \cdots & a_{rn} \\ & & & & & & & \\ \mathbf{0} & & & & & & & \end{bmatrix}. \tag{15.1}$$

$AX = O$ has r pivot variables $x_1, \dots, x_r$ and $n - r$ free variables $x_{r+1}, \dots, x_n$. To solve the system we should move the free variables to the right-hand side

$$\begin{cases} x_1 \qquad\qquad = -a_{1r+1}x_{r+1} - \cdots - a_{1n}x_n \\ \quad x_2 \qquad\quad = -a_{2r+1}x_{r+1} - \cdots - a_{2n}x_n \\ \qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \qquad\qquad x_r = -a_{rr+1}x_{r+1} - \cdots - a_{rn}x_n, \end{cases}$$

then assign them any values, and compute the values of pivot variables $x_1, \dots, x_r$.

If we assign the values as follows: $x_{r+1} = -1, x_{r+2} = 0, \dots, x_n = 0$, then the values for $x_1, \dots, x_r$ will be equal to the first r entries of the $(r+1)$'th column of rref(A). Denote this solution of the system by e_1. Next assign: $x_{r+1} = 0, x_{r+2} = -1, \dots, x_n = 0$. The values for $x_1, \dots, x_r$ will be equal to the first r entries of the $(r+2)$'th column of rref(A).

Denote this solution by e_2. Continue the process, and on the $(n-r)$'th step eventually assign: $x_{r+1} = 0, x_{r+2} = 0, \ldots, x_n = -1$. The values for $x_1, \ldots, x_r$ will be the first r entries of the n'th column of rref(A). Denote this solution by e_{n-r}. We get $n-r$ solutions

$$e_1 = \begin{bmatrix} a_{1r+1} \\ \vdots \\ a_{rr+1} \\ \mathbf{-1} \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} a_{1r+2} \\ \vdots \\ a_{rr+2} \\ 0 \\ \mathbf{-1} \\ \vdots \\ 0 \end{bmatrix}, \quad e_{n-r} = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{rn} \\ 0 \\ 0 \\ \vdots \\ \mathbf{-1} \end{bmatrix}. \tag{15.2}$$

Which, clearly, are linearly independent in F^n.

It is easy to show that *any* solution of $AX = O$ is a linear combination of the vectors of (15.2). Indeed, if $g = (c_1, \ldots, c_r,\ c_{r+1}, \ldots, c_n)$ is any such solution, g is uniquely defined by the values assigned to the free variables: $x_{r+1} = c_{r+1}, \ldots, x_n = c_n$. But we already have a solution with exactly those values for free variables: the linear combination $-c_{r+1}e_1 - \cdots - c_n e_{n-r}$. Thus, g is equal to this combination, and (15.2) is a spanning set, thus, also a basis for null(A).

The general case when the pivots are not the first r columns of rref(A), but are in arbitrary r columns with numbers $j_1, \ldots, j_r$, is similar to the above. In that case we move to the right-hand side the free variables $x_{t_1}, \ldots, x_{t_{n-r}}$. We get the analogs of the $n-r$ vectors (15.2) with following differences: the values -1 and 0 for free variables stand not in the last $n-r$ coordinates, but in coordinates number $t_1, \ldots, t_{n-r}$. And the values for r pivot variables stand not in the first r coordinates, but in coordinates number $j_1, \ldots, j_r$. □

Notice that in the above proof we could take other values for free variables (for example, using 1 instead of -1 would be sufficient for this proof), but we intentionally took those values which allow to *directly use the columns* of rref(A) in construction of the basis vectors $e_1, \ldots, e_{n-r}$. In other words, the solutions of the system $AX = O$ *already are partially present* in the columns of rref(A), and we just add some extra 0's and -1's.

How to find a basis for null space. The method of the proof for Theorem 15.1 gives us:

Algorithm 15.2 (Finding a basis for null space)**.** We are given a matrix $A \in M_{m,n}(F)$ over a field F.

► Find a basis for the null space null(A).

1. Bring A to the reduced row-echelon form rref(A) by elementary row-operations.
2. Set r to be the rank of A, i.e., the number of non-zero rows in rref(A).
3. Set $j_1, \ldots, j_r$ to be the numbers of pivot columns of rref(A), and set $t_1, \ldots, t_{n-r}$ to be the numbers of non-pivot columns of rref(A) (both sequences in ascending order).
4. For each $i = 1, \ldots, n-r$ define a vector e_i in F^n as follows:
   all the coordinates number $t_1, \ldots, t_{n-r}$ in e_i are 0, except t_i'th coordinate -1;
   the coordinates number $j_1, \ldots, j_r$ in e_i are equal to the first r entries in the t_i'th column of rref(A).
5. Output $\{e_1, \ldots, e_{n-r}\}$ as a basis for null(A).

$$A \sim \operatorname{rref}(A) = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 2 & 0 & 3 \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \underset{e_1}{\begin{bmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix}} \quad \underset{e_2}{\begin{bmatrix} -1 \\ 3 \\ 0 \\ 4 \\ -1 \end{bmatrix}} \qquad \operatorname{null}(A) = \operatorname{span}(e_1, e_2)$$

FIGURE 15.1. Construction of a basis $\{e_1, e_2\}$ for null(A).

Example 15.3. Let us find a basis for the null space of the matrix:

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

The matrix A has the reduced row-echelon form:

$$\operatorname{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & 1 & 0 & -1 \\ 0 & \mathbf{1} & 2 & 0 & 3 \\ 0 & 0 & 0 & \mathbf{1} & 4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We have $r = \operatorname{rank}(A) = 3$ and $\operatorname{nullity}(A) = n - r = 2$. So the solutions space null(A) is a 2-dimensional subspace of $\mathbb{R}^5$. To find the basis of null(A) move two free variables x_3 and x_5 to the right-hand side. First assign them the values $x_3 = -1, x_5 = 0$ and find the solution

$$e_1 = \begin{bmatrix} 1 \\ 2 \\ \mathbf{-1} \\ 0 \\ \mathbf{0} \end{bmatrix}.$$

Next assign them the values $x_3 = 0, x_5 = -1$ and find the solution

$$e_2 = \begin{bmatrix} -1 \\ 3 \\ \mathbf{0} \\ 4 \\ \mathbf{-1} \end{bmatrix}.$$

Figure 15.1 shows how e_1, e_2 are "assembled" from the columns of rref(A). Namely, since the non-pivot columns have numbers 3 and 5, we put the values -1 and 0 in the 3'rd and 5'th coordinates of e_1 respectively. The remaining $r = 3$ coordinates of e_1 are filled-in by the first 3 entries $1, 2, 0$ of the 3'rd column of rref(A). Then we build e_2 by putting the values 0 and -1 in the 3'rd and 5'th coordinates of e_2. The remaining $r = 3$ coordinates of e_2 are filled-in by the first 3 entries $-1, 3, 4$ of the 5'rd column of rref(A).

The general solution of $AX = O$ fills the span $\operatorname{null}(A) = \operatorname{span}(e_1, e_2)$, and it can be given as:

$$\operatorname{span}(e_1, e_2) = \left\{ \alpha \begin{bmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} -1 \\ 3 \\ 0 \\ 4 \\ -1 \end{bmatrix} \mid \alpha, \beta \in \mathbb{R} \right\}.$$

$$= \left\{ \begin{bmatrix} \alpha - \beta \\ 2\alpha + 3\beta \\ -\alpha \\ 4\beta \\ -\beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{R} \right\}$$

Example 15.4. Applying this method on finite fields we should take care what we use as -1. In a field like $\mathbb{Z}_5$ we use $4 = -1$, as 4 is the *additive inverse* of 1. Consider the following matrix on the finite field $\mathbb{Z}_5$:

$$A = \begin{bmatrix} 2 & 1 & 0 & 3 \\ 0 & 0 & 3 & 4 \\ 1 & 3 & 0 & 4 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & 0 & 3 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 2 & 1 & 0 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 3 & 0 & 4 \\ 0 & 0 & \mathbf{1} & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(A).$$

Thus, a basis for null(A) is:

$$e_1 = \begin{bmatrix} 3 \\ \mathbf{4} \\ 0 \\ \mathbf{0} \end{bmatrix}, \quad e_2 = \begin{bmatrix} 4 \\ \mathbf{0} \\ 3 \\ \mathbf{4} \end{bmatrix},$$

and it can be given as:

$$\operatorname{null}(A) = \operatorname{span}(e_1, e_2) = \left\{ \begin{bmatrix} 3\alpha + 4\beta \\ 4\alpha \\ 3\beta \\ 4\beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_5 \right\}.$$

Remark 15.5. In Part 2 we considered the solutions of a homogeneous system of linear equations just as a *set* without any special organization inside it. Now we see that they form a subspace in F^n, and we have a basis for it. Also, we have a handy matrix tool to study it: null(A). The solutions $e_1, \ldots, e_{n-r}$ in (15.2) are the "most important" solutions of $AX = O$: they can be built using the columns of rref(A), and all other solutions are their linear combinations. The vectors (15.2) (and in general any basis of null(A)) sometimes is called the *fundamental* system of solutions for $AX = O$.

15.2. Solutions of systems of linear equations using null spaces

Now let us turn to a more general question: can we find a similar description for solutions of *arbitrary* system of linear equations which may not be homogeneous? The bad news is that solutions of a non-homogeneous system are *not* a subspace. But we still can find a way to describe them.

For a system $AX = B$ we can consider its *associated homogeneous system* $AX = O$, which is obtained from $AX = B$, if we replace all constant terms $b_1, \ldots, b_m$ by 0.

Proposition 15.6. *Assume we are given any system of linear equations $AX = B$, and $AX = O$ is its associated homogeneous system.*

1. *If u is any solution of $AX = O$, and v is any solution of $AX = B$, then $u + v$ is a solution of $AX = B$.*
2. *Fix a solution v_0 of $AX = B$, and take an arbitrary solution v of $AX = B$. Then there exists a solution u of $AX = 0$, such that $v = u + v_0$.*

***Proof*.** The first point is easy to verify by substituting the coordinates of $u + v$ in variables of $AX = B$. To prove the second point present v as $v = (v - v_0) + v_0$, and notice that $u = v - v_0$ is a solution for $AX = 0$. □

This proposition gives as the idea how to describe the solutions set of $AX = B$. First consider the associated homogeneous system $AX = O$. We already know that the solutions of $AX = O$ form the subspace null(A), which can be given by its basis $e_1, \ldots, e_{n-r}$. By proposition an arbitrary solution v of $AX = B$ is a sum $u + v_0$, where u is any linear combination of $e_1, \ldots, e_{n-r}$, and v_0 is any fixed solution of $AX = B$.

To find v_0 we in system of linear equations corresponding to rref$\big(\bar{A}\big)$ move to right-hand side the free variables $x_{t_1}, \ldots, x_{t_{n-r}}$ and assign to all of them, say, the value 0. Then the values of the pivot variables $x_{j_1}, \ldots, x_{j_r}$ will be equal to the first r entries of the last column of rref$\big(\bar{A}\big)$. We built an algorithm:

How to solve a system of linear equations, the free columns method.

Algorithm 15.7 (Solving a system of linear equations, the free columns method)**.** We are given a system $AX = B$ of m linear equations in n variables over a field F.

► Solve the system and describe the solution using null(A).

1. Compute rank(A) and rank$\big(\bar{A}\big)$ by bringing $\bar{A}$ to a row-echelon form R by elementary row-operations.
2. If $r = $ rank(A) is less than rank$\big(\bar{A}\big)$, output: the system is inconsistent. End of the process.

3. Else bring R to the reduced row-echelon form $\mathrm{rref}(R) = \mathrm{rref}(\bar{A})$ by elementary row-operations. The first n columns of $\mathrm{rref}(\bar{A})$ form the matrix $\mathrm{rref}(A)$.

4. Set $j_1, \dots, j_r$ to be the numbers of pivot columns of $\mathrm{rref}(A)$, and set $t_1, \dots, t_{n-r}$ to be the numbers of non-pivot columns of $\mathrm{rref}(A)$ (both sequences in ascending order).

5. For each $i = 1, \dots, n-r$ define a vector e_i in F^n as follows:
all the coordinates number $t_1, \dots, t_{n-r}$ in e_i are 0, except t_i'th coordinate -1;
the coordinates number $j_1, \dots, j_r$ in e_i are equal to the first r entries in the t_i'th column of $\mathrm{rref}(A)$.

6. Define a vector v_0 in F^n as follows:
all the coordinates number $t_1, \dots, t_{n-r}$ in v_0 are 0;
the coordinates number $j_1, \dots, j_r$ in v_0 are equal to the first r entries in the last column of $\mathrm{rref}(\bar{A})$.

7. Output the solutions of $AX = B$ in either of the following forms: $\mathrm{null}(A) + v_0$, or $\mathrm{span}(e_1, \dots, e_{n-r}) + v_0$, or $\{\alpha_1 e_1 + \cdots + \alpha_{n-r} e_{n-r} + v_0 \mid \alpha_1, \cdots, \alpha_{n-r} \in F\}$.

Let us apply the algorithm to examples:

$$\bar{A} \sim \mathrm{rref}(\bar{A}) = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & -1 & 3 \\ 0 & 1 & 2 & 0 & 3 & 2 \\ 0 & 0 & 0 & 1 & 4 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \end{array}$$

$$\begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \quad \underset{e_1}{\begin{bmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix}} \quad \underset{e_2}{\begin{bmatrix} -1 \\ 3 \\ 0 \\ 4 \\ -1 \end{bmatrix}} \quad \underset{v_0}{\begin{bmatrix} 3 \\ 2 \\ 0 \\ -3 \\ 0 \end{bmatrix}} \qquad \begin{aligned} &\mathrm{null}(A) + v_0 \\ &= \mathrm{span}(e_1, e_2) + v_0 \end{aligned}$$

FIGURE 15.2. Assembling the general solution for $AX = B$ by free columns method.

Example 15.8. Consider the system $AX = B$ of linear equations:

$$\begin{cases} x_1 + x_2 + 3x_3 + x_4 + 6x_5 = 2 \\ 2x_1 - x_2 + x_4 - x_5 = 1 \\ -2x_1 + 2x_2 + x_3 - 2x_4 + x_5 = 1 \\ x_1 + x_2 + 6x_3 + x_4 + 3x_5 = 11. \end{cases}$$

The matrix A of this system is that of Exercise 15.3, and the augmented matrix is:

$$\bar{A} = \left[\begin{array}{ccccc|c} 1 & 1 & 3 & 1 & 6 & 2 \\ 2 & -1 & 0 & 1 & -1 & 1 \\ -3 & 2 & 1 & -2 & 1 & 1 \\ 4 & 1 & 6 & 1 & 3 & 11 \end{array}\right].$$

$\bar{A}$ has a row-echelon form:

$$\left[\begin{array}{ccccc|c} \mathbf{1} & 1 & 3 & 1 & 6 & 2 \\ 0 & \mathbf{-3} & -6 & 0 & -9 & -6 \\ 0 & 0 & 0 & \mathbf{1} & 4 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

from which it is clear that the system does have a solution, since $\mathrm{rank}(A) = \mathrm{rank}(\bar{A})$. So we proceed to the reduced row-echelon form:

$$\mathrm{rref}(\bar{A}) = \begin{bmatrix} \mathbf{1} & 0 & 1 & 0 & -1 & 3 \\ 0 & \mathbf{1} & 2 & 0 & 3 & 2 \\ 0 & 0 & 0 & \mathbf{1} & 4 & -3 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

We have $r = \mathrm{rank}(A) = \mathrm{rank}(\bar{A}) = 3$ and $\mathrm{nullity}(A) = n - r = 2$. Two basis vectors

e_1, e_2 for null(A) already are computed in Exercise 15.3 (see earlier Figure 15.1):

$$e_1 = \begin{bmatrix} 1 \\ 2 \\ -\mathbf{1} \\ 0 \\ \mathbf{0} \end{bmatrix}, \quad e_2 = \begin{bmatrix} -1 \\ 3 \\ \mathbf{0} \\ 4 \\ -\mathbf{1} \end{bmatrix}$$

using the 3'rd and 5'th columns of rref(A). These also are the basis for the solutions subspace of the associated homogeneous system $AX = 0$.

A single solution v_0 of the initial system $AX = B$ can be obtained, if we assign, say, zero values to all free variables: $x_3 = x_5 = 0$. I.e., the 3'rd and 5'th coordinates of v_0 are zero. Then the values of the coordinates number $1, 2, 4$ (pivot column numbers) will be equal to the first 3 entries of the last column of rref$\big(\bar{A}\big)$ (see Figure 15.2 above):

$$v_0 = \begin{bmatrix} 3 \\ 2 \\ \mathbf{0} \\ -3 \\ \mathbf{0} \end{bmatrix}.$$

So the general solutions of the system $AX = B$ can be presented in any of the following forms:

$$\text{null}(A) + v_0 = \text{span}(e_1, e_2) + v_0$$
$$= \{\alpha e_1 + \beta e_2 + v_0 \mid \alpha, \beta \in \mathbb{R}\},$$
$$= \left\{\alpha \begin{bmatrix} 1 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} -1 \\ 3 \\ 0 \\ 4 \\ -1 \end{bmatrix} + \begin{bmatrix} 3 \\ 2 \\ 0 \\ -3 \\ 0 \end{bmatrix} \mid \alpha, \beta \in \mathbb{R}\right\}$$
$$= \left\{ \begin{bmatrix} \alpha - \beta + 3 \\ 2\alpha + 3\beta + 2 \\ -\alpha \\ 4\beta - 3 \\ -\beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{R}\right\}.$$

Example 15.9. We are given a system on $\mathbb{Z}_5$:

$$\begin{cases} 2x_1 + x_2 + 3x_4 = 4 \\ 3x_3 + 4x_4 = 2 \\ x_1 + 3x_2 + 4x_4 = 2. \end{cases}$$

Notice that its matrix A is that considered in Example 15.4, so we skip the details of row-reduction:

$$\bar{A} = \left[\begin{array}{cccc|c} 2 & 1 & 0 & 3 & 4 \\ 0 & 0 & 3 & 4 & 2 \\ 1 & 3 & 0 & 4 & 2 \end{array}\right] \sim \left[\begin{array}{cccc|c} \mathbf{1} & 3 & 0 & 4 & 2 \\ 0 & 0 & \mathbf{1} & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] = \text{rref}\big(\bar{A}\big).$$

Since in $\mathbb{Z}_5$ we have $-1 = 4$, we can take:

$$e_1 = \begin{bmatrix} 3 \\ \mathbf{4} \\ 0 \\ \mathbf{0} \end{bmatrix}, \quad e_2 = \begin{bmatrix} 4 \\ \mathbf{0} \\ 3 \\ \mathbf{4} \end{bmatrix}, \quad v_0 = \begin{bmatrix} 2 \\ \mathbf{0} \\ 4 \\ \mathbf{0} \end{bmatrix},$$

and the general solutions of the system is:

$$\text{null}(A) + v_0 = \text{span}(e_1, e_2) + v_0$$
$$= \{\alpha e_1 + \beta e_2 + v_0 \mid \alpha, \beta \in \mathbb{Z}_5\},$$
$$= \left\{\alpha \begin{bmatrix} 3 \\ \mathbf{4} \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 4 \\ 0 \\ 3 \\ \mathbf{4} \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \\ 4 \\ 0 \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_5\right\}$$
$$= \left\{ \begin{bmatrix} 3\alpha + 4\beta + 2 \\ 4\alpha \\ 3\beta + 4 \\ 4\beta \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_5\right\}.$$

Remark 15.10. The formula null$(A) + v_0$ is a generalization of a geometric concept we learned much earlier in the topic of lines and planes in sections 2.1 and 2.2. Namely, the set null$(A) + v_0$ can be understood as the subspace null(A) *shifted to the position* v_0, just like we constructed each plane $\mathcal{P}$ in $\mathbb{R}^3$ starting by a plane passing by the origin O, then *shifting* it by some position vector p, see Figure 2.3. The following example provides a retrospective view to that topic:

Example 15.11. To solve the system $AX = B$ given as:

$$\begin{cases} -x - 3y + 4z = 5 \\ 2x + 6y - 8z = -10 \end{cases}$$

we calculate a row-echelon form of its augmented matrix $\bar{A}$ in a singe step:

$$\bar{A} = \begin{bmatrix} -1 & -3 & 4 & 5 \\ 2 & 6 & -8 & -10 \end{bmatrix} \sim \begin{bmatrix} -1 & -3 & 4 & 5 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

As $r = \text{rank}(A) = \text{rank}\big(\bar{A}\big) = 1$, the system is consistent. And since $n - r = 3 - 1 = 2$, then null(A) is a 2-dimensional subspace in $\mathbb{R}^3$, i.e., null(A) is noting but a *plane* in the space $\mathbb{R}^3$. Continuing the solution by Algorithm 15.7 we get the matrix:

$$\text{rref}\big(\bar{A}\big) = \begin{bmatrix} 1 & 3 & -4 & -5 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and three vectors:

$$e_1 = \begin{bmatrix} 3 \\ -1 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 4 \\ 0 \\ 1 \end{bmatrix}, \quad v_0 = \begin{bmatrix} -5 \\ 0 \\ 0 \end{bmatrix}$$

with $\mathrm{null}(A) = \mathrm{span}(e_1, e_2)$ (we multiplied e_2 by -1 to avoid the minus sign).

Now please jump back to Example 2.7 in which the same vectors occur as two *direction* vectors $d = (3, -1, 0)$, $k = (4, 0, 1)$, and a *position* vector $p = (-5, 0, 0)$ of a certain plane $\mathcal{P}$.

Do you see the geometric meaning? The solutions of $AX = B$ are the plane $\mathrm{null}(A)$ (spanned by direction vectors $e_1 = d, e_2 = k$) *shifted to the position* $v_0 = p$, see Figure 2.3. What we earlier took as direction vectors, were the basis for $\mathrm{null}(A)$, and what we fixed as a position vector, was a certain fixed solution v_0 of the system $AX = B$.

Exercises

E.15.1. Find the null space $U = \mathrm{null}(A)$ (i.e. give a basis for U) of the matrix A by Algorithm 15.2:

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

E.15.2. Built a basis for the solutions of the homogeneous system of linear equations:

$$\begin{cases} x_1 + x_2 - x_3 + x_5 = 0 \\ -x_1 + x_2 + x_3 + 2x_4 + 2x_5 = 0 \\ 2x_1 + x_2 - 2x_3 - x_4 = 0 \end{cases}.$$

E.15.3. Solve the system by Algorithm 15.7:

$$\begin{cases} x_1 + x_2 - x_3 + x_5 = -1 \\ -x_1 + x_2 + x_3 + 2x_4 + 2x_5 = 1 \\ 2x_1 + x_2 - 2x_3 - x_4 = 2 \end{cases}.$$

Hint: to save on computations you can use your computations in previous exercise.

E.15.4. What it the nullity of a matrix $A \in M_{4,5}$, if $\mathrm{rank}(A) = 3$? *Hint*: you can answer the question without any row-echelon computations.

E.15.5. We are given the real matrices

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

(1) Find the nullity of A. **(2)** Without any new row-elimination operations, using the result of previous point tell what is the rank of A. **(3)** Find the null space of A by computing a basis for it by Algorithm 15.2. **(4)** Can you without any row-elimination operations tell if the system of linear equations $AX = B$ is consistent or not? **(5)** Find the general solution for the system of linear equations $AX = B$ using $\mathrm{null}(A)$.

CHAPTER 16

Subspaces calculus

16.1. Identifying the subspaces

In this section we will detect how the subspace relate to each other. Namely, weather two subspaces given by some spanning sets are *equal*, or weather one of them *contains* the other.

How to compare subspaces.

Algorithm 16.1 (Comparing two subspaces given by spanning sets)**.** We are given two subspaces $U = \operatorname{span}(u_1, \ldots, u_m)$ and $W = \operatorname{span}(w_1, \ldots, w_s)$ of a vector space V over a field F.

► Find if or not U and W are equal.

1. If $V = F^n$, then the vectors $u_1, \ldots, u_m$ and $w_1, \ldots, w_s$ are coordinate sequences, and we form two matrices by their coordinates, putting them by *rows*:

$$A = \begin{bmatrix} u_1 \\ \cdots \\ u_m \end{bmatrix}, \quad B = \begin{bmatrix} w_1 \\ \cdots \\ w_s \end{bmatrix}. \tag{16.1}$$

2. Else, if V is another space, fix any coordinate system with a basis E, and build the matrices A and B using the respective coordinate vectors $[u_1]_E, \ldots, [u_m]_E$ and $[w_1]_E, \ldots, [w_s]_E$.
3. Bring A and B to row-echelon forms, respectively, R and L by elementary row-operations.
4. If the number of non-zero rows in R and L are not equal, then output: $U \neq W$. End of the process.
5. Else bring R and L to reduced row-echelon forms respectively $\operatorname{rref}(A)$ and $\operatorname{rref}(B)$ by elementary row-operations.
6. If non-zero rows of $\operatorname{rref}(A)$ and $\operatorname{rref}(B)$ coincide, then output: $U = W$. Else output: $U \neq W$.

***Proof*.** The condition of step 4 is clear: if the ranks of A and B are distinct, then the dimensions of U and W are distinct, and so $U \neq W$. Otherwise we proceed to the reduced row-echelon forms and apply Theorem 14.15, by which $\operatorname{row}(A)$ and $\operatorname{row}(B)$ are equal if and only if the non-zero rows in $\operatorname{rref}(R)$ and $\operatorname{rref}(L)$ coincide. Since m and s may not be equal, $\operatorname{row}(A)$ and $\operatorname{row}(B)$ may contain different number of zero rows, but they do not alter the subspaces. □

We could skip the condition of step 4, and compare two matrices only after they are in reduced row-echelon form. However, if $\operatorname{rank}(A) \neq \operatorname{rank}(B)$, we may discover the inequality $U \neq W$ earlier in step 4.

Example 16.2. Assume we are given two sets of vectors in $\mathbb{R}^4$:

$$\begin{aligned} u_1 &= (1,0,2,1), \\ u_2 &= (1,2,-1,0), \\ u_3 &= (2,3,1,3), \\ u_4 &= (0,1,0,2). \end{aligned}$$

$$\begin{aligned} w_1 &= (2,2,1,1), \\ w_2 &= (3,3,3,4), \\ w_3 &= (1,1,2,3), \\ w_4 &= (2,0,4,2), \\ w_5 &= (5,3,7,6). \end{aligned}$$

To detect if they span the same subspace first compose two matrices by their coordinates:

$$A = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 1 & 2 & -1 & 0 \\ 2 & 3 & 1 & 3 \\ 0 & 1 & 0 & 2 \end{bmatrix}, \ B = \begin{bmatrix} 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 4 \\ 1 & 1 & 2 & 3 \\ 2 & 0 & 4 & 2 \\ 5 & 3 & 7 & 6 \end{bmatrix},$$

Some row-echelon forms for matrices A and B respectively are:

$$R = \begin{bmatrix} \mathbf{1} & 0 & 2 & 1 \\ 0 & \mathbf{2} & -3 & -1 \\ 0 & 0 & \mathbf{3} & 5 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ L = \begin{bmatrix} \mathbf{2} & 2 & 1 & 1 \\ 0 & -\mathbf{2} & 3 & 1 \\ 0 & 0 & \mathbf{3} & 5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

They both have three non-zero rows, and all we can say is that both spans are 3-dimensional.

Next compute the reduced row-echelon forms of our matrices:

$$\operatorname{rref}(A) = \operatorname{rref}(R) = \begin{bmatrix} \mathbf{1} & 0 & 0 & -\frac{7}{3} \\ 0 & \mathbf{1} & 0 & 2 \\ 0 & 0 & \mathbf{1} & \frac{5}{3} \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\operatorname{rref}(B) = \operatorname{rref}(L) = \begin{bmatrix} \mathbf{1} & 0 & 0 & -\frac{7}{3} \\ 0 & \mathbf{1} & 0 & 2 \\ 0 & 0 & \mathbf{1} & \frac{5}{3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Although R and L are different, $\operatorname{rref}(R)$ and $\operatorname{rref}(L)$ have the same non-zero rows, and so

$$\operatorname{span}\big(u_1, u_2, u_3, u_4\big) = \operatorname{span}\big(w_1, w_2, w_3, w_4, w_5\big).$$

How to find if a given subspace contains the other subspace. If we are given $U = \operatorname{span}(u_1, \dots, u_m)$ and $W = \operatorname{span}(w_1, \dots, w_s)$, then U contains W if and only if each w_i, $i = 1, \dots, s$, is a linear combination of $u_1, \dots, u_m$. So we could repeat Algorithm 14.29 s times to test this. However, the process may be simplified:

Algorithm 16.3 (Detecting if one of the given subspaces contains the other)**.** We are given two subspaces $U = \operatorname{span}(u_1, \dots, u_m)$ and $W = \operatorname{span}(w_1, \dots, w_s)$ of a vector space V over a field F.

► Find if or not U contains W.

1. If $V = F^n$, then the vectors $u_1, \dots, u_m$ and $w_1, \dots, w_s$ are coordinate sequences, and we form two matrices by their coordinates, putting them by *columns*:
$$A = \begin{bmatrix} u_1 & \vdots & \cdots & \vdots & u_m \end{bmatrix}, \qquad B = \begin{bmatrix} w_1 & \vdots & \cdots & \vdots & w_s \end{bmatrix}.$$
2. Else, if V is another space, fix any coordinate system with a basis E, and build the matrices A and B using the respective coordinate vectors $[u_1]_E, \dots, [u_m]_E$ and $[w_1]_E, \dots, [w_s]_E$.
3. Bring the block matrix $[A\,|\,B]$ to a row-echelon form R by elementary row-operations.
4. If the last s columns of R contain no pivot, output: $U \supseteq W$. Else $U \not\supseteq W$.

Proof. Suppose $u_{j_1}, \dots, u_{j_r}$ form a maximal linearly independent subsystem of vectors among the vectors $u_1, \dots, u_m$.

If we bring A to a row-echelon form, the pivots will be in columns $j_1, \dots, j_r$ (see Algorithm 14.24). If each w_i is a linear combination of $u_1, \dots, u_m$, we get no new pivots. In other words $\operatorname{rank}(A) = \operatorname{rank}[A\,|\,B]$. □

Example 16.4. We are given the polynomials $f_1(x) = 1 - x + x^2$, $f_2(x) = 3x + 3x^2$, $f_3(x) = -2-4x^2$, and the polynomials $g_1(x) = 3+6x^2$, $g_2(x) = 3 + x + 7x^2$, $g_3(x) = 4 + x + 9x^2$.

Finding their coordinates in the basis $E = \{1, x, x^2\}$ of $\mathcal{P}_2$ we fill-in the matrix $[A|B]$ and compute:

$$\left[\begin{array}{ccc|ccc} 1 & 0 & -2 & 3 & 3 & 4 \\ -1 & 3 & 0 & 0 & 1 & 1 \\ 1 & 3 & -4 & 6 & 7 & 9 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} \mathbf{1} & 0 & -2 & 3 & 3 & 4 \\ 0 & \mathbf{3} & -2 & 3 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right],$$

which by Algorithm 16.3 means that

$$\operatorname{span}(f_1, f_2, f_3) \supseteq \operatorname{span}(g_1, g_2, g_3).$$

Remark 16.5. We could replace Algorithm 16.1 by double application of Algorithm 16.3 to check if U contains W, *and* W contains U. However, Algorithm 16.1 requires computation of the reduced row-echelon form of *one* $m \times n$ matrix and of *one* $s \times n$ matrix, whereas double application of Algorithm 16.3 would require computation of the row-echelon form of *two* $n \times (m + s)$ matrices.

How to continue a basis of a subspace to a basis for the space. In some important algorithms below we are going to *continue* the given basis G of a given subspace U in a space V to a basis for the whole space V. This can be done by an adaptation of Algorithm 14.24:

Algorithm 16.6 (Continuing a basis of a subspace)**.** We are given a basis $G = \{g_1, \dots, g_m\}$ for subspaces U of a vector space V over F. The space V is defined by its basis or spanning set $\{u_1, \dots, u_s\}$.

► Find vectors $h_1, \dots, h_k \in V \backslash U$ such that $E = \{g_1, \dots, g_m;\ h_1, \dots, h_k\}$ is a basis for V.

1. If $V = F^n$, then the vectors $g_1, \dots, g_m$ and $u_1, \dots, u_s$ are coordinate sequences, and we form a matrix by their coordinates, putting them by *columns*:

$$A = \left[\begin{array}{c:c:c:c:c:c} h_1 & \cdots & h_m & u_1 & \cdots & u_s \end{array}\right].$$

2. Else, if V is another space, fix any coordinate system with a basis E, and build the matrix A using the respective coordinate vectors $[h_1]_E, \dots, [u_s]_E$.

3. Bring the matrix A to a row-echelon form R by elementary row-operations.

4. If in the last s columns of R the pivots stand in columns with numbers $m+j_1, \dots, m+j_r$, then output the continued basis: $\{g_1, \dots, g_m;\ v_{j_1}, \dots, v_{j_r}\}$ for V.

Example 16.7. Assume U is the plane spanned in $\mathbb{R}^3$ by the vectors $g_1 = (1, 0, 1)$ and $g_2 = (2, 0, 0)$. Then using the standard basis of $\mathbb{R}^3$:

$$A = \begin{bmatrix} 1 & 2 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 \\ 1 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & -1 & 0 & 1 \end{bmatrix}$$

$$\sim \begin{bmatrix} \mathbf{1} & 2 & 1 & 0 & 0 \\ 0 & \mathbf{-2} & -1 & 0 & 1 \\ 0 & 0 & 0 & \mathbf{1} & 0 \end{bmatrix}.$$

Which means that we should continue the basis vectors g_1, g_2 by the vector $e_2 = (0, 1, 0)$ from the standard basis.

16.2. Computation of the sum and intersection of subspaces

In Section 10.2 we introduced the *intersection* $U \cap W$ and the *sum* $U + W$ of any two subspaces U, W of a space V. Natural generalizations to intersation $U_1 \cap \ldots \cap U_k$ and to sum $U_1 + \cdots + U_k$ for any number of subspaces $U_1, \dots, U_k$, along with some basic examples were given. The matrix methods we learned now allow to compute these intersections and sums, i.e., to find bases for them.

How to find the sum of two subspaces. Computation of the sum of subspaces, each given by a spanning set, i.e., finding a *basis* for that sum, is an easy task by Algorithm 14.27: just merge all those spanning sets (to have a spanning set for the whole sum), and then choose a maximal linearly independent subset of that set.

Example 16.8. Let the subspace U of $V = \mathbb{R}^4$ be spanned by the vectors:

$$u_1=\begin{bmatrix}1\\0\\1\\3\end{bmatrix},\ u_2=\begin{bmatrix}0\\2\\0\\-1\end{bmatrix},\ u_3=\begin{bmatrix}1\\4\\-1\\0\end{bmatrix},$$

and the subspace W be spanned by:

$$w_1=\begin{bmatrix}1\\0\\-1\\2\end{bmatrix},\ w_2=\begin{bmatrix}2\\-2\\-1\\3\end{bmatrix},\ w_3=\begin{bmatrix}0\\1\\1\\0\end{bmatrix},\ w_4=\begin{bmatrix}1\\1\\0\\2\end{bmatrix}.$$

It is easy to check that $\dim(U) = \dim(W) = 3$. Compute a basis for the sum $U + W$ using Algorithm 14.27).

If A is the matrix composed by columns u_1, u_2, u_3, and B is the matrix composed by columns w_1, w_2, w_3, w_4, then we form the matrix $[A\,|\,B]$, and bring it to a row-echelon form:

$$[A\,|\,B]=\left[\begin{array}{ccc|cccc}1&0&1&1&2&0&1\\0&2&4&0&-2&1&1\\1&0&-1&-1&-1&1&0\\3&-1&0&2&3&0&2\end{array}\right]$$

$$\sim\left[\begin{array}{ccc|cccc}\mathbf{1}&0&1&1&2&0&1\\0&\mathbf{1}&2&0&-1&\frac12&\frac12\\0&0&\mathbf{1}&1&\frac32&-\frac12&\frac12\\0&0&0&0&\mathbf{1}&0&0\end{array}\right].$$

The maximal linearly independent subset of the columns of this matrix are in columns $1, 2, 3, 5$. Thus, we find:

$$U + W = \operatorname{span}(u_1, u_2, u_3, w_2)$$

$$= \operatorname{span}\left(\begin{bmatrix}1\\0\\1\\3\end{bmatrix},\begin{bmatrix}0\\2\\0\\-1\end{bmatrix},\begin{bmatrix}1\\4\\-1\\0\end{bmatrix},\begin{bmatrix}2\\-2\\-1\\3\end{bmatrix}\right).$$

Since $U + W$ is 4-dimensional, it is clear that in this case $U + W = V = \mathbb{R}^4$.

Calculation of *intersection* of subspaces, each given by a spanning set, is a less trivial task because the basis of an intersection $U\cap W$ may *not* be found among the vectors of the given spanning sets of U and W. Say, in $\mathbb{R}^3$ the intersection of the subspace U spanned by $u_1 = (1,1,0)$, $u_2 = (1,2,0)$, and of the subspace W spanned by $w_1 = (1,0,1)$, $w_2 = (1,0,2)$ is the line Ox. But none of the vectors u_1, u_2, w_1, w_2 belongs to Ox, so we cannot choose a basis for $U \cap W$ from those vectors.

Let us construct the algorithm for intersection $U \cap W$ of two summands

$$U = \operatorname{span}(u_1, \dots u_m), \quad W = \operatorname{span}(w_1, \dots w_s).$$

Denote $A = \left[\, u_1 \,\vdots\, \cdots \,\vdots\, u_m \,\right]$ and $B = \left[\, w_1 \,\vdots\, \cdots \,\vdots\, w_s \,\right]$. A vector $v \in V$ belongs to $U \cap W$ if and only if v can be presented as two linear combinations $v = c_1u_1 + \cdots + c_mu_m \in U$ and $v = d_1w_1 + \cdots + d_sw_s \in W$, i.e.,

$$c_1u_1 + \cdots + c_mu_m - d_1w_1 - \cdots - d_sw_s = v - v = 0$$

which is equivalent to the fact that the $(m+s)$-dimensional vector $(c_1, \dots c_m,\, d_1, \dots d_s)$ is in null space of the matrix $[A|-B]$. So all we need is to find *a basis for the subspace of vectors of type $c_1u_1 + \cdots + c_mu_m$, where $c_1, \dots c_m$ are the first m coordinates of vectors in* $\operatorname{null}[A|-B]$.

How to find the intersection of two subspaces, basic method.

Algorithm 16.9 (Computing the intersection of two subspaces)**.** We are given two subspaces $U = \operatorname{span}(u_1, \dots, u_m)$ and $W = \operatorname{span}(w_1, \dots, w_s)$ of a vector space V over a field F.

► Find a basis for the intersection $U \cap W$.

1. If $V = F^n$, then the vectors $u_1, \dots, u_m$ and $w_1, \dots, w_s$ are coordinate sequences, and we form two matrices by their coordinates, putting them by *columns*:

$$A = \left[\, u_1 \;\vdots\; \cdots \;\vdots\; u_m \,\right], \qquad B = \left[\, w_1 \;\vdots\; \cdots \;\vdots\; w_s \,\right].$$

2. Else, if V is another space, fix any coordinate system in V with a basis E, and build the matrices A and B using the respective coordinate vectors $[u_1]_E, \dots, [u_m]_E$ and $[w_1]_E, \dots, [w_s]_E$.
3. Find a basis $G = \{g_1, \dots, g_t\}$ for null$[A| - B]$ by Algorithm 15.2.
4. For each $i = 1, \dots, t$
5. Set $h_i = c_1 u_1 + \cdots + c_m u_m$, where $c_1, \dots c_m$ are the first m coordinates of g_i.
6. Find a basis for span$(h_1, \dots, h_t)$ by Algorithm 14.27.

Clearly, if s is less than m, then in step 5 of the algorithm we may prefer to work with $d_1 w_1 + \cdots + d_s w_s$ instead. Also, in order to shorten computation of null$[A| - B]$ we may first drop the linearly dependent columns in A and in B, i.e., find maximal linearly independent subset of columns of A and of B by Algorithm 14.24.

Example 16.10. Let the subspace U of $\mathbb{R}^4$ be spanned by the vectors:

$$u_1 = \begin{bmatrix} 1 \\ -2 \\ 0 \\ -1 \end{bmatrix},\ u_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix},\ u_3 = \begin{bmatrix} 1 \\ 0 \\ 2 \\ -2 \end{bmatrix},\ u_4 = \begin{bmatrix} 1 \\ 3 \\ 2 \\ 0 \end{bmatrix},$$

and the subspace W be spanned by:

$$w_1 = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix},\ w_2 = \begin{bmatrix} 1 \\ 0 \\ -1 \\ 2 \end{bmatrix},\ w_3 = \begin{bmatrix} 2 \\ 2 \\ 0 \\ 3 \end{bmatrix},\ w_4 = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix}.$$

Compute a basis for the intersection $U \cap W$.

It is easy to detect a maximal linearly independent subsets, i.e., bases in each subspace (Algorithm 14.24):

$$U = \mathrm{span}(u_1, u_2, u_3),\ \ W = \mathrm{span}\big(w_1, w_2, w_4\big).$$

Let us form the matrix $[A| - B]$ and bring it to the reduced row-echelon form:

$$[A| - B] = \left[\begin{array}{rrr|rrr} 1 & 1 & 1 & -1 & -1 & -1 \\ -2 & 1 & 0 & -2 & 0 & -2 \\ 0 & 0 & 2 & -1 & 1 & -1 \\ -1 & 1 & -2 & -1 & -2 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{rrr|rrr} \mathbf{1} & 0 & 0 & 0 & -1 & 1 \\ 0 & \mathbf{1} & 0 & 0 & 0 & -2 \\ 0 & 0 & \mathbf{1} & 0 & 1 & -1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & -1 \end{array}\right].$$

(Thanks to the fact that we first dropped the "unscarcenessy" vectors u_4 and w_3, we now have not a 4×8 matrix but a *smaller* 4×6 matrix.) The null space of $[A| - B]$ is spanned by $6 - 4 = 2$ vectors which we can find by Algorithm 15.2:

$$e_1 = \begin{bmatrix} -1 \\ 0 \\ 1 \\ 1 \\ -\mathbf{1} \\ \mathbf{0} \end{bmatrix}, \quad e_2 = \begin{bmatrix} 1 \\ -2 \\ -1 \\ -1 \\ \mathbf{0} \\ -\mathbf{1} \end{bmatrix}.$$

Since both bases $\{u_1, u_2, u_3\}$ and $\{w_1, w_2, w_4\}$ contain *equal* number of vectors, we may use either the *first* three or the *last* three coordinates of e_1, e_2. Let us use the first three coordinates. As a spanning set (and basis) of $U \cap W$ we take:

$$h_1 = -u_1 + u_3 = -\begin{bmatrix} 1 \\ -2 \\ 0 \\ -1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 2 \\ -2 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 2 \\ -1 \end{bmatrix},$$

$$h_2 = u_1 - 2u_2 - u_3 = \begin{bmatrix} 1 \\ -2 \\ 0 \\ -1 \end{bmatrix} - 2\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 2 \\ -2 \end{bmatrix} = \begin{bmatrix} -2 \\ -4 \\ -2 \\ -1 \end{bmatrix},$$

and eliminating -1 in h_2 we output:

$$U \cap W = \mathrm{span}\left(\begin{bmatrix} 0 \\ 2 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \\ 2 \\ 1 \end{bmatrix} \right).$$

How to find the intersection of two subspaces, handy method. The method above allows a simplification suggested to us by V. Atabekyan. We start by the matrix $[A| - B]$, and bring it to a row-echelon form R. Denote by $u'_1, \dots, u'_m$ the first m columns of R, and by $w'_1, \dots, w'_s$ the last s columns of R. If $r = \dim(U)$, then the first m columns of R contain exactly r pivots (and exactly r non-zero rows). Let C be the matrix consisting of all non-zero rows below the r'th row in the last s columns in R.

Any vector $l \in W$ is linear combination $l = a_1 w_1 + \cdots + a_s w_s$. Denote $l' = a_1 w'_1 + \cdots + a_s w'_s$. Clearly, $l \in U$ if and only if $\operatorname{rank}(u_1, \ldots, u_m, l) = r$. By point 2 in Lemma 14.5 this is possible if and only if $\operatorname{rank}\big(u'_1, \ldots, u'_m, l'\big) = r$, that is, if and only if all the coordinates of l' after the r'th coordinate are zero. I.e., if $(a_1, \ldots, a_s) \in \operatorname{null}(C)$.

To find *all* such vectors $l \in U \cap W$ we find a basis for $\operatorname{null}(C)$ by Algorithm 15.2, then compute the linear combinations of the vectors $w_1, \ldots, w_s$ by the coordinates of those basis vectors of $\operatorname{null}(C)$. This outputs a spanning set for $U \cap W$, and it remains to choose a linearly independent subset of it as a basis for $U \cap W$.

Example 16.11. Suppose for some subspaces U and W in $\mathbb{R}^5$ we have already constructed the matrix:

$$[A| -B] = \left[\begin{array}{ccc|ccccc} 4 & 9 & 5 & 4 & 5 & 4 & 9 & 5 \\ 0 & 1 & 3 & 2 & 0 & 3 & 6 & 3 \\ 2 & 4 & 1 & 1 & 2 & 1 & 2 & 0 \\ 0 & 1 & 3 & 2 & 0 & 1 & 2 & 1 \\ 2 & 5 & 4 & 3 & 2 & 2 & 4 & 1 \end{array}\right],$$

and we have already calculated its row-echelon form as:

$$R = \left[\begin{array}{ccc|ccccc} \mathbf{2} & 4 & 1 & 1 & 2 & 1 & 2 & 0 \\ 0 & \mathbf{1} & 3 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 1 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{2} & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

Then the matrix C, clearly, is

$$C = \begin{bmatrix} 0 & 1 & 1 & 3 & 4 \\ 0 & 0 & 2 & 4 & 2 \end{bmatrix}.$$

To find a basis for $\operatorname{null}(C)$ compute the reduced row-echelon form:

$$C \sim \operatorname{rref}(C) = \begin{bmatrix} 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix},$$

from where the vectors

$$e_1 = \begin{bmatrix} -\mathbf{1} \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} 0 \\ 1 \\ 2 \\ -\mathbf{1} \\ 0 \end{bmatrix}, \quad e_3 = \begin{bmatrix} 0 \\ 3 \\ 1 \\ 0 \\ -\mathbf{1} \end{bmatrix}$$

form a basis for $\operatorname{null}(C)$ by Algorithm 15.2. Thus, as a spanning set for $U \cap W$ we can take:

$$h_1 = -1 \cdot w_1 + 0 \cdot w_2 + 0 \cdot w_3 + 0 \cdot w_4 + 0 \cdot w_5 = \begin{bmatrix} -4 \\ -2 \\ -1 \\ -2 \\ -3 \end{bmatrix},$$

$$h_2 = 0 \cdot w_1 + 1 \cdot w_2 + 2 \cdot w_3 - 1 \cdot w_4 + 0 \cdot w_5 = \begin{bmatrix} 4 \\ 0 \\ 2 \\ 0 \\ 2 \end{bmatrix},$$

$$h_3 = 0 \cdot w_1 + 3 \cdot w_2 + 1 \cdot w_3 + 0 \cdot w_4 - 1 \cdot w_5 = \begin{bmatrix} 14 \\ 0 \\ 7 \\ 0 \\ 7 \end{bmatrix}.$$

From these vectors h_1, h_2, h_3 we get the following basis for $U \cap W$:

$$\left\{ \begin{bmatrix} 4 \\ 2 \\ 1 \\ 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}.$$

Example 16.12. Let us apply this modification to Example 16.10. Bring the matrix

$$[A| -B] = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & -1 & -1 & -1 \\ -2 & 1 & 0 & -2 & 0 & -2 \\ 0 & 0 & 2 & -1 & 1 & -1 \\ -1 & 1 & -2 & -1 & -2 & 0 \end{array}\right]$$

to a row-echelon form:

$$\left[\begin{array}{ccc|ccc} \mathbf{1} & 1 & 1 & -1 & -1 & -1 \\ 0 & \mathbf{3} & 2 & -4 & -2 & -4 \\ 0 & 0 & \mathbf{2} & -1 & 1 & -1 \\ 0 & 0 & 0 & \mathbf{1} & 1 & -1 \end{array}\right].$$

The matrix C then is

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

The reduced row-echelon form of C is C itself, and so the vectors

$$e_1 = \begin{bmatrix} 1 \\ -\mathbf{1} \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} -1 \\ 0 \\ -\mathbf{1} \end{bmatrix}$$

form a basis for $\operatorname{null}(C)$. Thus, as a spanning set for $U \cap W$ we can take:

$$h_1 = 1 \cdot w_1 - 1 \cdot w_2 + 0 \cdot w_3 = \begin{bmatrix} 2 \\ 4 \\ 2 \\ 1 \end{bmatrix},$$

$$h_2 = -1 \cdot w_1 + 0 \cdot w_2 - 1 \cdot w_3 = \begin{bmatrix} 0 \\ -2 \\ -2 \\ 1 \end{bmatrix}.$$

As these vectors are independent, it is clear that $U \cap W$ is a 2-dimensional subspace in $\mathbb{R}^4$ with a basis $\{h_1, h_2\}$.

Remark 16.13. As these examples show, the modified method is more economical because, after the row-echelon form R of $[A| -B]$ is found, we compute *not* the $\operatorname{rref}(R)$ but just rref(C). The larger is the dimension of the space V, i.e., the more are the rows in R, the smaller is C relative to R. You may find further intriguing questions in Exercise E.16.4 and Exercise E.16.5.

16.3. Dimensions of the sum and the intersection

The following fundamental theorem shows correlation between dimensions of the sum and the intersection of subspaces, and it in many cases is very handy in problem solving:

Theorem 16.14. *If U and W are subspaces of a vector space V, then:*

$$\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

Proof. Let $E = \{e_1, \dots, e_m\}$ be a basis for $U \cap W$. By point 1 of Proposition 11.27 we can add to E some new vectors $G = \{g_1, \dots, g_r\}$ to get a basis $E \cup G$ for W. In the same way we can add some new vectors $H = \{h_1, \dots, h_s\}$ to E to get a basis $H \cup E$ for U. If we show that the union $H \cup E \cup G$ is a basis for $U+W$, the theorem will be proved because then:

$$\dim(U+W) = s+m+r = s+m+r+m-m = \dim(U)+\dim(W)-\dim(U\cap W).$$

$H \cup E \cup G$ spans $U+W$ because every vector $v \in U+W$ has a presentation $v = u+w$, where $u \in U$ is a linear combination of vectors of $H \cup E$, and $w \in W$ is a linear combination of vectors of $E \cup G$. To show linear independence suppose a linear combination of vectors of $H \cup E \cup G$ is zero:

$$a_1h_1 + \cdots + a_sh_s \ + \ b_1e_1 + \cdots + b_me_m \ + \ c_1g_1 + \cdots + c_rg_r \ = \ 0. \tag{16.2}$$

Denote by f the sum of the first $s+m$ summands in (16.2). Clearly, f is in U. On the other hand, since $f = -c_1g_1 - \cdots - c_rg_r$, the vector f also is in W. Thus, $f \in U \cap W$ and as such f is a linear combination of vectors of E. Since $H \cup E$ is a basis, f cannot have two distinct presentations by its vectors, and we get $a_1 = \cdots = a_s = 0$. But then (16.2) is a linear combination of vectors of $E \cup G$ only. Since $E \cup G$ is a basis, $b_1 = \cdots = b_m = c_1 = \cdots = c_r = 0$. □

Most typically, Theorem 16.14 is used in cases when $U+W=V$. And then we have $\dim(V) = \dim(U)+\dim(W)-\dim(U\cap W)$.

Example 16.15. In Example 16.8 we saw that $\dim(U) = \dim(W) = 3$ and $\dim(U+W) = 4$. This means that we by Theorem 16.14 can deduce $\dim(U \cap W) = 3+3-4 = 2$. Therefore, if we by any method find *two* non-collinear vectors in the intersection $U \cap W$, then they will form a basis for $U \cap W$.

Example 16.16. As we found in Example 16.10, $\dim(U) = \dim(W) = 3$ and $\dim(U \cap W) = 2$. By Theorem 16.14 we get find that $\dim(U+W) = 3+3-2 = 4$. Since all these subspaces are in the 4-dimensional space $\mathbb{R}^4$, we already deduce that $U+W = \mathbb{R}^4$.

Example 16.17. From the row-echelon matrix R of Example 16.11 it is clear that $\dim(U) = 2$ and $\dim(U+W) = 4$. By computations in that example we got $\dim(U \cap W) = 2$. We can now deduce that $\dim(W) = 4$ because $2+4-2 = 4$ by Theorem 16.14. In particular, $U \subseteq W$.

16.4. Direct sums

Definition 16.18. The sum $U+W$ of subspaces U, W of a space V is called *direct* sum, and is denoted $U \oplus W$, if every vector $v \in U+W$ has a *unique* presentation $v = u + w$ with $u \in U$ and $w \in W$.

Under *unique* presentation we mean that, if $v = u' + w'$ for some vectors $u' \in U$ and $w' \in W$, then $u = u'$ and $w = w'$.

This definition has evident generalization for the case of more then two subspaces $U_1, \ldots, U_k$. Then the direct sums can be denoted by $U_1 \oplus \cdots \oplus U_k$ or $\bigoplus_{i=1}^k U_i$.

Example 16.19. $\mathbb{R}^2$ is a direct sum of the lines Ox and Oy, i.e., $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$. And $\mathbb{R}^2 = \ell_1 \oplus \ell_2$ for any distinct lines ℓ_1, ℓ_2 passing via O.

In the same way $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} = \ell_1 \oplus \ell_2 \oplus \ell_3$ for any non-coplanar lines ℓ_1, ℓ_2, ℓ_3 passing via O.

Example 16.20. Turning back to the matrix subspaces of Example 10.20, we have:

$$M_{2,2}(F) = U_1 \oplus U_2 \oplus U_3 \oplus U_4$$

for $U_1 = \{aE_{1,1} \mid a \in F\}$, $U_2 = \{aE_{1,2} \mid a \in F\}$, $U_3 = \{aE_{2,1} \mid a \in F\}$, $U_4 = \{aE_{2,2} \mid a \in F\}$.

Theorem 16.21. *If the space V is the sum of its subspaces U and W, then the following conditions are equivalent:*

1. *$V = U \oplus W$, i.e., the sum $V = U + W$ is direct;*
2. *$U \cap W = \{0\}$;*
3. $\dim(U) + \dim(W) = \dim(V)$*;*
4. *if E is any basis in U, and G is any basis in W, then $E \cup G$ is a basis in V.*

***Proof*.** Let us prove the theorem by a circular chain of arguments:

1. Let $V = U \oplus W$, but $U \cap W$ contains a non-zero vector v. Since W is a subspace, it contains $-v$. Then we have *two* distinct presentations for the zero vector: $0 = 0 + 0$ and $0 = v + (-v)$ with $0, v \in U$ and $0, -v \in W$. Contradiction.

2. If $U \cap W = \{0\}$, then $\dim(U) + \dim(W) = \dim(V)$ follows from Theorem 16.14.

3. Supposing $\dim(U)+\dim(W) = \dim(V)$, consider the union $E \cup G$ of any two bases of U and W respectively. $E \cup G$ clearly spans $U+W$ and, since in this case $\dim(V) = |E \cup G|$, this union is a basis by point 6 of Proposition 11.27.

4. Assume the union $E \cup G$ for any bases E and G of, respectively, U and W is a basis in V. Let there be a vector $v \in V$ with two *distinct* presentations $v = u + w = u' + w'$ with $u, u' \in U$ and $w, w' \in W$ ($u \neq u'$ or $w \neq w'$). The vectors u, u' are distinct linear combinations of vectors of E, or the vectors v, v' are distinct linear combinations of vectors of G. The sums $u + v$ and $u' + v'$, thus, are two distinct presentations of v as linear combinations of vectors of the basis $E \cup G$. Contradiction. □

Corollary 16.22. *If the intersection of subspaces U and W of the space V is trivial, then $U + W = U \oplus W$.*

Example 16.23. Let U, W be the subspaces in $V = \mathbb{R}^4$ defined in Example 16.8. By Theorem 16.14 the intersection $U \cap W$ is non-zero, as $\dim(U \cap W) = 3 + 3 - 4 = 2$. So the sum $U + W$ is *not* direct (also see Example 16.15).

Example 16.24. If U, W are the subspaces defined in Example 16.10, then $\dim(U \cap W) = 2$. So, the sum $U + W$ is *not* direct. We detected this before even finding the sum $U + W$ (by Example 16.16 we have $U + W = \mathbb{R}^4$).

Definition of direct sum can be generalized for any finite number of summands: $V = U_1 \oplus \cdots \oplus U_k$, if any $v \in V$ has a *unique* presentation $v = u_1 + \cdots + u_k$, that is, if we also have a presentation $v = u'_1 + \cdots + u'_k$, then $u_i = u'_i$ for all $i = 1, \dots, k$.

It is easy to see that adding brackets to the direct sum does not change the result. Say, $U_1 \oplus U_2 \oplus U_3 = (U_1 \oplus U_2) \oplus U_3 = U_1 \oplus (U_2 \oplus U_3)$. This means that in direct sums of subspaces we can write (or omit) the brackets when needed (see Exercise 16.9). This approach will be used later in Section 25.3.

Theorem 16.21 has its evident analog for this case: the second condition turns to: $U_i \cap U_j = \{0\}$ for any distinct indices $i, j = 1, \dots, k$.

Exercises

E.16.1. In the space $V = \mathbb{R}^4$ we are given two subspaces U and W spanned by vector sets respectively $u_1 = (2,0,2,0)$, $u_2 = (1,2,5,0)$, $u_3 = (2,2,6,3)$ and $w_1 = (3,1,5,0)$, $w_2 = (0,1,2,0)$, $w_3 = (0,2,4,1)$, $w_4 = (0,1,2,1)$. Using Algorithm 16.1 detect if $U = W$.

E.16.2. Let $u_1 = (2,0,-1)$, $u_2 = (1,2,0)$, $u_3 = (-2,1,1)$ and $w_1 = (3,3,-1)$, $w_2 = (2,5,1)$. Set $U = \operatorname{span}(u_1,u_2,u_3)$ and $W = \operatorname{span}(w_1,w_2)$. Using Algorithm 16.3 detect if U is contained in W or vise versa. Are these subspaces equal?

E.16.3. In the real matrix space $M_{2,2}$ we are given the matrices

$$A_1 = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} -1 & 1 \\ 1 & 2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}, \qquad B_1 = \begin{bmatrix} -1 & 3 \\ 1 & 6 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0 & 3 \\ 1 & 0 \end{bmatrix},$$

and two subspaces are defined by them: $U = \operatorname{span}(A_1, A_2, A_3)$ and $W = \operatorname{span}(B_1, B_2)$. **(1)** Find the sum and intersection of subspaces U and W. **(2)** Indicate what does Theorem 16.14 state for the sum $U + W$ in this case. Deduce if this sum is direct or not according to Theorem 16.21.

E.16.4. In Remark 16.13 we estimated why the modified method with the matrix C is more economical for subspace intersection calculation. Can we make the method even more economical by erasing the zero columns in C? For instance, can we in Example 16.11 use *not* the matrix $C = \left[\begin{smallmatrix} 0 & 1 & 1 & 3 & 4 \\ 0 & 0 & 2 & 4 & 2 \end{smallmatrix}\right]$ but the smaller matrix $C = \left[\begin{smallmatrix} 1 & 1 & 3 & 4 \\ 0 & 2 & 4 & 2 \end{smallmatrix}\right]$?

E.16.5. Let U and W be subspaces in V with bases E and G respectively. Let $\dim(U) = m$ and $\dim(W) = s$. Form the $(m+s) \times 2m$ matrix $Z = \left[\begin{smallmatrix} E & E \\ G & 0 \end{smallmatrix}\right]$, assuming that the coordinates of vectors in E and G are written in Z by *rows*. Bring Z to a row-echelon form $R = \left[\begin{smallmatrix} M & * \\ O & N \end{smallmatrix}\right]$, where O is a zero matrix, M is an $r \times m$ matrix without any zero rows, N is an $(m+s-r) \times m$ matrix. **(1)** Prove that the rows of M form a basis for $U + W$. **(2)** Prove that the non-zero rows of N form a basis for $U \cap W$. This method is attributed to H. Zassenhaus.

E.16.6. In $\mathbb{R}^3$ we are given three subspaces U, V, W. The subspace U is spanned by the vectors:

$$u_1 = (1,-1,-2), \quad u_2 = (-2,2,4), \quad u_3 = (0,1,3), \quad u_4 = (-1,2,5).$$

The subspace V has the basis $\{v_1, v_2\}$ where $v_1 = (1,0,2)$, $v_2 = (0,1,5)$. And the subspace W is the plane with direction vectors $w_1 = (1,0,1)$, $w_2 = (1,1,4)$, passing by the origin O. **(1)** Find the dimension and a basis for the subspace U. **(2)** Detect if there are equal subspaces among the subspaces U, V, W. **(3)** Compute a basis for the sum $U + V$. Detect if $U + V = \mathbb{R}^3$. **(4)** Deduce from information obtained in points (a), (b) and (c) what is the dimension of the intersection $U \cap V$. Then compute a basis for $U \cap V$ by any method.

E.16.7. Four subspaces are given in the space $\mathbb{R}^4$, and we have the following information on them. The subspace U is spanned by four vectors $u_1 = (1,0,0,1)$, $u_2 = (-2,0,0,-2)$, $u_3 = (1,1,0,0)$, $u_4 = (4,1,0,3)$. All the vectors of the subspace V are collinear to the vector u_4. The subspace W has a basis consisting of vectors $w_1 = (0,0,1,0)$, $w_2 = (8,2,0,6)$, $w_3 = (5,2,1,3)$. The subspace Y is given by its basis $\{(5,2,0,3), (2,1,0,1)\}$. **(1)** Comparing the subspaces dimensions *and* using Algorithm 16.1 find out which of the subspaces U, V, W, Y are equal. *Hint*: do not apply Algorithm 16.1 to *each* pair of subspaces. Consider their dimensions first! **(2)** Using the dimensions of the subspaces *only* deduce if U, V or Y may contain W as a subspace. Using Algorithm 16.3 *and* the results from point (1) above find out if W contains U, V or Y.

E.16.8. In the space $\mathbb{R}^3$ the following two subspaces are given. The subspace U is the plane passing via O, and it has the direction vectors $u_1 = (0,1,1)$, $u_2 = (2,0,1)$. The subspace W is spanned by the vectors $w_1 = (2,2,3)$, $w_2 = (0,0,1)$, $w_3 = (1,1,2)$. **(1)** Find a basis for $U + W$. Deduce if this sum is equal to $\mathbb{R}^3$. Find the dimensions of U and W, and using the dimensions of U, W and of $U + W$ deduce by Theorem 15.12 weather the intersection $U \cap W$ is a line. **(2)** Compute a basis for the intersection $U \cap W$ in two methods (the mathod used in Example 16.10 and the mathod used in Example 16.11).

E.16.9. Assume we have $V = U_1 \oplus \cdots \oplus U_k$. Prove that we will get the same direct sum V if we put brackets in this sum. E.g., $U_1 \oplus U_2 \oplus U_3 \oplus U_4 \oplus U_5 \oplus U_6 = (U_1 \oplus U_2) \oplus \big(U_3 \oplus U_4 \oplus (U_5 \oplus U_6)\big)$.

E.16.10. Assume $V = U_1 + \cdots + U_k$, and for any any distinct indices $i, j = 1, \ldots, k$ we have $U_i \cap U_j = \{0\}$. Prove that the sum $U_1 + \cdots + U_k$ is direct.

E.16.11. We are given the real polynomial space $V = \mathcal{P}_3$. **(1)** Present P as a direct sum of four subspaces. **(2)** Present P as a direct sum of four subspaces each of which contains a polynomial of degree 3.

E.16.12. Can the sum of four non-zero subspaces of $\mathbb{R}^3$ be a direct sum?

Part 6

Determinants and their Applications

CHAPTER 17

Definitions and basic properties of determinant

"The mathematical sciences particularly exhibit order, symmetry, and limitation; and these are the greatest forms of the beautiful."
Aristotle

In older linear algebra courses determinants were one of the first concepts to learn, and all other topics, such as systems of linear equations, linear independence, inverse matrices, etc., were considered using the determinants. This reflected the importance of determinants and the historical role they played in development of modern linear algebra (actually, the determinants were invented long before matrices). However, we now are witnessing a shift in emphasis away from determinants. This mainly is caused by newer, better computation methods developed in linear algebra. In our course we present all main properties of determinants without making them the central tool of the course.

17.1. Defining determinant by cofactor expansion

The *determinant* $\det(A)$ or $|A|$ is a scalar value holding some key information about square matrix $A \in M_{n,n}(F)$ or about the system of vectors (formed by rows or by columns of A). We may think of determinant as of a kind of generalization for the notions of *length*, *area* or *volume*. Let us start by the some illustrations.

Firstly, for any vector $u = \overrightarrow{OA} = (a_{11})$ in the 1-dimensional space $\mathbb{R}^1 = \mathbb{R}$ the length $|u|$ clearly is equal to absolute value of a_{11}. In general, considering the vector $u \in F^1 = F$ over a field F as a 1×1 matrix $A = [a_{11}] \in M_{1,1}(F)$ we define the determinant of this matrix as:

$$\det(A) = \left|a_{11}\right| = a_{11}.$$

Next, two non-collinear vectors $u = \overrightarrow{OA} = (a_{11}, a_{12})$ and $v = \overrightarrow{OB} = (a_{21}, a_{22})$ are defining a parallelogram with sides u and v on the plane $\mathbb{R}^2$. From Figure 17.1 (a) it is easy to see that the area of this parallelogram is $a_{11}a_{22} - a_{12}a_{21}$ (the area of $OADB$ is equal to the area of the large green rectangle minus the area marked by darker green). Putting the coordinates of u and v together we get the matrix

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

which is correlated with the parallelogram's area, since $a_{11}a_{22} - a_{12}a_{21}$ is the difference of the products of entries on diagonals of this matrix, as shown in Figure 17.2 (a). Generalizing this approach for any matrix $A \in M_{2,2}(F)$ over any field F we define its determinant $\det(A)$ as:

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} \tag{17.1}$$

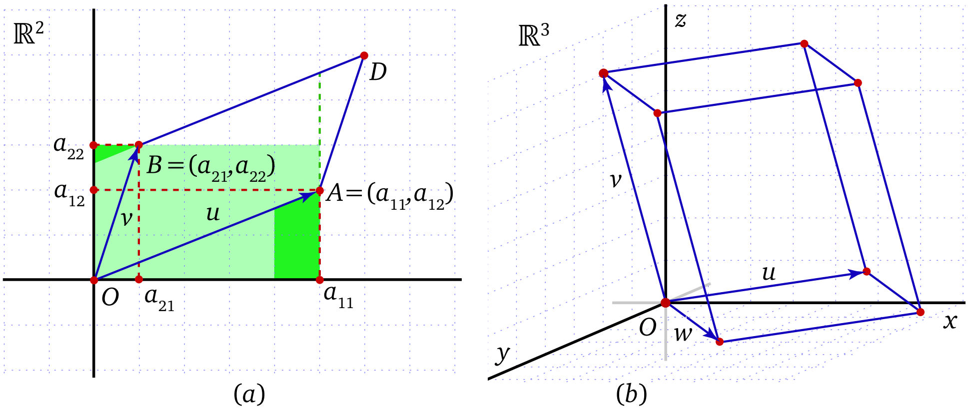


FIGURE 17.1. Visualization of determinants in $\mathbb{R}^2$ and $\mathbb{R}^3$.

(notice how it is denoted like a matrix, but with straight lines at both sides).

Next, for any three non-coplanar vectors $u = \overrightarrow{OA} = (a_{11}, a_{12}, a_{13})$, $v = \overrightarrow{OB} = (a_{21}, a_{22}, a_{23})$ and $w = \overrightarrow{OC} = (a_{31}, a_{32}, a_{33})$ a parallelepiped with edges u, v and w can be given in space $\mathbb{R}^3$ (see Figure 17.1 (b)). Its volume can be expressed by the coordinates a_{ij} as the absolute value of the sum:

$$a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} \tag{17.2}$$

(we bring it without proof, as the routine geometrical argument has no relevance for our course). The analog of this formula can be considered for any matrix $A \in M_{3,3}(F)$ over any field F. Grouping the summands by a_{11}, by a_{21}, and by a_{31}, and then using the previous definition of determinants of degree 2 we get the definition of determinant of degree 3:

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

$$= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \tag{17.3}$$

$$= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{21}(a_{12}a_{33} - a_{13}a_{32}) + a_{31}(a_{12}a_{23} - a_{13}a_{22}).$$

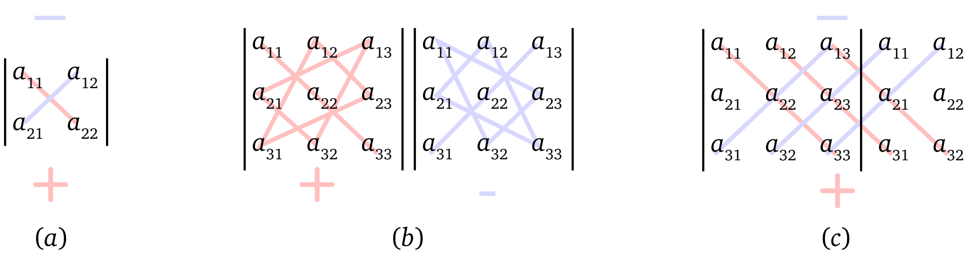


FIGURE 17.2. Computing determinants of degree 2 and 3.

There are easy ways to memorize this formula. (17.3) in fact consists of six summands, of which three are with sign +, and three are with sign −. Figure 17.2 (*b*) shows how the three summands with + sign can be found on the red line: a_{11}, a_{22}, a_{33} and on two red triangles: a_{12}, a_{23}, a_{31} and a_{13}, a_{21}, a_{32}, while three summands with − sign can be found on the blue line: a_{13}, a_{22}, a_{31} and on blue triangles: a_{12}, a_{21}, a_{33} and a_{11}, a_{23}, a_{32}. Figure 17.2 (*c*) displays another method: copy the 1'st and 2'nd columns of the determinant to its right-hand side. Then draw three parallel red lines and three parallel blue lines. Three summands with + sign will be on red lines, and three summands with − sign will be on blue lines.

Example 17.1. Using technique of Figure 17.2 we compute:

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

$$+2\cdot 0\cdot 4 - 2\cdot 6\cdot 5 - 3\cdot 0\cdot 2 - 1\cdot 1\cdot 4 = -37.$$

Example 17.2. For a matrix on complex field $F=\mathbb{C}$ we get:

$$\begin{vmatrix} i & 0 & 1 \\ 1 & 2 & 1+i \\ 0 & -1 & 0 \end{vmatrix} = i\cdot 2\cdot 0 + 0\cdot(i+1)\cdot 0 + 1\cdot 1\cdot(-1)$$

$$-1\cdot 2\cdot 0 - 0\cdot 1\cdot 0 - i\cdot(i+1)\cdot(-1) = i-2.$$

Example 17.3. Compute a determinant over the finite field $F=\mathbb{Z}_3$:

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

$$-1\cdot 0\cdot 0 - 2\cdot 1\cdot 1 - 1\cdot 2\cdot 1$$

$$= +1-2-2 = +1+1+1 = 0.$$

Notice that in this example all computations are done modulo 3 as we are in the field $F=\mathbb{Z}_3$.

To generalize the determinants for matrices $A\in M_{n,n}(F)$ of any degree n we need some special terms. Assume we are given any $n\times n$ matrix on F. Fix some $i,j=1,\ldots,n$ and mark the i'th row and the j'th column of A:

$$A = \begin{bmatrix} a_{11} \cdots \boldsymbol{a_{1j}} \cdots a_{1n} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \boldsymbol{a_{i1}} \cdots \boldsymbol{a_{ij}} \cdots \boldsymbol{a_{in}} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1} \cdots \boldsymbol{a_{nj}} \cdots a_{nn} \end{bmatrix}.$$

Denote by M_{ij} the matrix obtained from A by removing its i-th row and j-th column.

Example 17.4. For the matrix

$$A = \begin{bmatrix} \mathbf{1} & 2 & 1 & 0 \\ 0 & 2 & \mathbf{4} & 2 \\ 1 & 0 & 1 & 1 \\ 5 & 0 & 0 & 7 \end{bmatrix}$$

it is very easy to get:

$$M_{11} = \begin{bmatrix} 2 & 4 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 7 \end{bmatrix}, \quad M_{23} = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 5 & 0 & 7 \end{bmatrix}.$$

Now it is easy to see that (17.1) can be re-written as

$$\det(A) = a_{11}\det(M_{11}) - a_{21}\det(M_{21}),$$

and (17.3) can be re-written as

$$\det(A) = a_{11}\det(M_{11}) - a_{21}\det(M_{21}) + a_{31}\det(M_{31}).$$

In other words, $\det(A)$ is the sum of the elements a_{i1} of the 1'st column, each multiplied by respective determinant $\det(M_{i1})$ times $(-1)^{i+1}$. This allows us do inductively define the determinants for matrices of any degree n, assuming that the determinants of degree $n-1$ already are defined. Namely:

$$\det(A) = a_{11}\det(M_{11}) - a_{21}\det(M_{21}) + a_{31}\det(M_{31}) + \cdots \pm a_{n1}\det(M_{n1}).$$

For any matrix $A \in M_{n,n}(F)$ call for each pair $i,j = 1,\dots,n$ the (i,j)-*cofactor of* A or the *cofactor of the entry* a_{ij} the product $A_{ij} = (-1)^{i+j}\det\big(M_{ij}\big)$. In this notation the definition of determinant can be written in shorter shape:

$$\textbf{det}(\boldsymbol{A}) = |\boldsymbol{A}| = \begin{vmatrix} \boldsymbol{a_{11}} & \cdots & \boldsymbol{a_{1n}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{n1}} & \cdots & \boldsymbol{a_{nn}} \end{vmatrix} = \sum_{i=1}^{n} \boldsymbol{a_{i1}A_{i1}}. \tag{17.4}$$

We call this *cofactor expansion* of $\det(A)$ by the 1'st column. The determinants $\det\big(M_{ij}\big)$ sometimes are called the (i,j)-*minors* of A.

Example 17.5. Let us compute the determinant of the matrix A below. Since A is of degree 4 we have to inductively reduce computation to the matrices of degree 3.

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

Start with calculation of all four cofactors:

$$A_{11} = (-1)^{1+1}\det(M_{11}) = \begin{vmatrix} 2 & 0 & 2 \\ 1 & 1 & 0 \\ 1 & 2 & 2 \end{vmatrix} = 6,$$

$$A_{21} = (-1)^{2+1}\det(M_{21}) = -\begin{vmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 2 & 2 \end{vmatrix} = 1,$$

$$A_{31} = (-1)^{3+1}\det(M_{31}) = \begin{vmatrix} 0 & 1 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 2 \end{vmatrix} = 2,$$

$$A_{41} = (-1)^{4+1}\det\big(M_{41}\big) = -\begin{vmatrix} 0 & 1 & 1 \\ 2 & 0 & 2 \\ 1 & 1 & 0 \end{vmatrix} = -4.$$

So we get the determinant as:

$$\det(A) = 2\cdot 6 + 0\cdot 1 + 1\cdot 2 + 1\cdot(-4) = 10.$$

Notice that we in fact could omit the computation of A_{21} because $a_{21} = 0$, and so $a_{21}A_{21}$ iz zero.

Although we now can compute any determinant of arbitrary degree, the method is very routine. We will get much better algorithms for determinant computation after we learn more about the properties of determinants.

17.2. Basic properties of determinants

This property shows how the determinant changes, if we apply an *elementary operation of the 2'nd type*:

Proposition 17.6. *If a row of a matrix $A = [a_{ij}]_n \in M_{n,n}(F)$ is multiplied by a scalar $c \in F$, then the determinant of A also is multiplied by c:*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{c\cdot a_{k1}} & \cdots & \boldsymbol{c\cdot a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = c\cdot \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = c\det(A). \tag{17.5}$$

Proof. Apply induction on n. For $n = 1$ we get the evident equality $|c\,a_{11}| = c\,a_{11} = c\,|a_{11}|$. Suppose the proposition holds for matrices of degree $n-1$. Denote by $B = [b_{ij}]_n$ the matrix obtained from A by multiplying the k'th row by c (so we have $\det(B)$ on the left-hand side of (17.5)). By definition $\det(B) = \sum_{i=1}^n b_{i1}B_{i1}$, where B_{i1} is the cofactor of b_{i1}. If here $i = k$, then $b_{i1} = b_{k1}$ is in the k'th row of B, i.e., $b_{k1} = c\,a_{k1}$. Since all rows of B, except the k'th, coincide with the rows of A, we have $B_{k1} = A_{k1}$, and so $b_{k1}B_{k1} = c\,a_{k1}A_{k1}$. And when $i \neq k$, then b_{i1} is outside the k'th row, i.e., $b_{i1} = a_{i1}$. Then B_{i1} necessarily includes the row multiplied by c. Since the degree of B_{i1} is $n-1$, by induction $B_{i1} = c\,A_{i1}$. So again $b_{i1}B_{i1} = a_{i1}\,c\,A_{i1}$. We have $\det(B) = \sum_{i=1}^n b_{i1}B_{i1} = \sum_{i=1}^n c\,a_{i1}A_{i1} = c\det(A)$. □

Taking the value $c = 0$ we easily get:

Proposition 17.7. *If a row of a matrix $A \in M_{n,n}(F)$ consists of zeros only, then* $\det(A) = 0$.

Example 17.8. It is easy to compute that

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

Thus, by Proposition 17.6:

$$\begin{vmatrix} 2 & 0 & 2 \\ 3 & 2 & 2 \\ -3 & -3 & 0 \end{vmatrix} = 2\cdot(-1)\cdot(-3) = 6$$

because in this determinant is obtained from the 1'st by multiplying the 1'st row by 2 and the third row by -3.

Example 17.9. By Proposition 17.7the following determinant is zero:

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

Proposition 17.10. *If each entry of a row in $A = [a_{ij}]_n \in M_{n,n}(F)$ is a sum of two numbers, then* $\det(A)$ *can be presented as a sum of two determinants:*

$$\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b_{k1} + c_{k1}} & \cdots & \boldsymbol{b_{kn} + c_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{b_{k1}} & \cdots & \boldsymbol{b_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{c_{k1}} & \cdots & \boldsymbol{c_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}. \tag{17.6}$$

Proof. Using induction on n, we for $n = 1$ get the equality $|a_{11} + b_{11}| = a_{11} + b_{11} = |a_{11}| + |b_{11}|$. Assume the statement holds for matrices of degree $n-1$.

Denote by B and C the matrices that coincide with A in all rows except the k'th. Define the k'th row of B as $[b_{k1} \ \cdots \ b_{kn}]$, and define the k'th row of C as $[c_{k1} \ \cdots \ c_{kn}]$. So the equality (17.6) now looks like $\det(A) = \det(B) + \det(C)$.

We by definition have $\det(A) = \sum_{i=1}^n a_{i1}A_{i1}$. Consider the k'th summand of this sum: if $i = k$, then $a_{i1} = a_{k1}$ is in the k'th row of A, i.e., $a_{k1} = b_{k1} + c_{k1}$. Since all rows of A, except the k'th, coincide with the rows of B and of C, we have $A_{k1} = B_{k1} = C_{k1}$, and so

$$a_{k1}A_{k1} = (b_{k1} + c_{k1})A_{k1} = b_{k1}A_{k1} + c_{k1}A_{k1} = b_{k1}B_{k1} + c_{k1}C_{k1}.$$

And when $i \neq k$, then a_{i1} is outside the k'th row of A, i.e., $a_{i1} = b_{i1} = c_{i1}$. Also, the cofactors A_{i1}, B_{i1}, C_{i1} necessarily include the k'th row consisting of the sums. Since the degrees of A_{i1}, B_{i1}, C_{i1} are $n-1$, by induction $A_{i1} = B_{i1} + C_{i1}$. So again

$$a_{i1}A_{i1} = a_{i1}(B_{i1} + C_{i1}) = a_{i1}B_{i1} + a_{i1}C_{i1} = b_{i1}B_{i1} + c_{i1}C_{i1}.$$

We have $\det(A) = \sum_{i=1}^n a_{i1}A_{i1} = \sum_{i=1}^n b_{i1}B_{i1} + \sum_{i=1}^n b_{i1}B_{i1} = \det(B) + \det(C)$. □

Example 17.11. If we know two determinants:

$$\begin{vmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 3 & -1 & 1 \end{vmatrix} = -4, \quad \begin{vmatrix} 1 & 0 & 1 \\ 3 & 3 & 1 \\ 3 & -1 & 1 \end{vmatrix} = -8,$$

then the following determinant can be obtained byProposition 17.10:

$$\begin{vmatrix} 1 & 0 & 1 \\ 3 & 5 & 1 \\ 3 & -1 & 1 \end{vmatrix} = -4 - 8 = -12.$$

The next property shows how does an *elementary operation of the* 1*'st type* change the determinant of a matrix:

Proposition 17.12. *Swapping any two rows in a matrix* $A = [a_{ij}]_n \in M_{n,n}(F)$ *negates its determinant* $\det(A)$*:*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \mathbf{a_{l1}} & \cdots & \mathbf{a_{ln}} \\ \cdots & \cdots & \cdots \\ \mathbf{a_{k1}} & \cdots & \mathbf{a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = - \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \mathbf{a_{k1}} & \cdots & \mathbf{a_{kn}} \\ \cdots & \cdots & \cdots \\ \mathbf{a_{l1}} & \cdots & \mathbf{a_{ln}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = -\det(A) \tag{17.7}$$

***Proof*.** Apply induction on n. For $n = 1$ get $|a_{11}| = a_{11} = |a_{11}|$ (no rows to swap, but if this is confusing, you may consider the matrices of degree 2). Assume the statement holds for matrices of degree $n-1$. Denote by $B = [b_{ij}]_n$ the matrix obtained from A by swapping the k'th and l'th rows. So (17.12) can be written as $\det(B) = -\det(A)$. First consider the case of "neighbor rows", i.e., $l = k+1$:

$$B = \begin{vmatrix} b_{11} & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ \mathbf{b_{k1}} & \cdots & \mathbf{b_{kn}} \\ \mathbf{b_{k+1\,1}} & \cdots & \mathbf{b_{k+1\,n}} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \mathbf{a_{k+1\,1}} & \cdots & \mathbf{a_{k+1\,n}} \\ \mathbf{a_{k1}} & \cdots & \mathbf{a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

Compare the cofactors B_{k1} and $A_{k+1\,1}$. Clearly, they include the same rows, but their signs are inverse, since $(-1)^{k+1} = -(-1)^{(k+1)+1}$. The same can be observed comparing $B_{k+1\,1}$ and A_{k1}. So we have two equalities:

$$b_{k1}B_{k1} = a_{k+1\,1} \cdot (-A_{k+1\,1}) \quad \text{and} \quad b_{k+1\,1}B_{k+1\,1} = a_{k1} \cdot (-A_{k1}).$$

Next compare the cofactors B_{i1} and A_{i1} for any $i \neq k, k+1$. They include exactly the same rows of A in the same order, except two rows swapped, that is, $B_{i1} = -A_{i1}$. And since $b_{i1} = -b_{i1}$, we have the equalities:

$$b_{i1}B_{i1} = a_{i1} \cdot (-A_{i1}) \quad \text{for any } i \neq k, k+1.$$

Therefore we get $\det(B) = \sum_{i=1}^{n} b_{i1}B_{i1} = -\left(\sum_{i=1}^{n} a_{i1}A_{i1}\right) = -\det(A)$.

Next consider the case of arbitrary k and l (suppose $k < l$). The swapping of the k'th and l'th rows can be achieved by a series of swappings of *neighbor* rows. Namely, swap the k'th row with the $(k+1)$'th row, then with $(k+2)$'th row, etc... then with $(l-1)$'th row. So we brought that row right before the l'th row using $l-k-1$ swapping operations. Then swap that row with the l'th row, and bring the l'th row to the former position of the k'th row using $l-k-1$ swappings of neighbor rows again. The final result is that we just swapped the k'th and l'th rows of A, and we did that using $(l-k-1)+1+(l-k-1) = 2(l-k-1)+1$ swappings of neighbor rows. The above number is odd, so we have negated the determinant odd times, i.e., $\det(B) = -\det(A)$. □

When a matrix A has two *equal* rows, then the swapping those rows at the one hand negates the matrix, on the other hand, nothing actually changes in A as the rows are equal. So we have $\det(A) = -\det(A)$, which gives us the following property:

Proposition 17.13. *If a matrix* $A \in M_{n,n}(F)$ *has two equal rows, then* $\det(A) = 0$.

The next proposition shows that the *elementary operation of the* 3*'rd type* does not alter a matrix's determinant:

Proposition 17.14. *The determinant of a matrix $A = [a_{ij}]_n \in M_{n,n}(F)$ will not change after adding to one of its rows another row multiplied by a scalar:*

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{l1} + c \cdot a_{k1}} & \cdots & \boldsymbol{a_{ln} + c \cdot a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{l1}} & \cdots & \boldsymbol{a_{ln}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \det(A)\,.$$

***Proof*.** Denote by B the matrix for the determinant of the left-hand side of the equation above. Applying Proposition 17.10 and then Proposition 17.6 to B we get:

$$\det(B) = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{l1}} & \cdots & \boldsymbol{a_{ln}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + c \cdot \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ \boldsymbol{a_{k1}} & \cdots & \boldsymbol{a_{kn}} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

The first of the summands above is nothing else but $\det(A)$. And the second summand iz zero by Proposition 17.13. So we have $\det(B) = \det(A) + c \cdot 0 = \det(A)$. □

Example 17.15. We in previous example got the determinant:

$$\begin{vmatrix} 1 & 0 & 1 \\ 3 & 5 & 1 \\ 3 & -1 & 1 \end{vmatrix} = -12.$$

Now using Proposition 17.14 we get:

$$\begin{vmatrix} 4 & -1 & 2 \\ 3 & 5 & 1 \\ 3 & -1 & 1 \end{vmatrix} = -12, \quad \begin{vmatrix} 1 & 0 & 1 \\ 3 & 5 & 1 \\ 9 & 9 & 3 \end{vmatrix} = -12.$$

Call a square matrix $A = [a_{ij}]_n \in M_{n,n}(F)$ an *upper triangle matrix*, if all the elements below its main diagonal are zero: $a_{ij} = 0$ for all $i > j$. And call A a *lower triangle matrix* if all the elements above its main diagonal are zero: $a_{ij} = 0$ for all $i < j$. An upper triangle matrix, clearly, is a *row-echelon* form. If a matrix is both upper- and lower triangle, then all its entries are zero except those on the main diagonal. Such matrices are called *diagonal* matrices.

Example 17.16. The first of these matrices is upper triangle, the second is lower triangle:

$$\begin{bmatrix} 3 & 2 & 2 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 7 \end{bmatrix}, \quad \begin{bmatrix} 6 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 3 & 1 & 0 \\ 1 & 0 & 2 & 3 \end{bmatrix}.$$

Here is an example of a diagonal matrix:

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

The identity matrix $I = I_n$ is a diagonal matrix for any $n = 1, 2, 3, \ldots$.

It turns out that the determinants of triangle matrices are especially easy to compute:

Proposition 17.17. *The determinant of an upper (lower) triangle matrix $A = [a_{ij}]_n \in M_{n,n}(F)$ is equal to the product of all elements on its diagonal:*

$$\det(A) = a_{11} \cdots a_{nn}.$$

***Proof*.** Apply induction on n. For $n = 1$ we trivially have $|a_{11}| = a_{11}$. Suppose the lemma holds for all matrices of degree $n-1$, and write the determinant by definition as

$\det(A) = \sum_{i=1}^{n} a_{i1}A_{i1}$. If $i = 1$, the cofactor $A_{i1} = A_{11}$ is a triangle matrix with elements $a_{22}, \dots, a_{nn}$ on its diagonal. So by induction $A_{11} = a_{22} \cdots a_{nn}$. When $i \neq 1$ and A is an *upper* triangle matrix, then the entry a_{i1} is zero by definition of upper triangle matrix. Thus we get:

$$\det(A) = \sum_{i=1}^{n} a_{i1}A_{i1} = a_{11} \cdot a_{22} \cdots a_{nn} + 0 \cdot A_{21} + \cdots + 0 \cdot A_{n1} = a_{11} \cdots a_{nn}.$$

When $i \neq 1$ and A is a *lower* triangle matrix, then the entries $a_{12}, \dots, a_{1n}$ all are zero since A is a lower triangle matrix. Thus, any of the cofactors $A_{21}, \dots, A_{n1}$ contains a zero row and is equal to zero by Proposition 17.7. This time we get:

$$\det(A) = \sum_{i=1}^{n} a_{i1}A_{i1} = a_{11} \cdot a_{22} \cdots a_{nn} + a_{21} \cdot 0 + \cdots + a_{n1} \cdot 0 = a_{11} \cdots a_{nn}.$$

□

Example 17.18. So the determinant of the first matrix in Example 17.16 is $3 \cdot 2 \cdot 1 \cdot 7 = 42$, and the determinant of the second is $6 \cdot 1 \cdot 1 \cdot 3 = 18$. The determinant of the third matrix is equal to $4 \cdot (-2) \cdot 1 \cdot 3 = -24$. And the determinant of an identity matrix $I = I_n$ is equal to 1 for any $n = 1, 2, 3, \dots$.

17.3. Determinants and matrix operations

The determinants of the elementary matrices are especially easy to find:

Lemma 17.19. *Let E be any elementary matrix.*

1. *If E is an elementary matrix of the 1'st type, then* $\det(E) = -1$.
2. *If E is an elementary matrix of the 2'nd type (for some non-zero c), then* $\det(E) = c$.
3. *If E is an elementary matrix of the 3'rd type, then* $\det(E) = 1$.

***Proof*.** These follow from the facts that $\det(I) = 1$, and that an elementary matrix is obtained from the identity matrix I by the respective elementary operation.

In the first case E is obtained from I by swapping two of its rows. By Proposition 17.12 $\det(E) = -\det(I) = -1$.

In the second case E is obtained from I by multiplying one of its rows by a non-zero scalar c. By Proposition 17.6 $\det(E) = c \cdot \det(I) = c$.

In the third case E is obtained from I by adding to one of its rows another row times a scalar. By Proposition 17.12 $\det(E) = \det(I) = 1$. □

From this lemma immediately follows:

Corollary 17.20. *If $E \in M_{n,n}(F)$ is any elementary matrix, then for any matrix $A \in M_{n,n}(F)$ we have:*

$$\det(EA) = \det(E) \cdot \det(A).$$

Earlier we gave equivalent conditions for invertible matrices (see Theorem 9.10 and corollaries 13.7, 14.14). Determinants provide one more equivalent condition:

Corollary 17.21 (Amendment to Theorem 9.10). *A matrix $A \in M_{n,n}(F)$ is invertible if and only if* $\det(A) \neq 0$.

Proof. By (9.4) we have $E_t \cdots E_1 \cdot A = \operatorname{rref}(A)$. Repeated application of Corollary 17.20 to this product gives:

$$\det(E_t \cdots E_1 \cdot A) = \det(E_t) \cdots \det(E_1) \cdot \det(A) = \det\big(\operatorname{rref}(A)\big). \tag{17.8}$$

By Lemma 17.19 none of $\det(E_t), \ldots, \det(E_1)$ is zero, that is, $\det(A)$ is zero if and only if $\det\big(\operatorname{rref}(A)\big)$ is zero. When A is invertible, then $\operatorname{rref}(A) = I$, so $\det(I) = 1 \neq 0$. And when A is *not* invertible, then $\operatorname{rank}(A) < n$, so the last row of $\operatorname{rref}(A)$ is zero, and $\det\big(\operatorname{rref}(A)\big) = 0$ by Proposition 17.7. □

Adaptation of the above technique yields the important:

Theorem 17.22. *The determinant of the product of any two matrices $A, B \in M_{n,n}(F)$ is equal to the product of determinants of A and B:*

$$\mathbf{det}(\boldsymbol{AB}) = \mathbf{det}(\boldsymbol{A}) \cdot \mathbf{det}(\boldsymbol{B}).$$

Proof. By Lemma 17.19 it is trivial to see that $\det\big(E^{-1}\big) = \det(E)^{-1}$ for any elementary matrix. From that and from (17.8) we have:

$$\det(A) = \det\big(E_1^{-1}\big) \cdots \det\big(E_t^{-1}\big) \cdot \det\big(\operatorname{rref}(A)\big). \tag{17.9}$$

Similarly, from $AB = \big(E_1^{-1} \cdots E_t^{-1} \operatorname{rref}(A)\big) B = E_1^{-1} \cdots E_t^{-1} \big(\operatorname{rref}(A) B\big)$ we have:

$$\det(AB) = \det\big(E_1^{-1}\big) \cdots \det\big(E_t^{-1}\big) \cdot \det\big(\operatorname{rref}(A) B\big). \tag{17.10}$$

If A is invertible, then $\operatorname{rref}(A) = I$, and (17.10) with (17.9) imply:

$$\det(AB) = \det\big(E_1^{-1}\big) \cdots \det\big(E_t^{-1}\big) \cdot \det(B) = \det(A) \cdot \det(B).$$

If A is *not* invertible, then $\det(A) = 0$ by Corollary 17.21, and so $\det(A) \cdot \det(B) = 0$. As we saw in previous proof, the last row of $\operatorname{rref}(A)$ is zero. Then the last row of the product $\operatorname{rref}(A) \cdot B$ also is zero (verify this using the matrix multiplication law), and so $\det\big(\operatorname{rref}(A) \cdot B\big) = 0$ also is zero. Then (17.10) implies $\det(AB) = 0$. □

Applying this theorem to the equality $A \cdot A^{-1} = I$ we get:

Corollary 17.23. *If the matrix $A \in M_{n,n}(F)$ is invertible, then:*

$$\mathbf{det}\,(\boldsymbol{A}^{-1}) = \big(\mathbf{det}(\boldsymbol{A})\big)^{-1}.$$

Example 17.24. Apply the above theorem on an example:

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

Then the product of these matrices is the following matrix:

$$AB = \begin{bmatrix} 1 & 3 & 3 \\ 5 & 8 & 4 \\ 1 & 3 & 7 \end{bmatrix}.$$

Computing all three determinants we get $\det(A) = 2$, $\det(B) = -14$, and

$$\det(AB) = -28 = 2 \cdot (-14).$$

Lemma 17.25. *For any matrix $A \in M_{n,n}(F)$ we have* $\det\big(A^T\big) = \det(A)$.

Proof. Applying point 4 of Proposition 8.15 to

$$A = E_1^{-1} \cdots E_t^{-1} \operatorname{rref}(A) \tag{17.11}$$

we have:

$$A^T = \operatorname{rref}(A)^T \left(E_t^{-1}\right)^T \cdots \left(E_1^{-1}\right)^T. \tag{17.12}$$

Each elementary matrix E_i^{-1} and its transpose $\left(E_i^{-1}\right)^T$ have the same determinant (an elementary matrix of the 1'st or 2'nd type coincides with its transpose, and an elementary matrix of the 3'type is a triangle matrix with diagonal consisting of 1's, see Proposition 17.17). Further, $\text{rref}(A)$ and $(\text{rref}(A))^T$ also have the same determinant, as they both are triangle matrices with the same diagonal.

Applying Theorem 17.22 to the products (17.11) and (17.12) we see that $\det(A)$ and $\det\left(A^T\right)$, in fact, are products of some *equal* factors, just written in reverse orders. □

This proposition allows us to at once get "column analogs" of all the properties we proved in Section 17.2 for determinants. Indeed, it is essential that after transposition all columns of a matrix are becoming rows. So if, say, a matrix A has a *zero column*, then $\det(A) = 0$ because the transpose A^T has a *zero row*, and $\det(A) = \det\left(A^T\right) = 0$.

Let us collect the obtained analogs as:

Proposition 17.26. *Let $A \in M_{n,n}(F)$ be any matrix.*

1. *If a column of A is multiplied by a scalar $c \in F$, then the determinant of A also is multiplied by c (see Proposition 17.6).*
2. *If a column of A consists of zeros only, then $\det(A) = 0$ (see Proposition 17.7).*
3. *If each entry in k'th column of A is a sum of a pair of numbers, then $\det(A)$ can be presented as a sum of two respective determinants (see Proposition 17.10).*
4. *Swapping any two columns in A negates its determinant (see Proposition 17.12).*
5. *If A has two equal columns, then its determinant is zero (see Proposition 17.13).*
6. *The determinant of A will not change after adding to one of its columns another column multiplied by a scalar (see Proposition 17.14).*

In analogy to shorthand notations $Ri \leftrightarrow Rj$, $c \cdot Ri$ $(c \neq 0)$, $Ri + cRj$ that we used for elementary *row* operations, we will wherever needed use the shorthand notations $Ci \leftrightarrow Cj$, $c \cdot Ci$ $(c \neq 0)$, $Ci + cCj$ to record the elementary operations with matrix *columns* ("C" stands for "column").

17.4. Defining determinant by permutations

Another method of determinant definition is its introduction by permutations. We assume you are familiar with permutations, their parity (inversions, odd and even permutations), products and inverses of permutations, transpositions (we bring a brief outline of them in appendices E.1–E.3).

Take a square matrix $A \in M_{n,n}(F)$, and choose an entry in each row (so that *only one* entry is choosen from each column):

$$A = \begin{bmatrix} a_{11} & \cdots\cdots\cdots & \boldsymbol{a_{1i_1}} & \cdots\cdots\cdots & a_{1n} \\ a_{21} & \cdots\cdots\cdots\cdots\cdots & \boldsymbol{a_{2i_2}} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & \cdots\ \boldsymbol{a_{ni_n}} & \cdots\cdots\cdots\cdots & & a_{nn} \end{bmatrix}.$$

Since each column is evolved one time only, this choice defines a permutation σ:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_2 & i_2 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Consider the product

$$\text{sgn}(\sigma) \cdot a_{1i_1} a_{2i_2} \cdots a_{ni_n} = \text{sgn}(\sigma) \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

The products of this type are the "building blocks" needed for determinant definition below. For a matrix $A \in M_{n,n}(F)$ there are exactly $n!$ products of the mentioned type, since each product is defined by a $\sigma \in S_n$, and there are $n!$ permutation of degree n.

The *determinant* $\det(A)$ of the matrix A is defined as the sum:

$$\det(A) = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}. \tag{17.13}$$

So the determinant $\det(A)$ is a sum of $n!$ summands, each consisting of the product $a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ (of entries taken from the matrix A), and of $\operatorname{sgn}(\sigma)$ which determines the sign $\pm$ of that summand.

Example 17.27. Compose the above sum for the matrix

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

First start by *one* the above products. Choose, say, the second entry $a_{12} = 3$ in first line, the third entry $a_{23} = 1$ in second line, and the first entry $a_{31} = 5$ in third line (marked in bold). The respective permutation is $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. It has 2 inversions, so σ is even, and $\operatorname{sgn}(\sigma) = 1$. Then the respective product of the above mentioned type is:

$$\operatorname{sgn}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot 3 \cdot 1 \cdot 5 = (+1) \cdot 15 = 15.$$

All 6 summands of the determinant are:

$$\begin{aligned} \det(A) = \operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \cdot 1 \cdot 6 \cdot 2 \\ +\operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot 3 \cdot 1 \cdot 5 \\ +\operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot 2 \cdot 0 \cdot 4 \\ +\operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot 2 \cdot 6 \cdot 5 \\ +\operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot 3 \cdot 0 \cdot 2 \\ +\operatorname{sgn}&\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot 1 \cdot 1 \cdot 4 \\ = 12 + 15 + 0 &- 60 - 0 - 4 = -37. \end{aligned}$$

We arrived to the formula already given in (17.2) or (17.3) (compare the above example with Example 17.1). By the way, we again established the rule of Figure 17.2 (b) and (c). Much simpler is the case of 2×2 determinants:

Example 17.28. Let us ompute $\begin{vmatrix} 3 & 6 \\ 5 & 4 \end{vmatrix}$. Then S_2 has just two permutations:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

of which the first is even, the second one is odd.

Therefore we get:

$$\begin{aligned} \begin{vmatrix} 3 & 6 \\ 5 & 4 \end{vmatrix} &= \operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \cdot 3 \cdot 4 \\ &+ \operatorname{sgn}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot 6 \cdot 5 \\ &= 12 - 30 = 18. \end{aligned}$$

Notice that we again found the rule given in Figure 17.2 (a) for computation of determinants of degree 2.

Computation of 1×1 determinants is straightforward: if $A = [a_{11}]$, then $\det(A) = a_{11}$ since we have only one permutation of degree 1, and it is even.

We see that two definitions of determinant output the same result for matrices of degree 1, 2 and 3. We yet have to show that for any degree n. Apply induction supposing the equality proved it for $n-1$. Clearly, each permutation in S_{n-1} can be considered as a permutation on the set $\{2, \ldots, n\}$. Denote their set by $S_{\{2,\ldots,n\}}$.

Fix any index $i = 1, \dots, n$. Since A_{i1} is of degree $n-1$, we have:

$$A_{i1} = \sum_{\sigma \in S_{\{2,\dots,n\}}} \operatorname{sgn}(\sigma) \cdot a_{1\,\sigma(2)} \cdots a_{i-1\,\sigma(i)} \cdot a_{i+1\,\sigma(i+1)} \cdots a_{n\,\sigma(n)}. \tag{17.14}$$

This sum has $(n-1)!$ summands of which the half is with plus sign $\operatorname{sgn}(\sigma)$, and the half is with minus sign $\operatorname{sgn}(\sigma)$. And none of the summands contains an entry from the 1'st column of A. Since the permutations

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & \cdots & n \\ \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

clearly have the same sign, the product $a_{i1}A_{i1}$ actually is a sum of $(n-1)!$ summands which also participate in (17.13) and which all start by a_{i1}. Therefore the sum $\det(A) = \sum_{i=1}^{n} a_{i1}A_{i1}$ is equal to the sum of *all* $n \cdot (n-1)! = n!$ summands of (17.13).

The basic properties of determinants from Section 17.2 can be equally easily deduced from the definition of determinant by permutations. As an illustration let us give alternative proof for Proposition 17.6, i.e., for equality (17.5):

Other proof for Proposition 17.6. Consider the matrix

$$B = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \boldsymbol{c \cdot a_{k1}} & \cdots & \boldsymbol{c \cdot a_{kn}} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

(k'th row is multiplied by c). Then in the sum of determinant

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

in *each* of $n!$ products $a_{1i_1} a_{2i_2} \cdots \boldsymbol{(c \cdot a_{k i_k})} \cdots a_{n i_n}$ the k'th factor is multiplied by c. Clearly, this does not alter the permutation σ, and so the sign $\operatorname{sgn}(\sigma)$ is not changed, at all. Therefore

$$\det(B) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} a_{2\sigma(2)} \cdots \boldsymbol{c \cdot a_{k\sigma(k)}} \cdots a_{n\sigma(n)} = c \det(A).$$

□

Definition of determinant by permutations allows to establish the main properties of determinants just a little bit easier than the cofactor expansion method. On the other hand, it requires knowledge of considerable material on permutations. Thus in this introductory course we first defined determinants by cofactors to make the course less dependent from auxiliary material.

Exercises

E.17.1. We are given the matrices:

$$M = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in M_{3,3}(\mathbb{R}),\ N = \begin{bmatrix} 1 & 3 \\ 5 & 2 \end{bmatrix} \in M_{2,2}(\mathbb{R}),\ K = \begin{bmatrix} i & 3 \\ 1 & 2i \end{bmatrix} \in M_{2,2}(\mathbb{C}),\ L = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in M_{3,3}(\mathbb{Z}_2).$$

(1) For each of these matrices write down its determinant using the definition by cofactor expansion (17.4). **(2)** Write the cofactor A_{23} of M, the cofactor A_{22} of N, the cofactor A_{12} of K, and the cofactor A_{33} of L.

E.17.2. Compute the determinants of matrices M, N, K, L in Exercise E.17.1 using the "graphical method" of Figure 17.2.

E.17.3. Apply each of the operations $R1 \leftrightarrow R3$, $C2 \leftrightarrow C1$, $3 \cdot C3$, $R3 + 2R2$, $C1 - 3C2$ to matrix M of Exercise E.17.1, and explain how its determinant changes after each operation.

E.17.4. We are given that the matrix A is a product of some elementary matrices E_1, E_2, E_3. **(1)** Can we find the matrix A, if we know the elementary matrices E_1, E_2, E_3, but we do *not* know in which order they appear in factorization of A? **(2)** Can we find the determinant $\det(A)$, if we know the elementary matrices E_1, E_2, E_3, but we do *not* know in which order they appear in factorization of A?

E.17.5. Using Theorem 17.22, Corollary 17.23 and Lemma 17.25 find determinants of the matrices M^{-1}, L^{-1}, K^T, $M\,M^{-1}M^T\,M$, where M, N, K, L are the matrices of Exercise E.17.1. *Hint*: you need not actually compute the inverses and transposes above.

E.17.6. We are given the matrices:

$$A = \begin{bmatrix} 3 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 2 & 0 \end{bmatrix} \in M_{3,3}(\mathbb{R}), \quad B = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \in M_{2,2}(\mathbb{R}), \quad C = \begin{bmatrix} 2 & 4 \\ 1 & 2 \end{bmatrix} \in M_{2,2}(\mathbb{Z}_5).$$

(1) For each matrix write down the formula (17.4) of determinant definition by cofactors expansion (write the values of the cofactors). **(2)** Then compute the determinant for each of the matrices by the "graphical" method of Figure 17.2. **(3)** How will the determinant of A change, if we apply the sequence of elementary operations $C1 \leftrightarrow C3$, $3 \cdot R2$, $R2 \leftrightarrow R3$, $R3 + 2^{100} R2$, $\frac{1}{3} \cdot C1$ to A? **(4)** Compute the determinant of the product $A^{-1} \cdot A^T \cdot A^3 \cdot (A^T)^{-1}$ using Using Theorem 17.22, Corollary 17.23 and Lemma 17.25.

E.17.7. Compute the determinants of matrices M, N, K, L in Exercise E.17.1 using the definition by permutations of (17.13).

CHAPTER 18

Determinant computation methods

18.1. The triangle method

Now we can suggest a shorter method for determinants computation. Every matrix A can be brought to a triangle form T by elementary row operations, because a row-echelon form already is a triangle form (using other rows- or column-related properties we can achieve to a triangle form even more quickly – see Example 18.2 below). By Proposition 17.17 $\det(T)$ is just the product of the diagonal elements in T. Now how does it differ from $\det(A)$? If during our steps we have swapped two rows (columns), then we have negated the determinant, so to keep the current value intact just add a minus sign to $\det(T)$. If we have multiplied a row (column) by a non-zero scalar c, we have multiplied the determinant by c, so just multiply $\det(T)$ by $\frac{1}{c}$. And if we added to one row (column) another row (column) times a scalar, then the determinant has not changed, nothing to care about in such a case.

How to compute a determinant by triangle method. The collected properties suggest the following basic method of determinant computation:

Algorithm 18.1 (Computation of a determinant by triangle method)**.** We are given a square matrix $A \in M_{n,n}(F)$.

► Find the determinant $\det(A)$.

1. Introduce an initial value $d = 1$.
2. Using the determinant row and column operations bring A to triangle form T. In this process each time we swap two rows (or two columns), set $d = -d$. And each time we multiply a row (or a column) by a non-zero scalar c, set $d = \frac{1}{c} \cdot d$.
3. Output the determinant $\det(A)$ as the product $\det(A) = d \cdot \det(T) = d \cdot a_{11} \cdots a_{nn}$, where $a_{11}, \ldots, a_{nn}$ are the diagonal elements of T.

Example 18.2. Compute the determinant of degree 5:

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

We could turn to zero all the entries in the 1'st column below $a_{11} = -1$ using four row-operations.

But it is much simpler to swap the 1'st column with the 3'rd which already has four zeros:

$$\det(A) = -\begin{vmatrix} 2 & 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -1 & 2 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 3 & -1 \\ 0 & 0 & 2 & -1 & 1 \end{vmatrix} \quad {\scriptstyle C1 \leftrightarrow C3}$$

(notice how we abbreviated the operation with columns). Next we turn to zero the entry a_{42} and multiply the entries of the 4'th row by 3 just not to have fractions in our determinant:

$$\det(A) = -\begin{vmatrix} 2 & 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -1 & 2 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & \frac{2}{3} & \frac{10}{3} & -\frac{5}{3} \\ 0 & 0 & 2 & -1 & 1 \end{vmatrix} \quad {\scriptstyle R4-\frac{1}{3}R2}$$

$$= -\frac{1}{3}\begin{vmatrix} 2 & 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -1 & 2 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 10 & -5 \\ 0 & 0 & 2 & -1 & 1 \end{vmatrix} \quad {\scriptstyle 3\cdot R4}.$$

Turn to zero the entries below $a_{33} = 2$:

$$\det(A) = -\frac{1}{3}\begin{vmatrix} 2 & 1 & -1 & 2 & 0 \\ 0 & 3 & 1 & -1 & 2 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 10 & -6 \\ 0 & 0 & 0 & -1 & 0 \end{vmatrix} \quad {\scriptstyle \begin{matrix} R4-R3 \\ R5-R3 \end{matrix}}.$$

Swap the 4'th and 5'th columns:

$$\det(A) = -\left(-\frac{1}{3}\right)\begin{vmatrix} \mathbf{2} & 1 & -1 & 0 & 2 \\ 0 & \mathbf{3} & 1 & 2 & -1 \\ 0 & 0 & \mathbf{2} & 1 & 0 \\ 0 & 0 & 0 & \mathbf{-6} & 10 \\ 0 & 0 & 0 & 0 & \mathbf{-1} \end{vmatrix} \quad {\scriptstyle C4\leftrightarrow C5}.$$

The matrix T of the determinant above already is in upper-triangle form, and $d = -\left(-\frac{1}{3}\right) = \frac{1}{3}$. So by Algorithm 18.1 we have:

$$\det(A) = d\cdot\det(T) = \frac{1}{3}\cdot 2\cdot 3\cdot 2\cdot(-6)\cdot(-1) = 24.$$

Example 18.3. Let us apply the algorithm to a matrix on finite field $\mathbb{Z}_5$:

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

$$\det(A) = -\begin{vmatrix} 2 & 2 & 1 \\ 0 & 4 & 2 \\ 0 & 3 & 1 \end{vmatrix} \quad {\scriptstyle C1\leftrightarrow C3}$$

$$= -\begin{vmatrix} 2 & 2 & 1 \\ 0 & 4 & 2 \\ 0 & 0 & 2 \end{vmatrix} \quad {\scriptstyle R3+3R2}$$

$$= -2\cdot 4\cdot 2 = -1 = 4 \in \mathbb{Z}_5$$

(remember that in $\mathbb{Z}_5$ the opposite of 1 is 4).

Remark 18.4. Notice that computing determinant we have somewhat more freedom to operate with rows *as well as* with columns in the same matrix A. We are not bothering about the row space or column space, since what we are looking for is just one single number $\det(A)$ to compute.

18.2. The Laplace expansion rule

Theorem 18.5 (Laplace Expansion Theorem)**.** *For any matrix $A = [a_{ij}]_{n,n} \in M_{n,n}(F)$ and any index $k = 1, \ldots, n$ the following decompositions hold:*

$$\det(A) = \sum_{i=1}^{n} a_{ik}A_{ik}, \qquad \det(A) = \sum_{i=1}^{n} a_{ki}A_{ki}. \tag{18.1}$$

When $k = 1$, the first of these decompositions is nothing else but the definition of the determinant, i.e., the cofactor expansion by the 1'st column of A. The theorem, thus, states that instead of the 1'st column we may take any k'th column, and the sum $a_{1k}A_{1k} + \cdots + a_{nk}A_{nk}$ will still be equal to $\det(A)$. We call this *cofactor expansion of A by its k'th column*.

And the analog of this holds for rows: for any k the sum $a_{k1}A_{k1} + \cdots + a_{kn}A_{kn}$ is equal to $\det(A)$. Call this *cofactor expansion of A by its k'th row*.

Proof of Theorem 18.1. It is simpler to prove using the definition with cofactor expansion, as the definition with permutations requires longer argument.

Since a transposition does not change the determinant (and it changes all rows to columns), it is enough to prove the first of decompositions in (18.5), and then apply Lemma 17.25 to get the second decomposition.

First assume $k=2$ and denote by $B=[b_{ij}]_{n,n}$ the matrix obtained from A by swapping its 1'st and 2'nd columns. Let $\det(B)=\sum_{i=1}^n b_{i1}B_{i1}$ be the cofactor expansion for B. For any i we have $b_{i1}=a_{i2}$. Also, the cofactors B_{i1} and A_{i2} consist of exactly the same rows, and their only difference is in sign: for B_{i1} we have $(-1)^{i+1}$, and for A_{i2} we have $(-1)^{i+2}=-(-1)^{i+1}$. That is, $b_{i1}B_{i1}=-a_{i2}A_{i2}$ for any i. We get that $\sum_{i=1}^n a_{i2}A_{i2}=-\sum_{i=1}^n b_{i1}B_{i1}=-\det(B)$. It remains to notice that $\det(B)=-\det(A)$ by Proposition 17.26 (point 4).

For $k=3$ we can swap the 2'nd and 3'rd columns, and apply a modification of the argument above, since we already know that $\det(A)=\sum_{i=1}^n a_{i2}A_{i2}$. Then we continue by induction for all $k=4,\dots,n$. □

The first straightforward idea of how to use the Laplace Expansion is: if we have a matrix of, say, degree 4, then we can expand its determinant by one of its rows (or columns) to a sum of four determinants of degree 3, which we can compute. However, this approach can be improved. If one of the rows (or columns) has only one non-zero element a_{kl}, then expanding by that row (column) we have to consider *only one* summand $a_{kl}A_{kl}=a_{kl}(-1)^{k+l}\det(M_{kl})$, as all other summands will be zero (M_{kl} is the matrix obtained from A after we erase the k'th row and l'th column).

And what to do, if our matrix fails to have such a "handy" row (column)? Just use the basic properties of determinant to eliminate some of the elements. Clearly, such an elimination process is reasonable to apply to a row (column), which already happens to have some number of zeros.

How to compute a determinant by the Laplace Expansion. The above presented approach suggests the following method:

Algorithm 18.6 (Computation of a determinant by the Laplace Expansion)**.** We are given a square matrix $A\in M_{n,n}(F)$.

► Find the determinant $\det(A)$.

1. Introduce initial integers $d=1$, $s=n$, and an initial matrix $M=A$.
2. If M contains a zero row (or a zero column), then output: $\det(A)=0$. End of the process.
3. Else choose a non-zero entry a_{kl} such that the k'th row of M (or the l'th column of M) has a maximal number of zeros.
4. If a_{kl} is the *only* non-zero element in k'th row (or in l'th column), go to Step 6.
5. Else, using the determinant row and column operations eliminate all the non-zero elements except a_{kl} in k'th row (or in l'th column). In this process each time we swap two rows (or two columns), set $d=-d$. And each time we multiply a row (or a column) by a non-zero scalar c, set $d=\frac{1}{c}\cdot d$.
6. Set $d=d\cdot a_{kl}\cdot(-1)^{k+l}$, and set $M=M_{kl}$.
7. If $s=2$, output $\det(A)=d\cdot\det(M)$ (now M is a matrix of degree 1).
8. Else set $s=s-1$, go to Step 2.

Example 18.7. Let us apply the method to the matrix considered in Example 18.2:

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

The bast location to apply Laplace Expansion is the 3'rd column. So we have

$$\det(A)=a_{13}A_{13}=2\cdot(-1)^{1+3}\begin{vmatrix}1&3&-1&2\\2&0&0&1\\1&1&3&-1\\2&0&-1&1\end{vmatrix}.$$

The 2'nd row of this determinant of degree 4 already has two zeros. We can turn the entry $a_{21} = 2$ to zero by column operation $C1 - 2C4$:

$$\det(A) = 2\begin{vmatrix} -3 & 3 & -1 & 2 \\ 0 & 0 & 0 & 1 \\ 3 & 1 & 3 & -1 \\ 0 & 0 & -1 & 1 \end{vmatrix}.$$

Apply an expansion by the 2'nd row:

$$\det(A) = 2 \cdot 1 \cdot (-1)^{4+2} \begin{vmatrix} -3 & 3 & -1 \\ 3 & 1 & 3 \\ 0 & 0 & -1 \end{vmatrix}.$$

The next expansion is by the 3'rd row:

$$\det(A) = 2 \cdot (-1) \cdot (-1)^{3+3} \begin{vmatrix} -3 & 3 \\ 3 & 1 \end{vmatrix}$$

(although you may prefer to compute that determinant of degree 3 in any other way). At this step $d = -2$ and M is a matrix of degree 2. Adding to the 2'nd row the 1'st row we get:

$$\det(A) = -2\begin{vmatrix} -3 & 3 \\ 0 & 4 \end{vmatrix},$$

and then the expansion by the 1'st column gives:

$$\det(A) = -2 \cdot (-3) \cdot (-1)^{1+1} \cdot \det[4] = 24$$

(here $d = 6$ and $\det(M) = 4$). Or you may prefer to do the final simple step differently:

$$\det(A) = -2(-3 \cdot 1 - 3 \cdot 3) = 24.$$

Example 18.8. To see how Laplace Expansion may look on finite fields use it for the matrix already used in Example 18.3 on finite field $\mathbb{Z}_5$:

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

Expand this by its 3'rd column and compute:

$$\det(A) = 2 \cdot (-1)^{3+1} \begin{vmatrix} 2 & 4 \\ 1 & 3 \end{vmatrix}$$

$$= 2(2\cdot 3 - 1 \cdot 4) = 2(1-4) = 2 \cdot (-3) = 2 \cdot 2 = 4$$

(all operations are modular in $\mathbb{Z}_5$).

Exercises

E.18.1. Compute the determinant of each of these matrices by triangle rule:

$$A = \begin{bmatrix} 0 & 1 & 0 & 2 \\ 1 & 2 & 0 & 0 \\ 2 & 2 & 0 & 1 \\ 0 & 2 & 3 & 0 \end{bmatrix} \in M_{4,4}(\mathbb{R}), \quad B = \begin{bmatrix} 0 & i & 1 \\ 1 & 0 & 2i \\ i & i & 1 \end{bmatrix} \in M_{2,2}(\mathbb{C}), \quad C = \begin{bmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix} \in M_{3,3}(\mathbb{Z}_3).$$

E.18.2. **(1)** Expand the matrix A in Exercise E.18.1 by its 3'rd row. **(2)** Expand the matrix C in Exercise E.18.1 by its 2'nd column.

E.18.3. Compute the determinants of three matrices in Exercise E.18.1 using the Laplace Expansion rule. Apply it to the rows or columns in which all entries except one are zero. If the matrix fails to have such a row or column, create it using row- and column operations.

E.18.4. We are given the real matrices:

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

(1) Compute $\det(A)$ and $\det(B)$ by triangle method (choose the row- and column operations so that you *minimize* the computations). **(2)** Compute $\det(A)$ and $\det(B)$ by Laplace expansion (choose the appropriate rows or columns to *minimize* the calculations).

CHAPTER 19

Applications: Using the determinants

In this chapter we present a few applications of determinants. They will mostly be without any proofs because their analogs based on other technique were in detail proved in previous parts. We also compare the methods with and without determinants to see the strong or weak sides of each.

19.1. The Cramer's Rule

Assume we are given any *square* systems of linear equations over a field F:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n. \end{cases} \tag{19.1}$$

How to solve a square system of linear equations, Cramer's method. Denote by

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

the matrix of the system (19.1), and suppose its determinant $d = \det(A)$ is non-zero.

Introduce a matrix A_k that coincides with A in all columns except the k'th column, and the k'th column of A_k consists of the constant terms $b_1, \dots, b_n$ of (19.1), i.e,

$$A_k = \begin{bmatrix} a_{11} & \cdots & a_{1\,k-1} & b_1 & a_{1\,k+1} & \cdots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \cdots & a_{n\,k-1} & b_n & a_{n\,k+1} & \cdots & a_{nn} \end{bmatrix}.$$

Denote $d_k = \det(A_k)$. Then by the *Cramer's Rule* the system (19.1) is consistent, and has a unique

$$\left(\tfrac{d_1}{d}, \dots, \tfrac{d_n}{d}\right).$$

And when $d = 0$, or when (19.1) is not a square system, then the Cramer's Rule gives *no answer*: the system may or may not be consistent.

Example 19.1. Let us apply the Cramer's Rule to the square system which we have considered for a series of solution methods, including ordinary elimination, the Gauss-Jordan method, matrix methods, etc. (see examples 5.9, 7.3, 7.10, 9.6, 9.8, etc.)

$$\begin{cases} \quad\;\; y + z = 1 \\ 2x - y + z = 9 \\ x \;\; - y - z = 2. \end{cases}$$

We have the burden to compute *four* determinants of degree 3:

$$d = \det(A) = \begin{vmatrix} 0 & 1 & 1 \\ 2 & -1 & 1 \\ 1 & -1 & -1 \end{vmatrix},$$

$$d_1 = \det(A_1) = \begin{vmatrix} 1 & 1 & 1 \\ 9 & -1 & 1 \\ 2 & -1 & -1 \end{vmatrix},$$

$$d_2 = \det(A_2) = \begin{vmatrix} 0 & 1 & 1 \\ 2 & 9 & 1 \\ 1 & 2 & -1 \end{vmatrix},$$

$$d_3 = \det(A_3) = \begin{vmatrix} 0 & 1 & 1 \\ 2 & -1 & 9 \\ 1 & -1 & 2 \end{vmatrix}.$$

Leaving aside the computation process just indicate the values $d = 2$, $d_1 = 6$, $d_2 = -2$, $d_3 = 4$. Thus, by Cramer's Rule this system has an only solution:

$$\left(\frac{6}{2}, -\frac{2}{2}, \frac{4}{2}\right) = (3, -1, 2).$$

Compare this with solution using the Gauss-Jordan method in Example 7.10. There we had to compute the reduced row-echelon form of one 3×4 matrix, which actually required about the same work as computation of *two* determinants of degree 3.

Remark 19.2. The Cramer's Rule is a inefficient method for large systems. For a square system of 10 linear equations in 10 variables we have to compute *eleven* determinants of degree 10, whereas by Gauss-Jordan method we have to bring *one* 10×11 matrix to its reduced row-echelon form.

Modern technologies often require computation of systems of thousands of linear equations over thousands of variables. Cramer's Rule is not efficient for large systems, as its complexity is about $O(n \cdot n!)$, whereas the Gauss-Jordan method's complexity is about $O(n^3)$. This is the reason why we present the Cramer's Rule here as a very famous historical artifact only.

19.2. Determinants and linear independence

Determinants are handy tools to study linear dependence. Assume in an n-dimensional space V over any field F we have n vectors:

$$\begin{gathered} v_1 = (a_{11}, \ldots, a_{1n}), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ v_n = (a_{n1}, \ldots, a_{nn}) \end{gathered}$$

given by coordinates in some basis. Form a square matrix by their coordinates:

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

Lemma 19.3. *In above notation the vectors $v_1, \ldots, v_n$ are linearly independent if and only if* $\det(A) \neq 0$.

Since $\det(A) = \det\left(A^T\right)$, the analog of this lemma also holds for a matrix formed by *column* vectors $v_1, \ldots, v_n$.

***Proof*.** By Corollary 14.14 the vectors $v_1, \ldots, v_n$ are linearly independent if and only if A is invertible. And by Corollary 17.21 A is invertible if and only if $\det(A) \neq 0$. □

Example 19.4. Using Example 18.2 above we can state that the vectors

$$\begin{aligned} v_1 &= (-1, 1, 2, 2, 0), \\ v_2 &= (1, 3, 0, -1, 2), \\ v_3 &= (2, 0, 0, 0, 1), \\ v_4 &= (1, 1, 0, 3, -1), \\ v_5 &= (2, 0, 0, -1, 1) \end{aligned}$$

are linearly independent in the space $\mathbb{R}^5$. And from Example 18.3 we get that the vectors

$$\begin{aligned} v_1 &= (1, 2, 2), \\ v_2 &= (2, 4, 0), \\ v_3 &= (1, 3, 0) \end{aligned}$$

are linearly independent in the space $\mathbb{Z}_5^3$.

Let us compare this method with other methods of linear independence detection we learned earlier, such as Algorithm 14.23, Algorithm 14.19 or Algorithm 14.24. The method with determinant only works for n vectors in an n-dimensional space. If the vectors $v_1, \dots, v_n$ are, say, independent, then Algorithm 14.23 finds this fact by consuming about the same amount work that is needed to bring A to triangle form to deduce that $\det(A) \neq 0$.

If the vectors $v_1, \dots, v_n$ are dependent, then by method with determinant we just get $\det(A) = 0$ with no *further* information. But the Algorithm 14.19 also provides the rank and the dimension of its span. And if we apply Algorithm 14.24, we also get *which ones* of the vectors $v_1, \dots, v_n$ do form the maximal linearly independent subset.

Nevertheless, there are cases when application of determinants saves some work.

Example 19.5. Are the following vectors linearly independent?

$$
\begin{aligned}
v_1 &= (4, 7, 2, 2, 4, 5, 2, 9),\\
v_2 &= (6, 3, 9, 8, 2, 0, 3, 4),\\
v_3 &= (2, 8, 5, 5, 1, 0, 2, 0),\\
v_4 &= (1, 6, 9, 8, 7, 0, 1, 0).
\end{aligned}
$$

If we try to answer this by standard row-echelon methods, then we will have to do much computations with the rows of a 4×8 matrix A formed by coefficients of v_1, v_2, v_3, v_4.

But notice that the 6'th column contains three zeros, and the 8'th column contains two zeros.Combine these two columns with some two other columns of A to get, say, the following determinant:

$$
d = \begin{vmatrix} 5 & 9 & 4 & 7\\ 0 & 4 & 6 & 3\\ 0 & 0 & 2 & 8\\ 0 & 0 & 1 & 6 \end{vmatrix}
$$

(the order of columns is not important, as swapping columns just changes the determinant sign).

Applying Laplace Expansion to this determinant twice we get

$$
d = 5 \cdot (-1)^2 \cdot 4 \cdot (-1)^2 (2 \cdot 6 - 8 \cdot 1) \neq 0.
$$

By Lemma 19.3 the rows of the above matrix are linearly independent. Thus, v_1, v_2, v_3, v_4 also are independent.

Tricks of the above type can also be used to speed up solution of a system of linear equations, when we in its matrix notice an “appropriate” determinant.

19.3. Inverse matrix computation with cofactors

Another well-known historical artifact we would like to mention is the inverse matrix computation method by cofactors. Suppose we are given a square matrix

$$
A = \begin{bmatrix} a_{11} & \cdots & a_{1n}\\ \multicolumn{3}{c}{\dotfill} \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}
$$

which is invertible (we have criteria to detect this using Theorem 9.10 or its corollaries, including Corollary 17.21 with condition $\det(A) \neq 0$).

How to compute the inverse matrix, adjoint matrix method. As above, we denote by A_{ij} the cofactor $(-1)^{i+j}\det\big(M_{ij}\big)$. The *adjoint matrix* $\operatorname{adj}(A)$ of A is defined as:

$$
\operatorname{adj}(A) = \begin{bmatrix} A_{11} & \cdots & A_{n1}\\ \multicolumn{3}{c}{\dotfill} \\ A_{1n} & \cdots & A_{nn} \end{bmatrix},
$$

i.e., this is the matrix obtained from A if we first replace each entry a_{ij} by its cofactor A_{ij}, and then transpose the matrix (notice that the last entry in the 1'st row of adj(A) is A_{n1}). It is easy to compute that the product $A \cdot \mathrm{adj}(A)$ is equal to $d \cdot I$ (a matrix that has d on the main diagonal, and 0 elsewhere). Thus, to get the inverse of A we should just divide all entries of adj(A) by d:

$$A^{-1} = \frac{1}{d}\mathrm{adj}(A).$$

Example 19.6. Compute the inverse of the matrix

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

In Example 19.1 we have already found that $d = \det(A) = 2$. So Acertainly is invertible. We have to compute nine cofactors:

$$A_{11} = \begin{vmatrix} -1 & 1 \\ -1 & -1 \end{vmatrix} = 2, \quad A_{12} = \begin{vmatrix} 2 & 1 \\ 1 & -1 \end{vmatrix} = 3,$$

$$A_{13} = \begin{vmatrix} 2 & -1 \\ 1 & -1 \end{vmatrix} = -1, \quad A_{21} = \begin{vmatrix} 1 & 1 \\ -1 & -1 \end{vmatrix} = 0,$$

$$A_{22} = \begin{vmatrix} 0 & 1 \\ 1 & -1 \end{vmatrix} = -1, \quad A_{23} = \begin{vmatrix} 0 & 1 \\ 1 & -1 \end{vmatrix} = 1,$$

$$A_{31} = \begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 2, \quad A_{32} = \begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} = 2,$$

$$A_{33} = \begin{vmatrix} 0 & 1 \\ 2 & -1 \end{vmatrix} = -2.$$

So we get:

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

The inverse of A by Algorithm 6.10 was computed earlier in Example 9.13.

Remark 19.7. Nevertheless, this approach of inverse matrix computation by cofactors is *too inefficient* to be a practical method. To calculate the inverse of, say, a 10×10 matrix A we have to compute *one hundred* determinants of degree 9 (the cofactors A_{ij}, $i, j = 1, \ldots, 10$). Plus, we have to compute one more determinant $\det(A)$ of degree 10.

Meanwhile, working with Algorithm 6.10 we compute the reduced row-echelon form of *just one* 10×20 matrix $[A \mid I]$. And the second half of $[A \mid I]$ consists of zeros mostly, which simplifies the task.

Exercises

E.19.1. Detect if Cramer's Rule can be applied to the following system of real linear equations. If yes, solve the system by Cramer's Rule:

$$\begin{cases} x + 2y + z = 3 \\ 3x + y + 2z = 1 \\ x + 3y + 1 = 4. \end{cases}$$

E.19.2. We are given the vectors:

$$v_1 = [1, 3, 1, 1], \quad v_2 = [0, 2, 1, 2], \quad v_3 = [0, 0, 3, 1], \quad v_4 = [0, 0, 0, 1].$$

(1) form the matrix $A = \begin{bmatrix} v_1 \\ \hdashline v_2 \\ \hdashline v_3 \\ \hdashline v_4 \end{bmatrix}$ and compute its determinant. **(2)** Without any calculations indicate if A is an invertible matrix or not. **(3)** Without any calculations deduce if the vectors v_1, v_2, v_3, v_4 are linearly independent.

E.19.3. Answer the questions below without any new calculations, just using your solutions for Exercise E.18.1. **(1)** Consider the rows of matrix A of Exercise E.18.1 as a set of vectors in $\mathbb{R}^4$. Is it linearly independent? **(2)** Consider the columns of matrix B of Exercise E.18.1 as a set of vectors in $\mathbb{C}^3$. Is it linearly independent?

E.19.4. Let A and B be the matrices of Exercise E.18.4. **(1)** Using the results of Exercise E.18.4 deduce without any row-elimination, if the rows of A are linearly independent? Are the columns of B linearly independent? **(2)** Is $\dim(\mathrm{col}(\mathrm{A}^{100}))$ equal to $\dim(\mathrm{row}(\mathrm{B}^{1000}))$?

E.19.5. In Exercise 9.8 you have already computed the inverses for the matrices $A = \begin{bmatrix} 2 & 0 & 1 \\ 2 & 3 & 2 \\ 1 & 1 & 1 \end{bmatrix} \in M_{3,3}(\mathbb{R})$, $B = \begin{bmatrix} i & 0 \\ 2 & -i \end{bmatrix} \in M_{2,2}(\mathbb{C})$, $C = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \in M_{2,2}(\mathbb{Z}_3)$ using the Gauss-Jordan method. Compute these inverses by the adjoint matrix method. Observe that when the matrices are small, then the adjoint matrix method is *not* much more complicated than the Gauss-Jordan method.

E.19.6. Let $A \in M_{n,n}(F)$ be a square matrix of degree n. Indicate how many determinants (and of which degrees) you need calculate in order to find A^{-1} by the adjoint matrix method.

Part 7

Linear Transformations

CHAPTER 20

Introduction to linear transformations

"La mathématique est l'art de donner le même nom à des choses différentes."
Henri Poincaré

20.1. Definition and main examples of transformations

We are at our third main step of *abstraction* – *linear transformations* (the first two being the concepts of the general fields and of the abstract vector spaces). The vector spaces we so far considered were "static" environments, and the concept of linear transformation brings "motion" to them. Here motion can be understood as a function sending points of the space to some new points.

Definition 20.1. Let V and W be two linear spaces over a field F. The map $T : V \to W$ is a *linear transformation* from V to W, if for any $u, v \in V$ and $c \in F$:
1) $T(u+v) = T(u) + T(v)$;
2) $T(c\,v) = c\,T(v)$.

If $W = V$, then $T : V \to V$ is called a linear transformation of the space V.
If $T : V \to W$ is a bijection, then T is called an *isomorphism* of the spaces V and W (or an isomorphism of the space V, when $W = V$). Of course, a transformation may also be denoted by characters other than T.

Example 20.2. Let V, W be any spaces on F. Define $T(v) = \vec{0}_W$, i.e., T maps to each vector $v \in V$ the zero vector of W. This is called a *zero* linear transformation V, and it is denoted by O.

When $W = V$, we can define $T(v) = v$. This is called a *identical* transformation of V, and is denoted by I. Clearly, I is an isomorphism.

Example 20.3. Let $W = V = F^n$ and define the following transformations of V:

1. Define $P(v) = P(a_1, \dots, a_k, \dots, a_n) = (a_1, \dots, 0, \dots, a_n)$. This map evidently is a linear transformation. It is called *projection* by k'th coordinate (notice how we denoted it not by T but by P). See Figure 20.1 (a).

2. Define $M(v) = M(a_1, \dots, a_k, \dots, a_n) = (a_1, \dots, -a_k, \dots, a_n)$. This is a linear transformation, and is called *mirror reflection* by k'th coordinate. See Figure 20.1 (a).

3. Define $S(v) = S(a_1, \dots, a_k, \dots, a_n) = (a_1, \dots, c \cdot a_k, \dots, a_n)$ for some scalar $c \in F$. S is a linear transformation, and it is called *scaling* by k'th coordinate. See Figure 20.1 (a).

In analogy width this we could define scaling by *all* coordinates:

$$S(v) = S(a_1, \dots, a_k, \dots, a_n)$$
$$= (c \cdot a_1, \dots, c \cdot a_k, \dots, c \cdot a_n) = c\,v.$$

Reflection by any coordinate is an isomorphism, while scaling is an isomorphism if and only if $c \neq 0$.

Example 20.4. Let $V = \mathbb{R}^3$ and $W = \mathbb{R}^2$, and define a map T as:

$$T(v) = T(x, y, z) = (2x + y, x + z)$$

It is trivial to check that T is a linear transformation.

Example 20.5. Let $V = F^m$ and $W = F^n$. Fix a matrix $A \in M_{mn}(F)$ and define the transformation T_A by matrix product:

$$T_A(v) = T_A\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = A \cdot \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Say, for $A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \in M_{2,3}(\mathbb{R})$ and for $v = (1,2,4) \in \mathbb{R}^3$ we have:

$$T_A(1,2,4) = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \in \mathbb{R}^2.$$

T_A is a linear transformation. $T_A(u+v) = T_A(u) + T_A(v)$ follows from right distributivity of matrix operations that we proved in Proposition 8.10. The condition $T_A(c\,v) = c\,T_A(v)$ is evident.

Later we will see that these transformations T_A are "universal": all other linear transformations can be described by such T_A's. Do you notice connection of this example with transformation T from previous example?

Example 20.6. Let V be either of the polynomial spaces $\mathcal{P}_n(F)$ or $F[x]$. Define a linear transformation of V using derivative:

$$T(f(x)) = f'(x).$$

T is linear because $(f(x)+g(x))' = f'(x) + g'(x)$ and $(cf(x))' = cf'(x)$ for any polynomials $f(x), g(x)$.

Example 20.7. For the space of (integrable over $[a,b]$) functions V and for $W = \mathbb{R}$ define a linear transformation $T : V \to \mathbb{R}$ as:

$$T(f(x)) = \int_a^b f(x)\,dx.$$

Example 20.8. For $V = \mathbb{R}^2$ a linear transformation R_φ can be defined by rotation of V by angle φ around the origin O:

$$R_\varphi(v) = R_\varphi(x,y)$$
$$= \big(\cos(\varphi)\,x - \sin(\varphi)\,y,\ \sin(\varphi)\,x + \cos(\varphi)\,y\big).$$

This formula is easy to prove, but later we will have a generic method to get it. R_φ is an isomorphism for any φ. See Figure 20.1 (b).

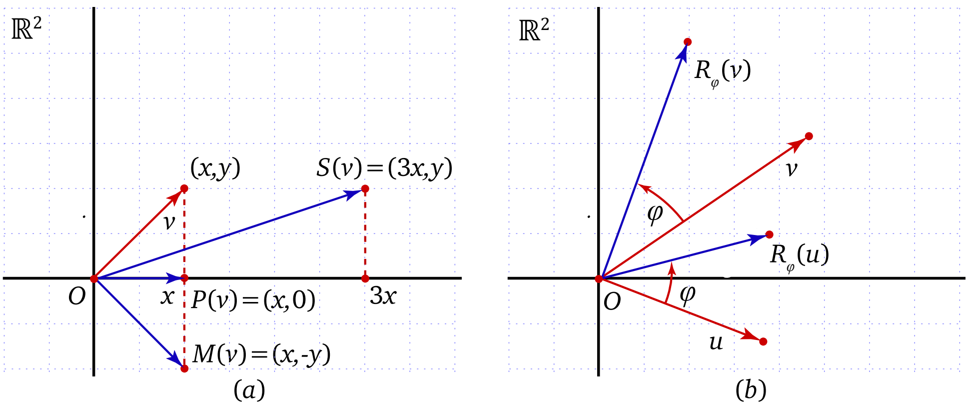


FIGURE 20.1. Linear transformations on $\mathbb{R}^2$.

Proofs of the following properties are left as easy exercises:

Proposition 20.9. *Let T be a linear transformation from the space V to the space W over F. Then:*

1. $T(0_V) = 0_W$;
2. $T(-v) = -T(v)$ *for any* $v \in V$;
3. $T(u-v) = T(u) - T(v)$ *for any* $u, v \in V$;
4. $T(c_1v_1 + \cdots + c_nv_n) = c_1T(v_1) + \cdots + c_nT(v_n)$ *for any* $v_1, \ldots, v_n \in V$; $c_1, \ldots, c_n \in F$.

20.2. The matrix of a linear transformation

Take any linear transformation $T : V \to W$ and assume a basis $E = \{e_1, \dots, e_n\}$ in V and a basis $G = \{g_1, \dots, g_m\}$ in W are fixed.

It turns out that the n values $T(e_1), \dots, T(e_n)$ of T on basis vectors already are enough to uniquely determine the values $T(v)$ for *any* $v \in V$. Indeed, for any vector $v = c_1 e_1 + \dots + c_n e_n \in V$:

$$T(v) = T(c_1 e_1 + \dots + c_n e_n) = c_1 T(e_1) + \dots + c_n T(e_n),$$

and so $T(v)$ is uniquely determined as a linear combination of $T(e_1), \dots, T(e_n)$.

Each image $T(e_i)$ as a vector of W is a linear combination of the basis vectors $g_1, \dots, g_m$ with some coefficients a_{ij}:

$$T(e_i) = a_{1i} g_1 + \dots + a_{mi} g_m.$$

Write these coefficients a_{ij} as column vectors:

$$T(e_1) = \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix}, \dots,\ T(e_n) = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix},$$

and compose by them the matrix:

$$A = [T]_{EG} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} = \left[\ T(e_1) \ \vdots\ \cdots \ \vdots\ T(e_n)\ \right].$$

Call $A = [T]_{EG}$ the *matrix of linear transformation $T : V \to W$ with respect to the bases E and G*.

Example 20.10. Build the matrix $[T]_{EG}$ for the transformation $T : \mathbb{R}^3 \to \mathbb{R}^2$ given in Example 20.4 by the rule

$$T(x, y, z) = (2x + y, x + z).$$

Fix the standard bases E and G in both spaces:

$$E = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\},\ G = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}.$$

Then:

$$T(e_1) = \begin{bmatrix} 2 \\ 1 \end{bmatrix},\ T(e_2) = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ T(e_3) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Therefore:

$$[T]_{EG} = \left[\ T(e_1) \ \vdots\ T(e_2) \ \vdots\ T(e_3)\ \right] = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Comparing this with above examples we see that in Example 20.5 we actually used the matrix $A = [T]_{EG}$ of transformation T from Example 20.4.

When $T : V \to V$ is a transformation of the space V (i.e., $W = V$), and the bases E and G are the same, then we may write shorter: $A = [T]_E$. Also, if in some cases the bases E and G already are known from the context of the problem, we may briefly write $A = [T]$. Notice similarity of these notations with the notation of vector coordinates with respect to a basis: $v = [v] = [v]_E$.

Now let us go in opposite direction. Assume we are given any matrix

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \in M_{m,n}(F).$$

Its columns are the coordinates of some vectors

$$h_1, \dots, h_n \in W$$

in basis G. Define a map $T : V \to W$ on vectors $v = c_1 e_1 + \cdots + c_n e_n \in V$ by the rule:

$$T(v) \stackrel{\text{def}}{=} T(c_1 e_1 + \cdots + c_n e_n) = c_1 h_1 + \cdots + c_n h_n.$$

Is T is a linear transformation? If $u = d_1 e_1 + \cdots + d_n e_n$ is any vector in V, then

$$\begin{aligned} T(u+v) &= T\Big((d_1 e_1 + \cdots + d_n e_n) + (c_1 e_1 + \cdots + c_n e_n)\Big) \\ &= T\Big((d_1 + c_1)e_1 + \cdots + (d_n + c_n)e_n\Big) \\ &= (d_1 + c_1)h_1 + \cdots + (d_n + c_n)h_n = T(u) + T(v). \end{aligned}$$

Next, for any scalar $c \in F$ we have:

$$\begin{aligned} T(c\,v) &= T\big(c\,(c_1 e_1 + \cdots + c_n e_n)\big) = T(c\,c_1 e_1 + \cdots + c\,c_n e_n) \\ &= c\,c_1 h_1 + \cdots + c\,c_n h_n = c\,T(v). \end{aligned}$$

So for each $A \in M_{m,n}(F)$ there is a linear transformation $T : V \to W$ mapping e_i to the i'th column h_i of A for each $i = 1, \dots, n$. By construction this T is unique. We established:

Theorem 20.11. *Let V be any n-dimensional space over a field F with a basis E, and W be any m-dimensional space over the same field with a basis G. There is a bijection between the linear transformations $T : V \to W$ and the matrices $A = [T]_{EG} \in M_{mn}(F)$.*

Important! These notation and bijection *depend on the bases* E and G. If we take other bases, the matrices $[T]_{EG}$ and the bijection may change.

How to compute the matrix of a transformation.

Algorithm 20.12 (Computation of the matrix of a transformation with respect to given bases)**.** We are given a transformation $T : V \to W$ from the space V to the space W over the same field F. Ordered bases $E = \{e_1, \dots, e_n\}$ and $G = \{g_1, \dots, g_m\}$ are given in spaces respectively V and W.

► Find the matrix $A = [T]_{EG}$ of transformation T with respect to E and G.

1. For each of $i = 1, \dots, n$ present the vector $T(e_i)$ as a linear combination

$$T(e_i) = a_{i1} g_1 + \cdots + a_{im} g_m$$

of vectors of G. This can be done by, say, Algorithm 14.29.

2. Output $A = [T]_{EG}$ as the matrix

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} = \Big[\, T(e_1) \;\vdots\; \cdots \;\vdots\; T(e_n) \,\Big].$$

in which the coefficients $a_{i1}, \dots, a_{in}$ of $T(e_i)$ are forming the i'th column of A for each $i = 1, \dots, n$.

See also Remark 20.25 which suggests a hint of how in many cases a transformation matrix computation can be simplified.

Agreement 20.13. Let us agree that whenever we do not mention the bases of the spaces evolved, it will be assumed that the transformation's matrix is computed with respect to the "default" bases of the spaces: the standard bases $E = \{e_1,\ldots,e_n\}$ in spaces F^n, the bases $E = \{E_{i,j} \,|\, i = 1,\ldots,m;\ j = 1,\ldots,n\}$ in matrix spaces $M_{m,n}(F)$, the finite or infinite bases $E = \{1,x,x^2,\ldots,x^n\}$ or $E = \{1,x,x^2,\ldots\}$ in polynomial spaces $\mathcal{P}_n(F)$ or $F[x]$, etc...

Example 20.14. For the spaces $V = W = F^n$ fix the standard basis E:

$$e_1 = \begin{bmatrix}1\\ \vdots\\ 0\\ \vdots\\ 0\end{bmatrix},\ldots,\ e_k = \begin{bmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{bmatrix},\ldots,\ e_n = \begin{bmatrix}0\\ \vdots\\ 0\\ \vdots\\ 1\end{bmatrix}$$

and consider the following transformations:

1. For the projection $P(a_1,\ldots,a_k,\ldots,a_n) = (a_1,\ldots,0,\ldots,a_n)$ we have:

$$P(e_1) = \begin{bmatrix}1\\ \vdots\\ 0\\ \vdots\\ 0\end{bmatrix} = e_1,\ldots,P(e_n) = \begin{bmatrix}0\\ \vdots\\ 0\\ \vdots\\ 1\end{bmatrix} = e_n$$

with only exception:

$$P(e_k) = \begin{bmatrix}0\\ \vdots\\ 0\\ \vdots\\ 0\end{bmatrix} = \vec{0}.$$

Therefore the matrix of P is:

$$A=[P]=[P]_E=\begin{bmatrix}1 & \cdots & 0 & 0 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & \mathbf{0} & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1\end{bmatrix}.$$

2. For the mirror reflection transformation given by $M(a_1,\ldots,a_k,\ldots,a_n) = (a_1,\ldots,-a_k,\ldots,a_n)$ we have the matrix

$$A=[M]=[M]_E=\begin{bmatrix}1 & \cdots & 0 & 0 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & \mathbf{-1} & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1\end{bmatrix}.$$

3. And for the scaling linear transformation given by $S(a_1,\ldots,a_k,\ldots,a_n) = (a_1,\ldots,c\,a_k,\ldots,a_n)$ we get:

$$A=[S]=[S]_E=\begin{bmatrix}1 & \cdots & 0 & 0 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 1 & 0 & 0 & \cdots & 0\\ 0 & \cdots & 0 & \mathbf{c} & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1\end{bmatrix}.$$

Example 20.15. In the space $\mathbb{R}^3$ consider the linear transformation given as $T(x,y,z)=(6x+6y-12z,\ 4x+2y-6z,\ 4x+3y-7z)$. Applying T on the standars basis vectors $E = \{e_1,e_2,e_3\}$ we have:

$$T\begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}6\\4\\4\end{bmatrix},\ T\begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}6\\2\\3\end{bmatrix},\ T\begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}-12\\-6\\-7\end{bmatrix},$$

and so T has the matrix:

$$A=[T]_E=\begin{bmatrix}6 & 6 & -12\\ 4 & 2 & -6\\ 4 & 3 & -7\end{bmatrix}.$$

This transformation will be an important actor when the drama with eigenvectors and diagonalization starts in Part 8.

Example 20.16. Take the basis $\{1,x,\ldots,x^n\}$ in the polynomial spaces $\mathcal{P}_n(F)$ and the linear transformation by derivation $T(f(x)) = f'(x)$. Apply T on basis vectors:

$$1' = 0 = \begin{bmatrix}0\\0\\ \vdots\\ 0\end{bmatrix},\ x' = 1 = \begin{bmatrix}1\\0\\ \vdots\\ 0\end{bmatrix},\ldots$$

$$\ldots,(x^{n-1})' = (n-1)x^{n-2} = \begin{bmatrix}0\\ \vdots\\ n-1\\ 0\\ 0\end{bmatrix},$$

$$(x^n)' = nx^{n-1} = \begin{bmatrix}0\\ \vdots\\ 0\\ n\\ 0\end{bmatrix}.$$

So the matrix we are looking for is:

$$A = [T]_E = \begin{bmatrix} 0 & 1 & & & \mathbf{0} \\ & 0 & 2 & & \\ & & \ddots & & \\ & & & 0 & n \\ \mathbf{0} & & & & 0 \end{bmatrix}.$$

Example 20.17. Let $V = \mathbb{R}^2$ and R_φ be the rotation by angle φ on V. Take the standard basis $e_1 = (1,0)$ and $e_2 = (0,1)$. As it is clear from Figure 20.2:

$$R_\varphi(e_1) = R_\varphi(1,0) = \begin{bmatrix} \cos(\varphi) \\ \sin(\varphi) \end{bmatrix},$$

$$R_\varphi(e_2) = R_\varphi(0,1) = \begin{bmatrix} -\sin(\varphi) \\ \cos(\varphi) \end{bmatrix}.$$

Thus, the matrix of R_φ is:

$$A = [R_\varphi]_E = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}.$$

Example 20.18. The algorithm is easy to apply over finite fields also. Let $F = \mathbb{Z}_5$ and two spaces are $V = \mathbb{Z}_5^3$ and $W = \mathbb{Z}_5^2$. Define T by the rule $T(x,y,z) = (2x+3z, 4y)$. Fix the standard bases $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$ in $\mathbb{Z}_5^3$; and $g_1 = (1,0)$, $g_2 = (0,1)$ in $\mathbb{Z}_5^2$. Now $T(e_1) = (2\cdot 1 + 3\cdot 0,\ 4\cdot 0) = (2,0)_G$, $T(e_2) = (2\cdot 0 + 3\cdot 0,\ 4\cdot 1) = (0,4)_G$, $T(e_3) = (2\cdot 0 + 3\cdot 1,\ 4\cdot 0) = (3,0)_G$. Thus,

$$A = [T]_{EG} = \begin{bmatrix} 2 & 0 & 3 \\ 0 & 4 & 0 \end{bmatrix}.$$

Like we mentioned, *a transformation may have different matrices in different bases*. Let us bring an example of this.

Example 20.19. Take $V = \mathbb{R}^2$ and consider the transformation $S : \mathbb{R}^2 \to \mathbb{R}^2$ given by the rule $S(x,y) = (x, 3y)$. So to say, S three times scales the 2-dimensional space vertically. As we have proved, in the standard basis $e_1 = (1,0)$, $e_2 = (0,1)$ the transformation has the matrix:

$$A = [S]_E = \left[\, S(e_1) \;\vdots\; S(e_2) \,\right] = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}.$$

Next take basis vectors $g_1 = (1,1)$, $g_2 = (-1,1)$ of $\mathbb{R}^2$, and compute the matrix in this basis.

$$S(g_1) = (1,3) = 2g_1 + 1g_2,$$

$$S(g_2) = (-1,3) = 1g_1 + 2g_2.$$

$$A = [S]_G = \left[\, S(g_1) \;\vdots\; S(g_2) \,\right] = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

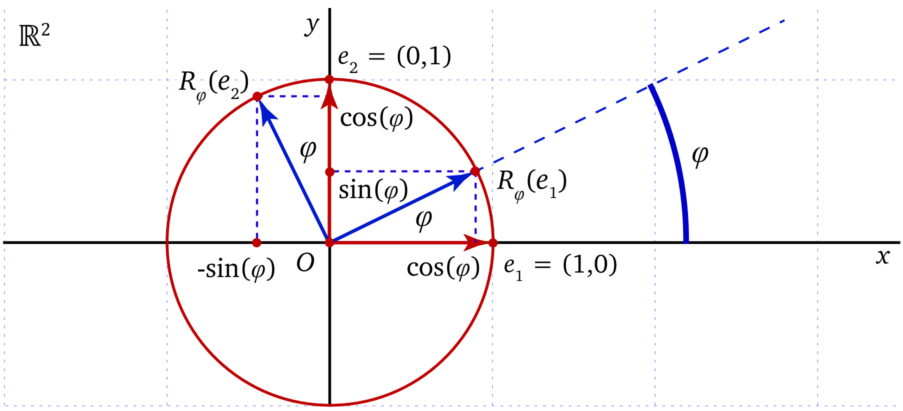


FIGURE 20.2. Constructing the matrix $[R_\varphi]_E$ of rotation on $\mathbb{R}^2$.

Now we are going to establish a key fact that shows *why the matrix of a transformation is important*. Assume we have a linear transformation $T : V \to W$ which for the given bases $E = \{e_1, \ldots, e_n\}$ and $G = \{g_1, \ldots, g_m\}$ has the matrix

$$A = [T]_{EG} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

Take any vector $v = c_1 e_1 + \cdots + c_n e_n \in V$. Then $T(v) = c_1 T(e_1) + \cdots + c_n T(e_n)$, and replacing here each $T(e_i)$ by the respective column of A we get:

$$T(v) = c_1 \begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} + \cdots + c_n \begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} c_1 a_{11} + \cdots + c_n a_{1n} \\ \dots\dots\dots\dots\dots\dots \\ c_1 a_{m1} + \cdots + c_n a_{mn} \end{bmatrix} = [T]_{EG} \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = [T]_{EG}[v]_E.$$

The obtained the equality

$$\boldsymbol{T(v) = Av} \tag{20.1}$$

means that the action $T(v)$ of the transformation T on vector v can be interpreted as ordinary *matrix product* $A \cdot v$. We may use any of them depending on the context.

Notice that Lemma 8.22 can now be interpreted as follows: if the transformations T and S accept the same values on all $v \in V$, i.e., if $T(v) = Av = Bv = S(v)$, then $T = S$.

Let us test the formula $T(v) = Av$ on some of our basic examples.

Example 20.20. Consider the projection $P : \mathbb{R}^3 \to \mathbb{R}^3$ that maps the second coordinate to zero: $P(x, y, z) = (x, 0, z)$. As we saw its matrix in standard basis is:

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

Take, say, $v = (3, 2, 5)$ and compute

$$Av = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \\ 5 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 5 \end{bmatrix} = P(v).$$

Example 20.21. Take the polynomial space $V = W = \mathcal{P}_3(\mathbb{R})$ and the transformation $T(f(x)) = f'(x)$. Take the polynomial, say,

$$f(x) = 4 + 3x + x^2 + 7x^3.$$

Its coordinates are $(4, 3, 1, 7)$. We have

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

So for this case:

$$A \cdot f = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 1 \\ 7 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 21 \\ 0 \end{bmatrix}.$$

The column vector on the right-hand side corresponds to $g(x) = 3 \cdot 1 + 2x + 21x^2$. To check that this is a correct result compute the derivative:

$$\begin{aligned} f'(x) &= 0 + 3x^{1-1} + 2x^{2-1} + 7 \cdot 3x^{3-1} \\ &= 3 + 2x + 21x^2 = g(x). \end{aligned}$$

So even such a "non-algebraic" operation, as differentiation, can be interpreted by matrix products language, and explained as a linear transformation!

Example 20.22. We have already computed the matrix for the rotation R_φ.

$$A = A_{R_\varphi} = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}.$$

We now get that for any (x, y) the result of rotation of (x, y) around the origin O is:

$$\begin{aligned} R_\varphi(x, y) &= \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\ &= \begin{bmatrix} \cos(\varphi)\, x - \sin(\varphi)\, y \\ \sin(\varphi)\, x + \cos(\varphi)\, y \end{bmatrix}. \end{aligned}$$

In particular, let us rotate the point $C = (5, 2)$ by $60°$ around O. We have $\varphi = \frac{\pi}{3}$. For this value the matrix A is:

$$\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$$

and we have:

$$R_{\frac{\pi}{3}}(5, 2) = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{5}{2} - \sqrt{3} \\ \frac{5\sqrt{3}}{2} + 1 \end{bmatrix}.$$

In particular, if we have a geometrical object, such as a square, we can find all its vertices (after rotation) by multiplication with a single matrix A.

The previous examples allow to build more complicated transformations:

Example 20.23. It is easy to understand that this matrix

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

defines the transformation T of $\mathbb{R}^3$ that rotates the space around the axis Oz (by plane xOy)

by angle φ, and also scales the space 5 times by the axis Oz.

If we replace 3 by -1, we will get mirror reflection by axis Oz.

And we can build transformations which, unlike the previous examples, are hard to visualize:

Example 20.24. It is easy to understand (but not to visualize) that this matrix

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 & 0 & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 & 0 & 0 \\ 0 & 0 & 3\cos(\theta) & -3\sin(\theta) & 0 \\ 0 & 0 & 3\sin(\theta) & 3\cos(\theta) & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}$$

is a transformation of $\mathbb{R}^5$ that rotates the space by plane xOy at angle φ, rotates the space by plane zOt at angle θ, *and* also scales everything at the directions of Oz and Ot by 3 times, *and* finally scales everything 5 times by the fifth axis Ou.

Remark 20.25. A helpful pattern is clear from examples above (in particular, from examples 20.10, 20.15, 20.18). If a transformation is given in its functional form, say:

$$T(x,y,z) = (\alpha_1 x + \alpha_2 y + \alpha_3 z,\quad \beta_1 x + \beta_2 y + \beta_3 z,\quad \gamma_1 x + \gamma_2 y + \gamma_3 z), \tag{20.2}$$

then in the standard basis it has the matrix:

$$A = [T]_E = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{bmatrix}. \tag{20.3}$$

I.e., we just put the coefficients $\alpha_1, \alpha_2, \ldots; \beta_1, \beta_2, \ldots; \gamma_1, \gamma_2, \ldots$ from (20.2) by *rows* to fill-in the matrix A. And vise versa, if the matrix (20.3) is given, we can reconstruct the form (20.2). And the analogs of this also are true when for $T: F^m \to F^n$ with any m, n (not necessarily $m = n$). See Exercise E.20.7.

In the sequel we will consider switching from the from (20.2) to the form (20.3) and vise versa a *trivial* task, ans will do this without proper explanations.

20.3. Change of basis for linear transformations

In Section 13.1 we saw how the coordinates of a vector $v \in V$ change when we switch from one basis of V to another. Namely, if E and G are two bases in V, and if $P = P_{EG}$ is the change of basis matrix from E to G, then the coordinates $[v]_E$ and $[v]_G$ of v in these bases are related as $[v]_E = P\,[v]_G$.

Let us use the matrix P to study the matrices $A = [T]_E$ and $B = [T]_G$ of a transformation T of V in bases E and G, respectively. $T(v)$ in these bases has the coordinates:

$$T(v) = [T(v)]_E = A\,[v]_E \quad \text{and} \quad T(v) = [T(v)]_G = B\,[v]_G. \tag{20.4}$$

In the left-hand side of (20.4) applying the change of basis formula to $[v]_E$ we get:

$$[T(v)]_E = A\big(P\,[v]_G\big) = (AP)[v]_G.$$

Using the change of basis formula $[T(v)]_E = P\,[T(v)]_G$ and the right-hand side of (20.4) we have:

$$[T(v)]_E = P\,[T(v)]_G = P\,\big(B\,[v]_G\big) = (PB)[v]_G.$$

We get $(AP)[v]_G = (PB)[v]_G$ for *any* vector $[v]_G$. By Lemma 8.22 we have $AP = PB$. Multiplying this by P^{-1} (we can do this because P is invertible by Theorem 13.4) we have $B = P^{-1}AP$. We proved a helpful:

Theorem 20.26. *Let $E = \{e_1, \ldots, e_n\}$ and $G = \{g_1, \ldots, g_n\}$ be any bases in the space V, and let $P = P_{EG}$ be the change of basis matrix from E to G. If a transformation T of V has the matrix $A = [T]_E$ in E, and the matrix $B = [T]_G$ in G, then*

$$\boldsymbol{B = P^{-1}AP}.$$

P is an invertible matrix, so we can also write $A = PBP^{-1}$ whenever we need to express B via A.

Remark 20.27. According to Theorem 13.6 for every basis E of V and for any invertible matrix P there is a (unique) basis G such that $P = P_{EG}$ is the change of basis matrix from E to G. In the vocabulary of Theorem 20.26 this implies that for each transformation T with a matrix A in a basis E, and for every invertible matrix P there is a (unique) basis G of V in which T has the matrix B, and two matrices A and B of the same transformation are related as $B = P^{-1}AP$.

Example 20.28. In Example 20.19 we saw that the transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ given by the rule $T(x, y) = (x, 3y)$ in the standard basis $e_1 = (1, 0)$, $e_2 = (0, 1)$ has the matrix $A = [T]_E = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$. And in basis $g_1 = (1, 1)$, $g_2 = (-1, 1)$ it has the matrix $B = [T]_G = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$.

The change of basis matrix $P = P_{EG}$ evidently is $P = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, and its inverse is $P^{-1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}$.

To check the equality of Theorem 20.26 for this case we compute:

$$B = P^{-1}AP = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

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

This means that knowing P and A *we no longer need compute the matrix B for T from the scratch*. Instead, we get B as $P^{-1}AP$. Later we will see why this has important computational potential, especially in matrix digitalization.

Exercises

E.20.1. We are given the following maps $T : V \to W$ from the space V to the space V over the field F. Find out if they are linear transformations. **(1)** $V = \mathbb{R}^3$, $W = \mathbb{R}^2$ and $T(x, y, z) = (x+y, 2y+z)$. **(2)** $V = \mathbb{C}^2$, $W = \mathbb{C}^3$ and $T(x, y) = (y, x, y+1)$. **(3)** $V = W = \mathcal{P}_3$ and $T(f(x)) = f'(x) + 2f(x)$.

E. 20.2. Prove that there is *no* linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^3$ satisfying the conditions $T(1, 0) = (3, 2, 1)$, $T(1, 1) = (-1, 0, 1)$, $T(3, 1) = (5, 0, -2)$.

E.20.3. Find the matrices of the following transformations choosing some suitable bases for the considered spaces. **(1)** $T : \mathbb{R}^2 \to \mathbb{R}^3$ defined as $T(x, y) = (x + y, 3y, 3x)$. **(2)** $T : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ defined as $T(x, y, z) = (2(y + z), 3x)$. **(3)** $T : \mathcal{P}_2 \to \mathcal{P}_2$ defined as $T(f(x)) = 3f'(x)$.

E.20.4. Build the matrix $[T]_{EE}$ of the transformation $T : V \to W$ when **(1)** $V = \mathbb{R}^2$, $W = \mathbb{R}^3$, E denotes the standard basis in each space, and T is defined by the rules $T(1, 0) = (3, 2, 1)$ and $T(1, 1) = (-1, 0, 1)$. **(2)** $V = W = \mathbb{R}^3$, E denotes the standard basis, and T is defined by the rule $T(x, y, z) = (x + z,\ 3z,\ y - x)$. **(3)** $V = W = \mathbb{R}^3$, E denotes the standard basis, and T is defined by the rule $T(x, y, z) = (0,\ x + y + z,\ 0)$. **(4)** $V = W = \mathcal{P}_3$, E denotes the standard basis, and T is defined by the rule $T(f(x)) = 3f(x) + f'(x)$.

E.20.5. Let T be the transformation $T(x, y, z) = (2x + y, x + z)$ of Example 20.10 with the matrix $A = \left[\begin{smallmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right]$. For $v = (3, 5, -1)$ compute the vector $T(v)$ in two ways. First compute it by formula $T(x, y, z) = (2x + y, x + z)$, next compute it as matrix product $A[v]$.

E.20.6. Let R be the rotation of the plane $\mathbb{R}^2$ about the origin by $30°$, and let $ABCD$ be a rectangle for which we know the vertices $A = (3,0)$, $B = (6,-3)$, $C = (8,-1)$. Using the rotation matrix found in Example 20.17 find the vertices of the image of $ABCD$ after rotation.

E.20.7. Prove the helpful pattern noticed in Remark 20.25, i.e., if a transformation is given in form (20.2), then in the standard basis its matrix $A = [T]_E$ is of form (20.2).

E.20.8. Let E and G be bases of $\mathbb{R}^2$ given in Example 20.28. **(1)** A transformation T has the matrix $\left[\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right]$ in basis E. Find its basis in G. **(2)** A transformation S has the matrix $\left[\begin{smallmatrix} 3 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ in basis G. Find its basis in E. *Hint*: use the matrices P_{EG}, P_{GE} of Example 20.28.

E.20.9. In $\mathbb{R}^3$ we are given the transformation $T(x,y,z) = (x+y,\ 2z,\ x-y)$. Also, E is the standard basis, and G is the basis consisting of vectors $g_1 = (2,1,0)$, $g_2 = (0,0,1)$, $g_3 = (1,1,3)$. **(1)** Find the matrix $B = [T]_G$ of T in G by expressing the vectors $T(g_1)$, $T(g_2)$, $T(g_3)$ in basis G (use Algorithm 14.29). **(2)** Find the matrix $B = [T]_G$ using the matrix $A = [T]_E$ of T in E and the change of basis matrix $P = P_{EG}$.

E.20.10. The linear transformation T is given on $\mathbb{R}^2$ by the rules $T\left[\begin{smallmatrix} 2 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 2 \\ 4 \end{smallmatrix}\right]$ and $T\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 6 \\ 2 \end{smallmatrix}\right]$ (coordinates are in standard basis E). We also have the basis $G = \{g_1, g_2\}$ where $g_1 = \left[\begin{smallmatrix} -2 \\ 3 \end{smallmatrix}\right]$ and $g_2 = \left[\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right]$. Find the matrix $B = [T]_G$ of T in G *in two ways* as follows. **(1)** Find the matrix $A = [T]_E$ of T in standard basis E, and then use the formula $B = P^{-1}AP$ (with the change of basis matrix $P = P_{EG}$). **(2)** Using the matrix A write T explicitly, in form $T(x,y) = (ax+by,\ cx+dy)$. By this form find the values $T(g_1)$ and $T(g_2)$, and calculating their coordinates in the basis G find the matrix $B = [T]_G = \big[[T(g_1)]_G\ \ [T(g_2)]_G\big]$ by definition.

CHAPTER 21

The kernel and range of transformations

21.1. The kernel of a linear transformation

We need two important subspaces related to linear transformation $T : V \to W$. The first one is defined as:

Definition 21.1. Let $T : V \to W$ be any linear transformation from V to W. The *kernel* of T is the set of all vectors of V the image of which under T is the zero vector of W:

$$\ker(T) \stackrel{\text{def}}{=} \{v \in V \mid T(v) = \vec{0}_W\}.$$

If T is, say, the projection of $\mathbb{R}^3$ mentioned in Example 20.20, then $\ker(T)$ is the axis Oy. Further examples will come later, after we find a method how to compute $\ker(T)$.

Using Definition 10.12 it is very easy to see that the kernel of a linear transformation $T : V \to W$ is a *subspace* of V. The dimension of $\ker(T)$ is called the *nullity* of T, and it is denoted by $\text{nullity}(T)$. This gives us a plan of how to describe the kernel: since $\ker(T)$ is a space, not a haphazard subset, just compute a *basis* for it, and consider $\ker(T)$ as the collection of all linear combinations of the basis vectors.

Take any vector $v = (x_1, \ldots, x_n) \in \ker(T)$ with for now unknown coordinates. If the matrix of T is $A = [T]$, then by (20.1):

$$T(v) = Av = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = O.$$

The above equality is equivalent to a homogeneous system of linear equations $AX = O$. So the kernel $\ker(T)$ is the subspace of all solutions of $AX = O$ (in the given coordinate system). You, surely, remember that we called that subspace the *null space* of A, and we already suggested the method of computation for its basis in Algorithm 15.2. And, clearly, $\text{nullity}(T) = \text{nullity}(A)$.

How to compute the kernel and nullity of a transformation.

Algorithm 21.2 (Computation of the kernel and nullity of a transformation)**.** We are given a transformation $T : V \to W$ from the space V to the space W on same field F. Coordinate systems with bases E and G with coordinate maps $\phi_E : V \to F^n$ and $\phi_G : W \to F^m$ are given.

► Find $\ker(T)$ and $\text{nullity}(T)$ for the transformation T.

1. Compute the matrix $A = [T]_{EG}$ of T by Algorithm 20.12.

2. Find a basis $\{e_1, \ldots, e_{n-r}\}$ for null space $\text{null}(A)$ by Algorithm 15.2, where $r = \text{rank}(A)$.

3. If V is a space other than F^n, then set $e_i = \phi_E^{-1}(e_i)$ for $i = 1, \ldots, n-r$.

4. Output $\ker(T) = \text{span}(e_1, \dots, e_{n-r})$, and $\text{nullity}(T) = n - r$.

It turns out that the important property of *injectivity* of T can be detected by its kernel or nullity:

Corollary 21.3. *The linear transformation $T : V \to W$ is an injective function if and only if* $\text{nullity}(T) = 0$.

***Proof*.** If $\text{nullity}(T) \neq 0$, i.e., if $\ker(T) \neq \{0\}$, there is a non-zero vector v for which $T(v) = 0$. Since also $T(0) = 0$ by Proposition 20.9, we have $T(v) = T(0)$ for $v \neq 0$.

On the other hand, if T is not injective, there are distinct vectors $u, v \in V$ for which $T(u) = T(v)$. Then $u - v \neq 0$, and $T(u - v) = T(u) - T(v) = 0$, i.e., $\ker(T) \neq \{0\}$. □

Example 21.4. Let the linear transformation $T : \mathbb{R}^5 \to \mathbb{R}^3$ be given by:

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

Since the matrix already is known, we can skip step **1** in Algorithm 21.2. To apply Algorithm 15.2 we need the reduced row-echelon form of A (computation is omitted):

$$\text{rref}(A) = \begin{bmatrix} \mathbf{1} & 2 & 0 & 0 & -\frac{3}{2} \\ 0 & 0 & \mathbf{1} & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & \mathbf{1} & 3 \end{bmatrix}.$$

Then by Algorithm 15.2 a basis for null space null(rref(A)) is:

$$e_1 = \begin{bmatrix} 2 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad e_2 = \begin{bmatrix} -\frac{3}{2} \\ 0 \\ -\frac{1}{2} \\ 3 \\ -1 \end{bmatrix}.$$

So we can write $\ker(T) = \text{span}(e_1, e_2)$. Or in a "simpler" form we can write $\ker(T)$ as a set of linear combinations of e_1 and e_2:

$$\ker(T) = \{\alpha e_1 + \beta e_2 \mid \alpha, \beta \in \mathbb{R}\}$$

$$= \left\{(-2\alpha + \tfrac{3}{2}\beta,\ \alpha,\ \tfrac{1}{2}\beta, -3\beta,\ \beta) \mid \alpha, \beta \in \mathbb{R}\right\}.$$

Clearly, $\text{nullity}(T) = 5 - 3 = 2$.

By Corollary 21.3 T is *not* injective.

Example 21.5. Take the projection transformation $P(x, y, z) = (x, 0, z)$ with matrix:

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

$\ker(P)$ is the axis Oy, and so $\text{nullity}(P) = \dim(Oy) = 1$. Let us apply Algorithm 21.2 to achieve the same fact differently:

$$\text{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix}.$$

By Algorithm 15.2 the space null(rref(A)) is 1-dimensional, as $3 - 2 = 1$. As a basis vector we can take

$$\begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}, \quad \text{or, equivalentlay,} \quad \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix},$$

i.e., we again get that $\ker(P)$ is the axis Oy.

Example 21.6. The linear transformation $T(f(x)) = f'(x)$ of polynomial space $V = \mathcal{P}_3(\mathbb{R})$ has the matrix

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

The reduced row-echelon form is:

$$\text{rref}(A) = \begin{bmatrix} 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since $4 - 3 = 1$ the space null(rref(A)) is 1-dimensional. By Algorithm 15.2 take

$$\begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{or, equivalentlay, } e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

We cannot yet declare that this vector is a basis for $\ker(T)$, as our space is not equal to $\mathbb{R}^4$, as it consists of polynomials. Use the coordinate map $\phi_E : \mathcal{P}_3(\mathbb{R}) \to \mathbb{R}^4$ to find the polynomial corresponding to e_1: it is the constant function $f(x) = 1$. So $\ker(T) = \{f(x) = c \mid c \in \mathbb{R}\}$. Even without these calculations if is clear that, if $f'(x)=0$, then $f(x)=c$. Also, $\text{nullity}(T)=4-3=1$.

Example 21.7. For the rotation transformations, such as

$$\begin{bmatrix}\cos(\varphi) & -\sin(\varphi)\\ \sin(\varphi) & \cos(\varphi)\end{bmatrix},$$

$$\begin{bmatrix}\cos(\varphi) & -\sin(\varphi) & 0\\ \sin(\varphi) & \cos(\varphi) & 0\\ 0 & 0 & 1\end{bmatrix},$$

$$\begin{bmatrix}\cos(\varphi) & 0 & -\sin(\varphi)\\ 0 & 1 & 0\\ \sin(\varphi) & 0 & \cos(\varphi)\end{bmatrix}$$

we evidently have $\ker(T)=\{0\}$, since a rotation is an isomorphism, and it maps any non-zero vector to a non-zero vector only. And $\text{nullity}(T)=0$ (compare with Corollary 21.3).

If needed, we could also establish this fact by Algorithm 21.2. Compute the reduced row-echelon form for the matrix of the first of these transformations:

$$A=[R_\varphi]=\begin{bmatrix}\cos(\varphi) & -\sin(\varphi)\\ \sin(\varphi) & \cos(\varphi)\end{bmatrix}.$$

We have

$$A\sim\begin{bmatrix}\cos(\varphi) & -\sin(\varphi)\\ 0 & \cos(\varphi)+\frac{\sin^2\varphi}{\cos(\varphi)}\end{bmatrix}\ \ R2-\frac{\sin\varphi}{\cos\varphi}R1$$

$$\sim\begin{bmatrix}\mathbf{1} & -\tan(\varphi)\\ 0 & \mathbf{1}\end{bmatrix}\ \ \begin{matrix}\frac{1}{\cos\varphi}\cdot R1\\ \cos\varphi\cdot R2\end{matrix}$$

$$=\text{rref}\big([R_\varphi]\big).$$

The rank of this matrix is 2, and we obtain the same result $\ker(T)=\{0\}$, since $2-2=0$, and the null space in this case is 0-dimensional. T is injective by Corollary 21.3.

21.2. The range of a linear transformation, the sum of rank and nullity

The second subspace related to a linear transformation is given by:

Definition 21.8. Let $T:V\to W$ be any linear transformation from V to W. The *range* of T is the set of all vectors of W which are images of some vectors of V:

$$\text{range}(T)\overset{\text{def}}{=}\{w\in W \mid T(v)=w \text{ for some } v\in V\}.$$

For, say, projection transformation of Exercise 20.20 we have its range equal to the plane xOz. By Definition 10.12 it is very easy to see that the range of a linear transformation $T:V\to W$ is a *subspace* of W. The dimension of $\text{range}(T)$ is called the *rank* of T, and it is denoted by $\text{rank}(T)$. Since $\text{range}(T)$ is a subspace, we have the idea how to describe it: just compute a basis for $\text{range}(T)$.

Present the matrix of T as a collection of column vectors:

$$A=[T]=\begin{bmatrix}a_{11} & \cdots & a_{1n}\\ \cdots & \cdots & \cdots\\ a_{m1} & \cdots & a_{mn}\end{bmatrix}=\left[\ T(e_1)\ \vdots\ \cdots\ \vdots\ T(e_n)\ \right]$$

(supposing coordinate systems with respective bases is fixed). Since $T(e_i)$ is the image of e_i for each $i=1,\dots,n$, all the $T(e_i)$ are in $\text{range}(T)$, and identifying each vector with its coordinates we get $\text{col}(A)\subseteq\text{range}(T)$.

On the other hand, for any $w\in\text{range}(T)$ there exists a $v\in V$ such that $T(v)=w$. Present v as a linear combination $v=c_1e_1+\cdots+c_ne_n$ and apply T to it:

$$T(v)=T(c_1e_1+\cdots+c_ne_n)=c_1T(e_1)+\cdots+c_nT(e_n).$$

So $w=T(v)$ belongs to the column space $\text{col}(A)$, and $\text{range}(T)\subseteq\text{col}(A)$, that is, $\text{range}(T)$ and $\text{col}(A)$ are equal (up to coordinate map ϕ_G). Also, clearly, $\text{rank}(T)=\dim(\text{col}(A))=\text{rank}(A)$.

How to compute the range and rank of a transformation.

Algorithm 21.9 (Computation of the range and rank of a transformation)**.** We are given a transformation $T : V \to W$ from the space V to the space W on same field F. Coordinate systems with bases E and G with coordinate maps $\phi_E : V \to F^n$ and $\phi_G : W \to F^m$ are given.

► Find range(T) and rank(T) for the transformation T.

1. Compute the matrix $A = [T]_{EG}$ of T by Algorithm 20.12.
2. Find a basis $\{e_1, \dots, e_r\}$ for column space col(A) by Algorithm 14.10, where $r =$ rank(A).
3. If V is a space other then F^n, then set $e_i = \phi_G^{-1}(e_i)$ for $i = 1, \dots, r$.
4. Output col$(T) =$ span$(e_1, \dots, e_r)$, and rank$(T) = r$.

The property of surjectivity can evidently be interpreted by range and rank:

Corollary 21.10. *The linear transformation $T : V \to W$ is a surjective function if and only if* rank$(T) =$ dim(W).

By Theorem 15.1 we for any matrix $A \in M_{m,n}(F)$ have rank(A) + nullity$(A) = n$. Since nullity$(T) =$ nullity(A) and rank$(T) =$ rank(A) and, we get:

Corollary 21.11. *For any linear transformation $T : V \to W$:*

$$\mathbf{rank}(T) + \mathbf{nullity}(T) = \mathbf{dim}(V).$$

Roughly speaking: "the larger is nullity(T)" (the "more" are vectors of V mapped to zero), "the smaller is rank(T)" (the "less" are the vectors in W to which T maps some vectors from V). In particular, when nullity$(T) =$ dim(V) and rank$(T) = 0$, we get the *zero* transformation $T(v) = \vec{0}$.

Let us review our basic examples, find the ranges, verify the equality rank(T) + nullity$(T) =$ dim(V), and test surjectivity for them.

Example 21.12. For projection $P(x, y, z) = (x, 0, z)$ we computed ker$(P) = Oy$ and nullity$(P) = 1$. Clearly, range$(P) = xOz$ which is isomorphic to $\mathbb{R}^2$. Thus, rank$(P) = 2$, and

$$\text{rank}(P) + \text{nullity}(P) = 2 + 1 = 3 = \dim\big(\mathbb{R}^3\big).$$

We can obtain the same using Algorithm 21.9. The reduced row-echelon form of the matrix A of P is:

$$\text{rref}(A) = \begin{bmatrix} \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix},$$

and as a basis for col(A) we can take the 1'st and 3'rd columns of A.

By Corollary 21.10 P is *not* surjective.

Example 21.13. We in Example 21.4 considered the transformation $T : \mathbb{R}^5 \to \mathbb{R}^3$ given by

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

We computed rref(A) and found:

$$\ker(T) = \text{span}(e_1, e_2)$$
$$= \text{span}\big((-2, 1, 0, 0, 0),\ (\tfrac{3}{2}, 0, \tfrac{1}{2}, -3, 1)\big),$$

and nullity$(T) = 2$. Since the pivot columns of rref(A) are the 1'st, 3'rd and 4'th columns, the linearly independent columns of A (i.e., the basis for col(A) and for range(T)) are $g_1 = (1, 2, -1)$, $g_2 = (-1, 0, 1)$, $g_3 = (1, 1, 0)$. As we see:

$$3 + 2 = 5 = \dim\big(\mathbb{R}^5\big),$$

and by Corollary 21.10 T is surjective.

Example 21.14. For the transformation $T(f(x)) = f'(x)$ on $\mathcal{P}_3(F)$ we in Example 21.6 computed ker$(T) = \{f(x) = c \mid c \in \mathbb{R}\}$ and also nullity$(T) = 1$.

We have:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \text{rref}(A) = \begin{bmatrix} 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since the pivots in rref(A) are in its last three columns, as a basis for col(A) we can take its last three columns

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix},\quad \begin{bmatrix}0\\2\\0\\0\end{bmatrix},\quad \begin{bmatrix}0\\0\\3\\0\end{bmatrix}.$$

The respective polynomials, i.e., basis vector for range(T) are $f_1(x) = 1$, $f_2(x) = 2x$, $f_3(x) = 3x^2$. Since they clearly span the same subspace as the polynomials $1, x, x^2$, we have:

$$\begin{aligned}\text{range}(T) &= \text{span}\big(1,\, 2x,\, 3x^2\big)\\ &= \text{span}\big(1,\, x,\, x^2\big) = \mathcal{P}_2(F).\end{aligned}$$

Then rank$(T) = 3$, and

$$3 + 1 = 4 = \dim(\mathcal{P}_3(F)).$$

Clearly, T is not surjective.

Example 21.15. In particular, for the rotation R_φ we have range$\big(R_\varphi\big) = \mathbb{R}^2$ and rank$\big(R_\varphi\big) = 2$. So, since $\ker(T) = \{0\}$, we get

$$2 + 0 = 2 = \dim\big((\mathbb{R}^2)\big).$$

R_φ is surjective.

Example 21.16. If T is any isomorphism on V, then $\ker(T) = \{0\}$, nullity$(T) = 0$, range$(T) = V$, rank$(T) = \dim(V)$, and the equation of Corollary 21.11 reads

$$\text{rank}(T) + 0 = \dim(V),$$

i.e., T is both injective and surjective (compare with Theorem 22.7).

Remark 21.17. Let us stress "evolution" of some ideas we used:

In Part 2 we started by a system of m *linear equations* on n variables over a *field* F, and called the system with zero constant terms a *homogeneous* system.

Then in Part 3 we interpreted such a system of linear equations as *matrix equation* $AX = B$ for some $A \in M_{m,n}(F)$ and $B \in M_{m,1}(F)$. When $B = 0$, we have a homogeneous system $AX = O$.

Next, in Part 4 denoting the columns of A by $\vec{v}_1, \dots, \vec{v}_n$, and taking $\vec{w} = B$, we interpreted $AX = B$ as *linear combination* $x_1\vec{v}_1 + \cdots + x_n\vec{v}_n = \vec{w}$. When $\vec{w} = \vec{0}$, then existence of non-zero solution is nothing but *linear dependence* of $\vec{v}_1, \dots, \vec{v}_n$.

Linear transformations in the current Part 7 suggest further interpretations: the transformation T defined by the matrix A maps an n-dimensional *space* V to an m-dimensional *space* W (both over the same field F), and the fact that $\vec{v}$ is a solution for the system $AX = B$ means $T : \vec{v} \to \vec{w}$ or $T(\vec{v}) = \vec{w}$, i.e., $\vec{w} \in \text{range}(T)$. And $\vec{v} \in \ker(T)$ means that the coordinates of $\vec{v}$ form a solution of $AX = O$. The inequality $\ker(T) \neq \{0\}$ means the columns of A are linearly dependent.

The observation that all n variables of the system $AX = B$ can be divided to *pivot* and *free* variables eventually transformed to equality rank(A) + nullity$(A) = n$ for $m \times n$ matrices, and later to equality rank(T) + nullity$(T) = \dim(V)$ for transformations.

La mathématique est l'art de donner le même nom à des choses différentes!

Exercises

E.21.1. The transformation $T : \mathbb{R}^4 \to \mathbb{R}^3$ is given by the rule: $T(x, y, z, t) = (x + 2z,\ 3x,\ x - y)$. **(1)** Describe $\ker(T)$ by finding a basis for it. **(2)** Describe range(T) by finding a basis for it. **(3)** Which is the sum of nullity(T) and rank(T)? Mention the theorem that you use to answer this question.

E.21.2. The transformation $T : \mathcal{P}_2(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R})$ is given by the rule: $T(f(x)) = 2f'(x) + f''(x)$. Describe its kernel and range based on Definition 21.1 and Definition 21.8 (i.e., without using Algorithm 21.2 and Algorithm 21.9).

E.21.3. Find $\ker(T)$ and range(T) for transformation $T : \mathcal{P}_2(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R})$ of Exercise E.21.2 using Algorithm 21.2 and Algorithm 21.9. *Hint*: make sure you get the same answer as in Exercise E.21.2.

E.21.4. The transformation $T : \mathbb{R}^5 \to \mathbb{R}^3$ is given by the matrix

$$A = \begin{bmatrix} 2 & 4 & 0 & 2 & 0 \\ 1 & 2 & 1 & 4 & 2 \\ 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

(1) Find a basis for the kernel of T, and the nullity of T. **(2)** Using the result of the previous point tell what is the rank of T, and the dimension of the range of T. What is the rank of the matrix A? **(3)** Find a basis for the range of T.

E.21.5. Read Remark 21.17 about "evolution" carefully. Then consider the system

$$\begin{cases} x_1 \phantom{{}+2x_2+x_3} + x_4 = 0 \\ \phantom{x_1+{}} 2x_2 \phantom{{}+x_3} + 2x_4 = 0 \\ x_1 + x_2 + x_3 + x_4 = 0 \end{cases}$$

of linear equations, and tell what each of the steps of the "evolution" is meaning for this system, including the matrix form, the linear dependence of columns, the transformation with its kernel and range.

E.21.6. Let $\phi_E : V \to F^n$ be the *coordinate map* from the n-dimensional space V to F^n (with respect to a basis E of ϕ_E). **(1)** Show that ϕ_E in fact is a linear transformation. **(2)** Find the kernel and nullity of ϕ_E. **(3)** Find the range and rank of ϕ_E. **(4)** Is ϕ_E an isomorphism? *Hint*: you may use the facts from Section 12.2.

CHAPTER 22

Operations with linear transformations

22.1. Compositions of linear transformations

Assume we have two linear transformations $T : V \to W$ and $S : W \to U$, where all three spaces V, W, U are over the same field F. We may consider the composition of $S \circ T$ of these two *functions*, which is defined because the range of T is contained in the domain W of S. The function $S \circ T$ also is a *linear transformation* because:

$$S \circ T\ (u+v) = S\big(T(u+v)\big) = S\big(T(u)+T(v)\big)$$
$$= S\big(T(u)\big) + S\big(T(v)\big) = S \circ T\ (u) + S \circ T\ (v).$$
$$S \circ T\ (c\,v) = S\big(T(c\,v)\big) = S\big(c\,T(v)\big) = c\,S\big(T(v)\big) = c\big(S \circ T\ (v)\big).$$

Denote $S \circ T$ by ST, and call this linear transformation the *product* or *composition* of T and S. Clearly, $ST : V \to U$ is from V into U.

Example 22.1. For spaces $V = W = U = \mathbb{R}^2$ consider transformations given by the rule $T(x, y) = (x, 3y)$ and $S(x, y) = (3x, y)$. Then, clearly, $ST(v) = ST(x, y) = (3x, 3y) = 3v$.

Example 22.2. On the plane $V = W = U = \mathbb{R}^2$ consider any two rotations R_φ and R_ψ then their product $R_\psi R_\varphi$ is the rotation $R_{\varphi+\psi}$. For, rotating the plane by angle φ and then by angle ψ is the same as rotating the plane by angle $\varphi + \psi$. This includes the case when one of the angles is negative. We may even have $\varphi = -\psi$, and then $R_\varphi R_\psi = R_0$ is the identical transformation, which we denoted by I.

Example 22.3. Take spaces $V = W = U = \mathcal{P}_3(F)$. If T and S are given by $T(f(x)) = f'(x)$, $S(f(x)) = f'(x)$, then the product ST maps $f(x) \in \mathcal{P}_3(F)$ to its *second derivative*: $ST(f(x)) = (f'(x))' = f''(x)$.

In analogy with product of two transformations, we can define the product of any number of linear transformations:

$$T_m \cdots T_2 T_1\ (u) = T_m\Big(\cdots\Big(T_2\big(T_1(u)\big)\Big)\cdots\Big).$$

Since the composition of any (not necessarily linear) maps is associative, we can write $T_m \cdots T_1\,(u)$ without any brackets.

Theorem 22.4. *Let $T : V \to W$ and $S : W \to U$ be any linear transformations, and let their matrices be $A = [T]$ and $B = [S]$. Then the matrix C of the product transformation ST is the product matrix BA, i.e.:*

$$\boldsymbol{C} = \boldsymbol{BA} \quad \textit{or} \quad [\boldsymbol{ST}] = [\boldsymbol{S}][\boldsymbol{T}].$$

Proof. Let $\dim(V) = n$, $\dim(W) = m$, $\dim(U) = k$. Then A is an $m \times n$ matrix and B is an $k \times m$ matrix. So the matrix product BA is correctly defined, and it is a $k \times n$ matrix.

Consider any $v \in V$ and identify it with its coordinates vector. $T(v)$ can be interpreted as the matrix product Av. Next identify $T(v)$ with Av, and interpret $S\big(T(v)\big)$ as the matrix product $B(Av)$. By matrix product associativity $B(Av) = (BA)v$. On the other hand $ST(v) = Cv$, and we get

$$Cv = (BA)v.$$

This holds for *any* v, and so $BA = C$ by Lemma 8.22. □

Example 22.5. Consider some projection, reflection, scaling, rotation transformations T_1, T_2, T_3, T_4 respectively defined by the matrices:

$$T_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ T_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},\ T_3 = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$T_4 = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The product of these four matrices is

$$\begin{bmatrix} 3\cos(\varphi) & -3\sin(\varphi) & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix},$$

which is the matrix of the product transformation $T_4T_3T_2T_1$.

In Example 9.6 we noticed that a series of elementary operations can be replaced by multiplication by a single matrix N. Now we got the generalization of that: each elementary operation corresponds to an elementary matrix, which causes a linear transformation. And the series of any linear transformations can be replaced by a single transformation.

Example 22.6. Let both T and S be the linear transformation of differentiation in $\mathcal{P}_3(F)$. We already found the matrix

$$A = [T] = B = [S] = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

in Example 20.21. The product ST has the matrix

$$C = BA = A^2 = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

ST is a transformation that maps each $f(x) \in \mathcal{P}_3(F)$ to its *second derivative* $f''(x) = (f'(x))'$. For the polynomial, say,

$$f(x) = 4 + 3x + x^2 + 7x^3$$

we have:

$$\begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 3 \\ 1 \\ 7 \end{bmatrix} = \begin{bmatrix} 2 \\ 42 \\ 0 \\ 0 \end{bmatrix},$$

which corresponds to:

$$2 \cdot 1 + 42x = f''(x) = (4 + 3x + x^2 + 7x^3)''.$$

We again see that the very “non-algebraic” operation of second derivation corresponds to operation of matrix multiplication.

22.2. Invertible linear transformations

Let $T : V \to W$ be a linear transformation. Like any function, T may or may *not* have an inverse $T^{-1} : W \to V$. For example, the rotation R_φ has an inverse function $R_{-\varphi}$, while the projection $P(x,y,z) = (x,0,z)$ has no inverse function because $P(1,1,1) = (1,0,1)$ and $P(1,2,1) = (1,0,1)$, so there is no uniquely defined value for $P^{-1}(1,0,1)$.

The inverse of a function exists if and only if the function a *bijection*. It turns out that when the bijection T is a linear transformation, then its inverse $T^{-1} : W \to V$ also is a *linear* transformation. Indeed, since $T\big(T^{-1}(w)\big) = w$ and $T^{-1}\big(T(w)\big) = w$, then for any $w, z \in W$ and $c \in F$ we by linearity of T have:

$$T^{-1}(w+z) = T^{-1}\Big(T\big(T^{-1}(w)\big) + T\big(T^{-1}(z)\big)\Big) = T^{-1}\Big(T\big(T^{-1}(w) + T^{-1}(z)\big)\Big) = T^{-1}(w) + T^{-1}(z)$$

$$T^{-1}(c\,w) = T^{-1}\Big(c\,T\big(T^{-1}(w)\big)\Big) = T^{-1}\Big(T\big(c\,T^{-1}(w)\big)\Big) = c\,T^{-1}(w).$$

Call the linear transformation T *invertible* if it has an inverse linear transformation T^{-1}. We just saw that T is invertible if and only if it is a bijection, that is, if it is an *isomorphism*.

It turns out that the invertible linear transformations may exist between spaces of *same dimension* only: if $\dim(V) \neq \dim(W)$, then there is no invertible transformation from V to W. Indeed, assume $\dim(V) = n < \dim(W) = m$ and $T : V \to W$ is invertible. For any element $w \in W$ the vector $T^{-1}(w) = v$ is defined. Fix a basis $\{e_1, \dots, e_n\}$ of V, and write $v = a_1 e_1 + \cdots + a_n e_n \in V$. Then

$$w = T(v) = T(a_1 e_1 + \cdots + a_n e_n) = a_1 T(e_1) + \cdots + a_n T(e_n).$$

This means that the system of n vectors $T(e_1), \dots, T(e_n)$ is a spanning set for an m-dimensional space V. Since $n < m$, we have a contradiction. The case $n > m$ is considered similarly. We get that we need only consider the cases when $\dim(V) = \dim(W)$.

Of course, the equality of $\dim(V)$ and $\dim(W)$ does *not* already guarantee that T is invertible, as the above example of projection $P(x, y, z) = (x, 0, z)$ on $\mathbb{R}^3$ shows. It turns out that invertability of T is easy to detect:

Theorem 22.7. *If* $\dim(V) = \dim(W) = n$, *then a linear transformation* $T : V \to W$ *is invertible if and only if any of the following conditions holds:*

1. *T is an isomorphism, i.e., is a bijective linear transformation;*
2. *the matrix $A = [T]$ is an invertible matrix (in any bases of V and W);*
3. $\operatorname{nullity}(T) = 0$*;*
4. $\operatorname{rank}(T) = n$*.*

***Proof*.** That T is invertible if and only if it is a bijection, was discussed above.

If $T : V \to W$ is invertible, then the product $T^{-1}T$ is the identical transformation $I : v \to v$ with the identity matrix $I = I_n$. But by Theorem 22.4 the matrix of $T^{-1}T$ is the product matrix $[T^{-1}][T]$. We get $[T^{-1}][T] = I$, so $[T]$ is an *invertible matrix*, and $[T^{-1}] = [T]^{-1}$. On the other hand, if the matrix $[T]$ for a given linear transformation $T : V \to W$ is invertible, then the transformation corresponding to the inverse matrix $[T]^{-1}$ evidently is the inverse of T.

Next, if $\operatorname{nullity}(T) = 0$, then T is injective by Corollary 21.3. According to Corollary 21.11 we have $\operatorname{rank}(T) = n - \operatorname{nullity}(T) = n - 0 = n$, which by Corollary 21.10 means that T is surjective and, thus, bijective.

Similarly, if $\operatorname{rank}(T) = n$, then T is surjective. Since $\operatorname{nullity}(T) = n - \operatorname{rank}(T) = n - n = 0$, the transformation T is injective, and, thus, bijective. □

As it follows from the above proof, if T is invertible and has the matrix $A = [T]$, then the matrix of the transformation T^{-1} is the inverse matrix A^{-1}.

In Theorem 9.10 and in corollaries 13.7, 14.14 and 19.3 we gave equivalent conditions for invertible matrices. Now we get one more condition:

Corollary 22.8 (Amendment to Theorem 9.10)**.** *A matrix $A \in M_{n,n}(F)$ is invertible if and only if it is a matrix of an invertible transformation $T : F^n \to F^n$.*

Example 22.9. The projection transformations are not invertible since the rank of, say,

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

is 2, and is less than 3.

Or, in other terms, a projection transformation is not invertible since its matrix A is a triangle matrix with a zero standing on diagonal. So $\det(A) = 0$.

Example 22.10. The differentiation transformation $T(f(x)) = f'(x)$ is not invertible since the rank of, say, this matrix

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

is 3, so is less than 4.

Example 22.11. If $c \neq 0$, then the scaling transformation is invertible, and its inverse is easy to compute. For instance:

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

This can be understood in two ways: we can either compute the inverse matrix, or figure out that after we scale c times and then compress c times, then no vector will be changed.

The reflection transformation always has an inverse. For example, if

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

then $A^{-1} = A$. Thus, a reflection is its own inverse.

Example 22.12. For the rotation transformations R_φ we have $R_\varphi^{-1} = R_{-\varphi}$ because

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}^{-1} = \begin{bmatrix} \cos(-\varphi) & -\sin(-\varphi) \\ \sin(-\varphi) & \cos(-\varphi) \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{bmatrix} = \begin{bmatrix} \cos(\varphi) & \sin(-\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}.$$

This can either be computed as an inverse matrix using trigonometric formulas, or we can just observe the inverse of rotation by φ angle is the rotation by $-\varphi$ angle (rotation by the same angle in opposite direction).

Example 22.13. As a combination of previous examples we get:

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} \cos(\varphi) & \sin(\varphi) & 0 \\ -\sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & \frac{1}{5} \end{bmatrix}.$$

Example 22.14. Let us check that the coordinate map $\phi_E : V \to F^n$ is an isomorphism of spaces V and F^n.

Lemma 12.9 means that ϕ_E is a bijection, and Lemma 12.10 in fact means that ϕ_E is a linear transformation.

So in Section 12.1 we actually defined an isomorphism ϕ_E for specific purposes, without yet mentioning that it is a linear transformation from V to F^n.

22.3. Sums and scalar multiples of transformations

Let $T : V \to W$ and $S : V \to W$ be two linear transformations from the space V to the space W, both spaces over the same field F. The *sum* $T + S$ of T and S is defined by:

$$(T + S)(v) = T(v) + S(v) \text{ for any } v \in V.$$

This is a *point-wise sum*, and it is very easy to check that the function $T + S$ also is a linear transformation. Let us find the matrix C of a sum of T and S, if we already know their matrices:

$$A = [T] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \quad \text{and} \quad B = [S] = \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ b_{m1} & \cdots & b_{mn} \end{bmatrix}.$$

Recall that the columns of these matrices are composed by the vectors $T(e_1), \ldots, T(e_n)$ and $S(e_1), \ldots, S(e_n)$. By definition:

$$(T + S)(e_i) = T(e_i) + S(e_i) = \begin{bmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{bmatrix} + \begin{bmatrix} b_{1i} \\ \vdots \\ b_{mi} \end{bmatrix} = \begin{bmatrix} a_{1i} + b_{1i} \\ \vdots \\ a_{mi} + b_{mi} \end{bmatrix}$$

for each $i = 1,\dots,n$. Thus:

$$C = [T+S] = \begin{bmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{m1}+b_{m1} & \cdots & a_{mn}+b_{mn} \end{bmatrix} = A+B.$$

So *the matrix of a sum $T+S$ is the sum of matrices $A = [T]$ and $B = [S]$.*

Example 22.15. In $\mathbb{R}^3$ take the transformations

$$T = (x,y,z) = (2x,\ y,\ 0),$$
$$S = (x,y,z) = (z,\ 3y,\ y+z).$$

Then $T+S$ acts as:

$$(T+S)(x,y,z) = (2x+z,\ 4y,\ y+z).$$

Let us compare their matrices.

The matrices of T and S in standard basis are

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

And, thus,

$$[T+S] = \begin{bmatrix} 2 & 0 & 1 \\ 0 & 4 & 0 \\ 0 & 1 & 1 \end{bmatrix} = A+B.$$

Let $T : V \to W$ be a linear transformations from V to W over the field F, and let $c \in F$ be any scalar. The $c\,T$ is defined by the rule:

$$(c\,T)(v) = c\,T(v) \text{ for any } v \in V.$$

This also ia a *point-wise product*, and $c\,T$ evidently is a linear transformation.

The matrix C of a $c\,T$ is easy to find. Take

$$A = [T] = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

the columns of which are the vectors $T(e_1),\dots,T(e_n)$. By definition:

$$(c\,T)(e_i) = c\,T(e_i) = c\begin{bmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{bmatrix} = \begin{bmatrix} c\,a_{1i} \\ \vdots \\ c\,a_{mi} \end{bmatrix}$$

for each $i = 1,\dots,n$. So we get:

$$C = [c\,T] = \begin{bmatrix} c\,a_{11} & \cdots & c\,a_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ c\,a_{m1} & \cdots & c\,a_{mn} \end{bmatrix} = c\,A.$$

We get that *the matrix of transformation cT is the matrix $c\,A = c[T]$.*

Example 22.16. In $\mathbb{R}^3$ take the transformation $T = (x,y,z) = (2x,\ y,\ x+y+z)$, and let $c = 3$. Then the transformation $c\,T = 3T$ acts as: $(3T)(x,y,z) = (6x,\ 3y,\ 3x+3y+3z)$, and its matrix is:

$$[3T] = \begin{bmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 3 & 3 & 3 \end{bmatrix} = 3\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = 3[T].$$

Assume $T : V \to V$ is any linear transformation of the space V over any field F. Using the products (compositions), sums and scalar multiples of T we can construct new transformation using *polynomials*. Take any polynomial $h(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, and define a new transformation:

$$h(T) = a_0T^n + a_1T^{n-1} + \cdots + a_nT^0$$

(here we assume $T^0 = I$ is the identity transformation defined in Section 22.2). If the matrix of T is $A = [T]$, then the matrix of $h(T)$ clearly is

$$h(A) = h([T]) = a_0 A^n + a_1 A^{n-1} + \cdots + a_n A^0.$$

Example 22.17. Suppose the linear transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ is given by the matrix

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

Then for the polynomial $h(x) = 2x^2+3x-4$ the transformation $h(T) = 2T^2 + 3T - 4I$ is given by the matrix:

$$[h(T)] = h(A) = 2A^2 + 3A - 4I = \begin{bmatrix} 1 & 27 \\ 0 & 10 \end{bmatrix}.$$

Exercises

E.22.1. Consider transformations T, S and their matrices A, B given on space $\mathbb{R}^3$ in Example 22.15. **(1)** Write the transformation $2T + S$ in the form $(2T + S)(x, y, z) = ...$ **(2)** Write the matrix of $2T + S$ *without* applying Algorithm 20.12, just using the already known matrices A, B. **(3)** Write the matrix of transformation ST^2. **(4)** Find out which ones of the transformations T, S, $2T + S$ or ST^2 are invertible.

E.22.2. The transformation $T : M_{2,2} \to M_{2,2}$ is defined by $T\left[\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right] = \left[\begin{smallmatrix} 3a_{12} & 2a_{11} \\ a_{22} & 2a_{21} \end{smallmatrix}\right]$. Show that T is an invertible transformation by any method you know.

E.22.3. Using Corollary 22.8 show that the product of any number of invertible matrices is invertible. *Hint*: you may consider determinants of transformation matrices.

E.22.4. The following three transformations are given on the space $\mathbb{R}^3$. The first transformation T is given by its matrix

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

The second transformation S is the *inverse* of T^2. And the third transformation L is given by formula $L(x, y, z) = (x - y,\ y + z,\ x + z)$. **(1)** Find the matrix $B = [S]$ of transformation S, and the matrix $C = [L]$ of L. **(2)** Compute the matrices of transformations LST, TSL, S^{-1}, $2L$, $S + T$. **(3)** Find out which ones of the transformations L^{100}, $(TS)^{100}$, $(100\,T)^{-1}$ are invertible. Explain why.

E.22.5. In the real space $V = \mathbb{R}^3$ we are given the following linear transformations. R rotates V around Oz by 30° counter-clockwise (i.e., in "positive" direction). S is given by $S(x, y, z) = (2z,\ x - y,\ x)$. P is the projection of V onto the plane xOy (parallel to Oz). **(1)** Find the matrices of the transformations $T_1 = RS$, $T_2 = R^6(3P)$, $T_3 = P^{120}R^{12}$, $T_4 = 2S + R^{-1}$ in standard basis. **(2)** Let $v = (7, 7, 7) \in \mathbb{R}^3$. Using the results of previous point find the vectors $T_1(v)$, $T_2(v)$, $T_3(v)$, $T_4(v)$. **(3)** Using Theorem 22.7 detect which ones of the transformations $T_1, \ldots, T_4$ are invertible.

E.22.6. Let U and W be two spaces of dimensions, respectively, m and n (over the same field F), and let $\mathcal{M}_{m,n}$ be the set of all possible linear transformations $T : V \to W$. In Section 22.3 we defined the operations $T + S$ and $c\,T$ in $\mathcal{M}_{m,n}$. **(1)** Show that $\mathcal{M}_{m,n}$ is a vector space with respect to the defined operations. **(2)** The space $\mathcal{M}_{m,n}$ is isomorphic to one of the basic spaces given in Section 10.1. Find that space and build the respective isomorphism.

Part 8

Eigenvectors and Diagonalization

CHAPTER 23

Eigenvectors and eigenvalues

"Ein Mathematiker, der nicht etwas Poet ist,
wird nimmer ein vollkommener Mathematiker sein."
Karl Weierstraß

23.1. Definition and examples of eigenvectors and eigenvalues

"Eigenvector" stands for the German words "proper vector", and "eigenvalue" stands for the German "proper value". Eigenvectors and eigenvalues are very handy tools to study linear transformations. All spaces below are finite-dimensional by Agreement 11.26.

Definition 23.1. Let T be a linear transformation of space V over a field F, and let for a non-zero vector $v \in V$ and for a scalar $\lambda \in F$ we have the equality

$$\boldsymbol{T(v) = \lambda v}.$$

Then v is called an *eigenvector* of T associated to an *eigenvalue* λ.

The condition $T(v) = \lambda v$ means that the transformation T has an especially simple action on vector v: it just scales the vector v by λ times, as seen in Figure 23.1 (a). Usually, the eigenvalues are denoted by the Greek letter $\boldsymbol{\lambda}$ (*Lámbda*).

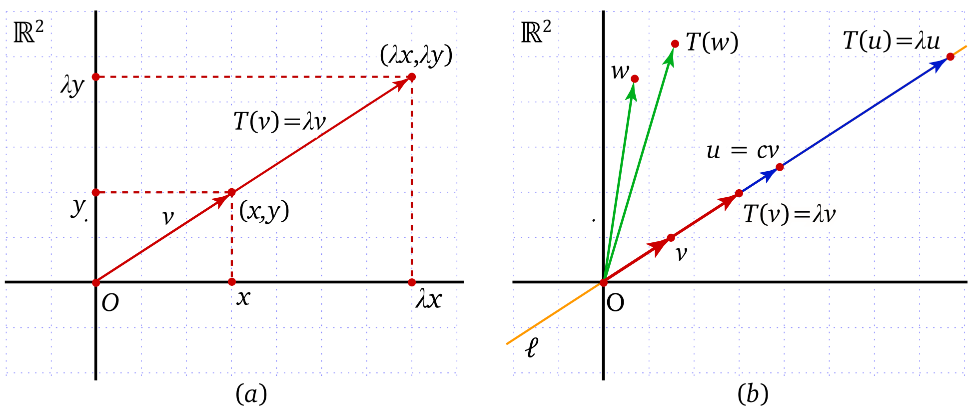


FIGURE 23.1. An eigenvector and the line directed by an eigenvector

Moreover, take *any* vector u in the one-dimensional subspace ℓ containing v, i.e., in the line ℓ directed by v as in Figure 23.1 (b). Then $u = cv$, and we have:

$$T(u) = T(cv) = c\,T(v) = c(\lambda v) = \lambda(cv) = \lambda u.$$

So on *each* vector of this line ℓ the transformation T acts just like "scaling". That is, T has particularly simple meaning on the line ℓ. Clearly, outside ℓ it may act differently: the image $T(w)$ of a vector $w \notin \ell$ may not be a multiple of w, see Figure 23.1 (*b*).

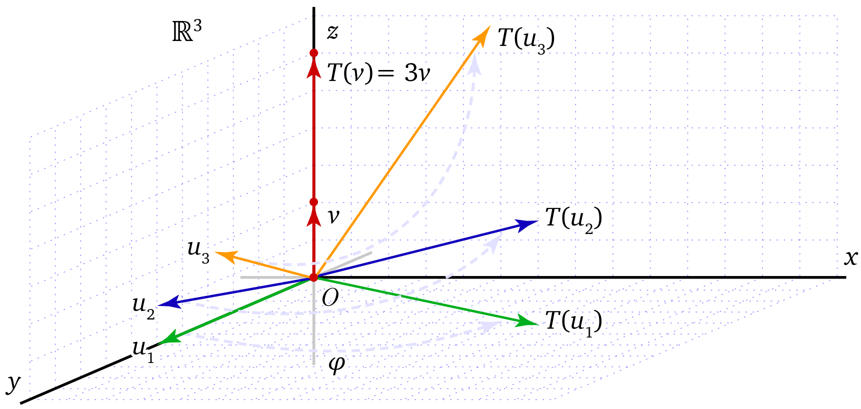


FIGURE 23.2. Eigenvectors of the "tornado" transformation.

Example 23.2. Consider the "tornado" transformation T of the space $\mathbb{R}^3$ given by matrix

$$A = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

It rotates the space by angle φ in the plane xOy, around the axis Oz, and it scales the space by 3 times along the axis Oz, see Figure 23.2. Any non-zero vector of axis Oz, say the vector $v = (0,0,2)$, is an eigenvector of T, since $T(v) = T(0,0,2) = (0,0,6) = 3T(v)$.

And T has no other eigenvectors outside Oz, if φ is not a multiple of π. See Example 23.12 for $\varphi = \pi$.

Example 23.3. Let T be the rotation of $\mathbb{R}^2$ by angle φ. Then its matrix is:

$$A = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}.$$

If φ is not a multiple of π, then T evidently has *no* eigenvectors, at all. For, no non-zero vector v is equal to a λv after rotation, whatever the value of λ be.

Example 23.4. In $\mathbb{R}^3$ consider the transformation given by $T(x,y,z) = (6x + 6y - 12z,\ 4x + 2y - 6z,\ 4x + 3y - 7z)$. It has the matrix

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}.$$

For now it is very complicated to figure out which is the action of T on $\mathbb{R}^3$. Maybe T is related to simpler transformation we so far considered (scaling, projection, rotation, etc.)?

In a few examples coming below we will fully analyze this transformation.

Take the scalar $\lambda = 2$ and the vector $v = (3,2,2)$. Then $T(v) = \lambda v$ because:

$$T(v) = 2(3,2,2) = (6,4,4) = 2v,$$

or by the matrix formula:

$$Av = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 4 \end{bmatrix} = 2v.$$

So although T seems to be a complicated transformation, but discovering the eigenvector v and eigenvalue λ helps us to understand this transformation better. We know that it scales the vectors 2 times along the line passing via $v = (3,2,2)$.

Another behaviour of T is that

$$T(1,1,1) = (0,0,0),$$

or by the matrix formula:

$$\begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

So $v = (1,1,1)$ is an eigenvector associated to the eigenvalue $\lambda = 0$.

For now leave aside the question *how we found* these v and λ.

Example 23.5. In polynomial space $V = \mathcal{P}_3(\mathbb{R})$ take the transformation of differentiation: $T\big(f(x)\big) = f'(x)$. It is easy to figure out that the constant polynomial $v = f(x) = c \neq 0$ is an eigenvector of T with eigenvalue $\lambda = 0$, for, we have:

$$T(f) = c' = 0 = 0 \cdot f.$$

Example 23.6. On a finite field the "scaling" may look differently. In the space $V = \mathbb{Z}_5^2$ consider the transformation T given by matrix $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, and the vector $v = (3,3)$. Then we have:

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

Therefore, $v = (3,3) \in \mathbb{Z}_5^2$ is an eigenvector associated to the eigenvalue $\lambda = 3 \in \mathbb{Z}_5$ for the transformation T.

Assume a transformation $T : V \to V$ has the eigenvalue $\lambda \in F$ and the associated eigenvector $v \in V$, i.e., $T(v) = \lambda v$. Then the *composition* transformation $T^2 = TT$ will have the eigenvalue λ^2 associated to the same eigenvector v. Indeed,

$$T^2(v) = (TT)(v) = T(T(v)) = T(\lambda v) = \lambda T(v) = \lambda(\lambda v) = \lambda^2 v.$$

By similar reasons for any natural $k \in \mathbb{N}$ the composition T^k will have the eigenvalue λ^k associated to the same eigenvector v.

If T is *invertible*, then the inverse transformation T^{-1} has the eigenvalue λ^{-1} associated to the same eigenvector v. Indeed, $T(v) = \lambda v$ and $T^{-1}(\lambda v) = v$. Then:

$$T^{-1}(v) = T^{-1}(\lambda^{-1}\lambda v) = \lambda^{-1}T^{-1}(\lambda v) = \lambda^{-1}T^{-1}(T(v)) = \lambda^{-1}v.$$

From this we get that a transformation T is invertible if and only if *it has no zero eigenvalue*. Indeed, T is invertible if and only if it is a bijective map (we called this isomorphism). Now, if T is *not* bijective, there are $v_1, v_2 \in V$ such that $v_1 \neq v_2$ and $T(v_1) = T(v_2)$. Then for $u = v_1 - v_2$ we have $T(u) = T(v_1 - v_2) = 0 = 0u$. So u is an eigenvector associated to eigenvalue $\lambda = 0$. On the other hand, if T has an eigenvalue $\lambda = 0$ and the associated eigenvector u, then it is *not* a bijective map, as for two distinct vectors u and 0 we have $T(u) = 0u = 0 = T(0)$. So to our list of equivalent conditions for invertible matrices (see Theorem 9.10 and corollaries 13.7, 14.14, 17.21, 22.8) we can add one more point:

Corollary 23.7 (Amendment to Theorem 9.10)**.** *A matrix $A \in M_{n,n}(F)$ is invertible if and only if $0 \in F$ is not an eigenvalue for A.*

Example 23.8. As we saw above, the transformation T defined by the matrix

$$\begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}$$

has an eigenvalue 2. The matrix of $T^2 = TT$ is

$$\begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}^2 = \begin{bmatrix} 12 & 12 & -24 \\ 8 & 10 & -18 \\ 8 & 9 & -17 \end{bmatrix}.$$

So the composition T^2 has the eigenvalue $2^2 = 4$ together with the same eigenvector $v = (3,2,2)$ associated to it.

Further, T also has an eigenvalue 0. Thus, T^2 also has 0 as an eigenvalue assosiated to the same vector $(1,1,1)$. So both T and T^2 are *not* invertible.

And we could check this fact directly, computing the ranks $\operatorname{rank}(A) = 2$ and $\operatorname{rank}\big(A^2\big) = 2$. We omit the simple verification.

23.2. Computation of eigenvectors

The more eigenvectors and eigenvalues we find for a given transformation $T : V \to V$, the better we know the structure of T. Let us start by finding all the eigenvectors of T associated to an *already known* eigenvalue λ (for now leave aside the question how we found the value λ).

Take the matrix $A = [T] = [T]_E$ of T for some basis $E = \{e_1, \dots, e_n\}$ of V:

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

Since the eigenvector v is yet unknown, denote its coordinates by variables: $v = (x_1, \dots, x_n)$. Then $T(v) = \lambda v$ is equivalent to matrix equation:

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \lambda \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{bmatrix}.$$

This is equivalent to the system of linear equations:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = \lambda x_1 \\ \dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = \lambda x_n. \end{cases}$$

So the task of finding the eigenvectors is reduced to finding the *solutions* of a system of linear equalities. The above system is equivalent to:

$$\begin{cases} (a_{11} - \lambda)x_1 + \cdots + \quad a_{1n}x_n \quad = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \quad a_{n1}x_1 \quad + \cdots + (a_{nn} - \lambda)x_n = 0. \end{cases}$$

Since this system is homogeneous, it always has at least one solution – the zero solution. But since a zero vector is not an eigenvector, we look for non-zero solutions, which may exist, if the rank r of the matrix of this system is less than n. The matrix of this system can be written as:

$$\begin{bmatrix} a_{11} - \lambda & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \cdots & a_{nn} - \lambda \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} - \begin{bmatrix} \lambda & \cdots & 0 \\ \dots & \dots & \dots \\ 0 & \cdots & \lambda \end{bmatrix} = A - \lambda I_n.$$

So the above homogeneous system can be re-written in the matrix form:

$$\boldsymbol{(A - \lambda I_n)X = O}.$$

We got a theorem which suggests hints how to find eigenvectors:

Theorem 23.9. *Let $T : V \to V$ be a transformation with a matrix $A = [T] = [T]_E$, let the scalar λ be an eigenvalue of T, and v be a non-zero vector in V with coordinates $v = (x_1, \dots, x_n)$. Then the following are equivalent:*

1. *the vector $v \in V$ is an eigenvector of T associated to λ;*
2. *coordinates $(x_1, \dots, x_n)$ form a solution of the homogeneous system of linear equations $(A - \lambda I_n)X = O$;*
3. *$(x_1, \dots, x_n)$ belongs to the null space* $\mathrm{null}(A - \lambda I_n)$*;*
4. *v is in the kernel of transformation corresponding to the matrix $A - \lambda I_n$.*

We see that *all the eigenvectors associated to λ together with the zero vector are forming a subspace in V*. Call it the *eigenspace* associated to the eigenvalue λ, and denote it by E_λ. Its dimension $\dim(E_\lambda)$ is called the *geometric multiplicity* of λ, and it is equal to $\mathrm{nullity}(A-\lambda I_n)$, i.e., to $n-r$ where $r = \mathrm{rank}(A-\lambda I_n)$.

The problem of finding the eigenvectors of T now is a better manageable task: just find a basis $e_1,\dots,e_{n-r}$ for E_λ. Then $E_\lambda = \mathrm{span}(e_1,\dots,e_{n-r})$, and the eigenvectors we are looking for are all the linear combinations of $e_1,\dots,e_{n-r}$ except the zero vector.

How to compute the eigenvectors associated to an eigenvalue.

Algorithm 23.10 (Computation of eigenvectors associated to an eigenvalue)**.** We are given a transformation $T : V \to V$ of the space V on same field F (a coordinate map $\phi_E : V \to F^n$ is fixed on V). An eigenvalue λ of T is given.

► Find the eigenspace E_λ; find all eigenvectors of T associated to λ; find the geometric multiplicity of λ.

1. Compute the matrix $A = [T]_E$ of T by Algorithm 20.12.
2. Find a basis $\{e_1,\dots,e_{n-r}\}$ for null space $\mathrm{null}(A-\lambda I_n)$ of the matrix $A-\lambda I_n$ by Algorithm 15.2, where $r = \mathrm{rank}(A-\lambda I_n)$.
3. If V is a space other than F^n, then replace each e_i by the unique vector in V corresponding to e_i under coordinate map $\phi_G : W \to F^m$, i.e., set $e_i = \phi_E^{-1}(e_i)$ for $i = 1,\dots,n-r$.
4. Output $E_\lambda = \mathrm{span}(e_1,\dots,e_{n-r})$, output the set of eigenvectors associated to λ as the difference $E_\lambda \backslash \{0\}$ and output the geometric multiplicity of λ as $n-r$.

Example 23.11. Earlier we saw in Example 23.4 that for $\lambda = 2$ the vector $v = (3,2,2)$ is an eigenvector for T given by the matrix

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}.$$

Now let us find *all* other eigenvectors associated to 2. To do this we need the eigenspace E_2. We have:

$$A-2I = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} - \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 6 & -12 \\ 4 & 0 & -6 \\ 4 & 3 & -9 \end{bmatrix}.$$

To find its null space by Algorithm 15.2 we bring it to reduced row-echelon form:

$$\begin{bmatrix} 4 & 6 & -12 \\ 4 & 0 & -6 \\ 4 & 3 & -9 \end{bmatrix} \sim \mathrm{rref}(A-2I) = \begin{bmatrix} \mathbf{1} & 0 & -\frac{3}{2} \\ 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 \end{bmatrix}.$$

So we get the geometric multiplicity $n-r = 3-2 = 1$.

As a basis for one-dimensional eigenspace E_2 we can take the vector

$$\begin{bmatrix} -\frac{3}{2} \\ -1 \\ -1 \end{bmatrix} \quad \text{or, its multiple} \quad v_1 = \begin{bmatrix} 3 \\ 2 \\ 2 \end{bmatrix}$$

(we intentionally wrote it as a column vector since by Algorithm 15.2 it is comfortable to write down the basis for null space using the non-pivot columns of $\mathrm{rref}(A)$ – see Example 15.3).

The vector $v = (3,2,2)$ we found earlier is nothing else but this v_1.

The eigenspace E_2 is equal to the line $\mathrm{span}(v_1)$, and the set of all eigenvectors associated to $\lambda = 2$ is $E_2 \backslash \{0\}$, i.e., the line minus the zero vector.

Example 23.12. Consider the transformation T given by

$$A = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

with $\varphi = \pi$, see Example 23.2 and Figure 23.2. It has a 1-dimensional eigenspace E_3, which is the Oz axis.

Since $\varphi = \pi$, every vector v of the plane xOy is rotated by $180°$, and is carried to $T(v) = -v = -1 \cdot v$. So every non-zero vector from xOy is an eigenvector associated to $\lambda = -1$. The eigenspace E_{-1} is 2-dimensional, and coincides with xOy.

And, as it is easy to verify, $\text{nullity}(A-3I) = 1$ and $\text{nullity}(A-(-1)I) = 2$. So the geometric multiplicities of the eigenvalues 3 and -1 respectively are 1 and 2.

23.3. Characteristic polynomials and the eigenvalues

Before we learn how to find the eigenvalues λ for a given linear transformation $T : V \to V$ we need some more information on *polynomials over fields* (check Appendix C.2). We will use polynomials given by determinants containing a variable:

Example 23.13. Define the polynomial

$$f(x) = \begin{vmatrix} x & 2 \\ 3x & x+1 \end{vmatrix}$$

$$= x(x+1) - 2 \cdot 3x = x^2 - 5x.$$

Since we are going to use such polynomials for eigenvalues only, let us denote the variable not by x but by λ. Say,

$$f(\lambda) = \begin{vmatrix} 2-\lambda & 3 \\ 5 & 4-\lambda \end{vmatrix}$$

$$= (2-\lambda)(4-\lambda) - 3 \cdot 5 = \lambda^2 - 6\lambda - 7.$$

For the given square matrix

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \hdotsfor{3} \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \in M_{n,n}(F)$$

a polynomial in variable λ can be defined as:

$$f(\lambda) = \begin{vmatrix} a_{11}-\lambda & \cdots & a_{1n} \\ \hdotsfor{3} \\ a_{n1} & \cdots & a_{nn}-\lambda \end{vmatrix} = \det\left(\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \hdotsfor{3} \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} - \begin{bmatrix} \lambda & \cdots & 0 \\ \hdotsfor{3} \\ 0 & \cdots & \lambda \end{bmatrix} \right)$$

$$= \det(A - \lambda I) = |A - \lambda I|.$$

Call this polynomial $f(\lambda) = |A - \lambda I|$ the *characteristic polynomial* of the matrix A.

Example 23.14. Compute the characteristic polynomial for the matrix A we considered in Example 23.4:

$$f(\lambda) = |A - \lambda I| = \begin{vmatrix} 6-\lambda & 6 & -12 \\ 4 & 2-\lambda & -6 \\ 4 & 3 & -7-\lambda \end{vmatrix}$$

$$= -\lambda^3 + \lambda^2 + 2\lambda$$

One might notice that the eigenvalue 2 of the transformation T defined by A is a *root* of this polynomial. As we will see soon, this is a general rule.

Example 23.15. You may notice that the polynomial $\lambda^2 - 6\lambda - 7$ given in Example 23.13 actually is the characteristic polynomial for the matrix

$$\begin{bmatrix} 2 & 3 \\ 5 & 4 \end{bmatrix}.$$

For a given transformation T of a space V over a field F call the *characteristic polynomial* of T the polynomial $f(\lambda) = |A - \lambda I|$, where $A = [T]$ is the matrix of T is some basis E of V.

Correctness of this definition is questionable yet. For, T may have *different* matrices A and B in different bases E and G, and so the matrices $A - \lambda I$ and $B - \lambda I$ may also be *distinct*. However, it turns out that their determinants are equal. Indeed, by Theorem 20.26 we have $B = P^{-1}AP$ where $P = P_{EG}$ is the change of basis matrix from E to G. Therefore:

$$|B - \lambda I| = |P^{-1}AP - \lambda I| = |P^{-1}AP - \lambda I \cdot P^{-1}P|$$
$$= |P^{-1}AP - P^{-1}\lambda IP| = |P^{-1}(A - \lambda I)P|$$

(we used the fact that any matrix is permutable with a diagonal matrix, and also used distributivity of matrix operations)

$$= |P^{-1}| \cdot |A - \lambda I| \cdot |P| = |P|^{-1} \cdot |A - \lambda I| \cdot |P| = |A - \lambda I|$$

(we used the fact that determinant of the product is equal to the product of determinant, and the determinant of the inverse matrix is equal to inverse of the determinant). So talking about characteristic polynomial $f(\lambda)$ of T we will no longer stress the matrix A and the basis E in which $|A - \lambda I|$ is computed.

Example 23.16. For the linear transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ of Example 23.4 given by the rule $T(x, y, z) = (6x + 6y - 12z,\ 4x + 2y - 6z,\ 4x + 3y - 7z)$ we in the standard basis E have the matrix:

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}.$$

So by previous example the characteristic polynomial of T is that of A, i.e.:

$$f(\lambda) = -\lambda^3 + \lambda^2 + 2\lambda.$$

And if we take *any* other basis G of $\mathbb{R}^3$ and compute $f(\lambda) = |B - \lambda I|$ using the matrix $B = [T]_G$, we will still get the *same* characteristic polynomial $f(\lambda)$.

The main tool for finding the eigenvalues is the following theorem:

Theorem 23.17. *Let $T : V \to V$ be a transformation on the space V over a field F. A scalar $\lambda \in F$ is an eigenvalue of T (and of its matrix $A = [T]$ in any basis) if and only if λ is a root of the characteristic polynomial $f(\lambda) = |A - \lambda I|$ of T.*

Proof. λ is an eigenvalue if and only if for an associated non-zero eigenvector $v \in V$ we have $T(v) = \lambda v$. Presenting v by its coordinates $v = (x'_1, \ldots, x'_n)$, and choosing the matrix $A = [T] = [T]_E$ of T in any basis E we get the equality:

$$T(v) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x'_1 \\ \vdots \\ x'_n \end{bmatrix} = \begin{bmatrix} \lambda x'_1 \\ \vdots \\ \lambda x'_n \end{bmatrix},$$

i.e., $v = (x'_1, \ldots, x'_n)$ is a solution of the system $(A - \lambda I)X = O$. But a homogeneous system has a non-zero solution if and only if the determinant of its matrix is zero, so $|A - \lambda I| = 0$, that is, λ is a root of $f(\lambda) = |A - \lambda I|$. □

Remark 23.18. Since the eigenvalues of a transformation T and of its matrix $A = [T]_E$ (on any basis E) are equal, and since we earlier agreed to identify the transformation action $T(v)$ with the matrix product $Av = [T]_E[v]_E$, we may for briefness call v the *eigenvector of the matrix* A, if $Av = \lambda A$.

Theorem 23.17 gives the following general plan how to find the eigenvalues and eigenvectors of a given transformation T:

1. Find the matrix $A = [T] = [T]_E$ of T in any basis E;
2. Compute the characteristic polynomial of T as the determinant $f(\lambda) = |A - \lambda I|$;
3. Find the roots $\lambda_1, \ldots, \lambda_s$ of the polynomial $f(\lambda)$;

4. For each of $i = 1,\dots,s$ find a basis of the eigenspace E_{λ_i} of λ_i. The eigenvectors associated to λ_i form the difference $E_{\lambda_i}\backslash\{0\}$. And the geometric multiplicity of λ_i is equal to $\dim\big(E_{\lambda_i}\big) = \text{nullity}(A-\lambda_i I)$.

Remark 23.19. Notice that we did *not* call the steps above an "algorithm" because successfulness of this plan depends on the fact *if or not we can find roots of* $f(\lambda)$. We always are able to find the roots of any real polynomial of degree not more than 4, but for higher degrees finding the roots may be an unsolvable problem (see Appendix D.2). We recommend that you for now just remember that the above plan allows to find all the eigenvalues, provided that $\dim(V) \le 4$ (in such cases also $\deg(|A-\lambda I|) \le 4$).

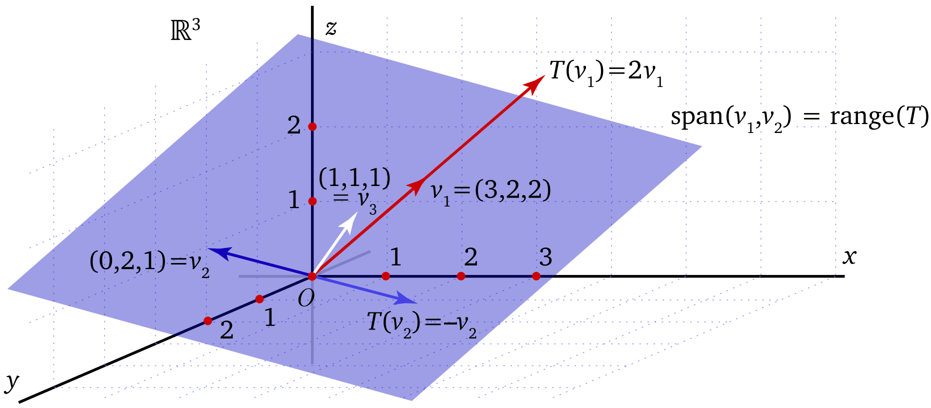


FIGURE 23.3. Complete description of a transformation by eigenvectors.

Example 23.20. In Example 23.16 we for the transformation $T(x,y,z) = (6x+6y-12z,\ 4x+2y-6z,\ 4x+3y-7z)$ computed the characteristic polynomial $f(\lambda) = -\lambda^3+\lambda^2+2\lambda$. Its roots are easy to find from:

$$f(\lambda) = -(\lambda-2)(\lambda+1)\lambda.$$

So the eigenvalues are $\lambda_1 = 2, \lambda_2 = -1, \lambda_3 = 0$.

For $\lambda_1 = 2$ we have already seen in Example 23.11 that the nullity of the matrix

$$A-2I = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} - \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 6 & -12 \\ 4 & 0 & -6 \\ 4 & 3 & -9 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{3}{2} \\ 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 \end{bmatrix}.$$

is $3-2 = 1$, and we have computed the (single) vector $v_1 = (3,2,2)$ in the null space of the matrix $A-2I$. Clearly, v_1 is a basis for E_2.

For $\lambda_2 = -1$ we have the matrix

$$A-(-1)I = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 7 & 6 & -12 \\ 4 & 3 & -6 \\ 4 & 3 & -6 \end{bmatrix}.$$

Its reduced row-echelon form is:

$$\begin{bmatrix} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & -2 \\ 0 & 0 & 0 \end{bmatrix}.$$

The rank of this matrix is $r = 2$, and the nullity is $3-2 = 1$. As a basis for its null space by Algorithm 15.2 take, say,

$$\begin{bmatrix} 0 \\ -2 \\ -1 \end{bmatrix} \text{ or, its multiple } v_2 = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}$$

which is an eigenvector associated to $\lambda_2 = -1$, and is a basis for E_{-1}.

Next, for $\lambda_3 = 0$ we have

$$A-0I = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}$$

with the reduced row-echelon form:

$$\begin{bmatrix} \mathbf{1} & 0 & -1 \\ 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

Again, the rank of this matrix is $r = 2$. The nullity is $3-2=1$. As a basis for subspace of solutions by Algorithm 15.2 take, say,

$$v_3 = \begin{bmatrix} -1 \\ -1 \\ -1 \end{bmatrix}, \text{ or, its multiple } \quad v_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

v_3 is an eigenvector for $\lambda_3 = 0$, and a basis for the eigenspace E_0.

We established that the transformation $T(x,y,z)=(6x+6y-12z,\ 4x+2y-6z,\ 4x+3y-7z)$ has eigenvalues

$$\lambda_1 = 2,\ \ \lambda_2 = -1,\ \ \lambda_3 = 0,$$

and they have one-dimensional eigenspaces E_2, E_{-1}, E_0 respectively. The three eigenvectors (each being a basis for its eigenspace) are:

$$v_1=(3,2,2),\ v_2=(0,2,1),\ v_3=(1,1,1).$$

As it is easy to check, these vectors are independent and, thus, they form a *basis* $G = \{v_1, v_2, v_3\}$ for the entire space $V = \mathbb{R}^3$.

If in this basis a vector, v has the coordinates (x,y,z), i.e., if

$$v = xv_1 + yv_2 + zv_3,$$

then we have:

$$T(v) = (2 \cdot x)\,v_1 + (-1 \cdot y)\,v_2 + (0 \cdot z)\,v_3,$$

so in the basis G we have

$$T(x,y,z) = (2x,\ -y,\ 0).$$

Compare this simple formula with what we had in *standard* basis:

$$T(x,y,z) = (6x+6y-12z,\\ 4x+2y-6z,\ 4x+3y-7z).$$

We have discovered a simple and *complete* description of the transformation T, see Figure 23.3. T acts on $\mathbb{R}^3$ first by scaling the space 2 times along v_1. Then it reflects the space along v_2. Finally, scaling by 0 times along v_3 means that T projects the space along the vector v_3 onto the plane spanned by v_1, v_2, i.e., onto range(T).

In the basis G the transformation T, clearly, has the matrix

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

This diagonal matrix is by far clearer than the initial matrix by which we started:

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix}.$$

And B also shows that T maps $\mathbb{R}^3$ onto a *plane* (because it has *two* non-zero columns).

Not every transformation possesses such a complete description, and some transformations may have no eigenvectors and eigenvalues, at all:

Example 23.21. We have already seen in Example 23.3 that in $\mathbb{R}^2$ the rotation transformation

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}$$

has no eigenvalues and no eigenvectors (if φ is not a multiple of π). Let us get the same result differently, using the characteristic polynomial:

$$f(\lambda) = \begin{vmatrix} \cos(\varphi)-\lambda & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi)-\lambda \end{vmatrix}$$

$$= (\cos(\varphi)-\lambda)^2 + \sin^2(\varphi).$$

If φ is not a multiple of π, then $\sin^2(\varphi)$ is a strictly positive number, and adding $(\cos(\varphi)-\lambda)^2$ to it we will never get zero. So the characteristic polynomial has no roots, and R_φ has no eigenvalues.

Example 23.22. Let us compute the eigenvectors and eigenvectors for the differentiation transformation $T\big(f(x)\big) = f'(x)$ in polynomial space $V = \mathcal{P}_3(\mathbb{R})$.

In Example 23.5 we have seen that $\lambda = 0$ is an eigenvalue and $f(x) = c$ is an eigenvector. Let us see if there are *other* eigenvectors and eigenvectors. The matrix

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

of T is computed in Example 20.16. So the determinant $|A-\lambda I|$ is:

$$\begin{vmatrix} -\lambda & 1 & 0 & 0 \\ 0 & -\lambda & 2 & 0 \\ 0 & 0 & -\lambda & 3 \\ 0 & 0 & 0 & -\lambda \end{vmatrix} = (-\lambda)^4 = \lambda^4.$$

The characteristic polynomial $f(\lambda) = \lambda^4$ has only one root $\lambda = 0$ (the only eigenvalue). The rank of the matrix $A - 0 \cdot I = A$ is 3 (A already is in row-echelon form). So nullity is $4-3=1$, and all the eigenvectors of T are inside a one-dimensional subspace in $\mathcal{P}_3(\mathbb{R})$.

Example 23.23. Consider a transformation T of $V = \mathbb{Z}_3^2$ given by the matrix:

$$A = \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix} \in M_{2,2}(\mathbb{Z}_3),$$

or by the rule $T(x,y) = (2(x+y),\ x)$. Its characteristic polynomial $f(\lambda)$ is:

$$|A - \lambda I| = \begin{vmatrix} 2-\lambda & 1 \\ 2 & -\lambda \end{vmatrix}$$

$$= -\lambda(2-\lambda) - 2 = \lambda^2 - 2\lambda - 2$$

$$= \lambda^2 + \lambda + 1 = f(\lambda) \in \mathbb{Z}_3[\lambda].$$

We seem to have an obstacle here: we have a polynomial over $\mathbb{Z}_3$, but we know no method to find the roots over *finite fields*! However, since $\mathbb{Z}_3$ contains three elements only, we can easily check the value of $f(\lambda)$ for each $\lambda \in \mathbb{Z}_3 = \{0,1,2\}$:

$$f(0) = 1 \neq 0, \quad f(1) = 0, \quad f(2) = 1 \neq 0.$$

The only eigenvalue is $\lambda = 1$. Then:

$$A - \lambda I = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 1 \\ 0 & 0 \end{bmatrix} = \operatorname{rref}(A - \lambda I).$$

Since $n - r = 2 - 1 = 1$, the eigenspace E_1 is 1-dimensional. Its basis vector by Algorithm 15.2 is

$$v = \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

(we wrote it vertically here to match Algorithm 15.2).

The set of all eigenvectors is $E_1 \backslash \{0\}$, which in our case is *finite*, consists of two multiples of the vector v:

$$E_1 \backslash \{0\} = \{v, 2v\} = \{(1,2),\ (2,1)\}.$$

The space $V = \mathbb{Z}_3^2$ consists of $3^2 = 9$ vectors of which 2 are eigenvectors: $T(1,2) = (1,2)$ and $T(2,1) = (2,1)$.

For any other non-zero $v \in V$ the vectors v and $T(v)$ are *not* collinear.

Comparison of previous examples show that the more linearly independent eigenvectors a transformation has, the simpler is to understand its structure. In the coming sections we are going to utilize this idea.

23.4. Eigenvectors and linear independence

Although the formula $T(v) = \lambda v$ by which we deined the eigenvectors contains no direct reference to linear independence, these two concepts are deeply interconnected, as we will see now.

Firstly, Example 23.20 suggested a special case, when the transformation T can simply be explained as a “collection of scalings” in some directions:

Theorem 23.24. *Let T be a linear transformation of an n-dimensional space V. If T has n linearly independent eigenvectors $v_1, \dots, v_n$, then in the basis $E = \{v_1, \dots, v_n\}$ the transformation T has a diagonal matrix:*

$$A = [T]_E = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{bmatrix} \tag{23.1}$$

where $\lambda_1, \dots, \lambda_n$ are eigenvalues of T associated to $v_1, \dots, v_n$.

A basis $E = \{v_1, \dots, v_n\}$ consisting of eigenvectors of a transformation T is called an *eigenbasis* for T. Theorem 23.24 states that if in a space there is an eigenbasis E for a transformation T, then the matrix $A = [T]_E$ is a diagonal matrix with associated eigenvalues on its diagonal. One of the helpful approaches to study a linear transformation T is to find out if such an eigenbasis can be found for T. We were able to do that in Example 23.20.

Lemma 23.25. *Eigenvectors corresponding to pairwise distinct eigenvalues of a linear transformation T are linearly independent.*

Proof. Assume T has distinct eigenvalues $\lambda_1, \dots, \lambda_k$, and the associated eigenvectors $v_1, \dots, v_k$ are linearly dependent:

$$c_1 v_1 + c_2 v_2 + \cdots + c_k v_k = 0, \tag{23.2}$$

where one the coefficients, say c_1, is non-zero. Applying T to (23.2) we get:

$$T(c_1 v_1 + c_2 v_2 + \cdots + c_k v_k) = c_1 \lambda_1 v_1 + c_2 \lambda_2 v_2 + \cdots + c_k \lambda_k v_k = T(0) = 0.$$

Next, multiplying (23.2) by the λ_1 we get:

$$c_1 \lambda_1 v_1 + c_2 \lambda_1 v_2 + \cdots + c_k \lambda_1 v_k = \lambda_1 0 = 0.$$

Subtracting this from the previous equality we get

$$c_2(\lambda_2 - \lambda_1) v_2 + \cdots + c_k(\lambda_k - \lambda_1) v_k = 0 - 0 = 0. \tag{23.3}$$

Since all eigenvalues are distinct, the differences $\lambda_2 - \lambda_1, \dots, \lambda_k - \lambda_1$ are non-zero.

If the vectors $v_2, \dots, v_k$ are independent, then from equality (23.3) we get that all $c_2, \dots, c_k$ have to be zero. And then also c_1 is zero by (23.2). Contradiction.

If the vectors $v_2, \dots, v_k$ are dependent, then we repeat the step above to exclude the v_2. Since this process cannot go infinitely, we get a contradiction in at most n steps. □

Corollary 23.26. *Let the transformation T of the n-dimensional space V have n pairwise distinct eigenvalues $\lambda_1, \dots, \lambda_n$. Then in the eigenbasis $\{v_1, \dots, v_n\}$ formed by associated eigenvectors the transformation T has a diagonal matrix* (23.1).

Example 23.27. Let us check that if a transformation T has a triangle matrix

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ 0 & \cdots & a_{nn} \end{bmatrix},$$

then its eigenvalues are the elements of the main diagonal:

$$\lambda_1 = a_{11}, \ \dots, \ \lambda_n = a_{nn} \quad \text{(repetitions allowed)}.$$

Indeed, the determinant of a triangle matrix is the product of its diagonal elements (see Algorithm 18.1):

$$f(\lambda) = |A - \lambda I| = \begin{vmatrix} a_{11} - \lambda & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ 0 & \cdots & a_{nn} - \lambda \end{vmatrix}$$
$$= (a_{11} - \lambda) \cdots (a_{nn} - \lambda).$$

So the only roots of the characteristic polynomial $f(\lambda)$ are $a_{11}, \dots, a_{nn}$.

In particular, if all the diagonal elements in triangle matrix A are distinct, then T in the basis of associated eigenvectors has the diagonal matrix:

$$\begin{bmatrix} a_{11} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & a_{nn} \end{bmatrix}.$$

Example 23.28. Assume the transformation T is given by its matrix

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

By the previous example the transformation T has eigenvalues

$$\lambda_1 = 2, \ \lambda_2 = 4, \ \lambda_3 = 1, \ \lambda_4 = 5,$$

which all are distinct. In the respective eigenbasis T has the matrix

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}.$$

Computation of actual eigenvectors v_1, v_2, v_3, v_4 for our four eigenvalues can be easily done by Algorithm 21.2.

Exercises

E.23.1. We are given three real matrices:

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

(1) A transformation T is given by the matrix A. Show that $v=(4,-2,-4)$ is an eigenvector for T associated to the eigenvalue $\lambda=2$. **(2)** A transformation T is given by the matrix B. Check if $v=(3,-6,0)$ is an eigenvector for it. If yes, indicate the eigenvalue. **(3)** A transformation T is given by the matrix C. Which one of the vectors $u=(2,2,2)$, $v=(0,2,2)$ and $w=(0,2,0)$ is an eigenvector for T?

E.23.2. In polynomials space $\mathcal{P}_2(\mathbb{R})$ we are given the transformations $T\big(f(x)\big)=-5f'(x)$. Find if T has eigenvectors and eigenvalues.

E.23.3. Write the characteristic polynomials $|A-\lambda I|$, $|B-\lambda I|$, $|C-\lambda I|$ of matrices (i.e., characteristic polynomials of respective transformations) in Exercise E.23.1. Find all of their roots. *Hint*: the characteristic polynomials are of degree 3. Here are some of their roots to help you to find the remaining roots: one of the roots of $|A-\lambda I|$ is 4; one of the roots of $|B-\lambda I|$ is 2; one of the roots of $|C-\lambda I|$ is 3.

E.23.4. We are given a transformation $T:\mathbb{R}^3\to\mathbb{R}^3$. Find basis for the eigenspaces E_λ for each of its eigenvalues λ, and indicate their geometric multiplicities, if **(1)** T is defined by the matrix A in Exercise E.23.1. **(2)** T is defined by the matrix B in same exercise. **(3)** T is defined by the matrix C in same exercise. *Hint*: you may use the eigenvalues already computed for Exercise E.23.3.

E.23.5. A transformation T is given in the space $\mathbb{R}^4$ by the rule $T(x,y,z,t)=(x,\ x+2y,\ z,\ -z+3t)$. **(1)** Write the matrix $A=[T]$ in standard basis. **(2)** Using the *definition* of eigenvalue and eigenvector detect if any of the vectors $v_1=(-1,1,2,1)$ or $v_2=(0,1,0,2)$ is an eigenvector for the values $\lambda=1$ or $\lambda=4$. **(3)** Write the characteristic polynomial for A and using it detect all the eigenvalues of T (or of A). **(4)** Detect all the eigenspaces of T (or of A) by finding a basis for each of them. Indicate the geometric multiplicities.

E.23.6. The transformations T, S, and L are given in $\mathbb{R}^3$ by the following rules. In the standard basis E of $\mathbb{R}^3$ we are given $[T]_E=\left[\begin{smallmatrix}2&3&0\\3&2&0\\0&0&5\end{smallmatrix}\right]$. The transformation S is the clockwise rotation of $\mathbb{R}^3$ by $120°$ around the line ℓ which passes by O, and which has the direction vector $d=(1,1,1)$ (i.e., S sends e_1 to e_2, etc...). The transformation L is given by $L(x,y,z)=(2x-z,\ 3y,\ -x+2z)$. **(1)** Without calculation of the characteristic polynomials, just using the geometric properties of these transformations find an eigenvalue *and* an eigenvector for each of these transformations. **(2)** Compute the characteristic polynomials for T, S, and L (you will have to find the matrix for S and the matrix for L first). **(3)** Compute all the real roots for each characteristic polynomial found above. *Hints*: you will get *cubic* equations, but you still can solve them, since you know a root (i.e., an eigenvalue) for each of them from the point (1) above. **(4)** Write all the eigenvalues for each of T, S, and L. For each of them find the respective eigenspace (by computing a basis for it). Indicate the respective geometric multiplicities.

E.23.7. Let T, S, and L be the transformations given by previous exercise in the space $\mathbb{R}^3$. Using the already obtained results answer the following questions: **(1)** Is the vector $(-3,3,0)$ an eigenvector for the transformation T^{101}? If yes, then for which eigenvalue? Is the vector $(-5,-5,-5)$ an eigenvector for the transformation S^{102}? If yes, then for which eigenvalue? **(2)** Is each of transformations T, S, and L invertible? If yes, then which are their eigenvalues, if any? Write an eigenvector for each of eigenvalues found. *Hint*: for this exercise you do not have to compute any characteristic polynomials or null spaces.

CHAPTER 24

Similar matrices and diagonalization

24.1. Similar matrices

As we saw, if a transformation T has an eigenbasis G, then T in G has a diagonal matrix. Let us investigate this more using the concept of *similar matrices*.

Definition 24.1. Let A and B be any matrices in $M_{n,n}(F)$. Call the matrices A and B *similar*, if there is an invertible matrix $P \in M_{n,n}(F)$ such that

$$\boldsymbol{P^{-1}AP = B.}$$

Example 24.2. In $M_{3,3}(\mathbb{R})$ take, say,

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

P is invertible, which is easy to see, say by expanding P by Laplace rule along its 1'st column, and noticing that $\det(P) \neq 0$.

Compute the inverse of P:

$$P^{-1} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -\frac{3}{4} & -\frac{1}{2} \\ 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{4} & \frac{1}{2} \end{bmatrix}.$$

We can get a matrix B similar to A:

$$P^{-1}AP = B = \begin{bmatrix} 1 & -3 & 2 \\ 0 & 3 & 0 \\ 1 & 2 & 2 \end{bmatrix}.$$

The following three properties show that similarity is an *equivalence relation*:

1. Any matrix is similar to itself. To prove this just take $P = I$.
2. If A is similar to B, then also B is similar to A. To prove this just consider the equality $P^{-1}AP = B$ (with an invertible P), and take $Q = P^{-1}$. Then Q is invertible, and $Q^{-1}BQ = Q^{-1}(P^{-1}AP)Q = IAI = A$.
3. If A is similar to B, and B is similar to C, then also A is similar to C. To prove this consider the equalities $P^{-1}AP = B$ and $R^{-1}BR = C$ (with invertible matrices P and R), and take $Q = PR$. Then Q also is invertible, and $Q^{-1}AQ = (R^{-1}P^{-1})A(PR) = R^{-1}(P^{-1}AP)R = R^{-1}BR = C$.

By Theorem 20.26 and by Remark 20.27 following it we know that if A and B are the matrices of the same transformation T in bases E and G respectively, then $B = P^{-1}AP$, where $P = P_{EG}$ is the invertible change of basis matrix. Moreover, if any basis E is given, then for *any* invertible matrix $P \in M_{n,n}(F)$ there is a basis G such that A and B are related as $B = P^{-1}AP$. We get:

Lemma 24.3. *The matrices $A, B \in M_{n,n}(F)$ are similar (i.e., $B = P^{-1}AP$ for some P) if and only if they are the matrices of the same transformation $T : F^n \to F^n$ in some bases E and G respectively. Moreover, P then is the change of basis matrix P_{EG}.*

Now we at once get a large list of basic properties of similar matrices:

Proposition 24.4. *Let $A, B \in M_{n,n}(F)$ be any similar matrices, then:*

1. *A and B have the same characteristic polynomials: $|A - \lambda I| = |B - \lambda I|$.*
2. *A and B have the same eigenvalues.*
3. *A and B have the same eigenvectors (written by coordinates in different bases).*
4. $\det(A) = \det(B)$.
5. $\operatorname{nullity}(A) = \operatorname{nullity}(B)$.
6. $\operatorname{rank}(A) = \operatorname{rank}(B)$.
7. *A^n is similar to B^n for any $n = 0, 1, \dots$*
8. *A is invertible if and only if B is invertible. Then A^{-1} is similar to B^{-1}.*

Proofs. A and B by Lemma 24.3 are the matrices of same transformation T in different bases. Since the characteristic polynomial of T does not depend on the basis, we get the points **1** above. Since definitions of eigenvector and eigenvalue also do not depend on the basis, we get the point **2** and **3**.

If $P^{-1}AP = B$, then the point **4** follows from $\det(B) = \det\big(P^{-1}AP\big) = \det\big(P^{-1}\big) \cdot \det(A) \cdot \det(P) = \det(A)$. In particular, $\det(A) \neq 0$ if and only if $\det(B) \neq 0$, from which the point **8** follows (determinants of invertible matrices are non-zero).

The kernel $\ker(T)$ of T does not depend on the choice of basis. Both $\operatorname{nullity}(A)$ and $\operatorname{nullity}(B)$ are the dimension of $\ker(T)$. This proves **5**. And **6** follows from point **5** and from equality $\operatorname{nullity}(A) + \operatorname{rank}(A) = n = \operatorname{nullity}(B) + \operatorname{rank}(B)$.

For **7** compute $B^n = (P^{-1}AP)^n = P^{-1}AP \cdot P^{-1}AP \cdots P^{-1}AP = P^{-1}A^n P$. □

Example 24.5. Let us illustrate points **1**, **2**, **3** above using the matrices A, B, P from Example 24.2. A has the characteristic polynomial

$$f(\lambda) = |A - \lambda I| = \begin{vmatrix} 2-\lambda & 0 & 1 \\ 0 & 3-\lambda & 0 \\ 2 & 1 & 1-\lambda \end{vmatrix}$$

$$= -\lambda^3 + 6\lambda^2 - 9\lambda$$

which is equal to

$$|B - \lambda I| = \begin{vmatrix} 1-\lambda & -3 & 2 \\ 0 & 3-\lambda & 0 \\ 1 & 2 & 2-\lambda \end{vmatrix}.$$

Presenting $f(\lambda) = -\lambda(\lambda - 3)^2$ we get that the eigenvalues for both A and B are $\lambda_1 = 0$ and $\lambda_2 = 3$.

For, say, $\lambda_1 = 0$ the matrix A has the eigenspace spanned by the single eigenvector $(-1, 0, 2)$, and the matrix B has the eigenspace spanned by the single eigenvector $(-2, 0, 1)$. These in fact are the coordinates of the same vector v written in different bases E and G, with a change of basis matrix $P = P_{EG}$. By (13.3) is is easy to verify that

$$[v]_E = \begin{bmatrix} -1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} -2 \\ 0 \\ 1 \end{bmatrix} = P\,[v]_G.$$

Using Proposition 24.4 it is easy to bring examples of matrices which are *not* similar and, thus, they cannot be the matrices of the same transformation in different bases.

Example 24.6. Matrices of different rank are not similar. Thus,

$$\begin{bmatrix} 3 & 2 & 0 \\ 0 & 7 & 2 \\ 0 & 0 & 5 \end{bmatrix} \text{ and } \begin{bmatrix} 6 & 8 & 6 \\ 0 & 9 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

are *not* similar because the first is of rank 3, and the second is of rank 2.

Example 24.7. Matrices with different determinants are not similar. Therefore

$$\begin{bmatrix} 3 & 2 & 0 \\ 0 & 7 & 2 \\ 0 & 0 & 5 \end{bmatrix} \text{ and } \begin{bmatrix} 7 & 6 & 8 \\ 0 & 3 & 9 \\ 0 & 0 & 4 \end{bmatrix}$$

are *not* similar (although they both have the same rank 3).

24.2. The diagonalization $P^{-1}AP = D$ and its first applications

Definition 24.8. The matrix $A \in M_{n,n}(F)$ is called a *diagonalizable matrix*, if it is similar to some diagonal matrix D, i.e., there is an invertible matrix P such that $P^{-1}AP = D$.

Definition 24.9. The linear transformation T of the space V is called a *diagonalizable linear transformation*, if it has a diagonal matrix in some basis of V, i.e., if there is an eigenbasis for T in V.

Resemblance of the names is clear: the matrices A and D are similar, i.e., $P^{-1}AP = D$, if and only if they are the matrices of the same transformation T in different bases E and G. Namely, for an "old" basis E and a "new" basis G we have:

$$A = [T]_E = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \quad \text{and} \quad D = [T]_G = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{bmatrix}.$$

Moreover, the elements $\lambda_1, \dots, \lambda_n$ (repetitions allowed) on the diagonal of D are all the eigenvalues of T. The columns of the matrix

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \cdots & \cdots & \cdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} = \left[\, v_1 \,\vdots\, \cdots \,\vdots\, v_n \,\right]$$

are the eigenvectors associated to the eigenvalues $\lambda_1, \dots, \lambda_n$ respectively, and they form the eigenbasis G for T in V. Finally, the invertible matrix $P = P_{EG}$ is the change of basis matrix from the "old" basis E and a "new" *eigen*basis G.

The key objective of the previous sections can be rephrased as follows: given a transformation $T : V \to V$, find out weather it is diagonalizable. Or in matrix language: given a matrix $A \in M_{n,n}(F)$, detect weather $P^{-1}AP = D$ holds for some P.

Example 24.10. For the transformation $T(x, y, z) = (6x + 6y - 12z,\ 4x + 2y - 6z,\ 4x + 3y - 7z)$ of the space $\mathbb{R}^3$ we already found its matrix

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix},$$

its characteristic polynomial $f(\lambda) = -\lambda^3 + \lambda^2 + 2\lambda = -(\lambda-2)(\lambda+1)\lambda$, and its three eigenvalues $\lambda_1 = 2, \lambda_2 = -1, \lambda_3 = 0$, see Example 23.20. So the matrix D is:

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

For these eigenvalues we have found the respective associated eigenvectors (eigenbasis):

$$v_1 = (3, 2, 2), \quad v_2 = (0, 2, 1), \quad v_3 = (1, 1, 1).$$

Putting them by columns we get the matrix P:

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

Let us check correctness of formula $P^{-1}AP = D$ for this case. We have:

$$P^{-1} = \begin{bmatrix} 1 & 1 & -2 \\ 0 & 1 & -1 \\ -2 & -3 & 6 \end{bmatrix}.$$

Therefore:

$$P^{-1}AP = \begin{bmatrix} 2 & 2 & -4 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{bmatrix} P$$

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

Let us do a slightly different example, where the number of independent eigenvectors is *not* equal to the number of eigenvalues.

Example 24.11. Consider the transformation $T(x, y, z) = (y,\ z,\ 2x - 5y + 4z)$ of the space $\mathbb{R}^3$. It has the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix},$$

the characteristic polynomial $f(\lambda) = -\lambda^3 + 4\lambda^2 - 5\lambda + 2 = -(\lambda-1)^2(\lambda-2)$, and *two* eigenvalues $\lambda_1 = 1$, $\lambda_2 = 2$, of which the first is a root of multiplicity 2 for $f(\lambda)$ (see Appendix C.2 for root multiplicity). Compute the eigenspaces E_1 and E_2.

$$A - \lambda_1 I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix} - 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 2 & -5 & 3 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -1 \\ 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A - \lambda_1 I).$$

It has rank 2, so the null space (eigenspace E_1) has the dimension $3 - 2 = 1$. As a basis for it take the eigenvector $v_1 = (1,1,1)$.

Next, for $\lambda_2 = 2$ we have

$$A - \lambda_2 I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix} - 2 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \\ 2 & -5 & 2 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{1}{4} \\ 0 & \mathbf{1} & -\frac{1}{2} \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A - \lambda_2 I).$$

It also has rank 2, so the null space (the eigenspace E_2) also has the dimension $3 - 2 = 1$. As a basis for it take the eigenvector $v_2 = (1,2,4)$.

Now we can conclude that A is not a diagonalizable matrix, since it cannot be presented in the form $P^{-1}AP = D$. If such as form existed, the invertible matrix P would consist of columns of eigenvectors. But we have just *two* maximal linearly independent eigenvectors v_1, v_2, at most.

Example 24.12. The linear transformation $T(x,y,z) = (-x+z,\ 3x-3z,\ x-z)$ of the space $\mathbb{R}^3$ has the matrix

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

the characteristic polynomial $f(\lambda) = -\lambda^3 - 2\lambda^2 = -\lambda^2(\lambda+2)$, and two eigenvalues $\lambda_1 = 0$, $\lambda_2 = -2$ of which the first is a root of multiplicity 2 for $f(\lambda)$. Compute the eigenspaces E_0 and E_{-2}.

$$A - \lambda_1 I = \begin{bmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{bmatrix} - 0 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A - \lambda_1 I).$$

It has rank 1, so the null space (eigenspace E_0) has the dimension $3 - 1 = 2$. As a basis for it take the eigenvectors $v_1 = (0,1,0)$ and $v_2 = (1,0,1)$.

Next, for $\lambda_2 = -2$ we have

$$A - \lambda_2 I = \begin{bmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{bmatrix} - (-2) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 \\ 3 & 2 & -3 \\ 1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & 1 \\ 0 & \mathbf{1} & -3 \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A - \lambda_2 I).$$

It has rank 2, so the null space (eigenspace E_{-2}) has the dimension $3 - 2 = 1$. As a basis for it take the eigenvector $v_3 = (-1,3,1)$. So the matrices P and D in this case are:

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

We put the eigenvalue 0 on the diagonal of D *twice* because there are two linearly independent eigenvectors associated to it: E_0 is 2-dimensional. And we put the eigenvalue -2 on diagonal *once* since E_{-2} is 1-dimensional.

We leave to you the pleasure of checking that the product $P^{-1}AP$ actually is equal to the diagonal matrix D.

Diagonalization is used in numerous areas of mathematics. For now let us mention just a few helpful applications of them.

If the matrix A is diagonalizable, then *its powers A^k are especially easy to compute*. Since $P^{-1}AP = D$, then $A = PDP^{-1}$, and we have:

$$A^2 = PDP^{-1} \cdot PDP^{-1} = PD(P^{-1}P)DP^{-1} = PDIDP^{-1} = PD^2P^{-1},$$

$$A^k = \underbrace{PDP^{-1} \cdot PDP^{-1} \cdots PDP^{-1}}_{k} = \underbrace{PDIDI \cdots IDP^{-1}}_{k} = PD^kP^{-1},$$

i.e., the burden of computation of A^k is reduced to easy computation of D^k:

$$D^k = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{bmatrix}^k = \begin{bmatrix} \lambda_1^k & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n^k \end{bmatrix}$$

(we just replace each eigenvalue λ_i by its power λ_i^k).

For a diagonalizable matrix A it is easy *to detect if A is invertible and, if yes, find the inverse A^{-1}*. By Corollary 23.7 A is invertible if and only if 0 is not its eigenvalue, i.e., if the diagonal of D contains *no* zero entry. If that is the case, we have

$$A^{-1} = \left(PDP^{-1}\right)^{-1} = (P^{-1})^{-1}D^{-1}P^{-1} = PD^{-1}P^{-1},$$

where the inverse D^{-1} is trivial to discover:

$$D^{-1} = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n \end{bmatrix}^{-1} = \begin{bmatrix} \lambda_1^{-1} & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & \lambda_n^{-1} \end{bmatrix}$$

(we just replcace each eigenvalue λ_i by its inverse λ_i^{-1}).

Combining the above two approaches we can easily compute negative powers of an invertible diagonalizable matrix A: for any negative $-k$ we have $A^{-k} = \left(PDP^{-1}\right)^{-k} = PD^{-k}P^{-1}$, where D^{-k} is obtained by replacing each entry λ_i on diagonal by λ_i^{-k}.

Example 24.13. Using calculations in Example 24.10 we have

$$A = \begin{bmatrix} 6 & 6 & -12 \\ 4 & 2 & -6 \\ 4 & 3 & -7 \end{bmatrix} = PDP^{-1}$$

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

Therefore, even high powers of A are not hard to compute:

$$A^{100} = \begin{bmatrix} 3 & 0 & 1 \\ 2 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2^{100} & 0 & 0 \\ 0 & -1^{100} & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & -2 \\ 0 & 1 & -1 \\ -2 & -3 & 6 \end{bmatrix}.$$

As to invertibility, A is not invertible as we have a zero entry on the diagonal of D.

Now that we have enough arguments why diagonalization is important, let us turn to methods of its computation.

24.3. Diagonalization criterion using geometric multiplicity

For eigenvalue λ of a transformation T we called the dimension $\dim(E_\lambda)$ the *geometric multiplicity* of λ. As we will see, computing $\dim(E_\lambda)$ for all eigenvalues of T we can find out, if the matrix $A = [T]$ is diagonalizable.

In Lemma 23.25 we proved that if $\lambda_1, \ldots, \lambda_k$ are any *distinct* eigenvalues, then eigenvectors $v_1, \ldots, v_k$ associated to them are linearly independent. Let us extend this fact: we can replace each v_i by "a brunch" of linearly independent eigenvectors:

Lemma 24.14. *Let $\lambda_1, \ldots, \lambda_k \in F$ be any distinct eigenvalues of T, and let for each $s = 1, \ldots, k$ the vectors $v_{s1}, \ldots, v_{sn_s}$ be some linearly independent vectors from the eigenspace E_{λ_s}. Then the combined set of eigenvectors is independent:*

$$v_{11}, \ldots, v_{1n_1}; \ \cdots \ ; v_{k1}, \ldots, v_{kn_k}.$$

***Proof*.** Assume a linear combination of the above vectors is zero:

$$c_{11}v_{11}+\cdots+c_{1n_1}v_{1n_1}\ +\cdots+\ c_{k1}v_{k1}+\cdots+c_{kn_k}v_{kn_k}=u_1\ +\cdots+\ u_k=0 \tag{24.1}$$

(we denoted $u_s = c_{s1}v_{s1}+\cdots+c_{sn_s}v_{sn_s}$ for all $s=1,\dots,k$). Clearly, u_s is in E_{λ_s} as it is a linear combination of vectors from E_{λ_s}. So each u_s either is an *eigenvector* associated to λ_s, or is *zero*. If some of u_s are eigenvectors, they are independent by Lemma 23.25. The right-hand side equality of (24.1) then implies that a linear combination of those eigenvectors u_s is zero while those independent vectors have coefficient 1 (for, u_s can be rewritten as $1\,u_s$). This is a contradiction, and the only way to avoid it is to assume that each u_s is zero. Then $0=u_s=c_{s1}v_{s1}+\cdots+c_{sn_s}v_{sn_s}$, for $s=1,\dots,k$, and so all $c_{s1},\dots,c_{sn_s}$ are zero, since $v_{s1},\dots,v_{sn_s}$ are linearly independent in E_{λ_s}. □

Theorem 24.15. *Let $\lambda_1,\dots,\lambda_k\in F$ be all the eigenvalues of a transformation T of a space V over F. Then T is diagonalizable if and only if the sum of geometric multiplicities of all $\lambda_1,\dots,\lambda_k$ is equal to* $\dim(V)$*:*

$$\dim\big(E_{\lambda_1}\big)+\cdots+\dim\big(E_{\lambda_k}\big)=\dim(V). \tag{24.2}$$

***Proof*.** Let $G_s=\{v_{s1},\dots,v_{sn_s}\}$ be an eigenbasis of E_{λ_s}. The combined set

$$G=G_1\cup\cdots\cup G_s=\{v_{11},\dots,v_{1n_1}\,;\,\dots\,;\,v_{k1},\dots,v_{kn_k}\}$$

is independent by Lemma 24.14. If (24.2) holds, then the number of vectors in G is equal to $\dim(V)$, that is, G is a basis for V. Since it consists of eigenvectors, the matrix $[T]_G$ of T in that eigenbasis is diagonal. It starts by n_1 copies of λ_1, and ends by n_k copies of λ_k.

On the other hand, if T is *not* diagonalizable, then $n_1+\cdots+n_k$ is *strictly less* than $\dim(V)$. For, otherwise the diagonal matrix could be obtained on G. □

Although the current topic is natural to visualize, and the proofs are shorter in transformations language, diagonalization is more often applied to matrices. Thus, we give the algorithm in matrix form:

How to diagonalize a matrix using geometric multiplicity. Now we can detect diagonalizability and find the diagonal form for any diagonalizable matrix $A\in M_{m,n}(F)$, provided that we are able to compute the eigenvalues of A (see Remark 23.19).

Algorithm 24.16 (Detection of diagonalizibility of a matrix, and computation of diagonal form by geometric multiplicity)**.** We are given a matrix $A\in M_{n,n}(F)$ over a field F, and we know its eigenvalues $\lambda_1,\dots,\lambda_k$.

► Detect if or not A diagonalizible. If yes, compute its diagonal form D, and write it as $D=P^{-1}AP$, where P is an invertible matrix.

1. For each $s=1,\dots,k$ compute $r_s=\operatorname{rank}(A-\lambda_s I)$ using Algorithm 14.7.
2. Find the geometric multiplicity $n_s=\dim\big(E_{\lambda_s}\big)=n-r_s$.
3. If $n_1+\cdots+n_k<n$, output: A is not diagonalizable. End of the process.
4. Else, output: A is diagonalizable.
5. For each $s=1,\dots,k$ compute a basis $v_{s1},\dots,v_{sn_s}$ for $\operatorname{null}(A-\lambda_s I)$ by Algorithm 15.2.
6. Set the matrix $P\in M_{n,n}(F)$ with columns consisting of coordinates of vectors: $v_{11},\dots,v_{1n_1}\,;\ \dots\ ;\,v_{k1},\dots,v_{kn_k}$.
7. Set the diagonal matrix $D\in M_{n,n}(F)$ with entries $\lambda_1,\dots,\lambda_k$ on its diagonal, each λ_s occurring n_s times.
8. Compute the inverse P^{-1} by Algorithm 9.12.
9. Output the equality $D=P^{-1}AP$ with matrices P, D, P^{-1} computed above.

Example 24.17. In Example 24.10 we have three eigenvalues, each with a one-dimensional eigenspace. So

$$\begin{aligned}&\dim(E_{\lambda_1})+\dim(E_{\lambda_2})+\dim(E_{\lambda_3})\\&=1+1+1=3=\dim(V),\end{aligned}$$

and A is diagonalizable. We have computed the form $D=P^{-1}AP$ in Example 24.10.

Example 24.18. In Example 24.11 we have two eigenvalues, each with a one-dimensional eigenspace. So

$$\begin{aligned}&\dim(E_{\lambda_1})+\dim(E_{\lambda_2})\\&=1+1=2<3=\dim(V),\end{aligned}$$

and the diagonalization of A was impossible.

Example 24.19. Finally, in Example 24.12 we have two eigenvalues. One has a 2-dimensional eigenspace, the other has a 1-dimensional eigenspace. So

$$\begin{aligned}&\dim(E_{\lambda_1})+\dim(E_{\lambda_2})\\&=2+1=3=\dim(V),\end{aligned}$$

and A is a diagonalizable matrix. We found the form $D=P^{-1}AP$ in Example 24.12.

Remark 24.20. Notice an optimization feature we used in this algorithm. We could record it a little shorter, if we in step **1** at once compute the bases for null spaces $\text{null}(A-\lambda_s I)$ by Algorithm 15.2. However, this could cause unnecessary computations because A may *not* be a diagonalizable matrix. We can detect this knowing the ranks r_s of matrices $A-\lambda_s I$. I.e., we only need the *row-echelon* forms of $A-\lambda_s I$ for that step yet. Only after we discover diagonalizibility of A in step **4**, we proceed to the *reduced row-echelon forms* of $A-\lambda_s I$ and to the bases by Algorithm 15.2.

24.4. Diagonalization criterion using algebraic multiplicity

We have already mentioned the *multiplicity* of a root for a polynomial $f(x)\in F[x]$ in Appendix C.2. Say, the polynomial $f(x)=-x^2(x+2)$ has the root 0 of multiplicity 2, and the root -2 of multiplicity 1.

Let T be a transformation of a space V over some field F. The eigenvalue $\lambda\in F$ of T is called an eigenvalue of *algebraic multiplicity* k, if λ is a root of multiplicity k for the characteristic polynomial $f(\lambda)=|A-\lambda I|$.

Example 24.21. As we have seen above in Example 24.12, the linear transformation $T(x,y,z)=(-x+z,\ 3x-3z,\ x-z)$ has the characteristic polynomial $f(\lambda)=-\lambda^3-2\lambda^2=-\lambda^2(\lambda+2)$. It has two eigenvalues $\lambda_1=0,\ \lambda_2=-2$ of which the first is of algebraic multiplicity 2, and the second is of algebraic multiplicity 1.

Lemma 24.22. *The geometric multiplicity of any eigenvalue of a transformation is less than or equal to its algebraic multiplicity.*

Proof. Assume the geometric multiplicity $\dim(E_{\lambda'})$ of a fixed eigenvalue λ' is k. Take any basis $v_1,\dots,v_k$ for $E_{\lambda'}$. Continue it to a basis for the whole space V:

$$v_1,\dots,v_k,e_{k+1},\dots,e_n,$$

and assume A is the matrix of T in this basis. A will be of the following type:

$$A=\left[\begin{array}{ccc:ccc}\lambda' & \cdots & 0 & a_{1\,k+1} & \cdots & a_{1\,n}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & \lambda' & a_{k\,k+1} & \cdots & a_{k\,n}\\ \hdashline 0 & \cdots & 0 & a_{k+1\,k+1} & \cdots & a_{k+1\,n}\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & \cdots & 0 & a_{n\,k+1} & \cdots & a_{n,n}\end{array}\right].$$

Compute $f(\lambda) = |A - \lambda I|$ by applying the Laplace expansion for k times:

$$f(\lambda) = (\lambda' - \lambda)^k \begin{vmatrix} a_{k+1\,k+1} - \lambda & \cdots & a_{k+1\,n} \\ \cdots & \cdots & \cdots \\ a_{n\,k+1} & \cdots & a_{n,n} - \lambda \end{vmatrix}.$$

So regardless of the value of the determinant on the right-hand side, $f(\lambda)$ is divisible by $(\lambda' - \lambda)^k = (-(\lambda - \lambda'))^k$, and λ' is a root of multiplicity at least k for $f(\lambda)$. □

Now we get one more criterion for diagonalization:

Theorem 24.23. *Let $\lambda_1, \ldots, \lambda_k \in F$ be all the eigenvalues of a transformation T of a space V over F. Then T is diagonalizable if and only if the geometric multiplicity of each eigenvalue λ_i, $i = 1, \ldots, k$, is equal to its algebraic multiplicity, and the sum of all algebraic multiplicities is equal to $n = \dim(V)$.*

***Proof*.** Assume the sum of algebraic multiplicities of all eigenvectors is n. If geometric multiplicity is equal to algebraic multiplicity for any λ_i, then the sum of geometric multiplicities also is n and diagonalizability follows from Theorem 24.15.

If the geometric multiplicity is strictly less than algebraic multiplicity for at least one λ_i, then the sum of geometric multiplicities of all eigenvectors by previous lemma is strictly less than n. We get non-diagonalizability by Theorem 24.15.

If the sum of algebraic multiplicities is less than n, then the sum of geometric multiplicities also is less than n (regardless if or not they are equal to respective algebraic multiplicities) by Lemma 24.22. □

How to diagonalize a matrix using algebraic multiplicity. Theorem 24.23 suggests an improved analog of Algorithm 24.16. We detect if the sum of algebraic multiplicities of all eigenvalues is equal to $\dim(V)$. If *yes*, we verify if the algebraic multiplicity is equal to geometric multiplicity for *each* eigenvalue of T (or of A). Since $\dim(V) = \deg(f(\lambda))$, we have two helpful optimization features over Algorithm 24.16:

First, after we find all the eigenvalues $\lambda_1, \ldots, \lambda_k$, we compare the sum of their algebraic multiplicities with $\deg(f(\lambda))$. If that sum is *less* than n, the matrix is *not* diagonalizable. So we do not need to compute any nullity to discover this fact.

Second, suppose the sum of algebraic multiplicities is *equal* to $\deg(f(\lambda))$, and we turn to calculations of geometric multiplicities by Algorithm 24.16. If we for one $i = 1, \ldots, k$ find that the geometric multiplicity of λ_i is less than its algebraic multiplicity, then we no longer need to compute the geometric multiplicities of the remaining eigenvalues. Instead, we at once deduce that the matrix is *not* diagonalizable.

Example 24.24. Check the transformation of real space $\mathbb{R}^3$ given by $T(x, y, z) = (3x - 2y + 2z,\ 4x - y + z,\ z)$. It has the matrix

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

and its characteristic polynomial is $f(\lambda) = -\lambda^3 + 3\lambda^2 - 7\lambda + 5 = (\lambda - 1)(-\lambda^2 + 2\lambda - 5)$. The factor $-\lambda^2 + 2\lambda - 5$ has *no real roots*, so the only eigenvalue of $f(\lambda)$ is $\lambda_1 = 1$.

Now do we need to compute the geometric multiplicity of λ_1 or a basis for the eigenspace E_{λ_1}? No, we do *not* have to perform those steps as we by Lemma 24.22 know that the geometric multiplicity of 1 is not more than is algebraic multiplicity.

Therefore by Theorem 24.15 or by Theorem 24.23 the matrix A is not diagonalizable, and we need *no* row-echelon calculations, at all, to establish this fact.

Example 24.25. In Example 24.11 we considered the characteristic polynomial $f(\lambda) = -\lambda^3 + 4\lambda^2 - 5\lambda + 2 = -(\lambda - 1)^2(\lambda - 2)$, and two eigenvalues $\lambda_1 = 1$, $\lambda_2 = 2$. This time λ_1

is a root of multiplicity 2, and λ_2 is a root of multiplicity 1. We have $1+2=3=\deg(f(\lambda))$, so we are motivated to study the dimensions of eigenspaces E_{λ_1} and E_{λ_2}.

However, E_{λ_1} turns out to be 1-dimensional, and so the diagonalization is impossible because the algebraic and geometric multiplicities of $\lambda_1 = 1$ are *not* equal. Here we do *not* have to study the eigenspace E_{λ_2} to give the answer. In Example 24.11 we had to do much more work to come to that answer.

Example 24.26. In Example 24.10 we have the characteristic polynomial $f(\lambda) = -\lambda^3 + \lambda^2 + 2\lambda = -(\lambda-2)(\lambda+1)\lambda$, and three eigenvalues $\lambda_1 = 2$, $\lambda_2 = -1$, $\lambda_3 = 0$. Each is a root of multiplicity 1, so we have $1+1+1=3=\deg(f(\lambda))$. Since each eigenspace need be at least 1-dimensional, we at once deduce that the matrix is dagonalizable. No need to calculate the nullities of matrices $A-2I$, $A+1I$, $A-0I$ like in Example 23.20.

Example 24.27. In Example 24.12 we have the characteristic polynomial $f(\lambda) = -\lambda^3 - 2\lambda^2 = -\lambda^2(\lambda+2)$, and two eigenvalues $\lambda_1 = 0$, $\lambda_2 = -2$. Here λ_1 is a root of multiplicity 2, and λ_2 is a root of multiplicity 1.

Since $2+1=3=\deg(f(\lambda))$, we go on to check the geometric multiplicities also. And since $\dim\big(E_{\lambda_1}\big) = 2$ and $\dim\big(E_{\lambda_2}\big) = 1$, the transformation is diagonalizable.

We can find the diagonalization, and that is done in Example 24.12.

A special case need be stressed. By Theorem D.8 *each polynomial $f(x)$ over the complex field $\mathbb{C}$ has roots, and the sum of their multiplicities is equal to* $\deg(f(x))$. The degree of characteristic polynomial in turn is equal to $\dim(V)$. So one of the requirements of Theorem 24.23 may be dropped, if we are over complex field $\mathbb{C}$:

Theorem 24.28. *Let $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ be all the eigenvalues of a transformation T of space V over $\mathbb{C}$. Then T is diagonalizable if and only if the geometric multiplicity of each eigenvalue λ_i, $i = 1, \dots, k$, is equal to its algebraic multiplicity.*

Example 24.29. Consider the transformation of complex space $\mathbb{C}^3$ given by:

$$T(x,y,z) = (3x-2y+2z,\ 4x-y+z,\ z).$$

This is the same formula used in Example 24.24, and so T has the same matrix

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

and the same characteristic polynomial $f(\lambda) = -\lambda^3+3\lambda^2-7\lambda+5 = (\lambda-1)(-\lambda^2+2\lambda-5)$. But this time the factor $-\lambda^2+2\lambda-5$ has two *complex* roots, i.e., the *complex* eigenvalues $\lambda_2 = 1-2i$ and $\lambda_3 = 1+2i$. We have three eigenvalues (one real and two complex) which are pairwise distinct, each having a one-dimensional eigenspace. Applying Theorem 24.15, or Theorem 24.23, or even the earlier Theorem 23.24 we get diagonalizibility of A. Let us compute the eigenspaces E_1, E_{1-2i}, E_{1+2i}.

For $\lambda_1 = 1$ we compute:

$$A - 1I = \begin{bmatrix} 3 & -2 & 2 \\ 4 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} - 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -2 & 2 \\ 4 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{1}{2} \\ 0 & \mathbf{1} & -\frac{3}{2} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(A-1I).$$

As a basis vector choose $v_1 = (-\frac{1}{2}, -\frac{3}{2}, -1)$ or, better, $v_1 = (1,3,2)$.

Next, for $\lambda_2 = 1-2i$ compute:

$$A-(1-2i)I = \begin{bmatrix} 3 & -2 & 2 \\ 4 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} - (1-2i) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2+2i & -2 & 2 \\ 4 & -2+2i & 1 \\ 0 & 0 & 2i \end{bmatrix}$$

$$\sim \begin{bmatrix} \mathbf{1} & -\frac{1}{2}+\frac{i}{2} & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(A-(1-2i)\cdot I).$$

As a basis vector choose $v_2 = (-\frac{1}{2}+\frac{i}{2}, -1, 0)$ or, better, $v_1 = (1-i,\ 2,\ 0)$.

And for $\lambda_3 = 1+2i$ we have:

$$A-(1+2i)I = \begin{bmatrix} 3 & -2 & 2 \\ 4 & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix} - (1+2i) \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2-2i & -2 & 2 \\ 4 & -2-2i & 1 \\ 0 & 0 & -2i \end{bmatrix}$$

$$\sim \begin{bmatrix} \mathbf{1} & -\frac{1}{2}-\frac{i}{2} & 0 \\ 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(A-(1+2i)\cdot I).$$

As a basis vector choose $v_2 = (-\frac{1}{2}-\frac{i}{2}, -1, 0)$ or, better, $v_1 = (1+i,\ 2,\ 0)$. We built the diagonalization $P^{-1}AP = D$ with the *complex* matrices:

$$P = \begin{bmatrix} 1 & 1-i & 1+i \\ 3 & 2 & 2 \\ 2 & 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1-2i & 0 \\ 0 & 0 & 1+2i \end{bmatrix}.$$

Exercises

E.24.1. Using Proposition 24.4 show that none two of the following matrices may be similar: $A = \left[\begin{smallmatrix} 7&3&0\\0&2&1\\0&0&0 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} 5&3&2\\0&1&2\\0&1&1 \end{smallmatrix}\right]$, $C = \left[\begin{smallmatrix} 3&1&7\\0&5&1\\0&0&2 \end{smallmatrix}\right]$, $D = \left[\begin{smallmatrix} 6&1&7\\0&5&1\\0&0&1 \end{smallmatrix}\right]$.

E.24.2. **(1)** Bring example of a matrix $B = P^{-1}AP$ similar to the real matrix $A = \left[\begin{smallmatrix} 1&2&4\\0&3&1\\0&0&2 \end{smallmatrix}\right]$. **(2)** Deduce from the matrix A only what is the characteristic polynomial of B, and what are the eigenvalues of B. **(3)** Can you find such a matrix P that the rank of B is *less* than the rank of A? **(4)** Can you find such a matrix P that $\det(B) \neq 6$?

E.24.3. Using geometric multiplicities find if the given transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ is diagonalizable, and compute the digitalization. **(1)** T is defined by the matrix A in Exercise E.23.1. **(2)** T is defined by the matrix B in same exercise. **(3)** T is defined by the matrix C in same exercise. *Hint*: you may use the eigenvalues and eigenspaces already computed for Exercise E.23.3 and Exercise E.23.4.

E.24.4. Using algebraic *and* geometric multiplicities find if $T : \mathbb{R}^3 \to \mathbb{R}^3$ is diagonalizable, when **(1)** T is defined by the matrix A in Exercise E.23.1. **(2)** T is defined by the matrix B in same exercise. **(3)** T is defined by the matrix C in same exercise. *Hint*: you may use the computations already done for exercises E.23.3, E.23.4 and E.24.3. You are *not* required to compute the digitalization (this is done in Exercise E.24.3). Just establish the fact of digitalizability by algebraic multiplicity, if it is possible.

E.24.5. We are given the *real* matrices:

$$A = \begin{bmatrix} 3 & 2 & 0 \\ 1 & 4 & 0 \\ 0 & 3 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 5 & -10 & 5 \\ 2 & -3 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 4 & -1 \\ 2 & -6 & 3 \end{bmatrix}.$$

(1) Find the eigenvalues for each of them. **(2)** Using geometric multiplicities *only* indicate if each matrix is diagonalizable. **(3)** Indicate if the matrix is diagonalizable using the algebraic multiplicity. Mention if or not usage of algebraic multiplicity may help to shorten the calculations for the given matrix. **(4)** Write the *real* diagonalizations, if possible.

E.24.6. The linear transformations T and S are given on $\mathbb{R}^3$ by $T(x,y,z) = (3x,\ 5y+2z,\ -3y)$ and $S(x,y,z) = (2x-y+z,\ x+2y,\ 2z)$. **(1)** Find its matrices $A = [T]_E$ and $B = [S]_E$. Then using *geometric* multiplicity detect if each of these matrices is diagonalizable. *Hint*: you can use the facts that A has the eigenvalue 3, and B has the eigenvalue 2 (they may have *other* eigenvalues also). **(2)** Write the diagonalization for A or B, if possible. **(3)** Use *algebraic* multiplicity to study B. Explain why in this case you get an answer much simpler than in previous points.

E.24.7. We are given that the real 4×4 matrices A and B have the characteristic polynomials, respectively, $f_1(\lambda) = (\lambda-7)^2(\lambda^2+2\lambda+5)$ and $f_2(\lambda) = (\lambda^2-1)(\lambda-2)(\lambda+3)$. Deduce from this information weather each of A and B is diagonalizable. If yes, can you find the respective diagonal matrix D from the characteristic polynomial alone?

CHAPTER 25

Invariant subspaces and generalized eigenspaces

25.1. Invariant subspaces and their direct sums

Definition 25.1. Let T be any linear transformation of the space V. A subspace U of V is called an *invariant subspace* of V, if $T(u) \in U$ for any $u \in U$.

To stress the transformation we may also call U a *T-invariant subspace of V*. The definition shows that the *restriction* of T on U is a correctly defined function on the invariant subspace U. This function also is a linear transformation on U, since both points of Definition 20.1 hold on U, as long as they hold on entire V. Denote the restriction of T on U by $T|_U$. Restrictions help to reduce consideration of a complicated transformation T to study of their "small parts" $T|_U$.

Example 25.2. The zero subspace $U = \{0\}$ and the entire space $U = V$ evidently are invariant subspaces for *any* transformation T of V.

Example 25.3. The transformation T defined in Example 20.23 on $\mathbb{R}^3$ by its matrix:

$$A = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

has some invariant subspaces. The subspace U spanned by $e_1 = (1,0,0)$ and $e_2 = (0,1,0)$ is invariant. It is the xOy plane, on which the restriction $T|_U$ acts as the rotation by angle φ. In the basis $\{e_1, e_2\}$ of U the restriction $T|_U$ has the matrix

$$A_1 = \begin{bmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{bmatrix}.$$

The subspace W spanned by $e_3 = (0,0,1)$ also is invariant. It is the Oz line, on which $T|_W$ acts as scaling by 5. In the basis $\{e_3\}$ of W the restriction $T|_W$ has the matrix $A_2 = [5]$. We get that A is a block-diagonal matrix with two blocks A_1 and A_2:

$$A = \begin{bmatrix} A_1 & \mathbf{0} \\ \mathbf{0} & A_2 \end{bmatrix}.$$

For specific values of φ there may be other T-invariant subspaces also. If, say, $\varphi = \pi$, then any plane of $\mathbb{R}^3$ passing by the line Oz is invariant. For simplicity take $\mathcal{P}$ to be the plane spaned by the basis $\{e_1, e_3\}$. Then in this basis $T|_{\mathcal{P}}$ has the matrix $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 25.4. For the derivation linear transformation $T\big(f(x)\big) = f'(x)$ of polynomial space $V = \mathcal{P}_n(\mathbb{R})$ every subspace $U = \mathcal{P}_m(\mathbb{R})$ with $m \le n$ is an invariant subspace because, if $f(x)$ is of degree at most m, then the degree of $f'(x)$ also is bounded by m. If, say, $n = 3$ and $m = 2$, then $T|_U$ is given by the matrix

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

Example 25.5. Let T be a transformation of a space V with an eigenvalue λ and a respective eigenvector v. Then the 1-dimensional space U spanned by v is invariant, and $T|_U$ clearly has the matrix $[\lambda]$.

An eigenspace E_λ also is invariant, and in the matrix consisting of eigenvectors the restriction has $T|_{E_\lambda}$ is given by the diagonal matrix

$$\begin{bmatrix} \lambda & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \lambda \end{bmatrix}$$

of degree equal to geometric multiplicity of λ.

Example 25.6. Let T be a transformation of a space V with the kernel $U = \ker(T)$ and the range $R = \text{range}(T)$. U is invariant because for any $u \in U$ we have $T(u) = 0 \in U$. And R is invariant because $T(u) \in R$ for any $u \in V$. The matrix of T_U has a very simple form: it is a zero matrix (of degree equal to nullity(T)).

As Examples above show, invariants subspaces in some sense are wide generalizations of eigenvectors and eigenspaces. The 1-dimensional invariant subspaces are nothing but the spaces spanned by single eigenvectors. Also, each eigenspace is a specific type of invariants subspace.

A remarkable property that we are going to use repeatedly was displayed in Example 25.3: the matrix A of T is a block-diagonal matrix consisting of two blocks which are the matrices of restrictions $T|_U$ and $T|_W$ respectively. From point 3 of Theorem 16.21 easily follows that V is the *direct sum* of these two invariant subspaces: $V = U \oplus W = \text{span}(e_1, e_2) \oplus \text{span}(e_3)$. And, in general:

Theorem 25.7. *Let T be a linear transformation of the space V, and let U and W be T-invariant subspaces of V with bases $E = \{e_1, \dots, e_t\}$ and $G = \{g_1, \dots, g_s\}$ respectively. If $V = U \oplus W$, then in the joint basis*

$$E \cup G = \{e_1, \dots, e_t, g_1 \dots, g_s\}$$

of V the matrix of T has the following block-diagonal form:

$$A = [T]_{E\cup G} = \begin{bmatrix} A_1 & \mathbf{0} \\ \mathbf{0} & A_2 \end{bmatrix} = \left[\begin{array}{ccc:ccc} a_{11} & \cdots & a_{1t} & & & \\ \cdots & \cdots & \cdots & & \mathbf{0} & \\ a_{t1} & \cdots & a_{tt} & & & \\ \hdashline & & & b_{11} & \cdots & b_{1s} \\ & \mathbf{0} & & \cdots & \cdots & \cdots \\ & & & b_{s1} & \cdots & b_{ss} \end{array}\right],$$

where A_1 is the matrix of $T|_U$ in E, and A_2 is the matrix of $T|_W$ in G.

Proof. That $E \cup G$ is a basis of V follow from point 3 of Theorem 16.21. For any $e_i \in E$, $i = 1, \dots, t$, we have:

$$T(e_i) = a_{1i}e_1 + \cdots + a_{ti}e_t + 0g_1 + \cdots + 0g_s$$

(the coefficients at g_j are zero because $T(e_i)$ is in U, and so $T(e_i)$ is a linear combination of vectors of E). It is easy to see that for each $i = 1, \dots, t$ the coefficients of the above linear combination form the i'th column of the block-diagonal matrix stated in the theorem. And the remaining column are obtained using the vectors $g_j \in G$. □

Theorem 25.7 can easily be generalized for more than one invariant direct summands. If $V = U_1 \oplus \cdots \oplus U_k$, where each U_i is a T-invariant subspace of dimension t_i with a basis E_i on which the restriction $T|_{U_i}$ has the matrix A_i, $i = 1, \dots, k$, then in the joint basis $E = E_1 \cup \cdots \cup E_k$ of V the transformation T has the block-diagonal matrix

$$A = [T]_E = \begin{bmatrix} A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A_k \end{bmatrix}. \tag{25.1}$$

From here it is easy to deduce that if $f(\lambda)$ is the characteristic polynomial of T, and if $f_i(\lambda)$ is the characteristic polynomial of the restriction $T|_{U_i}$, then

$$\boldsymbol{f(\lambda) = f_1(\lambda) \cdots f_k(\lambda).} \tag{25.2}$$

This equality will have a key role later, in particular, in Jordan normal form construction.

Example 25.8. An application of Theorem 25.7 is the above Example 25.3: on the direct sum space $\mathbb{R}^3 = V = U \oplus W$ the transformation T has a block-diagonal form.

By Laplace expansion rule the characteristic polynomial of T is

$$f(\lambda) = \big((\cos(\varphi) - \lambda)^2 + \sin^2(\varphi)\big)(5-\lambda)$$
$$= (\lambda^2 - 2\lambda\cos(\varphi) + 1)(5-\lambda).$$

By (25.2) the first of these factors is the characteristic polynomial $f_1(\lambda)$ of $T|_U$, and the second is the characteristic polynomial $f_2(\lambda)$ of $T|_W$.

Example 25.9. Turning back to earlier Example 20.24 we may notice that

$$\mathbb{R}^5 = V = U \oplus W \oplus R$$

is a direct sum of three invariant subspaces. If $E = \{e_1, \ldots, e_5\}$ is the standard basis of $\mathbb{R}^5$, then $U = \operatorname{span}(e_1, e_2)$, $W = \operatorname{span}\big(e_3, e_4\big)$, $R = \operatorname{span}(e_5)$.

The matrices of restrictions $T|_U$, $T|_W$, $T|_R$ respectively are three blocks seen on the diagonal of the 5×5 matrix in Example 20.24.

The characteristic polynomial of T is a product of three factors:

$$f(\lambda) = (\lambda^2 - 2\lambda\cos(\varphi) + 1)$$
$$\cdot(\lambda^2 - 6\lambda\cos(\theta) + 9)(5-\lambda)$$

which by (25.2) are the characteristic polynomials of the restrictions $T|_U$, $T|_W$, $T|_R$.

25.2. Generalized eigenspaces

Let v be an eigenvector corresponding to a fixed eigenvalue λ of a linear transformation T of V, i.e., $T(v) = \lambda v$. Recall that we denoted by I the identity transformation $I : v \to v$ with identity matrix $I = I_n$ (see Section 22.2). Since $(\lambda I)(v) = \lambda\, I(v) = \lambda v$, we can interpret the equality $T(v) = \lambda v$ as

$$(T - \lambda I)(v) = T(v) - (\lambda I)(v) = \lambda v - \lambda v = 0,$$

which means that v is a (non-zero) vector in the kernel $\ker(T - \lambda I)$ of the transformation $T - \lambda I$. This leads to the following characterization of the eigenspace E_λ:

$$\boldsymbol{E_\lambda = \ker(T - \lambda I)}.$$

Agreement 25.10. We need two conventions which will very much simplify the notations below. Firstly, introduce the transformation $N = T - \lambda I$. A non-zero vector v is an eigenvector for T if and only if it is in kernel of N, i.e., $E_\lambda = \ker(N)$. Secondly, set $N = A - \lambda I = [T - \lambda I]_E$, i.e., we use the same character N to denote the transformation N and its matrix. λ is *not* included in notation of N, but whenever we use N, it will be clear from the context which λ is assumed.

Example 25.11. Let T be the transformation given by the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix}$$

in Example 24.11. It has the characteristic polynomial $f(\lambda) = -\lambda^3 + 4\lambda^2 - 5\lambda + 2 = -(\lambda - 1)^2(\lambda - 2)$ and two eigenvalues $\lambda_1 = 1$, $\lambda_2 = 2$, of algebraic multiplicities 2 and 1 respectively.

For $\lambda_1 = 1$ we have:

$$N = T - \lambda_1 I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix} - 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

A basis for $\ker(N)$ (or, equivalently, for $\operatorname{null}(N)$) can be computed by Algorithm 15.2.

$$N = \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 2 & -5 & 3 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -1 \\ 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(N)$$

(compare with Example 24.11). $E_1 = \ker(N)$ has the dimension $3 - \operatorname{rank}(N) = 3 - 2 = 1$, and as its basis vector we can take $u = (1, 1, 1)$.

And for $\lambda_2 = 2$ we have

$$N = T - \lambda_2 I = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix} - 2 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \\ 2 & -5 & 2 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{1}{4} \\ 0 & \mathbf{1} & -\frac{1}{2} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}(N).$$

$E_2 = \ker(N)$ also has the dimension $3 - \operatorname{rank}(N) = 3 - 2 = 1$, and as its basis vector we can choose $w = (1, 2, 4)$.

Example 25.12. Let us study the kernels of squares $N^2 = NN$ of transformations N from previous example (defined for each of eigenvalues λ_1, λ_2). Since for any $v \in \ker(N)$

$$N^2(v) = N\big(N(v)\big) = N(0) = 0,$$

we get that $\ker(N) \subseteq \ker\big(N^2\big)$.

Can these kernels be equal?

For $\lambda_1 = 1$ we have:

$$N^2 = \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & -2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}\big(N^2\big),$$

i.e., $\ker\big(N^2\big)$ has the dimension $3 - \operatorname{rank}\big(N^2\big) = 3 - 1 = 2$, and as its basis vectors we can take $v_1 = (2, 1, 0)$ and $v_2 = (1, 0, -1)$. We get:

$$\ker(N) \subset \ker\big(N^2\big)$$

(strict inclusion). Besides the basis $\{v_1, v_2\}$ we can suggest other bases for the kernel $\ker\big(N^2\big)$. For example, we can take the vector $u = (1, 1, 1)$ which already is in $\ker\big(N^2\big)$ as we saw above, and add to it any one of the vectors v_1, v_2. For example $\{u, v_1\}$ or $\{u, v_2\}$ both are bases for $\ker\big(N^2\big)$ as each of the vectors v_1, v_2 is linearly independent with u.

For $\lambda_2 = 2$ we have another N, and to find $\ker\big(N^2\big)$ we compute:

$$N^2 = \begin{bmatrix} 4 & -4 & 1 \\ 2 & -1 & 0 \\ 0 & 2 & -1 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{1}{4} \\ 0 & \mathbf{1} & -\frac{1}{2} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}\big(N^2\big),$$

i.e., $\ker\big(N^2\big)$ has the dimension $3 - \operatorname{rank}\big(N^2\big) = 3 - 2 = 1$. Since $\ker\big(N^2\big)$ contains the 1-dimensional subspace $\ker(N)$, we get:

$$\ker(N) = \ker\big(N^2\big).$$

We will return back to the matrix A of above two examples soon.

As examples above show, some vectors v may not be eigenvectors, i.e., the equality $(T - \lambda I)(v) = N(v) = 0$ may not hold for them, but v may be "rather similar" to eigenvectors, as the equality $(T - \lambda I)^2(v) = N^2(v) = 0$ does hold for v.

Here $\ker\big(N^2\big)$ may be *strictly* larger than $\ker(N)$ because $v \notin \ker(N)$. It may also turn out that $\ker\big(N^3\big)$ is *strictly* larger than $\ker\big(N^2\big)$, etc... Since we are in a finite-dimensional space V, this process cannot go on *infinitely* long, and at some r'th step we eventually get $\ker(N^r) = \ker\big(N^{r+1}\big)$ for some $r \le \dim(V)$.

Let us show that then also $\ker\big(N^{r+2}\big) = \ker(N^r)$. Indeed, if $N^{r+2}(v) = 0$ for some $v \in \ker\big(N^{r+2}\big)$, then

$$N^{r+2}(v) = N^{r+1}\big(N(v)\big) = 0,$$

and so $N(v) \in \ker\big(N^{r+1}\big) = \ker(N^r)$. Then

$$0 = N^r\big(N(v)\big) = N^{r+1}(v),$$

that is, $v \in \ker\big(N^{r+1}\big)$.

In the same manner we can show that $\ker\big(N^{r+i}\big) = \ker(N^r)$ for *any* $i = 1, 2, \ldots$ We get the following sequence of kernels:

$$\ker\big(N^1\big) \subset \ker\big(N^2\big) \subset \cdots \subset \mathbf{ker(N^r)} = \ker\big(N^{r+1}\big) = \ker\big(N^{r+2}\big) = \cdots \tag{25.3}$$

the first r members of which are strictly ascending, and all the remaining kernels are equal to the r'th kernel, in other words, the sequence is *stabilising* at its r'th member. Denote the r'th kernel by

$$\boldsymbol{G_\lambda = \ker(N^r) = \ker(T - \lambda I)^r},$$

and call it the *generalized eigenspace* associated to the eigenvalue λ. Let $t = \dim(G_\lambda)$ be its dimension. The non-zero vectors in G_λ are called the *generalized eigenvectors*. Also denote $R = \operatorname{range}(N^r) = \operatorname{range}(T-\lambda I)^r$.

Example 25.13. Let us check how will the sequence (25.3) look like for the matrix considered in Example 25.11 and Example 25.12.

For $\lambda_1 = 1$:

$$N^3 = \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} = N^2$$

$$\sim \begin{bmatrix} \mathbf{1} & -2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}\big(N^3\big) = \operatorname{rref}\big(N^2\big),$$

i.e., $\ker\big(N^2\big) = \ker\big(N^3\big)$. Here $r = 2$, and the sequence (25.3) looks like:

$$\ker(N) \subset \ker\big(N^2\big) = \ker\big(N^3\big) = \cdots$$

In this case the eigenspace is strictly less than the generalized eigenspace:

$$E_1 \subset G_1 = \ker\big(N^2\big).$$

Next, for $\lambda_2 = 2$ we have:

$$N^3 = \begin{bmatrix} -6 & 7 & -2 \\ -4 & 4 & -1 \\ -2 & 1 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} \mathbf{1} & 0 & -\frac{1}{4} \\ 0 & \mathbf{1} & -\frac{1}{2} \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}\big(N^3\big) = \operatorname{rref}\big(N^2\big) = \operatorname{rref}(N),$$

that is, $\ker(N) = \ker\big(N^2\big) = \ker\big(N^3\big)$. In this case $r = 1$, and so the sequence (25.3) is shorter:

$$\ker(N) = \ker\big(N^2\big) = \cdots$$

The eigenspace and the generalized eigenspace coincide:

$$E_2 = G_2 = \ker(N).$$

As we saw in Example 25.6 the kernel and range of any transformation T are T-invariant. Moreover:

Lemma 25.14. *If the linear transformation T of the space V has an eigenvalue λ with a generalized eigenspace G_λ, and $R = \operatorname{range}(N^r)$, then V is the direct sum:*

$$V = G_\lambda \oplus R.$$

***Proof*.** First show that $G_\lambda \cap R = \{0\}$. Take any v in this intersection. Since $v \in G_\lambda$, then $N^r(v) = 0$. Since also $v \in R$, there is a $u \in V$ such that $N^r(u) = v$. Thus,

$$N^{2r}(u) = N^r\big(N^r(u)\big) = N^r(v) = 0,$$

i.e., $u \in \ker\big(N^{2r}\big)$. By construction $\ker\big(N^{2r}\big) = \ker(N^r) = G_\lambda$, and so $v = N^r(u) = 0$.

Applying point 2 of Theorem 16.21 to the sum $G_\lambda + R$ we get that it is *direct* sum $G_\lambda \oplus R$. On the other hand, applying Corollary 21.11 to transformation N^r we get that this sum has dimension $\operatorname{nullity}(N^r) + \operatorname{rank}(N^r) = \dim(V)$, i.e., it is equal to entire V. $\square$

It turns out that restriction $T|_{G_\lambda}$ of T on G_λ has a relatively simple structure which we are going to reveal now. Let $\{w_1, \dots, w_h\}$ be a basis for $\ker(N) = E_\lambda$ (thus, h is the geometric multiplicity of λ). Since $\ker(N) \subset \ker\big(N^2\big)$, then by point 1 of Proposition 11.27 we can add some new vectors $v_1, \dots, v_l$ to this basis to get a basis $\{w_1, \dots, w_h;\ v_1, \dots, v_l\}$ for $\ker\big(N^2\big)$. Continuing the process by induction we on r'th step add some new vectors $u_1, \dots, u_m$ to get a basis

$$E = \big\{w_1, \dots, w_h;\ v_1, \dots, v_l\ ; \dots;\ u_1, \dots, u_m\big\} \tag{25.4}$$

for G_λ. It is clear that $t = \dim(G_\lambda) = h + l + \cdots + m$.

Lemma 25.15. *In above notation the matrix A of the restriction $T|_{G_\lambda}$ in basis E is an upper triangle matrix of degree t, with all entries λ on the diagonal:*

$$A = [T|_{G_\lambda}]_E = \begin{bmatrix} \lambda & & * \\ & \ddots & \\ \mathbf{0} & & \lambda \end{bmatrix}. \tag{25.5}$$

***Proof*.** Each vector w_i of (25.4) is an eigenvector. Hence, $T(w_i) = \lambda w_i$, and the i'th column of A has λ on diagonal, and zeros elsewhere.

Each vector v_i no longer is an eigenvector, but $N(v_i)$ is an eigenvector because $(T - \lambda I)\big(N(v_i)\big) = N^2(v_i) = 0$. Thus, $N(v_i) \in E_\lambda$, and we have $(T-\lambda I)(v_i) = c_1 w_1 + \cdots + c_h w_h$, i.e., $T(v_i) = c_1 w_1 + \cdots + c_h w_h + \lambda v_i$. Hence, the respective column of A has λ on diagonal, zeros below the diagonal (and $c_1, \dots, c_h$ somewhere above the diagonal).

Continuing by induction we at the r'th step get that each vector $N(u_i)$ is in $\ker\big(N^{r-1}\big)$ because $N^{r-1}\big(N(u_i)\big) = N^r(u_i) = 0$. So each $(T - \lambda I)(u_i)$ is a linear combination of the frist $t - m$ vectors of (25.4). Hence the last m columns of A have λ on diagonal, and zeros below the diagonal. □

Example 25.16. Let as apply Lemma 25.14 to the transformation T considered earlier in this section. In Example 25.13 we calculated that

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & -5 & 4 \end{bmatrix}$$

has an eigenvalue $\lambda_1 = 1$ for which $r = 2$, i.e., the sequence (25.3) has two distinct members. Then the generalized eigenspace is:

$$G_1 = \ker\big(N^2\big) = \operatorname{span}(u, v_1) = \operatorname{span}\left(\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}\right)$$

(see Example 25.12). Next from

$$N^2 = \begin{bmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 4 & -8 & 4 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & -2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rref}\big(N^2\big)$$

it is clear that the range

$$R = \operatorname{range}\big(N^2\big) = \operatorname{span}\left(\begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}\right)$$

is one dimensional. The decomposition in Lemma 25.14 now looks like:

$$V = \mathbb{R}^3 = G_1 \oplus R$$
$$= \operatorname{span}\left(\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}\right) \oplus \operatorname{span}\left(\begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}\right).$$

Next test Theorem 25.7 on this example. Find the matrix B of T on the basis we colleted:

$$E = \left\{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix}\right\}.$$

We, of course, can compute the matrix $B = [T]_E$ from the scratch as in Section 20.1. However, it is simpler to use the change of basis method from Section 20.3. By Theorem 20.26 $B = P^{-1}AP$ where P is the change of basis from the standard basis matrix to the new basis E.

$$P = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & 4 \end{bmatrix} \quad \text{and} \quad P^{-1} = \begin{bmatrix} -4 & 8 & -3 \\ 2 & -3 & 1 \\ 1 & -2 & 1 \end{bmatrix}.$$

The routine of computation gives us

$$B = P^{-1}AP = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

I.e., we have a block-diagonal matrix corresponding to the direct sum $G_1 \oplus R$ according to Theorem 25.7.

The block $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ in upper left-hand corner of B corresponds to the restriction $T|_{G_1}$, and is of type (25.5) according to Lemma 25.15.

Remark 25.17. Above we saw situations when V has a subspace U contained inside a larger subspace W, and we have *to continue* some basis E of U to a basis of W, that is, to add some new vectors $w_1, \dots, w_k$ such that $E \cup \{w_1, \dots, w_k\}$ is a basis for W. For example, we continued a basis of $U = \ker(N)$ to a basis of $W = \ker\big(N^2\big)$, etc. Since below, too, we are going to have many such situations, let us remark that continuing a basis is a simple job by Algorithm 16.6.

Example 25.18. Apply this to the transformation in Example 25.11 and Example 25.12 for $\ker(N)$ and $\ker(N^2)$ with $N = T - I$. By Example 25.11 $\ker(N)$ can be spanned by $u = (1,1,1)$. And by Example 25.12 the kernel $\ker(N^2)$ can be spanned by $v_1 = (2,1,0)$ and $v_2 = (1,0,-1)$. Then following Remark 25.17 and Algorithm 16.6:

$$[E\,|\,H] = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 2 & 1 \\ 0 & \mathbf{1} & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

and as a continued basis for $\ker(N^2)$ we take $\{u, v_1\}$.

25.3. Direct sums of the generalized eigenspaces

Denote by $\lambda_1, \dots, \lambda_k \in F$ all the eigenvalues of a linear transformation T in the space V over F. Suppose the characteristic polynomial $f(\lambda) = |A - \lambda I|$ of T can be presented as a product of its *linear* factors $\lambda - \lambda_i$ (see Appendix D.2 and decomposition (D.5)). This requirement always is met when V is over the field $\mathbb{C}$ or over any algebraically closed field (see the remark at the end of Appendix D.2).

Applying results of previous section to λ_1 we get the generalised eigenspace G_{λ_1} (with dimension t_1 and with a basis E_1 composed as (25.4)) and the range R_1 such that $V = G_{\lambda_1} \oplus R_1$ by Lemma 25.15. On E_1 the restriction $T|_{G_{\lambda_1}}$ has the matrix A_1 of triangle shape (25.5) from which it is clear that the characteristic polynomial of the restriction $T|_{G_{\lambda_1}}$ is $(\lambda_1 - \lambda)^{t_1}$ (notice that λ no longer means a specific eigenvalue, but it acts as a variable in polynomial).

By Lemma 25.15 and by (25.2) the characteristic polynomial $f(\lambda)$ of T is of form $f(\lambda) = (\lambda_1 - \lambda)^{t_1} f_2(\lambda)$, where $f_2(\lambda)$ is the characteristic polynomial of the restriction $T|_{R_1}$ of T on R_1.

If λ_1 were a root for $f_2(\lambda)$, then by Theorem 23.17 the subspace R_1 would contain an eigenvector corresponding to λ_1 (for transformation $T|_{R_1}$ and, thus, also for T). But since all such eigenvectors already are loaded into G_{λ_1}, then λ_1 is *not* a root for $f_2(\lambda)$, and *all* linear factors $\lambda_1 - \lambda$ of $f(\lambda)$ already are in $(\lambda_1 - \lambda)^{t_1}$ and, thus, $t_1 = \dim(G_{\lambda_1})$ is the algebraic multiplicity of λ_1. And in the basis E_1 of G_{λ_1} the restriction $T|_{G_{\lambda_1}}$ has a matrix A_1 (of degree t_1) in triangle from (25.5), with λ_1 on diagonal.

Repeat the above consideration taking R_1 as new V, and $T|_{R_1}$ as new T. The second eigenvalue λ_2 is a root of $f_2(\lambda)$ and, thus, R_1 contains the generalized eigenspace G_{λ_2} (of dimension t_2) and the respective range R_2. On G_{λ_2} the restriction $T = T|_{R_1}$ has a basis E_2 of t_2 vectors of type (25.4), on which it has a matrix A_2 in triangle from (25.5), with λ_2 on its diagonal. Thus, $f_2(\lambda) = (\lambda_2 - \lambda)^{t_2} f_3(\lambda)$, and and all linear factors $\lambda_2 - \lambda$ of $f(\lambda)$ already are in $(\lambda_2 - \lambda)^{t_2}$. We have $V = G_{\lambda_1} \oplus R_1 = G_{\lambda_1} \oplus G_{\lambda_2} \oplus R_2$ (see Exercise E.16.9).

Continuing by induction we on the k'th step get the direct decomposition

$$\boldsymbol{V = G_{\lambda_1} \oplus \cdots \oplus G_{\lambda_k}}. \tag{25.6}$$

such that in the combined basis $E = E_1 \cup \cdots \cup E_k$ the transformation T has the block-diagonal matrix:

$$A = [T]_E = \begin{bmatrix} A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A_k \end{bmatrix}, \tag{25.7}$$

and the characteristic polynomial of T has the decomposition

$$|\boldsymbol{A}-\boldsymbol{\lambda I}| = \boldsymbol{f(\lambda)} = (\boldsymbol{\lambda_1}-\boldsymbol{\lambda})^{t_1}\cdots(\boldsymbol{\lambda_k}-\boldsymbol{\lambda})^{t_k} = |\boldsymbol{A_1}-\boldsymbol{\lambda I}|\cdots|\boldsymbol{A_k}-\boldsymbol{\lambda I}|.$$

This brings us to an interesting generalization of results of Section 24.4:

Remark 25.19. By Lemma 24.22 the geometric multiplicity $\dim\big(E_{\lambda_s}\big)$ of any eigenvalue λ_s is less than or equal to its algebraic multiplicity. The algebraic multiplicity turned out to be the $\dim\big(G_{\lambda_s}\big)$. I.e., whenever the factor $(\lambda_s-\lambda)^{t_s}$ is present in factorisation of the characteristic polynomial $f(\lambda)$, we have a sequence of nested kernels:

$$\boldsymbol{E_{\lambda_s}} = \ker(N) \subset \ker\big(N^2\big) \subset \cdots \subset \ker\big(N^{r-1}\big) \subset \ker(N^r) = \boldsymbol{G_{\lambda_s}}$$

for $N = T-\lambda_s I$. The condition of Theorem 24.23 can be translated to: $E_{\lambda_s} = G_{\lambda_s}$ for each λ_s (i.e., each block of type (25.5) contains no zeros above the diagonal), and the sum of degrees of those blocks is the dimension of the entire space. And Theorem 24.28 states that, if we are over $\mathbb{C}$ (or other algebraically closed field), then the condition about the sum of degrees can be dropped.

Example 25.20. Let us continue the above Example 25.16. The transformation T on the basis

$$E = \left\{\begin{bmatrix}1\\1\\1\end{bmatrix}, \begin{bmatrix}2\\1\\0\end{bmatrix}, \begin{bmatrix}1\\2\\4\end{bmatrix}\right\}$$

has the matrix

$$B = \begin{bmatrix}1 & -1 & 0\\0 & 1 & 0\\0 & 0 & 2\end{bmatrix},$$

with the first two vectors of E being the basis for $G_1 = \ker\big(N^2\big)$ for $\lambda_1 = 1$ where $N = T-\lambda_1 I = T-I$.

And for $\lambda_2 = 2$ and $N = T-\lambda_2 I = T-2I$ the generalized eigenspace G_2 by Lemma 25.14 is inside the range

$$R = \operatorname{span}\left(\begin{bmatrix}1\\2\\4\end{bmatrix}\right).$$

As direct computation shows

$$(T-\lambda_2 I)\begin{bmatrix}1\\2\\4\end{bmatrix} = \begin{bmatrix}-2 & 1 & 0\\0 & -2 & 1\\2 & -5 & 2\end{bmatrix}\begin{bmatrix}1\\2\\4\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix},$$

and this spanning vector from range$(T-\lambda_1 I)$ actually is in $\ker(T-\lambda_2 I)$.

I.e., the generalized eigenspace G_2 is 1-demisional, and the matrix (25.7) in our case is the matrix

$$B = \begin{bmatrix}1 & -1 & 0\\0 & 1 & 0\\0 & 0 & 2\end{bmatrix} = \begin{bmatrix}A_1 & \mathbf{0}\\\mathbf{0} & A_2\end{bmatrix}$$

found in Example 25.13. Its two blocs are $A_1 = \begin{bmatrix}1 & -1\\0 & 1\end{bmatrix}$ and $A_2 = [2]$.

Exercises

E.25.1. Let T by the transformation discussed in Example 25.3 for an arbitrary value of φ. Is it true that T has no invariant subspaces other than the subspace $U = \text{span}(e_1, e_2)$ and $W = \text{span}(e_3)$? *Hint*: consider the values of φ multiple to π, and also consider Example 25.2

E.25.2. Find examples of subspaces which are *not* invariant respectively **(1)** in Example 25.3; **(2)** in Example 25.4.

E.25.3. Which is the number of invariant subspaces in Example 25.9 if: **(1)** None of φ and θ is a multiple of π; **(2)** One of φ or θ is a multiple of π, and the other is not; **(3)** Both φ and θ are a multiples of π.

E.25.4. Find the sequence (25.3) and the decomposition $V = G_\lambda \oplus R$ of Lemma 25.14, if $V = \mathcal{P}_3(\mathbb{R})$ and $T\big(f(x)\big) = f'(x)$ is the transformation of derivation.

E.25.5. Find the decomposition (25.6) for the transformation given by the matrix:

$$A = \begin{bmatrix} 3 & 0 & 0 & 0 \\ -10 & -1 & 0 & 1 \\ 22 & 8 & 3 & -2 \\ 10 & -1 & 0 & -3 \end{bmatrix}.$$

CHAPTER 26

The Jordan normal form

26.1. The Jordan blocks and the Jordan decomposition $P^{-1}AP = J$

A *Jordan block* is a square matrix $J(\lambda, r) \in M_{r,r}(F)$ of the following type:

$$J(\lambda, r) = \begin{bmatrix} \lambda & 1 & & & \mathbf{0} \\ & \lambda & 1 & & \\ & & \ddots & & \\ & & & \lambda & 1 \\ \mathbf{0} & & & & \lambda \end{bmatrix}. \tag{26.1}$$

A matrix $J \in M_{n,n}(F)$ is in *Jordan normal form*, if it is a block-diagonal matrix

$$J = \begin{bmatrix} J(\lambda_1, r_1) & & & \mathbf{0} \\ & J(\lambda_2, r_2) & & \\ & & \ddots & \\ \mathbf{0} & & & J(\lambda_k, r_k) \end{bmatrix} \tag{26.2}$$

(the values $\lambda_1, \dots, \lambda_k$ need not be distinct). In the literature this form also is called *Jordan canonical form*.

Example 26.1. Consider the Jordan blocks:

$$J(2,3) = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix},$$

$$J(2,1) = [2],$$

$$J(-1,1) = [-1].$$

Here is a 5×5 matrix consisting of these blocts:

$$J = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} J(2,3) & & \mathbf{0} \\ & J(2,1) & \\ \mathbf{0} & & J(-1,1) \end{bmatrix}.$$

Below we are going to meet these blocks and this matrix again.

Notice that the matrix J may contain more than one blocks $J(\lambda, r)$ with the same λ or with the same r. The above matrix contains two blocks $J(2,3)$ and $J(2,1)$ for the same the same $\lambda = 2$. The matrix

$$J' = \begin{bmatrix} J(2,1) & & \mathbf{0} \\ & J(-1,1) & \\ \mathbf{0} & & J(2,3) \end{bmatrix}$$

consists of the same blocks, just placed in a different *order* on the diagonal. We say that J' is obtained from J by *permutations of Jordan blocks*, or that J' and J are equal *up to permutations of Jordan blocks*.

You surely have already noticed how similar is the Jordan normal form J to diagonal form D studied earlier. So to say, J is in an "almost" diagonal form, and differs from D by some entries which can be 1 just above the diagonal. In Section 24.1 we studied diagonalizability of matrices, and found criteria under which the given matrix A can *or* cannot have the diagonalization $P^{-1}AP = D$, i.e., A is *or* is not similar to some D. Interestingly, even if a matrix A is not similar to some diagonal matrix D, it still is similar to a matrix J in Jordan normal form, at least over the complex field $\mathbb{C}$.

Theorem 26.2 (Jordan's Theorem)**.** *Let T be a transformation of a vector space V over $\mathbb{C}$. There is a basis E of V on which the matrix A of T is in Jordan normal form*

$$\boldsymbol{A = [T]_E = J.}$$

J is unique up to permutations of Jordan blocks.

Since both A and J are matrices of the same transformation in respective bases of V, we for some change of basis matrix P by Theorem 20.26 get:

Corollary 26.3. *Any complex square matrix $A \in M_{n,n}(\mathbb{C})$ is similar to a matrix J in Jordan normal form. That is, there is an invertible matrix $P \in M_{n,n}(\mathbb{C})$ such that*

$$\boldsymbol{P^{-1}A\,P = J.}$$

J is unique up to permutations of Jordan blocks.

The above presentation $P^{-1}A\,P = J$ or, equivalently, the presentation $A = P\,JP^{-1}$ is called *Jordan decomposition*.

In fact, Theorem 26.2 and Corollary 26.3 are true not only for complex spaces and matrices, but for any *algebraically closed* field (see Appendix D.2).

26.2. Construction of the Jordan decomposition

Turning to the proof of Theorem 26.2 let us make a few agreements which will much simplify the wording below. Since in the proof below we are going to consider one generalized eigenspace for a single eigenvalue at a time, let us simplify the notations by denoting by $\lambda = \lambda_s$ one of the eigenvalues $\lambda_1, \ldots, \lambda_k$ of our transformation. Also set $T = T|_{G_\lambda} = T|_{G_{\lambda_s}}$ to denote a restriction. We still use our earlier notations $N = T - \lambda I$ and $N = A - \lambda I$.

By Lemma 25.15 T has a triangle matrix of type (25.5) on a basis of type (25.4). Let us modify the basis to get a matrix even simpler than (25.5). Start by the vectors

$$u_1, \ldots, u_m \tag{26.3}$$

which we found in $\ker(N^r) \setminus \ker\big(N^{r-1}\big)$ for (25.4) (the vectors (26.3) can be found continuing any basis of $\ker\big(N^{r-1}\big)$ to a basis of $\ker(N^r)$, say, by Algorithm 16.6) The images $N(u_1), \ldots, N(u_m)$ belong to $\ker\big(N^{r-1}\big)$ because $N^{r-1}\big(N(u_i)\big) = N^r(u_i) = 0$, but these images do *not* belong to $\ker\big(N^{r-2}\big)$ because $N^{r-2}\big(N(u_i)\big) = 0$ would mean that $N^{r-1}(u_i) = 0$, whereas we have selected the vectors u_i to be outside $\ker\big(N^{r-1}\big)$.

Show that the vectors $u_1, \ldots, u_m$; $N(u_1), \ldots, N(u_m)$ are not only linearly independent, but their linear combination is in $\ker\big(N^{r-2}\big)$ only if it is a trivial combination. If

$$c_1u_1 + \cdots + c_mu_m \;+\; d_1N(u_1) + \cdots + d_mN(u_m) \in \ker\big(N^{r-2}\big),$$

then

$$c_1u_1 + \cdots + c_mu_m = -d_1N(u_1) - \cdots - d_mN(u_m) \in \ker\big(N^{r-1}\big)$$

which only is possible when $c_1, \ldots, c_m = 0$. Then

$$d_1N(u_1) + \cdots + d_mN(u_m) = N(d_1u_1 + \cdots + d_mu_m) \in \ker\big(N^{r-2}\big)$$

and so

$$d_1u_1 + \cdots + d_mu_m \in \ker\big(N^{r-1}\big)$$

which only is possible, when $d_1, \ldots, d_m = 0$.

Since the linearly independent vectors $N(u_1), \ldots, N(u_m)$ all are outside $\ker\big(N^{r-2}\big)$, we can add some new vectors $v_1, \ldots, v_s$ so that the vectors

$$N(u_1), \ldots, N(u_m)\ ;\ v_1, \ldots, v_p \tag{26.4}$$

together with any basis of $\ker\big(N^{r-2}\big)$ form a basis for $\ker\big(N^{r-1}\big)$.

Repeating the step consider the images

$$N^2(u_1), \ldots, N^2(u_m)\ ;\ N(v_1), \ldots, N(v_p). \tag{26.5}$$

It is easy to show that they all are in $\ker\big(N^{r-2}\big)$. Moreover, the union of all vectors in (26.3), (26.4), (26.5) is not only linearly independent, but their linear combination is in $\ker\big(N^{r-3}\big)$, only if it is a trivial combination. We can add to that union some new vectors $w_1, \ldots, w_q$ so that the new set together with any basis of $\ker\big(N^{r-3}\big)$ form a basis for $\ker\big(N^{r-2}\big)$.

Continuing the process by induction we on the r'th step add the last portion of vectors $z_1, \ldots, z_c$, and get a basis for entire G_λ consisting of $t = mr + (m-1)p + (m-2)q + \cdots + c$ vectors in total:

$$\begin{array}{llll}
u_1, \ldots, u_m; & & & \\
N(u_1), \ldots, N(u_m); & v_1, \ldots, v_p; & & \\
N^2(u_1), \ldots, N^2(u_m); & N(v_1), \ldots, N(v_p); & w_1, \ldots, w_q; & \\
\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \\
N^{r-1}(u_1), \ldots, N^{r-1}(u_m); & N^{r-2}(v_1), \ldots, N^{r-2}(v_p); & N^{r-3}(w_1), \ldots, N^{r-3}(w_q); & \ldots; z_1, \ldots, z_c.
\end{array} \tag{26.6}$$

This already is the basis E we are looking for.

Denote $e_1 = N^{r-1}(u_1), \ldots, e_{r-1} = N(u_1),\ e_r = u_1$ and set $V_1 = \operatorname{span}(e_1, \ldots, e_r)$, i.e., V_1 is the span of vectors in the 1'st column of the system (26.6)). V_1 is T-invariant. Indeed, since $T(v) = N(v) + \lambda v$ for any $v \in V$, we have $T(u_1) = N(u_1) + \lambda u_1 \in V_1$, and $T\big(N(u_1)\big) = N^2(u_1) + \lambda N(u_1) \in V_1$, etc...

Let us show that the matrix of $T|_{V_1}$ in this basis is a Jordan block. $(T - \lambda I)(e_1) = N(e_1) = N^r(u_1) = 0$, i.e., $T(e_1) = \lambda e_1$ and the 1'st column of the matrix of $T|_{V_1}$ starts by 1 followed by zeros, i.e., we get the frist column of (26.1). Next, $(T - \lambda I)(e_2) = N(e_2) = N^{r-1}(u_1) = e_1$, i.e., $T(e_2) = e_1 + \lambda e_2$ and the 2'nd column of the matrix starts by 1, then λ followed by zeros, i.e., we get the 2'nd column of (26.1). Continuing the process we fill-in the matrix (26.1).

In analogy with V_1 define further subspaces as spans of columns in (26.6):

$$V_2 = \operatorname{span}\big(N^{r-1}(u_2), \ldots, u_2\big); \ldots; V_{m+1} = \operatorname{span}\big(N^{r-2}(v_1), \ldots, v_1\big); \ldots; V_d = \operatorname{span}(z_c),$$

where $d = m + s + q + \cdots + c$. They all are invariant subspaces, and in each V_i the restriction $T|_{V_i}$ will have a matrix of type (26.1) (perhaps of degree smaller than r).

Now the main job is done, and it remains to enjoy the construction of the Jordan normal form. Since the union of bases of $V_1, \ldots, V_d$ (i.e., of columns of (26.6)) is the basis E for entire G_λ, we by point 3 of Theorem 16.21 have

$$G_\lambda = V_1 \oplus \cdots \oplus V_d.$$

Since on each V_i the restriction of T has a Jordan block matrix of type (26.1), then by (25.1) we get that the matrix of T in G_λ is a block-diagonal matrix (all blocks being for the same eigenvalue).

Now go back to the general situation, where T is a transformation on entire space V. Since by (25.6) the entire space $V = G_{\lambda_1} \oplus \cdots \oplus G_{\lambda_k}$ is a direct sum of generalized eigenspaces on each of which the restriction $T|_{G_{\lambda_i}}$ as we just saw has a block-diagonal form, we again apply (25.1) to get the Jordan normal form (26.2) we are looking for.

And *uniqueness* of the Jordan normal form follows from the observation that the degrees of Jordan blocks are determined by the dimensions of the kernels of N^i computed for different i and different eigenvalues λ_s. None of them depends on the choice of basis, so J is unique up to permutations of blocks (blocks will stand in other order, if we reorder the columns of the system (26.6)). The proof of Theorem 26.2 is completed.

How to find the Jordan decomposition of a matrix. The applications of the Jordan normal form often use not just the Jordan matrix J but also the invertible matrix P for the decomposition $P^{-1}AP = J$. Thus, we suggest an algorithm of the Jordan normal form J computation together with calculation of the matrix P.

Improvements shortening some steps of this algorithm are possible. They are not included in the pseudocode below but are considered in examples below.

Algorithm 26.4 (Computation of the Jordan normal form and Jordan decomposition of a matrix)**.** We are given a matrix $A \in M_{n,n}(\mathbb{C})$, and we know its eigenvalues $\lambda_1, \dots, \lambda_k$.
► Compute the Jordan normal form J, and write Jordan decomposition $P^{-1}AP = J$, where P is an invertible matrix.

1. Write the characteristic polynomial $f(\lambda) = |A - \lambda I|$ of A.
2. Find the eigenvalues anf their algebraic multiplicities from the decomposition $f(\lambda) = (\lambda_1 - \lambda)^{t_1} \cdots (\lambda_k - \lambda)^{t_k}$.
3. Set zero matrices J and P in $M_{n,n}(\mathbb{C})$.
4. For each $s = 1, \dots, k$
5. Set $N = A - \lambda_s I$;
6. Set $d_1 = \text{nullity}(N)$, $\dots$, $d_{r-1} = \text{nullity}\big(N^{r-1}\big)$, $d_r = \text{nullity}(N^r) = t_s$ (continue till the r'th step when $\text{nullity}(N^r) = t_s$ is achieved);
7. Add to J the Jordan blocks corresponding to λ_s. We have:
d_1 Jordan blocks in *total* corresponding to λ_s, of which:
$d_2 - d_1$ blocks of degree *at least* 2,
$d_3 - d_2$ blocks of degree *at least* 3,
....
$d_{r-1} - d_{r-2}$ blocks of degree *at least* $r - 1$,
$d_r - d_{r-1}$ blocks of degree *exactly* r (start by these blocks, then go upwards).
8. Find bases for null spaces (kernels) $\ker(N), \dots, \ker(N^r)$ by Algorithm 15.2;
9. Set $E = \emptyset$ and $\mathcal{E} = \emptyset$;
10. For each $i = r, \dots, 1$
11. Add to $\mathcal{E}$ any vectors from the basis of $\ker\big(N^i\big)$ which form a basis for $\ker\big(N^i\big)$ together with any basis of $\ker\big(N^{i-1}\big)$ (we may use Algorithm 16.6);
12. Set $E = E \cup \mathcal{E}$;
13. If $i > 1$ replace the vectors of $\mathcal{E}$ by their images under N.
14. E is the basis (26.6) for λ_s. Add its vectors as columns of P in reverse order.
15. Compute the inverse P^{-1} by Algorithm 6.10.
16. Output the matrix J.
17. Output the equality $P^{-1}AP = J$ with matrices P, J, P^{-1} computed above.

Example 26.5. A simple case of Jordan normal form, clearly, is when the matrix is diagonalizable. Considered the real transformation T given by its matrix:

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

with characteristic polynomial $f(\lambda) = -(\lambda+3)(\lambda+9)\lambda$, and with three eigenvalues $\lambda_1 = -3$, $\lambda_2 = -9$, $\lambda_3 = 0$.

For each eigenvalue the geometric and the algebraic multiplicities both are equal to 1. So for each $s = 1, 2, 3$ the eigenspace E_{λ_s} coincides with the generalized eigenspace G_{λ_s} (or, in terms of the sequence (25.3), we have $r = 1$ for each $s = 1, 2, 3$).

We have three Jordan blocks of degree 1 each: $J(-3,1) = [-3]$, $J(-9,1) = [-9]$, $J(0,1) = [0]$, and so the Jordan normal form is

$$J = \begin{bmatrix} -3 & 0 & 0 \\ 0 & -9 & 0 \\ 0 & 0 & 0 \end{bmatrix} = D.$$

The respective basis and the change of basis matrix P are computed in Example 24.10:

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

As it is easy to verify:

$$P^{-1}AP = J = D,$$

i.e., the Jordan normal form coincides to diagonalization of A.

Example 26.6. Let us build the Jordan decomposition for

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

Its characteristic polynomial is $f(\lambda) = -\lambda^3 + 3\lambda^2 - 3\lambda + 1 = -(1-\lambda)^3$, i.e., we have one eigenvalue $\lambda = 1$ of algebraic multiplicity 3. Since $f(\lambda)$ is a product of its real linear factors, the Jordan normal form of A is real.

Bring to the reduced row-echelon form the matrix $N = A - \lambda I$ for $\lambda = 1$:

$$N = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ -1 & -2 & -3 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Thus, $\operatorname{rank}(N) = 1$ and $d_1 = \operatorname{nullity}(N) = 3 - 1 = 2$, i.e., we have 2 Jordan blocks corresponding to $\lambda = 1$. We already are able to deduce that

$$J = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} J(1,2) & \mathbf{0} \\ \mathbf{0} & J(1,1) \end{bmatrix}$$

(because this is the only way to fit two Jordan blocks in a 3×3 matrix, up to the order of blocks).

To find the matrix P we need more information. Apply Algorithm 15.2 to compute a basis for $\ker(N)$:

$$\begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix}$$

(this is why we computed $\operatorname{rref}(N)$ above).

According to our construion the respective basis in $V = G_1$ will be of shape:

$$\begin{aligned} &u_1; \\ &N(u_1); \quad v_1 \end{aligned}$$

(compare with (26.6)), where u_1 is any vector in $V = \ker(N^2)$ not belonging to $\ker(N)$, and forming a basis for V together with any basis of $\ker(N)$. Such a basis is found above by Algorithm 16.6, or we can take, say:

$$u_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

(just because it is independent with the above basis of $\ker(N)$). Then

$$N(u_1) = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix},$$

and by logic of the proof $N(u_1)$ falls into the eigenspace $\ker(N)$, and we must continue it to a basis for $\ker(N)$ by one vector v_1. We know a basis for $\ker(N)$, so we take any one of its vectors (just making sure it is linearly independent with $N(u_1)$):

$$v_1 = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix},$$

and then form the matrix:

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

The Jordan decomposition

$$P^{-1}AP = J$$

is easy to verify.

Example 26.7. The transformation T is given on $\mathbb{R}^5$ by the matrix

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

Find its Jordan normal form, compute the respective basis and the matrix P.

The characteristic polynomial $|A - \lambda I| = f(\lambda) = -\lambda^5 + 7\lambda^4 - 16\lambda^3 + 8\lambda^2 + 16\lambda - 16$ is easy to factorize applying Laplace expansion to the determinant of $A-\lambda I$:

$$f(\lambda)=-(\lambda-2)^4(\lambda+1).$$

We have two eigenvalues $\lambda_1=2$ and $\lambda_2=-1$ of algebraic multiplicities 4 and 1 respectively. Since $f(\lambda)$ is a product of its real linear factors, A does have a real Jordan normal form.

Let us start by the simpler case of $\lambda_2=-1$. Since its algebraic multiplicity and geometric multiplicity both are 1, we have only one Jordan block $J(-1,1)=[-1]$ of degree 1. As an eigenvector w corresponding to it take

$$w=\begin{bmatrix}0\\1\\0\\0\\0\end{bmatrix},$$

which can be computed as a basis for null(N) with $N=A-\lambda_2 I=A+I$.

Turn to the eigenvalue $\lambda_1=2$, and set:

$$N=A-\lambda_1 I=A-2I=\begin{bmatrix}0&0&0&-1&0\\0&-3&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\1&0&0&0&0\end{bmatrix}.$$

If we only wanted to find the Jordan normal form J for A without the respective basis and without the matrix P, we would only need the nullity of N. But since we want to get the complete Jordan decomposition $P^{-1}AP=J$, we need a *basis* for null space of N also. To use Algorithm 15.2 we reduce:

$$N\sim\begin{bmatrix}\mathbf{1}&0&0&0&0\\0&\mathbf{1}&0&0&0\\0&0&0&\mathbf{1}&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}=\text{rref}(N).$$

So rank$(N)=3$ and $d_1=$ nullity$(N)=5-3=2$. As a basis for ker(N) take:

$$\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}.$$

Next compute N^2 and rref(N^2):

$$N^2=\begin{bmatrix}0&0&0&0&0\\0&9&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&-1&0\end{bmatrix}\sim\begin{bmatrix}0&\mathbf{1}&0&0&0\\0&0&0&\mathbf{1}&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}=\text{rref}(N^2).$$

Thus, rank$(N^2)=2$ and $d_2=$ nullity$(N^2)=5-2=3$. As a basis for ker(N^2) take:

$$\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}.$$

(Notice that some of the vectors of this bases already are included in the previous basis, but this may not be so, in general. All we can say is that these vectors span a larger subspace.)

We already can tell the value of d_3 *without* computing rank(N^3) because we know that $d_3>d_2$, and we know that the maximum of parameters d_i is $t_1=\dim(G_{\lambda_1})=4$. So the only possible option is $d_3=4$ (i.e., in (25.3) we have $r=3$). However, to find P we still need a basis of ker(N^3). Thus, we have to compute:

$$N^3=\begin{bmatrix}0&0&0&0&0\\0&-27&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}\sim\begin{bmatrix}0&\mathbf{1}&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix}=\text{rref}(N^3).$$

As a basis for ker(N^3) take:

$$\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix},\quad\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}.$$

An important *new* signal we get here is that d_3 already is equal to algebraic multiplicity 4 of eigenvalue $\lambda_1=2$, i.e., to the dimension of the generalized eigenspace G_2. This means that all the needed powers N,N^2,N^3 are already discussed (with $3=r$).

Here is the information about the Jordan blocks we collected. For $\lambda_1=2$ we have:

$d_1=2$ Jordan blocks, of which

$d_2-d_1=1$ blocks of degree *at least* 2,

$d_3-d_2=1$ blocks of degree *exactly* 3.

Plus, as mentioned above, we have only one Jordan block of degree 1 corresponding to $\lambda_2=-1$.

Start the Jordan matrix assembly process by the largest blocks. Besides the block $J(2,3)$ only one block $J(2,1)$ is fitting. Plus, one more block $J(-1,1)$ need be added for $\lambda_2=-1$. We get the Jordan normal form:

$$J=\begin{bmatrix}2&1&0&0&0\\0&2&1&0&0\\0&0&2&0&0\\0&0&0&2&0\\0&0&0&0&-1\end{bmatrix}=\begin{bmatrix}J(2,3)&&\mathbf{0}\\&J(2,1)&\\\mathbf{0}&&J(-1,1)\end{bmatrix}.$$

Now find a *basis* on which T has the Jordan normal matrix J. By our construion the basis in generalized eigenspace G_2 will be of shape:

$$\begin{aligned}&u_1;\\&N(u_1);\\&N^2(u_1);\quad v_1\end{aligned}$$

(see the system (26.6)). Here u_1 is a vector in $G_2 = \ker\big(N^3\big)$ not belonging to $\ker\big(N^2\big)$, and forming a basis for $\ker\big(N^3\big)$ together with any basis of $\ker\big(N^2\big)$.

To continue these bases we could use Algorithm 16.6, but in our example it is not needed, as comparing the above computed bases for $\ker\big(N^3\big)$ and $\ker\big(N^2\big)$ we can simply take

$$u_1 = \begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}.$$

Compute the images of u_1 under N and N^2:

$$N(u_1) = \begin{bmatrix}-1\\0\\0\\0\\0\end{bmatrix},\quad N^2(u_1) = \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}.$$

By the earlier proof $N^2(u_1)$ falls into the eigenspace $\ker(N)$, and we need continue it to a basis for $\ker(N)$ by some vector v_1. Since a basis for $\ker(N)$ already is found, simply take

$$v_1 = \begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}.$$

Now we can assemble the matrix P as:

$$\begin{aligned}P &= [N^2(u_1)\ N(u_1)\ u_1\ v_1\ w]\\ &= \begin{bmatrix}0&-1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\\-1&0&0&0&0\end{bmatrix}.\end{aligned}$$

The inverse P^{-1} can be computed by the Gauss-Jordan method, or we can notice that P is an *orthogonal* matrix and so:

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

We got the Jordan decomposition:

$$P^{-1}AP = J = \begin{bmatrix}J(2,3)&&\mathbf{0}\\&J(2,1)&\\\mathbf{0}&&J(-1,1)\end{bmatrix} = [T]_E$$

on the basis $E = \{N^2(u_1),\ N(u_1),\ u_1,\ v_1,\ w\}$.

Example 26.8. To show a *possible* simplification in the process let us turn back to to the transformation given by matrix

$$A = \begin{bmatrix}0&1&0\\0&0&1\\2&-5&4\end{bmatrix}$$

in Example 24.11. It has the characteristic polynomial $f(\lambda) = -(\lambda-1)^2(\lambda-2)$, and two eigenvalues $\lambda_1 = 1$, $\lambda_2 = 2$.

As we have seen in Example 24.11, A is *not* diagonalizable, since the geometric multiplicity of $\lambda_1 = 1$ is equal to 1, and is strictly less than its algebraic multiplicity 2. As to $\lambda_2 = 2$, its geometric and algebraic multiplicities both are 1. A has a real Jordan normal form since the eigenvalues are real. We can already guess the Jordan normal form:

$$J = \begin{bmatrix}1&1&0\\0&1&0\\0&0&2\end{bmatrix} = \begin{bmatrix}J(1,2)&\mathbf{0}\\\mathbf{0}&J(2,1)\end{bmatrix}$$

because there is only one option for Jordan block for $\lambda_2 = 2$, namely, $J(2,1) = [2]$, and there are *two* options for Jordan blocks for $\lambda_1 = 1$, namely, we have either *one* block

$$J(1,2) = \begin{bmatrix}1&1\\0&1\end{bmatrix},$$

or *a pair* of blocks $J(1,1) = [1]$. The second option is ruled out, as it would mean that A is diagonalizable, which is not so. So J is built by $J(1,2)$ and $J(2,1)$.

As the third column of P, i.e., as the third vector in the basis we can take the eigenvector

$$w = \begin{bmatrix}1\\2\\4\end{bmatrix}$$

computed for E_2 in Example 24.11. From Example 24.11 we also know a vector

$$h_1 = \begin{bmatrix}1\\1\\1\end{bmatrix}.$$

in E_1. We can a little simplify the process here. Since E_1 is *one dimensional*, it is enough to take such a pre-image of h_1 under N which is linearly independent with h_1. To find that pre-image just solve the system:

$$N\begin{bmatrix}x\\y\\z\end{bmatrix} = h_1,$$

i.e.,

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

Since

$$\begin{bmatrix} -1 & 1 & 0 & 1 \\ 0 & -1 & 1 & 1 \\ 2 & -5 & 3 & 1 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & 0 & -1 & -2 \\ 0 & \mathbf{1} & -1 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

as the pre-image we can take

$$h_2 = \begin{bmatrix} -2 \\ -1 \\ 0 \end{bmatrix}.$$

The matrix $P = [h_1 \ h_2 \ w]$ is:

$$P = \begin{bmatrix} 1 & -2 & 1 \\ 1 & -1 & 2 \\ 1 & 0 & 4 \end{bmatrix}.$$

It is easy to verify the Jordan decomposition

$$P^{-1}AP = J.$$

Hint. As the above example shows, the Jordan normal form computation can be simplified, if we for some reason know that *only one* Jordan block is present for each eigenvalue λ_s, i.e., if the system (26.6) consists of one column only each λ_s. Then the eigenspace $E_\lambda = \ker(N)$ is 1-dimensional. Denote by h_1 any vector spanning $\ker(N)$.

Find any pre-image of h_1 (linearly independent with h_1) under N. This can be done by solving the system of linear equations

$$N \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = h_1.$$

Denote the found solution by h_2. Since $\ker(N^2)$ is 2-dimensional, h_1, h_2 are forming a basis for $\ker(N^2)$.

Since $\ker(N^3)$ is 3-dimensional, and since we already have two vectors, we just add the next vector h_3 as a solution of the system

$$N \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = h_2$$

(linearly independent to h_1, h_2).

Continue this process till all r vectors $h_1, \dots, h_r$ are found (r is the degree of the only Jordan block for λ_s, i.e., the dimension of G_{λ_s}).

In other words, we are filling-in the single column of system (26.6) from the bottom to the top, and not vise versa.

Warning! In some sources the above hint with pre-images is suggested as a general method for Jordan normal form calculation for *any* matrix. Since this prejudice is surprisingly popular, let us intentionally warn: if $\ker(N)$ is not 1-dimensional, then we cannot be sure that the pre-images of the given basis vectors for $\ker(N)$ do belong to $\ker(N^2)$. The next example illustrates that danger:

Example 26.9. Turn back to the matrix

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

from Example 26.6. We have already found the characteristic polynomial $f(\lambda) = -(1-\lambda)^3$ and the only eigenvalue $\lambda = 1$. We also know that the matrix

$$N = A - \lambda I = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ -1 & -2 & -3 \end{bmatrix}$$

is or rank 1, i.e., $d_1 = \text{nullity}(N) = 3 - 1 = 2$. And we have found a basis for $\ker(N)$:

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

Can we build the other vectors of the system (26.6) computing the pre-images of these basis vectors? *No*, because both systems of linear equations

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ -1 & -2 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ -1 & -2 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix}$$

are *inconsistent*. So pride of prejudice above is unreasonable.

Exercises

E.26.1. We are given the real matrix

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

(1) Detect, if A can be brought to a *real* Jordan normal form J, and find J for A, if possible. **(2)** Find the Jordan decomposition $P^{-1}AP = J$. **(3)** Apply the hint mentioned after Exercise 26.8 to this case (first detect, if that hint can be applied, at all).

Solution: **E.26.1**. The characteristic polynomial is $f(\lambda) = -(\lambda-2)^2(\lambda+1)$, i.e., $\lambda_1 = 2$, $\lambda_2 = -1$. $f(\lambda)$ is a product of its *real* linear factors, so A *can* be brought to a *real* Jordan normal form J. We have one block $J(\lambda_2, 1) = [-1]$ of degree 1. As basis vector for E_{-1} take $\left[\begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix}\right]$. For $\lambda_1 = 2$ compute $N = A - 2I = \left[\begin{smallmatrix} 0 & 4 & -3 \\ 0 & 0 & 0 \\ 0 & 3 & -3 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right] = \operatorname{rref}(N)$, which means that $\ker(N) = \operatorname{span}\left[\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right]$. Also, $d_1 = 3 - 2 = 1$, i.e., we have 1 Jordan block for $\lambda_1 = 2$. The Jordan blocks are known, and so $J = \left[\begin{smallmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right]$. We already know that $\ker\big(N^2\big) = G_2$. To find the missing one vector in G_2 compute $N^2 = \left[\begin{smallmatrix} 0 & -9 & 9 \\ 0 & 0 & 0 \\ 0 & -9 & 9 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 0 & 1 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right] = \operatorname{rref}\big(N^2\big)$, which means that $\ker\big(N^2\big) = \operatorname{span}\big(\left[\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right]\big)$ (we could again deduce that $d_2 = 3 - 1 = 2$, i.e., we have $2 - 1 = 1$ Jordan block of degree at least 2 for $\lambda_1 = 2$, but this information is not necessary). Clearly, $\left[\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right]$ together with vector $\left[\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right] \in \ker(N)$ forms a basis for $\ker\big(N^2\big)$. Thus, $P = \left[\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right]$ and $P^{-1}AP = J$. The hint given after Exercise 26.8 *can* be a applied because we have only one Jordan block for each eigenvalue. After we find $\ker(N) = \operatorname{span}\left[\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right]$ solve the system $N\left[\begin{smallmatrix} x \\ y \\ z \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right]$ by reducing $\left[\begin{smallmatrix} 0 & 4 & -3 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 3 & -3 & 0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. As a linearly independent pre-image we can take $\left[\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right]$ (or any other vector given by general solution $\alpha\left[\begin{smallmatrix} -1 \\ 0 \\ 0 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right]$). So we can put $\alpha = 0$ and get $P = \left[\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right]$, put $\alpha = -5$ and get $P = \left[\begin{smallmatrix} 1 & 5 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right]$, etc.

E.26.2. By Theorem 26.2 the matrix J of the Jordan decomposition $P^{-1}A\,P = J$ is unique for the given matrix A. Is the change of basis matrix P also unique? *Hint*: Use the solution given for Exercise E.26.1.

E.26.3. For the 7×7 matrix A we know that: A has the eigenvalue 5 of algebraic multiplicity 3 and the eigenvalue 7 of algebraic multiplicity 4. The parameters d_i for the eigenvalue 5 are: $d_1 = 1$, $d_2 = 2$, $d_3 = 3$. The parameters d_i for the eigenvalue 7 are: $d_1 = 2$, $d_2 = 4$. Can J be constructed with this information already?

Solution: **E.26.3**. J consists of three blocks $J(5,3)$, $J(7,2)$, $J(7,2)$.

E.26.4. Bring example of a matrix A such that **(1)** A is a real matrix with a Jordan normal form J, which also is a real matrix. **(2)** A is a real matrix with a Jordan normal form J, which is *not* a real matrix. **(3)** A is a complex *non*-real matrix with a Jordan normal form J, which is a real matrix.

Solution: **E.26.4**. **(2)** Take a real matrix with real characteristic polynomial $f(\lambda)$ such that $f(\lambda)$ has complex, not real roots. **(3)** Take a complex matrix with at lest one not real entry. Choose it so that all the roots of its characteristic polynomial $f(\lambda)$ are real. For example $A = \left[\begin{smallmatrix} 1 & i & i \\ 0 & 2 & i \\ 0 & 0 & 3 \end{smallmatrix}\right]$.

Part 9

Inner Product Spaces and Orthogonality

CHAPTER 27

Orthogonal systems of vectors

"Musik ist die versteckte arithmetische Tätigkeit der Seele,
die sich nicht dessen bewußt ist, daß sie rechnet."
Gottfried Wilhelm Leibniz

27.1. Orthogonal and orthonormal bases

We turn to study of linear transformation using *metrics* (vector length, angle between vectors) defined on space by dot product. Within this part we always assume the main field $F = \mathbb{R}$ is real. Also all spaces here are finite-dimensional by Agreement 11.26. Since we can present each vector $u \in V$ by the sequence of its coordinates as $u = (x_1, \dots, x_n)$, we may assume V is a subspace in $\mathbb{R}^n$.

Recall the dot product $u \cdot v$ we defined on $\mathbb{R}^n$ in Section 1.3:

$$u \cdot v = (x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = x_1 y_1 + \dots + x_n y_n.$$

Using matrix products we can represent the dot product differently. First rewrite both u and v as *column vectors*. Then the transpose u^T will be the same u written as a row vector. Then the matrix product

$$u^T v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}^T \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = [x_1, \dots, x_n] \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = [x_1 y_1 + \dots + x_n y_n] = [u \cdot v]$$

clearly consists of just one entry coinciding with the dot product $u \cdot v$. Sometimes it will be comfortable to identify this 1×1 matrix with its only entry and write

$$\boldsymbol{u \cdot v = u^T v}, \tag{27.1}$$

i.e., to switch from the dot product to matrix product.

We defined the vector's norm (length) as $|u| = \sqrt{u \cdot u}$, and the angle φ between u and v by $\cos(\varphi) = \frac{u \cdot v}{|u| \cdot |v|}$. We called u and v *orthogonal*, if $u \cdot v = 0$, and we designate this as $u \perp v$. In matrix notation of (27.1) this looks like $u^T v = 0$.

Call a set of vectors $\{v_1, \dots, v_n\}$ an *orthogonal* set, if any two distinct vectors in it are orthogonal: $v_i \cdot v_j = 0$ for any $i \neq j$. We called a vector v *normalized*, if $|v| = 1$. A vector set $\{v_1, \dots, v_n\}$ is called *orthonormal*, if it is orthogonal and each vector v_i is normalized. In particular, a basis $E = \{e_1, \dots, e_n\}$ of the space V is called an *orthogonal basis* or *orthonormal basis*, if it is orthogonal or orthonormal respectively.

Example 27.1. The standard basis of $\mathbb{R}^n$ is orthonormal. The basis

$$u_1 = \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}, \quad u_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad u_3 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$$

is different from the standard basis, but it also is orthonormal in $\mathbb{R}^3$, as well as, the following:

$$v_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}, \quad v_2 = \begin{bmatrix} 0 \\ -1 \\ 0 \end{bmatrix}, \quad v_3 = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Here is a basis in $\mathbb{R}^3$ which is orthogonal, but not orthonormal

$$w_1 = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix}, \quad w_3 = \begin{bmatrix} 0 \\ 0 \\ 4 \end{bmatrix},$$

since its vectors are not normalized. We can normalize each of these w_i, $i = 1, 2, 3$, to get an orthonormal basis. In fact, it will be the standard basis.

Let us establish some interesting properties that show why orthogonality and orthonormality are very useful, desirable features.

Firstly, orthogonality implies linear independence:

Lemma 27.2. *Any orthogonal set of non-zero vectors is linearly independent. In particular, any orthonormal set of vectors is linearly independent.*

***Proof*.** Assume $v_1, \dots, v_n$ is the set mentioned in the lemma, and

$$c_1 v_1 + \cdots + c_n v_n = 0$$

is its linear combination, where one of the coefficients is non-zero, say, $c_1 \neq 0$. Then:

$$\begin{aligned} 0 = v_1 \cdot 0 = v_1 \cdot (c_1 v_1 + \cdots + c_n v_n) &= c_1(v_1 \cdot v_1) + c_2(v_1 \cdot v_2) + \cdots + c_n(v_1 \cdot v_n) \\ &= c_1(v_1 \cdot v_1) + 0 + \cdots + 0, \end{aligned}$$

since $v_1 \cdot v_1 \neq 0$ and $v_1 \cdot v_i = 0$ for all $i = 2, \dots, n$. We get $c_1 = 0$, contradiction. □

Secondly, the coordinates of any vector in an orthonormal basis are very easy to find. No row-elimination operations (similar to those in Section 14.3) are required. All you need is to take some dot products:

Lemma 27.3. *Assume $E = \{e_1, \dots, e_n\}$ is any orthonormal basis of the space V, and the vector $v \in V$ in this basis has the coordinates $[v]_E = (a_1, \dots, a_n)$. Then $a_i = v \cdot e_i$ for all $i = 1, \dots, n$.*

***Proof*.** Show this for, say, $i = 1$. The dot product $v \cdot e_1$ is equal to

$$\begin{aligned} (a_1 e_1 + \cdots + a_n e_n) \cdot e_1 &= a_1(e_1 \cdot e_1) + a_2(e_2 \cdot e_1) + \cdots + a_n(e_n \cdot e_1) \\ &= a_1(e_1 \cdot e_1) + 0 + \cdots + 0 = a_1 \cdot 1 = a_1. \end{aligned}$$

□

This lemma implies that for any vector $v \in V$ we have:

$$\boldsymbol{v = [v]_E = (v \cdot e_1, \dots, v \cdot e_n)}.$$

Another feature of orthonormal bases is that they allow higher degree of *measurement accuracy*, as the example below shows:

Example 27.4. Assume we are given the vector $v = \overrightarrow{OA}$ in Figure 27.1. In the orthonormal (standard) basis $E = \{e_1, e_2\}$ the actual coordinates of v are $[v]_E = (2.2,\ 1.2)$.

But as it often happens in real life, we may have not the accurate point A but a approximate point A' close to it (say, if the coordinates of A were *irrational*, we will always have to give to our computer a nearby point A' with *rational* coordinates).

How close are the coordinates of $v = \overrightarrow{OA}$ and $\overrightarrow{OA'}$ in E? The coordinates of A' are $(2.3,\ 1.1)$, and they are close to the right coordinates of A up to 0.1.

Next, take the non-orthogonal basis $G = \{g_1, g_2\}$. For simplicity we have drown them so that $v = \overrightarrow{OA}$ has the coordinates $[v]_G = (1, 1)$. Use Figure 27.1 to find the coordinates of $\overrightarrow{OA'}$ in G. Do you notice that the first coordinate is much larger than 1, and the second coordinate is much less than 1? The coordinates of $\overrightarrow{OA'}$ in G are $(1.7, 0.5)$. So a *slight difference* in locations of A and A' brings to a *big difference* in their coordinates.

Having the coordinates $(1.7, 0.5)$ of A' in G we *cannot* be sure how different is this point from A actually!

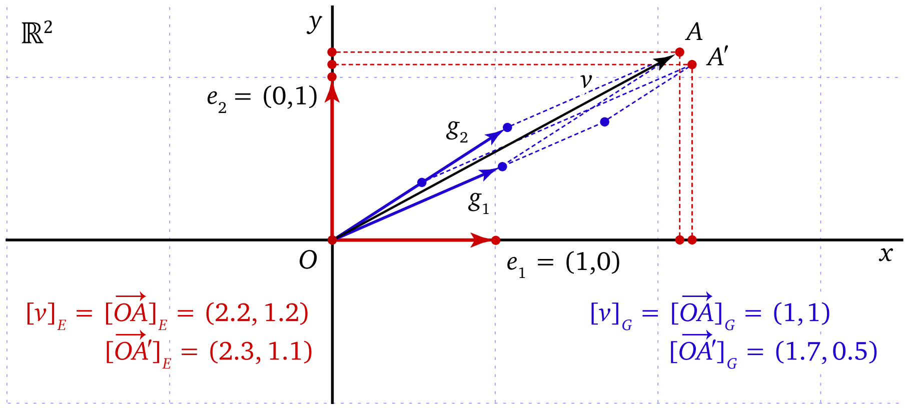


FIGURE 27.1. The measurement accuracy in two bases.

27.2. The Gram-Schmidt process

As we saw, the orthonormal bases are very helpful tools. But does *any* real space V have an orthonormal basis? And if yes, then *how to find* such a basis? The positive answer will be given by the *Gram-Schmidt orthogonalization process*: it takes any basis $v_1, \dots, v_n$ of V and transforms it to an orthonormal basis.

The method is based on the following trick. In Section 1.3 we defined the projection $\text{proj}_u(v)$ of the vector v onto u:

$$\text{proj}_u(v) = \frac{u \cdot v}{u \cdot u} u.$$

The difference $v - \text{proj}_u(v)$ is orthogonal to u because

$$u \cdot (v - \text{proj}_u(v)) = u \cdot v - u \cdot \left(\frac{u \cdot v}{u \cdot u} u \right) = u \cdot v - \frac{u \cdot v}{u \cdot u}(u \cdot u) = u \cdot v - u \cdot v = 0.$$

Take a basis $v_1, \dots, v_n$ of V and repeatedly apply the trick above. Namely:

Define $h_1 = v_1$.

Define $h_2 = v_2 - \text{proj}_{h_1}(v_2)$. It is easy to check that $h_2 \perp h_1$.

Define $h_3 = v_3 - \text{proj}_{h_1}(v_3) - \text{proj}_{h_2}(v_3)$. Easy to check that $h_3 \perp h_1$, $h_3 \perp h_2$.

On the n'th step define $h_n = v_n - \text{proj}_{h_1}(v_n) - \dots - \text{proj}_{h_{n-1}}(v_n)$. It is easy to check that $h_n \perp h_1$,..., $h_n \perp h_{n-1}$.

We got *orthogonal* vectors $h_1, \dots, h_n$.

None of the vectors h_i is zero. Indeed,

$$h_i = v_i - \text{proj}_{h_1}(v_i) - \dots - \text{proj}_{h_{i-1}}(v_i),$$

and each of the $i-1$ projections above is defined as some linear combination of $v_1, \dots, v_{i-1}$. Loading them all in above expression we (after simplification) get

$$h_i = v_i + b_1 v_1 + \cdots + b_{i-1} v_{i-1}$$

for certain coefficients $b_1, \dots, b_{i-1}$. Therefore h_i cannot be zero because it is a linear combination of some independent vectors of which at least one has a non-zero coefficient 1. By Lemma 27.2 $\{h_1, \dots, h_n\}$ is independent, so it is a basis of V.

After the orthogonal basis is found it is easy to get the orthonormal basis $E = \{e_1, \dots, e_n\}$ by normalizing each vector:

$$e_1 = \frac{1}{|h_1|} h_1, \ \dots\ , e_n = \frac{1}{|h_n|} h_n.$$

Remark 27.5. From the way we constructed the vectors h_i and e_i, $i = 1, \dots, n$, it is clear that $\operatorname{span}(v_1) = \operatorname{span}(e_1)$, $\operatorname{span}(v_1, v_2) = \operatorname{span}(e_1, e_2)$, $\dots$, $\operatorname{span}(v_1, \dots, v_i) = \operatorname{span}(e_1, \dots, e_i)$ for any $i = 1, \dots, n$.

How to find an orthonormal basis. Above we argumented the Gram-Schmidt process which transforms a given basis to an orthonormal basis:

Algorithm 27.6 (Application of the Gram-Schmidt process to a basis)**.** We are given any basis $\{v_1, \dots, v_n\}$ of a real finite-dimensional space V.

► Find an orthonormal basis of V.

1. Set $h_1 = v_1$.
2. For each $i = 2, \dots, n$ set $h_i = v_i - \operatorname{proj}_{h_1}(v_i) - \cdots - \operatorname{proj}_{h_{i-1}}(v_i)$.
3. For each $i = 1, \dots, n$ set$e_i = \frac{1}{|h_i|} h_i$.
4. Output the basis $E = \{e_1, \dots, e_n\}$.

Example 27.7. Take $v_1 = (1,1)$, $v_2 = (2,-1)$. We have:

$$h_1 = v_1 = (1,1);$$
$$h_2 = v_2 - \operatorname{proj}_{h_1}(v_2) = v_2 - \tfrac{h_1 \cdot v_2}{h_1 \cdot h_1} h_1$$
$$= (2,-1) - \tfrac{(1,1)\cdot(2,-1)}{(1,1)\cdot(1,1)}(1,1)$$
$$= (2,-1) - \tfrac{2-1}{1+1}(1,1)$$
$$= (2,-1) - \left(\tfrac{1}{2}, \tfrac{1}{2}\right) = \left(\tfrac{3}{2}, -\tfrac{3}{2}\right).$$

Since $|h_1| = \sqrt{2}$ and $|h_2| = \frac{3}{\sqrt{2}}$, we have

$$e_1 = \tfrac{1}{|h_1|} h_1 = \tfrac{1}{\sqrt{2}}(1,1) = \left(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}\right),$$
$$e_2 = \tfrac{1}{|h_2|} h_2 = \tfrac{\sqrt{2}}{3}\left(\tfrac{3}{2}, -\tfrac{3}{2}\right) = \left(\tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}}\right).$$

Example 27.8. Let V be the subspace in $\mathbb{R}^4$ spanned by three vectors:

$$v_1 = (1,-1,-1,1),$$
$$v_2 = (2,1,0,1),$$
$$v_3 = (2,2,1,2).$$

First set

$$h_1 = v_1 = (1,-1,-1,1).$$

Then

$$h_2 = v_2 - \operatorname{proj}_{h_1}(v_2) = v_2 - \tfrac{h_1 \cdot v_2}{h_1 \cdot h_1} h_1$$
$$= (2,1,0,1) - \tfrac{2}{4}(1,-1,-1,1) = \left(\tfrac{3}{2}, \tfrac{3}{2}, \tfrac{1}{2}, \tfrac{1}{2}\right).$$

Before we proceed let us do a simple trick: all we need in this step is just an *orthogonal* system. The orthogonality will not brake if we multiply h_2 by a non-zero scalar. So we can multiply h_2 by 2 in order to get rid of fractions in coordinates. We take

$$h_2 = 2\left(\tfrac{3}{2}, \tfrac{3}{2}, \tfrac{1}{2}, \tfrac{1}{2}\right) = (3,3,1,1).$$

Then find

$$h_3 = v_3 - \operatorname{proj}_{h_1}(v_3) - \operatorname{proj}_{h_2}(v_3)$$
$$= v_3 - \tfrac{h_1 \cdot v_3}{h_1 \cdot h_1} h_1 - \tfrac{h_2 \cdot v_3}{h_2 \cdot h_2} h_2$$
$$= (2,2,1,2) - \left(\tfrac{1}{4}, -\tfrac{1}{4}, -\tfrac{1}{4}, \tfrac{1}{4}\right) - \left(\tfrac{9}{4}, \tfrac{9}{4}, \tfrac{3}{4}, \tfrac{3}{4}\right)$$
$$= \left(-\tfrac{1}{2}, 0, \tfrac{1}{2}, 1\right),$$

which we can replace by

$$h_3 = 2\left(-\tfrac{1}{2}, 0, \tfrac{1}{2}, 1\right) = (-1,0,1,2).$$

In the final step we normalize the vectors:

$$e_1 = \tfrac{1}{|h_1|} h_1 = \tfrac{1}{2}(1,-1,-1,1)$$
$$= \left(\tfrac{1}{2}, -\tfrac{1}{2}, -\tfrac{1}{2}, \tfrac{1}{2}\right),$$

$$e_2 = \frac{1}{|h_2|}h_2 = \frac{1}{2\sqrt{5}}(3,3,1,1) = \left(\frac{3}{2\sqrt{5}}, \frac{3}{2\sqrt{5}}, \frac{1}{2\sqrt{5}}, \frac{1}{2\sqrt{5}}\right),$$

$$e_3 = \frac{1}{|h_3|}h_3 = \frac{1}{\sqrt{6}}(-1,0,1,2) = \left(-\frac{1}{\sqrt{6}}, 0, \frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right).$$

Exercises

E.27.1. Give an example of a set of vectors which: **(1)** is orthogonal but *not* orthonormal. **(2)** is *not* orthogonal but each vector in it is normalized.

E.27.2. We are given the vectors:

$$v_1 = (-3,5,-1), \quad v_2 = (3,2,1), \quad v_3 = (1,1,-2), \quad v_4 = (1,0,-3).$$

(1) Drop *one* of the vectors of this system to get an *orthogonal* system of vectors. **(2)** Then multiply the vectors of the obtained system by some scalars to get an *orthonormal* system. **(3)** Is the matrix, the *rows* of which are the vectors obtained in previous point, orthogonal?

E.27.3. Using the Gram-Schmidt process orthonormalize the linearly independent vectors $v_1 = (1,0,-1,0)$, $v_2 = (0,5,0,0)$, $v_3 = (0,1,0,-1)$, $v_4 = (0,0,3,1)$.

E.27.4. Check if the following vectors are linearly independent. If yes orthonormalize them by the Gram-Schmidt process: $v_1 = (1,0,-1)$, $v_2 = (0,1,1)$, $v_3 = (2,0,-1)$.

E.27.5. Find an orthonormal basis in $\mathbb{R}^3$ such that *none* of its vectors belongs to the planes xOy, yOz or zOx.

E.27.6. Build an orthonormal basis in $\mathbb{R}^3$ such that one of its vectors is collinear to $(1,1,-1)$. *Hint*: first take $v_1 = (1,1,-1)$ and choose *any* two other vectors v_2, v_3 such that the system v_1, v_2, v_3 is linearly independent. Then apply the Gram-Schmidt process on v_1, v_2, v_3.

CHAPTER 28

Orthogonal compliments and projections, least square solutions

28.1. The orthogonal complement and orthogonal subspaces

Definition 28.1. Let U be a subspace in a real space V. Then the subspace $\{w \in V \mid w \perp u \text{ for each } u \in U\}$ of vectors orthogonal to all $u \in U$ is called the *orthogonal complement* of U, and is denoted by $U^{\perp}$.

It is trivial to verify that $U^{\perp}$ actually is a *subspace* in V, so this definition is correct.

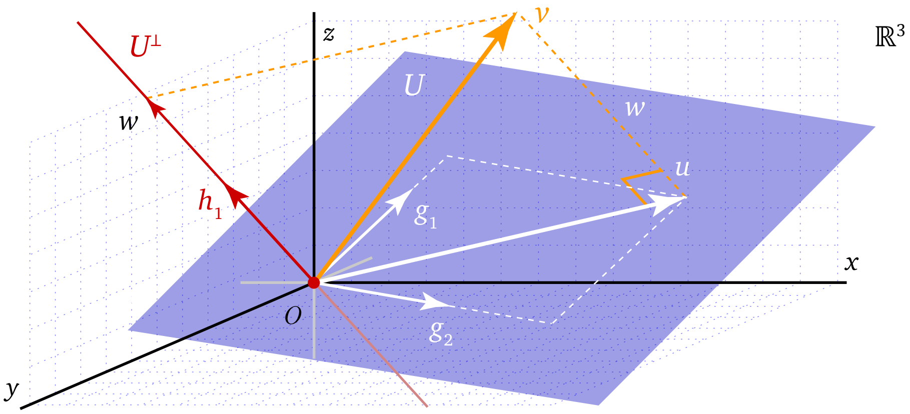


FIGURE 28.1. The orthogonal compliment $U^{\perp}$ of the plane $U = \text{span}(g_1, g_2)$.

Example 28.2. In $V = \mathbb{R}^2$ any two orthogonal lines passing by the origin O are orthogonal complements of each other.

In $V = \mathbb{R}^3$ the orthogonal complement of a plane, i.e., of a 2-dimensional subspace U is the line $U^{\perp}$ passing by O, orthogonal to U, see Figure 28.1. And when U is a line, then $U^{\perp}$ is the plane orthogonal to it.

Example 28.3. The orthogonal complement of the orthogonal complement $U^{\perp}$ is the original subspace U, i.e., $(U^{\perp})^{\perp} = U$.

In particular, taking $U = \{0\}$ or $U = V$ we have $\{0\}^{\perp} = V$ and $V^{\perp} = \{0\}$.

Example 28.4. Since the only vector orthogonal to itself is $\vec{0}$, we have $U \cap U^{\perp} = \{0\}$.

As the following trivial lemma shows, in order to check if a given vector w is in $U^{\perp}$ it suffices to only check if w is orthogonal to the vectors in a basis of U:

Lemma 28.5. *Let $w \in V$ be a vector, and let U be a subspace with a basis $\{g_1, \ldots, g_k\}$. Then $w \in U^{\perp}$ if and only if $w \perp g_i$, $i = 1, \ldots, k$.*

Example 28.6. Let $V = \mathbb{R}^3$ and the subspace U be the plane $U = \operatorname{span}(g_1, g_2)$ with $g_1 = (2,-1,2)$, $g_2 = (1,1,1)$. Then for the vector $w = (2,2,-1)$ we have $w \cdot g_1 = 0$, but $w \cdot g_2 = 3 \neq 0$. So by Lemma 28.5 $w \notin U^{\perp}$. On the other hand, for $w' = (-2,0,2)$ we have $w' \cdot g_1 = 0$ and $w' \cdot g_2 = 0$. Thus, $w' \in U^{\perp}$.

Theorem 28.7. *Any real space V can be decomposed into a direct sum $V = U \oplus U^{\perp}$ for an arbitrary subspace U in V. In other words, any vector $v \in V$ has a unique presentation:*

$$v = u + w, \quad \text{where } u \in U \text{ and } w \in U^{\perp}.$$

***Proof*.** That the direct decomposition $V = U \oplus U^{\perp}$ means existence of the unique presentation $v = u + w$ is nothing but Definition 16.18.

Choose any orthonormal basis $G = \{g_1, \ldots, g_k\}$ in U. By point 1 in Proposition 11.27 it can be continued to a basis $\{g_1, \ldots, g_k;\ v_1, \ldots, v_{n-k}\}$ in the whole V, where $n = \dim(V)$ (see also Algorithm 16.6). Apply the Gram-Schmidt process to this basis to get an orthonormal basis for V:

$$G \cup H = \{g_1, \ldots, g_k;\ h_1, \ldots, h_{n-k}\}. \tag{28.1}$$

Since the vectors in G already were orthonormal, the Gram-Schmidt process changes noting in them. And since the remaining $n-k$ vectors in H are orthogonal to the initial k vectors of G, they all are in $U^{\perp}$ by Lemma 28.5. Each vector $v \in V$ can be written as:

$$v = a_1 g_1 + \cdots + a_k g_k \ + \ b_1 h_1 + \cdots + b_{n-k} h_{n-k} \ = \ u + w, \tag{28.2}$$

where $a_1 g_1 + \cdots + a_k g_k = u \in U$, and $b_1 h_1 + \cdots + b_{n-k} h_{n-k} = w \in U^{\perp}$.

To see that $v = u + w$ is unique we just use point 2 in Theorem 16.21 and the above mentioned fact that $U \cap U^{\perp}$ is zero (Example 28.4). □

From the above and from point 3 in Theorem 16.21 it follows:

Corollary 28.8. *If U is a subspace in V, then* $\dim\big(U^{\perp}\big) = \dim(V) - \dim(U)$.

How to find a basis for the orthogonal complement by the left null space. Let A be the $n \times k$ matrix the columns of which are the vectors $g_1, \ldots, g_k$ from any (not necessarily orthonormal) basis in U. By Lemma 28.5 a vector $w \in V$ is in $U^{\perp}$ if and only if it is orthogonal to all columns of A or, equivalently, to the rows of A^T. This can be rewritten as $A^T w = \vec{0}$, i.e., $w \in \operatorname{null}\big(A^T\big)$. Thus, we get the equality $U^{\perp} = \operatorname{null}\big(A^T\big)$.

The subspace $\operatorname{null}\big(A^T\big)$ often is called the *left null space* of the matrix A.

Algorithm 28.9 (Finding a basis for the orthogonal complement). We are given a basis $G = \{g_1, \ldots, g_k\}$ of a subspace U in an n-dimensional real space V.

► Find a basis for the orthogonal complement $U^{\perp}$.

1. Form a matrix putting the coordinates of $g_1, \ldots, g_k$ by *columns*: $A = \big[\, g_1 \,\vdots\, \cdots \,\vdots\, g_k \,\big]$.

2. Construct a basis H for $\operatorname{null}\big(A^T\big)$ by Algorithm 15.2 (i.e., get a basis H for the left null space of A).

3. Output H as a basis for $U^{\perp}$.

(If necessary, we can apply Gram-Schmidt process to G and to H to get *orthonormal* bases for U, for $U^{\perp}$, and also for V.)

Example 28.10. Like in Example 28.6 let U be the plane spanned by $g_1 = (2,-1,2)$, $g_2 = (1,1,1)$. Applying Algorithm 28.9 we first get $A = \big[\, g_1 \,\vdots\, g_2 \,\big] = \begin{bmatrix} 2 & 1 \\ -1 & 1 \\ 2 & 1 \end{bmatrix}$ and $A^T = \begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \end{bmatrix}$. Then we compute the null space as $\begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \sim$

$\left[\begin{smallmatrix}1&0&1\\0&1&0\end{smallmatrix}\right] = \operatorname{rref}(A^T)$. So $U^\perp = \operatorname{null}(A^T)$ is spanned by the vector $h_1 = (1,0,-1)$.

We, of course, could solve this with information of Section 2.2 already. For, all we need is to compute the cross product

$$\left[\begin{smallmatrix}2\\-1\\2\end{smallmatrix}\right] \times \left[\begin{smallmatrix}1\\1\\1\end{smallmatrix}\right] = \left[\begin{smallmatrix}-3\\0\\3\end{smallmatrix}\right].$$

This cross product certainly spans the same subspace as the vector $h_1 = (1,0,-1)$ above.

Example 28.11. Let U be the line in $\mathbb{R}^3$ spanned by the vector $g_1 = (2,6,4)$. Then $A^T = \left[\begin{smallmatrix}2&6&4\end{smallmatrix}\right]$, and to get its null space we proced $\left[\begin{smallmatrix}2&6&4\end{smallmatrix}\right] \sim \left[\begin{smallmatrix}1&3&2\end{smallmatrix}\right] = \operatorname{rref}(A^T)$. Thus, $U^\perp = \operatorname{null}(A^T)$ is the plane spanned by two vectors $h_1 = (3,-1,0)$, $h_2 = (2,0,-1)$.

If needed, we could apply Gram-Schmidt process to the bases constructed in these examples to get orthonormal bases for U and for $U^\perp$.

Definition 28.12. The subspaces U and W of a real space V are called orthogonal subspaces, if $u \perp w$ for any $u \in U$ and $w \in W$. This fact is denoted via $U \perp W$.

As evident samples of orthogonal subspaces take any U with $U^\perp$.

How to detect if the given subspaces are orthogonal. If U and W are any subspaces with bases respectively $g_1,\dots,g_k$ and $h_1,\dots,h_r$, then let us form the matrices $A = \left[\, g_1 \;\vdots\; \cdots \;\vdots\; g_k \,\right]$ and $B = \left[\, h_1 \;\vdots\; \cdots \;\vdots\; h_r \,\right]$. It is easy to see that $U \perp W$ if and only if the product matrix $A^T B$ consists of zero entries only.

Example 28.13. In $V = \mathbb{R}^4$ take the subspace U spanned by:

$$g_1 = (2,4,0,6),$$

$$g_2 = (0,0,1,1),$$

$$g_3 = (1,2,1,4);$$

and the subspace W spanned by a pair of vectors:

$$h_1 = (2,-1,0,0),$$

$$h_2 = (3,0,1,-1).$$

Then $A^T B$ is equal to:

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

And so we have $U \perp W$. In this example $V = \mathbb{R}^4$ is the direct sum of its two subspaces U and W (each of which is of dimension 2).

This, however, is not a general rule, as a space may *not* be the sum of its two orthogonal subspaces. To see an example just take the same U, and a new space W spanned by a single vector $(7,-2,1,-1)$ only.

The following important cases of orthogonal subspaces can be obtained as applications of the above method:

Theorem 28.14 (on four fundamental subspaces). *For any real matrix A:*

1. $\operatorname{null}(A) = \big(\operatorname{col}(A^T)\big)^\perp$,
2. $\operatorname{null}(A^T) = \big(\operatorname{col}(A)\big)^\perp$,
3. $\operatorname{col}(A) = \big(\operatorname{null}(A^T)\big)^\perp$,
4. $\operatorname{col}(A^T) = \big(\operatorname{null}(A)\big)^\perp$.

Corollary 28.15. *If A is an $m \times n$ real matrix, then:*

1. *$\mathbb{R}^n$ is equal to the direct sum* $\operatorname{null}(A) \oplus \operatorname{col}(A^T)$,
2. *$\mathbb{R}^m$ is equal to the direct sum* $\operatorname{null}(A^T) \oplus \operatorname{col}(A)$.

Example 28.16. For the matrix $A = \begin{bmatrix} 2 & 6 & 0 \\ 1 & 3 & 1 \end{bmatrix}$ we have $A \sim \mathrm{rref}(A) = \begin{bmatrix} 1 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, and so $\mathrm{null}(A) = \mathrm{span}(e)$ where $e = (3, -1, 0)$. Also, $A^T = \begin{bmatrix} 2 & 1 \\ 6 & 3 \\ 0 & 1 \end{bmatrix}$. It remains to see that $\begin{bmatrix} 3 & -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 6 & 3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$, that is, the subspaces $\mathrm{null}(A)$ and $\mathrm{col}(A^T)$ are orthogonal. Their direct sum is $\mathbb{R}^3$.

28.2. Projection onto a subspace

Let us start with quick rephrasing of some retro concepts from Section 1.3. The projection $\mathrm{proj}_u(v) = \frac{u \cdot v}{u \cdot u} u$ of the vector v onto the vector u can be interpreted as a projection of v onto the line ℓ passing by u (see Figure 1.5). Keeping in mind that ℓ is a subspace, we may think of ℓ as of a subspace $U = \mathrm{span}(u)$ in the Cartesian plane $\mathbb{R}^2$, and interpret $\mathrm{proj}_u(v)$ as a *projection* $\mathrm{proj}_U(v)$ *onto the subspace* U. Then the difference $v - \mathrm{proj}_U(v)$ is orthogonal to the subspace U in the sense that it is orthogonal to *any* vector in the line U. Also, $\mathrm{proj}_U(v)$ is the *closest* vector in the subspace U to the vector v in the sense that $|v - \mathrm{proj}_U(v)| \le |v - u|$ for *any* $u \in U$. Now let us see how these features can be generalized for cases when U is not necessarily a line.

Assume V is an n-dimensional real space, U is its subspace with orthogonal complement $U^\perp$. Adopting some constructions from the previous section assume orthonormal bases $E = \{g_1, \dots, g_k\}$ and $G = \{h_1, \dots, h_{n-k}\}$ are given respectively in U and in $U^\perp$. Clearly, the union $G \cup H$ is an orthonormal basis in V.

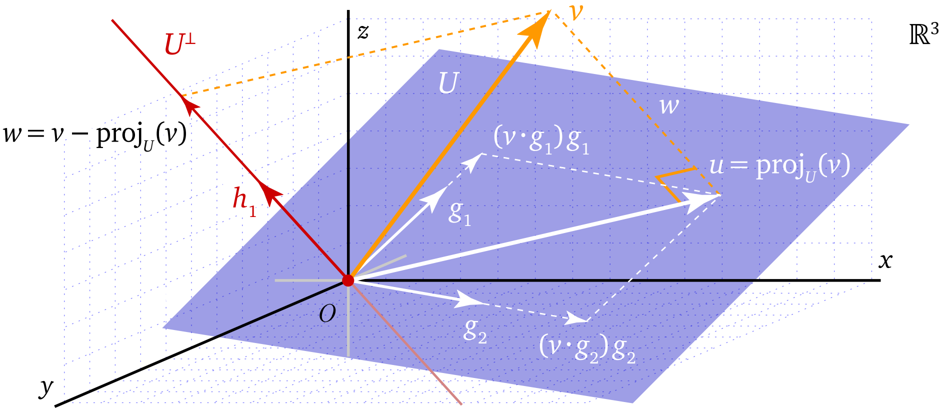


FIGURE 28.2. An example of projection onto $U = \mathrm{span}(g_1, g_2)$ in $V = \mathbb{R}^3$.

Definition 28.17. For any subspace U and for any vector v in a real space V we have $v = u + w$ where $u \in U$ and $w \in U^\perp$. Define the vector u to be the *projection* of vector v onto the subspace U, and denote it by $u = \mathrm{proj}_U(v)$.

Correctness of this definition follows from Theorem 28.7 because the sum $V = U \oplus U^\perp$ is *direct*, and for the given $v \in V$ the above vector $u = \mathrm{proj}_U(v) \in U$ is *unique*. It also is clear that the second vector $w \in U^\perp$ is the projection $w = \mathrm{proj}_{U^\perp}(v)$ of v onto $U^\perp$. So v is presented as a sum of two projections onto two orthogonal subspaces (which are complements of each other, see simple example in Figure 28.2).

A projection is easy to compute by:

Lemma 28.18. *If $G = \{g_1, \dots, g_k\}$ is an orthonormal basis for the subspace U in V, then for any vector $v \in V$ we have:*

$$\mathrm{proj}_U(v) = (v \cdot g_1)\, g_1 + \cdots + (v \cdot g_k)\, g_k.$$

***Proof*.** From equality (28.2) it is clear that $\mathrm{proj}_U(v) = a_1 g_1 + \cdots + a_k g_k$, and Lemma 27.3 provides the coefficients $a_i = v \cdot g_i$ for all $i = 1, \dots, k$. □

Example 28.19. In in Figure 28.2 we see a visualization of the vectors $(v \cdot g_1)\, g_1$, $(v \cdot g_2)\, g_2$ in the simple situation when $U = \mathrm{span}(g_1, g_2)$ is a plane in $V = \mathbb{R}^3$. The compliment $U^\perp = \mathrm{span}(h_1)$ is a line.

If we for this example take the basis with $g_1 = (2, -1, 2)$, $g_2 = (1, 1, 1)$ in U, then applying Gram-Schmidt process we get the orthonormal basis vectors $g_1 = \frac{1}{3}(2, -1, 2)$, $g_2 = \frac{1}{\sqrt{18}}(1, 4, 1)$ (we used the same letters g_1, g_2 for simplicity).

Then for, say, $v = (8, 2, 9)$ we can by Lemma 28.18 compute:

$$\begin{aligned}\mathrm{proj}_U(v) &= (v \cdot g_1)\, g_1 + (v \cdot g_2)\, g_2 \\ &= \tfrac{32}{9}(2, -1, 2) + \tfrac{25}{18}(1, 4, 1) \\ &= \left(\tfrac{17}{2}, 2, \tfrac{17}{2}\right).\end{aligned}$$

It is interesting to compare Lemma 28.18 with the initial formula by which we introduced projection in Section 1.3. For the line $U = \mathrm{span}(u)$ we are free to choose $g_1 = u$ to be *normalized* vector, i.e., $u \cdot u = 1$. Then $G = \{u\}$ is an orthonormal basis for U, and by Lemma 28.18 we have:

$$\mathrm{proj}_U(v) = (v \cdot u)\, u = \frac{u \cdot v}{u \cdot u}\, u$$

which is a nostalgic flashback to (1.1).

The next expected feature is:

Lemma 28.20. $\mathrm{proj}_U(v)$ *is the closest vector in the subspace U to the vector v in the sense that* $\;|v - \mathrm{proj}_U(v)| \le |v - u|\;$ *for any $u \in U$.*

***Proof*.** Denote $v' = \mathrm{proj}_U(v)$ and $w = v - v' \in U^\perp$. For arbitrarily chosen $u \in U$ denote $b = v' - u$ so that $u = v' - b$. Then:

$$v - u = (v' + w) - (v' - b) = w + b;$$

$$|v - u|^2 = |w + b|^2 = (w + b) \cdot (w + b) = w \cdot w + 2(b \cdot w) + b \cdot b = |w|^2 + |b|^2$$

(in the last step we used $b \cdot w = 0$). But since w is fixed, the above sum of two squares achieves its least value when $|b|^2 = 0$, i.e., when $v' = u$. □

Lemma 28.20 allows to introduce the *distance* from a vector v to a subspace U which can be expressed as:

$$|v - \mathrm{proj}_U(v)|. \tag{28.3}$$

Example 28.21. Using calculations done for Example 28.19 it is trivial to get the distance from $v = (8, 2, 9)$ to the plane U spanned by $g_1 = (2, -1, 2)$, $g_2 = (1, 1, 1)$. We have:

$$\begin{aligned}|v - \mathrm{proj}_U(v)| &= |(8, 2, 9) - (\tfrac{17}{2}, 2, \tfrac{17}{2})| \\ &= |(-\tfrac{1}{2}, 0, \tfrac{1}{2})| = \tfrac{1}{\sqrt{2}} \approx 0.707.\end{aligned}$$

Next, taking $v' = (-9, 1, 8)$ we have:

$$\begin{aligned}|v' - \mathrm{proj}_U(v')| &= |(-9, 1, 8) - (-\tfrac{1}{2}, 1, \tfrac{1}{2})| \\ &= |(-\tfrac{17}{2}, 0, \tfrac{15}{2})| \approx 12.020.\end{aligned}$$

So the distances of the vector v and v' from U are considerably different. We are going to use this in Section 28.4.

28.3. Projections as transformations

For any subspace U in a real space V the map

$$\boldsymbol{P : v \to \mathrm{proj}_U(v)}$$

defined by projection onto U is a *linear transformation*. This is very easy to verify by Definition 20.1 using the unique presentation $v = u + w$ given for any $v \in V$ in Theorem 28.7.

The simplest matrix of P is that in the basis $G \cup H$ where $G = \{g_1, \ldots, g_k\}$ is a basis for U, and $H = \{h_1, \ldots, h_{n-k}\}$ is a basis for $U^\perp$. Since P leaves intact all the g_i and sends all h_j to zero, we get the diagonal matrix:

$$D = [P]_{G\cup H} = \begin{bmatrix} 1 & & & & \mathbf{0} \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots & \\ \mathbf{0} & & & & & 0 \end{bmatrix} \tag{28.4}$$

where on the diagonal the eigenvalue 1 occurs k times, and 0 occurs $n-k$ times. Here we already can deduce a series of properties for P:

Proposition 28.22. *Let U be any subspace in a real space V, and $P : v \to \mathrm{proj}_U(v)$ be the projection onto U. If $\dim(U) = k$ and $\dim(V) = n$, then:*

1. *The characteristic polynomial of P is $f(\lambda) = (-1)^n(\lambda-1)^k\,\lambda^{n-k}$.*
2. *The eigenvalues of P are $\lambda = 1$ with algebraic and geometric multiplicity k, and $\lambda = 0$ with algebraic and geometric multiplicity $n-k$*
   (the only exceptions are $P = O$ or $P = I$; then P does not have the eiganvalue $\lambda = 1$ or $\lambda = 0$, respectively).
3. *P is diagonalizable.*
4. $\mathrm{rank}(P) = k$ *and* $\mathrm{nullity}(P) = n-k$.
5. $\mathrm{range}(P) = U$ *and* $\ker(P) = U^\perp$.
6. *$P^r = P$ for any $r = 1, 2, \ldots$*

Disadvantage of the matrix (28.4) is that it is given in basis $G \cup H$, and we cannot use it just like matrix $[P]_E$ to compute projection of a vector v by $P(v) = [P]_E[v]_E$, whenever E is another basis for V (for example, the standard basis E).

We start construction of $[P]_E$ by noticing that $\mathrm{proj}_U(v) \in U$ implies $\mathrm{proj}_U(v) = y_1g_1 + \cdots + y_kg_k = AY$ where A is an $n \times k$ matrix with columns $g_1, \ldots, g_k$ (written in E) and $Y = \left[\begin{smallmatrix} y_1 \\ \cdots \\ y_k \end{smallmatrix}\right]$. Let us express the unknown matrix Y by the other components.

Since $w = v - \mathrm{proj}_U(v)$ is orthogonal to U, we have:

$$0 = A^T\big(v - \mathrm{proj}_U(v)\big) = A^T v - A^T A Y.$$

Since A^TA is a square *invertible* matrix (see Lemma 28.24 below), we from above get $Y = (A^TA)^{-1}A^T v$ and so:

$$\boldsymbol{\mathrm{proj}_U(v) = A\,(A^TA)^{-1}A^T v,} \tag{28.5}$$

and

$$\boldsymbol{[P]_E = A\,(A^TA)^{-1}A^T} \tag{28.6}$$

is the matrix of projection P onto U in E.

It remains to complete the missing routine steps used above:

Lemma 28.23. *For any real matrix A we have* $\operatorname{null}(A) = \operatorname{null}(A^T A)$.

Proof. If $v \in \operatorname{null}(A)$, then $(A^T A)v = A^T(Av) = A^T 0 = 0$, and so $v \in \operatorname{null}(A^T A)$.

On the other hand, if $v \in \operatorname{null}(A^T A)$, then $A^T A v = 0$, and so $v^T A^T A v = v^T 0 = 0$, that is, $0 = (Av)^T Av = (Av) \cdot (Av) = |Av|^2$. Then $Av = 0$, i.e., $v \in \operatorname{null}(A)$. □

Lemma 28.24. *If the columns of the real matrix A are linearly independent, then $A^T A$ is an invertible matrix.*

Proof. Since A has k independent columns, then $\operatorname{rank}(A) = k$ and so $\operatorname{nullity}(A) = k - k = 0$. By previous lemma we also have $\operatorname{nullity}(A^T A) = 0$. Hence $A^T A$ is invertible. □

Example 28.25. Let us apply the constructed method to the projection given in Example 28.19. Since U is spanned by $g_1 = (2, -1, 2)$ and $g_2 = (1, 1, 1)$, we have $A = \begin{bmatrix} 2 & 1 \\ -1 & 1 \\ 2 & 1 \end{bmatrix}$. Then:

$$A^T A = \begin{bmatrix} 9 & 3 \\ 3 & 3 \end{bmatrix}, \quad (A^T A)^{-1} = \frac{1}{6}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}.$$

From here for an example vector $v = (8, 2, 9)$ we can either use (28.5):

$$\operatorname{proj}_U(v) = A\,(A^T A)^{-1} A^T v$$

$$= \begin{bmatrix} 2 & 1 \\ -1 & 1 \\ 2 & 1 \end{bmatrix} \cdot \frac{1}{6}\begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 2 \\ 9 \end{bmatrix} = \begin{bmatrix} \frac{17}{2} \\ 2 \\ \frac{17}{2} \end{bmatrix}.$$

Or else we may prefer to use (28.6) to first find the matrix of projection as of a linear transformation P:

$$[P]_E = A\,(A^T A)^{-1} A^T = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

and then to get the projection as:

$$P(v) = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{bmatrix}\begin{bmatrix} 8 \\ 2 \\ 9 \end{bmatrix} = \begin{bmatrix} \frac{17}{2} \\ 2 \\ \frac{17}{2} \end{bmatrix}.$$

Compare these with the projection found in Example 28.19.

28.4. *Applications*: Least squares approximation

Dealing with the systems of linear equations $AX = B$ we so far were focused on methods how to find solutions, in case the system is *consistent*. And when it is *inconsistent*, we just declared that fact without any further analysis.

But what if we are given a system which is inconsistent, but it still holds some valuable information we need? For example, assume solving a real-life problem we measured some natural objects, and inserted the obtained lengths as coefficients or constants in $AX = B$. But as it often happens our measurements is not very precise, and some slight inaccuracy may make our system inconsistent. But we still are aware that $AX = B$ *just slightly differs* from the right system (with precise values) that has the solution we are seeking. To visualize how that difference may be *estimated* let us represent $AX = B$ as

$$g_1 x_1 + \cdots + g_n x_n = B \tag{28.7}$$

where $g_1, \ldots, g_n$ are the columns of A. Then (28.7) holds for some $x_1, \ldots, x_n$ if and only if $B \in \operatorname{span}(g_1, \ldots, g_n) = \operatorname{col}(A)$. If $AX = B$ is inconsistent due to some measurement inaccuracy, then B, while still being outside $\operatorname{col}(A)$, may be "rather close" to $\operatorname{col}(A)$. Check the figure below:

$U = \operatorname{col}(A)$ is the subspace spanned by g_1, g_2.

The vector b_1 is in U, so the system $AX = B$ is consisten for $B = b_1$.

The vector b_2 is *outside* U, but it is rather close two it. So taking $B = \operatorname{proj}_U(b_2)$ we may get a new system $AX = B$ that may probably provide an approximate solution to our real-life problem.

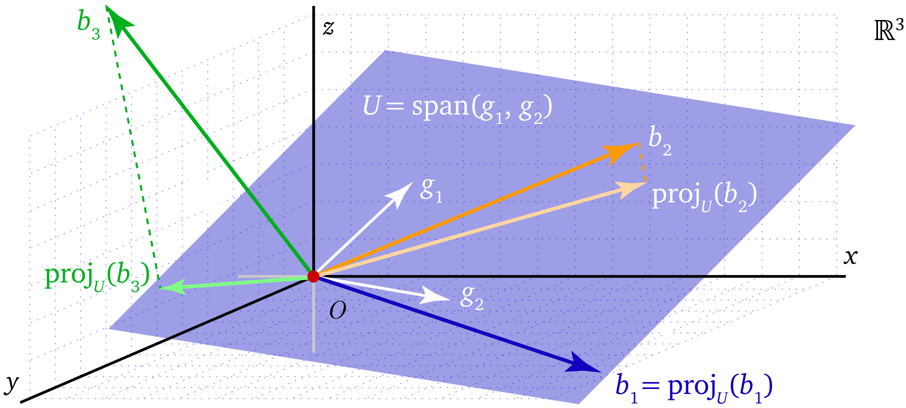


FIGURE 28.3. Vectors far or near to col(A).

As to the vector b_3, it is "too far" from U to hold relevant information. Rephrasing Orwell: *"All inconsistent systems are are inconsistent but some are more inconsistent".*

Call the solutions of $AX = \operatorname{proj}_U(B)$ the *least square solutions* of $AX = B$, keeping in mind that they may be close to the actual solutions, or even be equal to them.

Although it is not hard to project B onto $U = \operatorname{col}(A)$, there can be hidden obstacles. For example, If the columns of A are *not* independent, we cannot use (28.6), since $A^T A$ may not be invertible. So we first could replace A by a matrix holding its independent columns only. But we have a much shorter algorithm which doesn't require that step.

How to find least square solutions for a system of linear equations. Assume $AX = B$ is a system of m real linear equations in n variables $x_1, \ldots, x_n$. Let $g_1, \ldots, g_n \in \mathbb{R}^m$ be the columns of A (linearly dependent or independent). This system can be interpreted as the equation $x_1 g_1 + \cdots + x_n g_n = B$, i.e., it is consistent if and only if B is in the subspace $\operatorname{span}(g_1, \ldots, g_n) = \operatorname{col}(A) = U$.

The projection $u = \operatorname{proj}_U(B)$ is in U, and so $u = y_1 g_1 + \cdots + y_n g_n$ for some *unknowns* $y_1, \ldots, y_n$. Denoting $Y = \left[\begin{smallmatrix} y_1 \\ \cdots \\ y_k \end{smallmatrix}\right]$ we have $u = AY$. Since $B - u$ is orthogonal to U, then $0 = A^T(B-u) = A^T(B-AY)$, and we get a system of linear equations with the coefficients $A^T A$, the constants column $A^T B$ and the variables Y:

$$(A^T A)\, Y = A^T B. \tag{28.8}$$

Vise versa, if Y is any solution for this system, then $A^T(B - AY) = 0$, and the vector $B - AY$ is orthogonal to $\operatorname{col}(A) = U$. Then $AY = \operatorname{proj}_U(B) = u$, that is, Y is a solution for the system $AX = \operatorname{proj}_U(B)$ which differs from $AX = B$ just by replacing B by its projection onto U, and by renaming x_i by y_i.

In case $AX = B$ is consistent, we have $\operatorname{proj}_U(B) = B$ and so the least squares solution is noting but the actual exact solution of $AX = B$. If we are asked to distinguish weather the solution we found is exact or not, we just feed any solution found for (28.8) into $AX = B$ to see if we get an equality.

To even more simplify the method, we can interpret finding the least-square solution for $AX = B$ as simple multiplication of its both sides by A^T to switch to the system:

$$\boldsymbol{(A^T A)X = A^T B} \tag{28.9}$$

(keeping the same X). This is helpful in practical examples to save time on renaming the variables, especially because the variable name plays no serious role.

We formulate the algorithm using the simpler looking formula (28.9) instead of (28.8), keeping in mind that the solution(s) X we find may *not* be solution(s) for the original system $AX = B$. So usage of the same character X shall not confuse us.

Algorithm 28.26 (Finding a least square solution for a real system of linear equations)**.** We are given a system $AX = B$ of m real linear equations in n variables.

► Find the least square solution for the system. Indicate if it is the actual solution (for a consistent system) or approximate solution (for an inconsistent system).

1. Compute the matrix products $A^T A$ and $A^T B$.
2. Find the general solution of the new system $(A^T A)X = A^T B$ using, say, Algorithm 15.7.
3. Output the found solution as the least square solution for $AX = B$.
4. Set v_0 to be any of the solutions found in previous point.
5. If $Av_0 \neq B$, output: The solution is approximate. Else, output: The solution is exact.

Example 28.27. As it is easy to verify, the following system is inconsistent:

$$\begin{cases} x + 2y = 55 \\ 3x \qquad = 63 \\ 2x + 5y = 126. \end{cases}$$

We have $A = \begin{bmatrix} 1 & 2 \\ 3 & 0 \\ 2 & 5 \end{bmatrix}$, $B = \begin{bmatrix} 55 \\ 63 \\ 126 \end{bmatrix}$. So we compute $A^T A = \begin{bmatrix} 14 & 12 \\ 12 & 29 \end{bmatrix}$, $A^T B = \begin{bmatrix} 496 \\ 740 \end{bmatrix}$ to arrive to another system

$$\begin{cases} 14x + 12y = 496 \\ 12x + 29y = 740 \end{cases}$$

which has a single solution $\begin{bmatrix} \frac{2752}{131} \\ \frac{2204}{131} \end{bmatrix} \approx \begin{bmatrix} 21.008 \\ 16.824 \end{bmatrix}$. Feeding these values into our original system we get the values:

$$\frac{2752}{131} + 2 \cdot \frac{2204}{131} = \frac{7160}{131} \approx 54.656,$$

$$3 \cdot \frac{2752}{131} = \frac{8256}{131} \approx 63.023,$$

$$2 \cdot \frac{2752}{131} + 5 \cdot \frac{2204}{131} = \frac{16524}{131} \approx 126.137$$

which indeed are close to the constant terms of the original system. And this solution is not exact but approximate, as we get different (although close) results.

Next lest us make use of formulas (28.5) and (28.6). Since the columns or A are linearly independent, we compute:

$$(A^T A)^{-1} = \frac{1}{262}\begin{bmatrix} 29 & -12 \\ -12 & 14 \end{bmatrix}.$$

Then by (28.5) we have:

$$\mathrm{proj}_U(B) = A\,(A^T A)^{-1} A^T B$$

$$= \frac{1}{262}\begin{bmatrix} 1 & 2 \\ 3 & 0 \\ 2 & 5 \end{bmatrix}\begin{bmatrix} 29 & -12 \\ -12 & 14 \end{bmatrix}\begin{bmatrix} 1 & 3 & 2 \\ 2 & 0 & 5 \end{bmatrix}\begin{bmatrix} 55 \\ 63 \\ 126 \end{bmatrix}$$

$$= \frac{1}{131}\begin{bmatrix} 7160 \\ 8256 \\ 16524 \end{bmatrix} \approx \begin{bmatrix} 54.656 \\ 63.023 \\ 126137 \end{bmatrix}.$$

Naturally, the coordinates of this projection are the same as the values we got above by feeding the approximate values into the original system.

If needed, we can also compute the rather small distance of B from U:

$$|B - \mathrm{proj}_U(B)| = \frac{3}{131}\sqrt{262} \approx 0.371,$$

and we again get a confirmation that B is rather close to U, so our least squares solution is a pretty accurate approximate solution for our original system.

Finally, we are able to find the transformation matrix of projection onto U using (28.6):

$$[P]_E = A\,(A^T A)^{-1} A^T = \frac{1}{262}\begin{bmatrix} 37 & 15 & 90 \\ 15 & 261 & -6 \\ 90 & -6 & 226 \end{bmatrix}.$$

And so we can arrive to the same projection via:

$$P(B) = [P]_E B = \frac{1}{262}\begin{bmatrix} 37 & 15 & 90 \\ 15 & 261 & -6 \\ 90 & -6 & 226 \end{bmatrix}\begin{bmatrix} 55 \\ 63 \\ 126 \end{bmatrix} = \frac{1}{131}\begin{bmatrix} 7160 \\ 8256 \\ 16524 \end{bmatrix}.$$

Example 28.28. Compare two systems:

$$\begin{cases} 2x + y = 8 \\ -x + y = 2 \\ 2x + y = 9 \end{cases} \quad \text{and} \quad \begin{cases} 2x + y = -9 \\ -x + y = 1 \\ 2x + y = 8. \end{cases}$$

Turning back to Example 28.21 we see that the coefficient terms form the column vectors $g_1 = (2, -1, 2)$ and $g_2 = (1, 1, 1)$ spanning the subspace U in that example. And the constant terms columns respectively are the vectors $v = (8, 2, 9)$ and $v' = (-9, 1, 8)$ used in Example 28.21 for projection.

We have already calculated the distances of v and of v' from U:

$$|v - \mathrm{proj}_U(v)| = |(-\tfrac{1}{2}, 0, \tfrac{1}{2})| \approx 0.707,$$

$$|v' - \mathrm{proj}_U(v')| = |(-\tfrac{17}{2}, 0, \tfrac{15}{2})| \approx 12.020.$$

So based on this information we already see that the least square approximate solution for the first system will be more accurate than that for the second system. See Exercise E.28.8.

Example 28.29. Consider the system:

$$\begin{cases} x + 2y + 4z = 43 \\ 3x \qquad + 6z = 45 \\ 2x + 5y + 9z = 99. \end{cases}$$

Then

$$A^T A = \begin{bmatrix} 1 & 2 & 4 \\ 3 & 0 & 6 \\ 2 & 5 & 9 \end{bmatrix} \begin{bmatrix} 1 & 3 & 2 \\ 2 & 0 & 5 \\ 4 & 6 & 9 \end{bmatrix} = \begin{bmatrix} 21 & 27 & 48 \\ 27 & 45 & 60 \\ 48 & 60 & 110 \end{bmatrix},$$

$$A^T B = \begin{bmatrix} 1 & 2 & 4 \\ 3 & 0 & 6 \\ 2 & 5 & 9 \end{bmatrix} \begin{bmatrix} 43 \\ 45 \\ 99 \end{bmatrix} = \begin{bmatrix} 529 \\ 723 \\ 1202 \end{bmatrix}.$$

To find the solution of the new system $A^T AX = A^T B$ we bring its augmented matrix to the reduced row-echelon form:

$$[A^T A \mid A^T B] = \begin{bmatrix} 21 & 27 & 48 & 529 \\ 27 & 45 & 60 & 723 \\ 48 & 60 & 110 & 1202 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & \frac{5}{2} & \frac{119}{6} \\ 0 & 1 & -\frac{1}{6} & \frac{25}{6} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then the general solution by Algorithm 15.7 consists of all vectors:

$$\alpha \begin{bmatrix} \frac{5}{2} \\ -\frac{1}{6} \\ -1 \end{bmatrix} + \begin{bmatrix} \frac{119}{6} \\ \frac{25}{6} \\ 0 \end{bmatrix},$$

for all $\alpha \in \mathbb{R}$. Any of such solutions is a least squares solution for the initial system.

Notice that this time we cannot use (28.6) directly because the matrix $(A^T A)^{-1}$ is *not* invertible. Thus, to get the projection matrix $[P]_E$ we first need a matrix A' with linearly *independent* columns spanning the same subspace $U = \mathrm{col}(A)$. As the first two columns of A are independent, take $A' = \begin{bmatrix} 1 & 2 \\ 3 & 0 \\ 2 & 5 \end{bmatrix}$. Notice that this is noting but the matrix used in Example 28.27. So we save on calculations and output:

$$[P]_E = A' \left((A')^T A'\right)^{-1} (A')^T = \frac{1}{262} \begin{bmatrix} 37 & 15 & 90 \\ 15 & 261 & -6 \\ 90 & -6 & 226 \end{bmatrix}.$$

Then the projection of B is:

$$P(B) = [P]_E B = \frac{1}{262} \begin{bmatrix} 37 & 15 & 90 \\ 15 & 261 & -6 \\ 90 & -6 & 226 \end{bmatrix} \begin{bmatrix} 43 \\ 45 \\ 99 \end{bmatrix} = \frac{1}{262} \begin{bmatrix} 11176 \\ 11796 \\ 26019 \end{bmatrix}.$$

28.5. *Applications*: Regression analysis

One of the main approaches of data science, machine learning and statistics is *regression analysis* including *linear* regression, *quadratic* regression *polynomial* regression, etc.

The key point of regression analysis is that in most cases the data sets are not just random collection of data, but they obey some general, often simple rules. Finding those rules not only helps to very much reduce the size of *stored* data, but also helps to *predict* the new data to come.

For example, apartment prices (in US$) depend on the their living areas (in square meters m^2). This does not mean that any $77m^2$ apartment need necessarily be more expensive than a $72m^2$ apartment, but some general correlation is evident. Assume we are given the prices for a series of apartment as follows:

Area:	51	55	64	72	77	89	94	105
Price:	61,000	57,000	75,000	84,000	70,000	90,000	125,000	115,000

TABLE 28.1. Apartment prices in US$ based on living area in m^2.

Denote the above area values by $a_1, \dots, a_8$, and the price values by $p_1, \dots, p_8$. To visualize correlation between a_i and p_i plot the data set as in Figure 28.4, e.g., for the pair $(a_1, p_1) = (55, 57.000)$ plot a green dot with those coordinates. We see that the dots are not absolutely random, but they mostly are located around certain line $f(x) = kx + c$. If we find that line *best fitting* the set of green dots, we get two advantages:

1. Instead of storing a large massive of data we can keep in mind a simple function $f(x)$. This is helpful as our database may contain millions of area/price pairs.
2. We can quickly predict what the typical price $f(x) = kx + c$ will be, if the area is x.

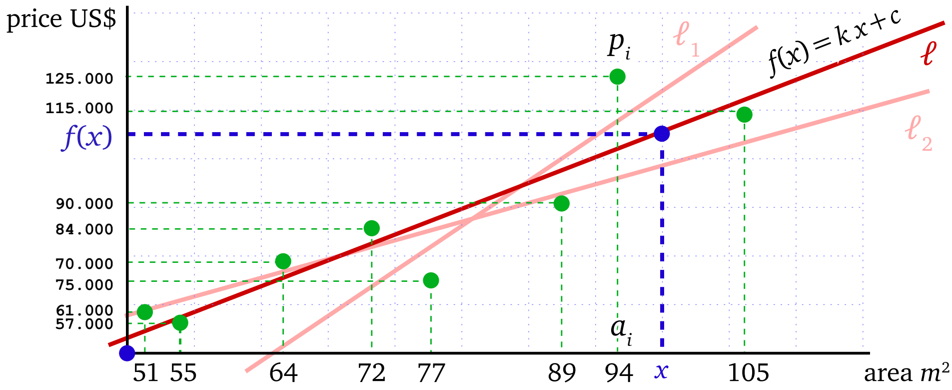


FIGURE 28.4. The data of Table 28.1 with a regression line.

Each of two pink lines ℓ_1, ℓ_2 in Figure 28.4 *seems* to be close to the green dots, but the red line ℓ *seems* to be the best fit. There is a simple trick to identify the best fit. We would like our function $f(x) = kx + c$ be so that for $x = 51$ it outputs the price $f(51) = 61,000$, i.e., we get the linear equation $51k + c = 61,000$. Doing the same with each data pair we get a system of 8 linear equations in two variables k, c:

$$(28.10) \qquad \begin{cases} 51k \ + c = 61,000 \\ 55k \ + c = 57,000 \\ 64k \ + c = 75,000 \\ 72k \ + c = 84,000 \\ 77k \ + c = 70,000 \\ 89k \ + c = 90,000 \\ 94k \ + c = 125,000 \\ 105k + c = 115,000. \end{cases}$$

The system is inconsistent, so there exist *no* line $f(x) = kx + c$ passing by all 8 points. But we don't give up, as we can find lest squares *approximate* solution. Let $g_1 = \left[\begin{smallmatrix} a_1 \\ \cdots \\ a_8 \end{smallmatrix}\right]$ and $g_2 = \left[\begin{smallmatrix} 1 \\ \cdots \\ 1 \end{smallmatrix}\right]$ be the column vectors of the matrix A of this system, and let $B = \left[\begin{smallmatrix} p_1 \\ \cdots \\ p_8 \end{smallmatrix}\right]$ be its constants column. With $A^TA = \begin{bmatrix} 48,617 & 607 \\ 607 & 8 \end{bmatrix}$ and $A^TB = \begin{bmatrix} 54,319,000 \\ 677,000 \end{bmatrix}$ we arrive to the system:

$$\begin{cases} 48,617k + 607c = 54,319,000 \\ \quad 607k \ + \ 8c \ = 677,000 \end{cases}$$

with a single solution $\begin{bmatrix} 7871/6829 \\ -19308/6829 \end{bmatrix} \approx \begin{bmatrix} 1.156 \\ -2.897 \end{bmatrix}$. So our approximate function is

$$\boldsymbol{f(x) = kx + c = 1.156x - 2.897.}$$

Using it we can, for example, predict that if an apartment is $100m^2$, then its likely price is 112,703 US$. What we did for the data set in Table 28.1 is called *linear regression analysis*, and the line ℓ we constructed is its *regression line*. The values (a_i, p_i) are often called *observed data*, while $\big(a_i, f(a_i)\big)$ are called *predicted data* of regression, see the orange dots in Figure 28.5.

Although the trick with (28.10) is simple, it keeps the geometric insight behind the scene. To see the power of the argument let us deduce it to projections.

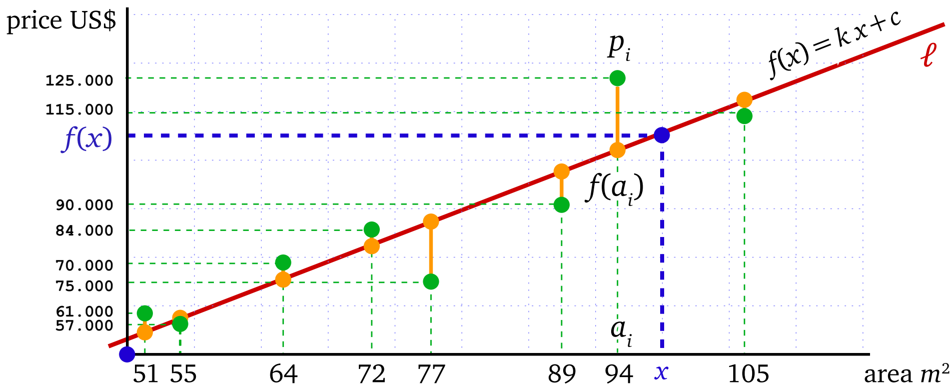


FIGURE 28.5. The distances between the *observed* and *predicted* data.

For any choice (k, c) the sum $kg_1 + cg_2$ is a vector in the subspace $U = \text{col}(A)$, while B is a vector outside U. For the same (k, c) we also have a function $f(x) = kx + c$. As x takes the values $a_1, \dots, a_8$, this function takes the values $f(a_1), \dots, f(a_8)$. For each $i = 1, \dots, 8$ distance between the green dot (a_i, p_i) and the orange dot $\big(a_i, f(a_i)\big)$ on our graph is $|p_i - f(a_i)|$, see Figure 28.5. Then $\sum_{i=1}^{8} \big(p_i - f(a_i)\big)^2$ is the sum of squares of all those distances. Clearly, the best fit is achieved, when it is *minimal*.

On the other hand, in $\mathbb{R}^8$ the sum $\sum_{i=1}^{8} \big(p_i - f(a_i)\big)^2$ is noting but the square of the *distance* between the fixed 8-dimensional vector B and the 8-dimensional vector $kg_1 + cg_2 = \begin{bmatrix} f(a_1) \\ \cdots \\ f(a_8) \end{bmatrix}$ picked in the 2-dimensional subspace U of $\mathbb{R}^8$. This distance will be minimal when $kg_1 + cg_2$ is the closest vector to B inside U, i.e., it is the projection $\text{proj}_U(B)$ of B onto U. This means that choosing the line ℓ via (k, c) we, in fact, made use of distances between 8-dimensional vectors in $\mathbb{R}^8$ which we cannot even visualize!

An adaptation of the simple linear regression is the *multivariate linear regression analysis*. A data set may depend on more than one parameters (say, apartment price may depend not only on area), and evolving more variable into the regression function we get more accurate predictions.

Area:	51	55	64	72	77	89	94	105
Year:	1996	1980	1998	2002	1989	1996	2017	2005
Price:	61,000	57,000	75,000	84,000	70,000	90,000	125,000	115,000

TABLE 28.2. Apartment prices in US$ based on living area in m^2 and on year.

Example 28.30. Table 28.2 presents apartment prices depending on living areas *and also* on built year. This time we look for a 2-variable linear function $f(x, y) = kx + sy + c$ so that for $x = 51$ and $y = 1996$ it outputs the price $f(51, 1996) = 61,000$, i.e., we put the condition $51k + 1996k + c = 61,000$. Doing the same with each data triple we in analogy with (28.10) get a system of 8 linear equations in three variables k, s, c. See Exercise E.28.14.

The next modification of the concept is the *polynomial regression analysis*. Not each data set has to be distributed about a line approximately. Some data may be distributed around an arch or another function graph, and so our linear regression may not be helpful in such cases.

But since many "natural" functions can be approximated by polynomials using methods like Taylor power series, we will be able to find regression for many data types, if we find the best fitting polynomial for the given data set. Let us illustrate that on an example of *quadratic regression*, i.e., finding a function $f(x) = ax^2 + bx + c$ best fitting the data in, say:

Angle:	0^o	15°	30°	45°	75°	85°	90°
Distance:	17	48	81	140	115	14	0

TABLE 28.3. Tennis ball hit distance in meters based on hit angle in degrees.

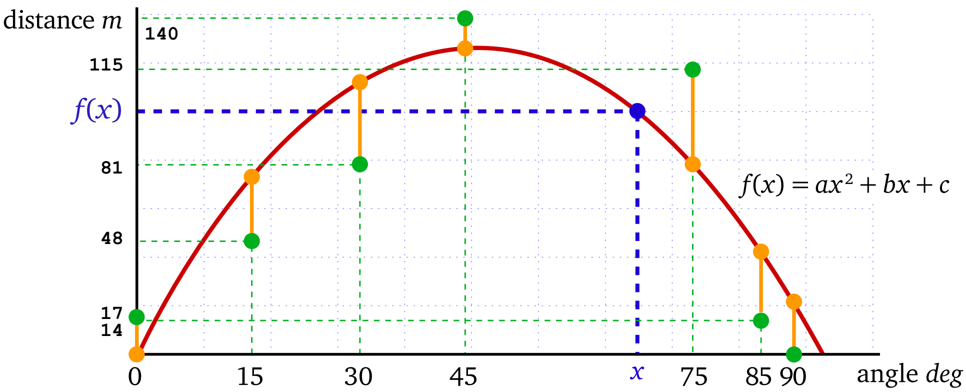


FIGURE 28.6. Quadratic regression of data in Table 28.3.

Example 28.31. Assume a tennis player hits the balls at certain angles, and he records the distances the ball reaches.

Table 28.3 presents data he gets via the green dots, and it certainly is not good to use *linear* regression this time, see Figure 28.6.

It would be good to have a polynomial

$$f(x) = ax^2 + bx + c$$

that for $x = 0^\circ$ outputs the distance $f(0) = 17$, or for $x = 15^\circ$ outputs the distance $f(0) = 48$, etc. We get the linear equations:

$$0a + 0b + c = 17,$$

$$225a + 15b + c = 48,$$

etc. Doing the same trick with each data pair in Table 28.3 we get a system of 7 linear equations in three real variables a, b, c:

$$\begin{cases} 0a + 0b + c = 17 \\ 225a + 15b + c = 48 \\ 900a + 30b + c = 81 \\ 2,025a + 45b + c = 140 \\ 5,625a + 75b + c = 115 \\ 7,225a + 85b + c = 14 \\ 8,100a + 90b + c = 0. \end{cases}$$

This system is inconsistent, but we still can find its lest squares approximate solution:

$$(-0.059245801,\ 5.4739234,\ -2.615735)$$

which suggests an approximate function:

$$f(x) = -0.059x^2 + 5.474x - 2.616$$

plotted in Figure 28.6. Check Exercise E.28.15.

Exercises

E.28.1. Detect if the vector $w \in V$ is in the compliment $U^\perp$ when: **(1)** $V = \mathbb{R}^3$, $w = (3,0,5)$ and U is spanned by $g_1 = (2,0,3)$, $g_2 = (3,2,1)$. **(2)** $V = \mathbb{R}^4$, $w = (0,2,3,0)$ and U is spanned by $g_1 = (2,-3,2,0)$, $g_2 = (1,1,-\frac{3}{2},1)$, $g_3 = (0,5,1,1)$. **(3)** $V = \mathbb{R}^3$, $w = (2,1,3)$ and U is the plane given by the equation $4x + 2y + 6z = 0$.

*** SOLUTION **E.28.1.** **(1)** $w \notin U^\perp$. **(2)** $w \notin U^\perp$. **(3)** $w \in U^\perp$. To see this find any two direction vectors for the plane, and notice they are orthogonal to w. Or simply notice that w is a normal vector for the equation $4x + 2y + 6z = 0$ (it is parallel to $n = (4,2,6)$).

E.28.2. Is it possible to find examples of *distinct* subspaces U_1 and U_2 in a real space V such that $U_1^\perp = U_2^\perp$?

*** SOLUTION **E.28.1.** According to Example28.3, $\left(U_1^\perp\right)^\perp = U_1$ and $\left(U_2^\perp\right)^\perp = U_2$. Thus, $U_1^\perp \neq U_2^\perp$.

E.28.3. In the proof of Theorem 28.7 we used point 2 in Theorem 16.21 to see that the presentation $v = u + w$ is *unique*. We refered to that theorem just for the sake of briefness. Deduce uniqueness of $v = u + w$ directly. *Hint*: assume another presentation $v = u' + w'$ is given, where $u' \in U$ and $w' \in U^\perp$. Use the fact that $u + w = u' + w'$ implies $u - u' = w - w'$.

E.28.4. Find a basis for the orthogonal compliment $U^\perp$ of the subspace U in the real space V when: **(1)** $V = \mathbb{R}^3$ and U is spanned by $g_1 = (1,2,0)$, $g_2 = (0,1,3)$. **(2)** $V = \mathbb{R}^3$ and U is spanned by a single vector $g_1 = (1,3,-2)$. **(3)** $V = \mathbb{R}^4$ and U is spanned by $g_1 = (1,0,2,0)$, $g_2 = (0,2,0,1)$.

E.28.5. Detect if the following subspaces U and W are orthogonal in $V = \mathbb{R}^3$ when: **(1)** U is spanned by $g_1 = (2,0,5)$, $g_2 = (0,3,3)$ and W is spanned by $h_1 = (5,-2,2)$, $h_2 = (1,3,0)$. **(2)** U is spanned by $g_1 = (1,1,0)$, $g_2 = (0,1,1)$ and W is the line passing by O directed by the vector $d = (3,-3,3)$.

E.28.6. Find the projection $\mathrm{proj}_U(v)$ of the vector $v \in V$ onto the subspace U when: **(1)** $V = \mathbb{R}^3$, $v = (2,1,-1)$ and U is spanned by $g_1 = \frac{1}{\sqrt{3}}(1,1,1)$, $g_2 = \frac{1}{\sqrt{2}}(1,0,-1)$. Notice that this basis of U already is orthonormal. **(2)** $V = \mathbb{R}^4$, $v = (1,2,0,3)$ and U is spanned by $g_1 = (1,1,1,0)$, $g_2 = (0,1,1,1)$. Notice that this basis of U is *not* yet orthonormal. So you may apply Gram-Schmidt first.

E.28.7. Compute the distance of the vector $v \in V$ from the subspace U when: **(1)** The space V, the vector v and the subspace U are those given in point (1) or Exercise E.28.6. **(2)** The space V, the vector v and the subspace U are those given in point (2) or Exercise E.28.6.

E28.8. Find the least squares solutions for both systems of linear equations in Example 28.28. Are those solutions exact or approximate? In which solution is the approximation more reasonable?

E.28.9. In the space $\mathbb{R}^4$ we are given the subspace U spanned by $g_1 = (1,0,2,0)$ and $g_2 = (0,3,1,1)$. **(1)** Write the appropriate matrix A, and compute A^TA. **(2)** Find the inverse $(A^TA)^{-1}$. **(3)** Calculate the projection of the vector $v = (1,0,2,1)$ onto U using formula (28.5). **(4)** Using (28.6) compute the matrix of the projection onto U as a linear transformation matrix $[P]_E$. **(5)** Find the projection of $v = (1,0,2,1)$ onto U using the matrix $[P]_E$ from the previous point.

*** SOLUTION **E.28.9.** **(1)** $A = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 3 & 1 & 1 \end{bmatrix}$ and $A^TA = \begin{bmatrix} 5 & 5 \\ 5 & 11 \end{bmatrix}$. **(2)** The inverse is $(A^TA)^{-1} = \begin{bmatrix} \frac{11}{51} & -\frac{2}{51} \\ -\frac{2}{51} & \frac{5}{51} \end{bmatrix}$. **(3)** By formula (28.5) $\mathrm{proj}_U(v) = A\,(A^TA)^{-1}A^T v = (\frac{49}{51}, \frac{5}{17}, \frac{103}{51}, \frac{5}{51}) = \frac{1}{51}(49,15,103,5)$. **(4)** By formula (28.6) we have $[P]_E = A\,(A^TA)^{-1}A^T = \frac{1}{51}\begin{bmatrix} 11 & -6 & 20 & -2 \\ -6 & 45 & 3 & 15 \\ 20 & 3 & 41 & 1 \\ -2 & 15 & 1 & 5 \end{bmatrix}$.

E.28.10. The statement of Lemma 28.23 is not true for all fields F. Take $F = \mathbb{Z}_5$ and verify that claim for the matrix $A = \begin{bmatrix} 1 & 3 \\ 2 & 1 \\ 0 & 1 \end{bmatrix}$.

E.28.11. The statement of Lemma 28.24 sounds very "natural" but it does not hold for all fields F. Take $F = \mathbb{Z}_5$ and check the lemma for the same matrix A mentioned in Exercise E.28.10.

E.28.12. We are given the systems of real equations:

$$\begin{cases} 3x+2y=6 \\ x\ +3y=3 \\ x\ +4y=5, \end{cases} \qquad \begin{cases} 5x+\ y\ =7 \\ 2x+\ y\ =4 \\ 3x+2y=7, \end{cases} \qquad \begin{cases} x_1\ +3x_2+x_3 \qquad =5 \\ 2x_1+\ x_2 \qquad +3x_4=7 \\ 3x_1+4x_2+x_3+3x_4=11. \end{cases}$$

For each of these systems: **(1)** Calculate its least square solutions. **(2)** Indicate if the system is consistent or not, i.e., if the solution is exact or approximate. **(3)** Indicate the distance $|B - \mathrm{proj}_U(B)|$ to estimate the accuracy or approximation. Which of the systems has the most accurate (least accurate) least squares solutions?

E.28.13. The ABC company spent the following amounts in US\$ on their advertisement campaigns: 110,000 in year 2017, 150,000 in 2018, 120,000 in 2019, 170,000 in 2020, 200,000 in 2021. And in those years their total revenues in US\$ respectively were: 90Mln., 100Mln., 140Mln., 130Mln., 170Mln. Find the linear regression function $f(x) = kx + c$ for this dataset. Draw the data set and the regression line.

E.28.14. Study data set in Table 28.2 by multivariate linear regression: **(1)** In analogy with (28.10) write a system of 8 linear equations in three variables k, s, c. **(2)** Find the lest squares approximate solution of that system. **(3)** Using the approximate solution predict what could be the typical price for an $100m^2$ apartment constructed in year 2015 or 2025.

E.28.15. **(1)** Do all steps of the lest squares solution for Example 28.31 to show how we got the function $f(x) = -0.059x^2 + 5.474x - 2.616$. **(2)** Check its value $f(x)$ at some points near to $x = 45$ to see if you get values near to 140.

CHAPTER 29

Orthogonal and symmetric transformations, Spectral Theorem

29.1. Orthogonal matrices and orthogonal transformations

The columns (or rows) of a matrix also are sets of vectors, and we may be interested if they are orthogonal or normalized. The following lemma establishes a simple but important criterion for that:

Lemma 29.1. *The columns (or rows) of the square matrix $Q \in M_{n,n}(\mathbb{R})$ are orthonormal if and only if equality $Q^T Q = I_n$ holds.*

***Proof*.** Set $Q = [q_{ij}]_{n,n}$, and present the equality $Q^T Q = I_n$ as:

$$Q^T Q = \begin{bmatrix} q_{11} & \cdots & q_{n1} \\ \multicolumn{3}{c}{\dotfill} \\ q_{1n} & \cdots & q_{nn} \end{bmatrix} \cdot \begin{bmatrix} q_{11} & \cdots & q_{1n} \\ \multicolumn{3}{c}{\dotfill} \\ q_{n1} & \cdots & q_{nn} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 0 \\ \multicolumn{3}{c}{\dotfill} \\ 0 & \cdots & 1 \end{bmatrix} = I_n.$$

That the *columns* of Q are orthonormal if and only if $Q^T Q = I_n$ holds, follow from row-by-column multiplication rule in the equality above (the rows of Q^T are the columns of Q). Nex, we in a similar way prove the statement concerning the *rows* of Q. □

Call a square matrix Q an *orthogonal matrix*, if its columns (or rows) form an orthonormal set of vectors or, equivalently, if $Q^T Q = I$.

Definition 29.2. A linear transformation Q of the real space V is called an *orthogonal linear transformation*, if it has orthogonal matrix Q in some orthonormal basis E of V.

Notice how for orthogonal matrices and orthogonal transformations we reserved the character Q. Since we agreed to identify transformations with matrices, we may write $Q = [Q] = [Q]_E$.

Example 29.3. For a mirror reflection transformation M of $\mathbb{R}^3$ we have computed:

$$Q = [M] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for which we clearly have:

$$Q^T Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^2 = I_3.$$

So this reflection $Q = M$ is orthogonal.

Example 29.4. For rotation transformation R_φ of $\mathbb{R}^2$ we have:

$$Q = [R_\varphi] = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix},$$

and it is easy to compute:

$$Q^T Q = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix} \cdot \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} = I_2.$$

Thus, $Q = R_\varphi$ also is orthogonal.

By Lemma 29.1 it is easy to verify, the *inverses*, *transposes*, and the *products* of orthogonal matrices also are orthogonal. Thus, also:

Proposition 29.5.
1. *Any orthogonal transformation Q is invertible, its inverse is $Q^{-1} = Q^T$, and it also is an orthogonal transformation;*
2. *if Q and R are orthogonal transformations, then the product QR also is orthogonal.*

Lemma 29.6. *A change of basis matrix P_{EG} from an orthonormal basis E to an orthonormal basis G of a space V is an orthogonal matrix.*

Proof. Indeed, let H be the basis of V in which the coordinates of E and G are given (typically, the standard basis). Then $P_{EG} = P_{EH}P_{HG} = P_{HE}^{-1}P_{HG}$, see Theorem 13.3 and Theorem 13.4. Since the columns of P_{HE} consist of the coordinates of vectors of E in H, they are orthonormal, as E is an orthonormal basis. Then the inverse P_{HE}^{-1} of P_{HE} is orthogonal by Proposition 29.5. Similarly P_{HG} is an orthogonal matrix. The product P_{EG} of two orthogonal matrices is orthogonal by the same proposition. □

It turns out that we *always* get an orthogonal matrix for an orthogonal transformation, regardless which orthonormal basis we take:

Lemma 29.7. *If the transformation Q of the space V has an orthogonal matrix in an orthonormal basis E of V, then its matrix is orthogonal in any orthonormal basis G of V.*

Proof. The change of basis matrix $P = P_{EG}$ is orthogonal by the previous lemma. If $Q = [Q]_E$, then in G the transformation Q has the matrix $B = P^{-1}Q\,P$ which is orthogonal by Proposition 29.5. □

Did you notice that the transformations of Example 29.3 (the reflection) and of Example 29.4 (the rotation) both are preserving the *lengths* of vectors? It turns out that this is a universal rule characterizing *all* the orthogonal transformations, in general:

Theorem 29.8. *Let Q be a transformation of a real space V. Then the following statements are equivalent:*
1. *Q is an orthogonal transformation;*
2. *Q "preserves" the vector lengths, i.e., $|Q(v)| = |v|$ for any $v \in V$;*
3. *Q "preserves" the dot product, i.e., $Q(u) \cdot Q(v) = u \cdot v$ for any $u, v \in V$.*

Proof. Below we are going to extensively use the matrix interpretation (27.1) for the dot products.

(1) ⇒ (2). Since the matrix $Q = [Q]_E$ is orthogonal, we have:

$$|Q(v)|^2 = Q(v)\cdot Q(v) = Qv\cdot Qv = (Qv)^T Qv = v^T Q^T Qv = v^T I v = v^T v = v\cdot v = |v|^2.$$

(2) ⇒ (3). For any vectors $u, v \in V$ we have $|u+v| = |Q(u+v)|$. Compute:

$$|u+v|^2 = (u+v)\cdot(u+v) = u\cdot u + u\cdot v + v\cdot u + v\cdot v = |u|^2 + 2(u\cdot v) + |v|^2;$$

$$|Q(u+v)|^2 = |Q(u)+Q(v)|^2 = \big(Q(u)+Q(v)\big)\cdot\big(Q(u)+Q(v)\big)$$

$$= Q(u)\cdot Q(u) + Q(u)\cdot Q(v) + Q(v)\cdot Q(u) + Q(v)\cdot Q(v) = |Q(u)|^2 + 2\big(Q(u)\cdot Q(v)\big) + |Q(v)|^2.$$

Since $|u| = |Q(u)|$ and $|v| = |Q(v)|$, we can eliminate them in the sums above:

$$2(u\cdot v) = 2\big(Q(u)\cdot Q(v)\big).$$

So $u\cdot v = Q(u)\cdot Q(v)$ for *any* $u, v \in V$.

(3) ⇒ (1). Assume $Q(u)\cdot Q(v) = u\cdot v$ for any u, v. Since

$$Q(u)\cdot Q(v) = Qu\cdot Qv = (Qu)^T Qv = (u^T Q^T)Qv = u^T(Q^T Q\,v) = u\cdot(Q^T Q\,v),$$

we have:

$$0 = u\cdot v - Q(u)\cdot Q(v) = u\cdot v - u\cdot(Q^T Q\,v) = u\cdot\big(v - (Q^T Q\,v)\big).$$

Taking $u = v - (Q^T Q\,v)$ we get $|v - (Q^T Q\,v)| = 0$, and so $Q^T Q\,v = v = I v$ for any v. By Lemma 8.22 we have $Q^T Q = I$, and the matrix Q is orthogonal. □

For vectors u, v in a real space V we defined the angle φ between u and v as $\varphi \in (-\pi, \pi]$ for which:

$$\cos(\varphi) = \frac{u\cdot v}{|u|\,|v|}$$

(see Definition 1.13). From Theorem 29.8 it now follows that if a transformation is orthogonal, then it “preserves” the angles between any two vectors, i.e., the angle between $T(u)$ and $T(v)$ is equal to the angle between u and v for any $u, v \in V$.

Moreover, the fact that a given transformation preserves the vector lengths already implies that it preserves the angles between vectors likewise! By the way, is the *inverse* statement true? Will a transformation preserve the vector lengths, if it preserves the angles between any two vectors? See Exercise E.29.3.

Lemma 29.9. *All the eigenvalues of a real orthogonal transformation are equal to either* 1 *or to* −1.

***Proof*.** If v is an eigenvector associated to an eigenvalue λ, then $Q(v) = \lambda v$. On the other hand $|Q(v)| = |v|$. So $|\lambda v| = |v|$ and $\lambda = \pm 1$. □

Lemma 29.10. *The eigenvectors of an orthogonal transformation corresponding to different eigenvalues are orthogonal.*

***Proof*.** Assume $Q(v_1) = \lambda_1 v_1$ and $Q(v_2) = \lambda_2 v_2$, with $\lambda_1 \neq \lambda_2$. By Lemma 29.9 this only is possible when one of the eigenvalues is 1, the other is −1.

Then by point 3 of Theorem 29.8:

$$v_1\cdot v_2 = Q(v_1)\cdot Q(v_2) = (\lambda_1 v_1)\cdot(\lambda_2 v_2) = \lambda_1\lambda_2(v_1\cdot v_2).$$

Since $\lambda_1\lambda_2 = -1 \neq 1$, the above equality is only possible when $v_1\cdot v_2 = 0$. □

By Theorem 29.8 it is easy to build examples of orthogonal and non-orthogonal transformations:

Example 29.11. As we have seen, rotation of $\mathbb{R}^2$ is orthogonal. In Example 29.4 we obtained that fact by computing $Q^T Q = I$ for the matrix

$$Q = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}.$$

For the space $\mathbb{R}^3$ we could notice that rotations around each of the axes Ox, Oy, Oz is an orthogonal transformation. Say, the rotation around Oy has the matrix:

$$Q = \begin{bmatrix} \cos\varphi & 0 & -\sin\varphi \\ 0 & 1 & 0 \\ \sin\varphi & 0 & \cos\varphi \end{bmatrix},$$

and it is easy to check that $Q^T Q = I$.

What about rotation R of $\mathbb{R}^3$ around an *arbitrary* line ℓ passing by O? Do we need to construct its matrix to check the condition $Q^T Q = I$?

No, it is enough just to notice that T does *not* change the lengths of vectors, so T is orthogonal by Theorem 29.8.

Example 29.12. As non-orthogonal transformation take, say, the scaling S given by

$$\begin{bmatrix} c & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad\text{or}\quad \begin{bmatrix} c & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{bmatrix}$$

for any $c \neq \pm 1$. Just apply Theorem 29.8 for $v = (1, 0, 0)$ to get $|v| \neq |S(v)|$.

29.2. *Applications*: *QR*-factorization

One of the applications of orthogonal matrices and of the Gram-Schmidt process is the *QR-factorization*. Its variations are available for *any* square matrices (and even for non-square matrices), but here we discuss QR-factorizations for real *invetible* square matrix only. We show that any such matrix A can be presented as a product $A = QR$, where:

1. Q is an orthogonal matrix;
2. R is an invertible upper-triangle matrix.

Let A be any real invertible matrix of degree n. Then it has n linearly independent column vectors $v_1, \dots, v_n$, and using the Gram-Schmidt process we can construct the respective orthonormal basis $E = \{e_1, \dots, e_n\}$.

By Lemma 27.3 the coordinates of vectors v_i in E can be computed using dot products: $[v_k]_E = (v_k \cdot e_1, \dots, v_k \cdot e_n)$ and so:

$$v_k = (v_k \cdot e_1)\, e_1 + (v_k \cdot e_2)\, e_2 + \dots + (v_k \cdot e_n)\, e_n \tag{29.1}$$

for each $k = 1, \dots, n$.

The Gram-Schmidt process creates the vectors $e_k, \dots, e_n$ so that they are orthogonal to the previously constructed vectors $e_1, \dots, e_{k-1}$. Since by Remark 27.5 we have

$$\operatorname{span}(v_1, \dots, v_{k-1}) = \operatorname{span}(e_1, \dots, e_{k-1}),$$

$e_k, \dots, e_n$ are orthogonal to the vectors $v_1, \dots, v_{k-1}$ also. So in (29.1) all the summands after the k'th summands are zero, and (29.1) can be rewritten as:

$$\begin{aligned} v_1 &= (v_1 \cdot e_1)\, e_1, \\ v_2 &= (v_2 \cdot e_1)\, e_1 + (v_2 \cdot e_2)\, e_2, \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ v_n &= (v_n \cdot e_1)\, e_1 + (v_n \cdot e_2)\, e_2 + \dots + (v_n \cdot e_n)\, e_n. \end{aligned} \tag{29.2}$$

Denote by $Q = \left[e_1 \,\vdots\, \cdots \,\vdots\, e_n \right]$ the matrix consisting of column vectors e_i, and set

$$R = \begin{bmatrix} v_1 \cdot e_1 & v_2 \cdot e_1 & \cdots & v_n \cdot e_1 \\ 0 & v_2 \cdot e_2 & \cdots & v_n \cdot e_2 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \cdots & v_n \cdot e_n \end{bmatrix}. \tag{29.3}$$

Then the first column of the product QR clearly is the vector $(v_1 \cdot e_1)\, e_1$ which is equal to v_1 by (29.2). The second column of QR is $(v_2 \cdot e_1)\, e_1 + (v_2 \cdot e_2)\, e_2$ which is v_2 by (29.2). Continuing the steps we conclude $QR = \left[v_1 \,\vdots\, \cdots \,\vdots\, v_n \right] = A$.

Next show that all the diagonal elements of R are non-zero. As we saw, e_k is orthogonal to the vectors $v_1, \dots, v_{k-1}$. If e_k also *were* orthogonal to v_k, it would be orthogonal to *all* the vectors $v_1, \dots, v_k$. Again by Remark 27.5 we have $\operatorname{span}(v_1, \dots, v_k) = \operatorname{span}(e_1, \dots, e_k)$, so e_k would be orthogonal to e_k, i.e., $e_k = \vec{0}$.

Since all the diagonal elements in (29.3) are non-zero, the determinant of R is non-zero, and R is invertible. We get:

Theorem 29.13. *Let A be any real invetible square matrix of degree n. Then there are an orthogonal matrix Q and an invertible upper-triangle matrix R of degree n such that:*

$$\boldsymbol{A = QR.} \tag{29.4}$$

How to find a QR-factorization of a matrix. We can simplify the process of finding the matrix R for the given invertible matrix $A = [v_1 \vdots \cdots \vdots v_n]$, as we do *not* need to compute all those $\frac{n(n+1)}{2}$ dot products in (29.3). Instead, first construct Q by bringing the initial basis $v_1, \ldots, v_n$ by the Gram-Schmidt process to an orthonormal basis $e_1, \ldots, e_n$, and by putting these vectors as columns in $Q = [e_1 \vdots \cdots \vdots e_n]$. To obtain the matrix R just multiply both sides of (29.4) by Q^T from the left:

$$Q^T A = Q^T(QR) = (Q^T Q)R = R, i.e.,$$

So after we find Q, directly take $R = Q^T A$.

Algorithm 29.14 (Computation of the QR-factorization)**.** We are given an invertible matrix A.

► Compute the QR-factorization of A.

1. Denote by $v_1, \ldots, v_n$ the column vectors of the matrix $A = [v_1 \vdots \cdots \vdots v_n]$.
2. Using the Gram-Schmidt process, i.e., Algorithm 27.6 bring $v_1, \ldots, v_n$ to an orthonormal basis with vectors $e_1, \ldots, e_n$.
3. Set the matrix $Q = [e_1 \vdots \cdots \vdots e_n]$ to consist of column vectors $[e_1], \ldots, [e_n]$.
4. Set the matrix $R = Q^T A$.
5. Output the QR-factorization: $A = QR$.

Example 29.15. For vectors $v_1 = (1,1)$, $v_2 = (2,-1)$ we have computed the orthonormal basis

$$e_1 = \left(\tfrac{1}{\sqrt{2}}, \tfrac{1}{\sqrt{2}}\right), \quad e_2 = \left(\tfrac{1}{\sqrt{2}}, -\tfrac{1}{\sqrt{2}}\right).$$

So we have:

$$A = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}, \; Q = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The matrix R can be found by:

$$R = Q^T A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$$

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

The equality $A = QR$ is very easy to verify.

Applications of QR-factorization are numerous, let us outline one of them:

Having the factorization $A = QR$ we can easily estimate the *determinant* of A. Indeed, since $Q^T Q = I$ and $\det(Q^T) = \det(Q)$, we have:

$$1 = \det(I) = \det(Q^T Q) = \det(Q^T)\, \det(Q) = \det(Q)\, \det(Q) = (\det(Q))^2.$$

That is, $\det(Q) = \pm 1$ for any orthogonal matrix Q. Further, since R is a triangle matrix, then $\det(R)$ is the product of diagonal elements of R. We have:

$$|\det(A)| = |\det(QR)| = |\det(Q)| \cdot |\det(R)| = |v_1 \cdot e_1 \, \cdots \, v_n \cdot e_n|,$$

i.e., *the absolute value of* $\det(A)$ is the product of all diagonal elements in (29.3).

Example 29.16. Let us verify this feature for the matrix A in previous example:

$$\det(A) = 1 \cdot (-1) - 2 \cdot 1 = -3.$$

On the other hand by triangle rule:

$$\det(R) = \sqrt{2} \cdot \tfrac{3}{\sqrt{2}} = 3.$$

So $\det(A) = \pm\det(R)$.

29.3. Symmetric transformations

The second important type of transformations are symmetric transformations which in some sense are "dual" to orthogonal transformations. And the properties we learned in previous section are going to have their analogs here.

Definition 29.17. A linear transformation S of the real space V is called a *symmetric linear transformation*, if it has symmetric matrix S in some orthonormal basis E of V.

Notice how we reserved the letter S for symmetric matrices and transformations, just like we reserved Q for orthogonal matrices and transformations. Since we agreed to identify transformations with their matrices, we can write $S = [S] = [S]_E$.

Compare the definitions of orthogonal and symmetric matrices (transformations):

$$\boldsymbol{Q^T = Q^{-1}} \quad \text{and} \quad \boldsymbol{S^T = S}.$$

Transposing Q we get its inverse, while transposing S we change nothing.

Example 29.18. The projections, such as, the transformation

$$T(x, y, z) = (x, 0, z)$$

with the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

are symmetric transformations. The scalings, such as, the transformation

$$T(x, y, z) = (2x, 3y, 4z)$$

with the matrix

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix},$$

also are symmetric. These perhaps are the most easily imaginable symmetric transformations.

And we can take any symmetric matrix S to define a transformation S by the rule:

$$S(v) = S \cdot v.$$

The analog of Lemma 29.7 holds for symmetric transformaions:

Lemma 29.19. *If the transformation S of the space V has a symmetric matrix in an orthonormal basis E of V, then its matrix is symmetric in any orthonormal basis G of V.*

Proof. As we have seen in Lemma 29.6 the change of basis matrix $P = P_{EG}$ is orthogonal. Thus, in G the transformation S has the matrix $P^{-1}S\,P = P^T S\,P$, which is symmetric because $(P^T S\,P)^T = P^T S^T \left(P^T\right)^T = P^T S\,P$. □

Cleary, the *sums* and *scalar multiples* of symmetric matrices are symmetric. Then:

Proposition 29.20.

1. *If S and L are symmetric transformations, then their sum $S + L$ also is a symmetric transformation;*
2. *if S is a symmetric transformation and $c \in \mathbb{R}$, then the scalar multiple cS also is a symmetric transformation.*

We have the "dual" of Theorem 29.8:

Theorem 29.21. *Let S be a transformation of a real space V. Then the following statements are equivalent:*

1. *S is a symmetric transformation;*
2. *S can be "swapped from one side of dot product to the other", i.e., $S(u) \cdot v = u \cdot S(v)$ for any $u, v \in V$.*

***Proof*.** Since S is symmetric, we have:

$$S(u) \cdot v = Su \cdot v = (Su)^T v = (u^T S^T)\, v = (u^T S)\, v = u^T (Sv) = u^T S(v) = u \cdot S(v).$$

On the other hand, if $S = [s_{ij}]_{n,n}$, then the (i, j)'th entry of s_{ij} is the i'th coordinate of $S(e_j) = Se_j$. By Lemma 27.3 we have $s_{ij} = S(e_j) \cdot e_i$. By the hypothesis and by symmetry of dot products (see point 1 of Proposition 1.6):

$$S(e_j) \cdot e_i = e_j \cdot S(e_i) = S(e_i) \cdot e_j = s_{ji}.$$

I.e., $s_{ij} = s_{ji}$, and so $S^T = S$. □

Comparing Theorem 29.8 with Theorem 29.21 we observe their "duality":
for an *orthogonal* transformation Q we have: $\boldsymbol{Q(u) \cdot Q(v) = u \cdot v}$,
and for a *symmetric* transformation S we have: $\boldsymbol{S(u) \cdot v \;=\; u \cdot S(v)}$.

According to Theorem D.8 in Appendix D.2 every complex polynomial $f(x) \in \mathbb{C}[x]$ has a complex root. If $f(x) \in \mathbb{R}[x]$ is a real polynomial, i.e., if its coefficients are real, $f(x)$ may still be viewed as a complex polynomial (yes, because all real numbers also are complex), but the root promised by Theorem D.8 may *not* be real. As an example check $f(x) = x^2 + 1$ which has two roots only $x = i$ and $x = -i$. We have much simpler situation, when the considered real polynomial is a *characteristic polynomial of a symmetric transformation*:

Lemma 29.22. *The characteristic polynomial $f(\lambda) = |S - \lambda I|$ of any real symmetric transformation S has roots, and all such roots are real.*

Before the proof we need the following notation. For a *complex* matrix $M = [m_{ij}]$ denote by $\overline{M} = [\overline{m}_{ij}]$ the matrix obtained from M after we replace each entry by its conjugate. And for any *complex* vector $v = (x_1, \dots, x_n)$ denote by $\overline{v} = (\overline{x}_1, \dots, \overline{x}_n)$ the vector obtained from v after we replace each coordinate by its conjugate.

***Proof of Lemma 29.22*.** Assume $S = [S]$ in some orthonormal matrix. Consider the n-dimensional complex space $U = \mathbb{C}^n$ on which the matrix S also defines a transformation S'. By Theorem D.8 the transformation S' always has an eigenvalue because its characteristic polynomial $f(\lambda) = |S - \lambda I|$ has a complex root λ. We want to show that λ in fact is real.

From the matrix equality $Sv = \lambda v$ the following follows:

$$\overline{Sv} = \overline{S}\overline{v} = \overline{\lambda v} = \overline{\lambda}\overline{v}.$$

Since S is real, $S = \overline{S}$, and so $S\overline{v} = \overline{\lambda}\overline{v}$. Multiplying the equality $Sv = \lambda v$ from the left by $\bar{v}^T$, and multiplying the equality $S\overline{v} = \overline{\lambda}\overline{v}$ from the left by v^T we get:

$$\bar{v}^T S v = \bar{v}^T \lambda v = \lambda \bar{v}^T v = \lambda z, \quad v^T S \overline{v} = v^T \overline{\lambda}\overline{v} = \overline{\lambda} v^T \overline{v} = \overline{\lambda} z,$$

where z is the sum of products of all coordinates of v times their conjugates (we identified the 1×1 matrix $[\lambda z]$ with λz for simplicity). Clearly, z is real, and it can never be zero unless all the coordinates of v are zero (and this may not happen as $v \neq 0$ is an eigenvector). Subtracting the above equalities we get

$$\bar{v}^T S v - v^T S \overline{v} = (\lambda - \overline{\lambda})\, z.$$

Present v as a column vector $v = \left[\begin{smallmatrix} a_1 \\ \cdots \\ a_n \end{smallmatrix}\right]$, and compute:

$$\bar{v}^T S v = \Big[\, \textstyle\sum_{i=1}^n \bar{a}_i s_{i1} + \cdots + \sum_{i=1}^n \bar{a}_n s_{in} \Big] \left[\begin{smallmatrix} a_1 \\ \cdots \\ a_n \end{smallmatrix}\right] = \Big[\, \textstyle\sum_{i=1}^n \sum_{j=1}^n \bar{a}_i s_{ij} a_j \Big].$$

In a similar way:

$$v^T S \bar{v} = \left[\sum_{i=1}^n \sum_{j=1}^n a_i s_{ij} \bar{a}_j\right].$$

Since S is a symmetric matrix, the right-hand sides of both equalities are equal: just swap the indices i and j (and use $s_{ij} = s_{ji}$) to get one from the other. So we have $(\lambda - \overline{\lambda})z = 0$. Since $z \neq 0$, the only option is $\lambda = \overline{\lambda}$, i.e., $\lambda \in \mathbb{R}$. □

Since any root of $f(\lambda) = |S - \lambda I|$ belongs to our *field of scalars* $F = \mathbb{R}$ over which our space V is defined, by Theorem 23.17 the scalar λ is an *eigenvalue* of S:

Corollary 29.23. *An arbitrary symmetric transformation S of a real space V has an eigenvalue $\lambda \in \mathbb{R}$.*

Lemma 29.24. *The eigenvectors of a symmetric transformation corresponding to different eigenvalues are orthogonal.*

***Proof*.** Assume $S(v_1) = \lambda_1 v_1$ and $S(v_2) = \lambda_2 v_2$, where $\lambda_1 \neq \lambda_2$. Then by point 2 of Proposition 1.6, Theorem 29.21 and by lemma's hypothesis:

$$\lambda_1(v_1 \cdot v_2) = (\lambda_1 v_1) \cdot v_2 = S(v_1) \cdot v_2 = v_1 \cdot S(v_2) = v_1 \cdot (\lambda_2 v_2) = \lambda_2(v_1 \cdot v_2).$$

So we have $\lambda_1(v_1 \cdot v_2) - \lambda_2(v_1 \cdot v_2) = (\lambda_1 - \lambda_2)(v_1 \cdot v_2) = 0$, i.e., $v_1 \perp v_2$. □

Comparing Lemma 29.9 with Lemma 29.22 we see that the roots λ of the characteristic polynomial satisfy $|\lambda| = 1$ for orthogonal transformations, whereas for a symmetric transformations they satisfy $\lambda \in \mathbb{R}$.

So, roughly speaking the orthogonal transformations are generalizations of *rotations, reflections*, whereas the symmetric transformations are generalizations of *scalings*.

29.4. Spectral theorem and the orthogonal diagonalization $Q^T S Q = D$

We called a matrix A is diagonalizable, if $P^{-1}AP = D$ for an invertible matrix P and a diagonal matrix D (see Section 24.2). In transformations language this means that for the transformation T given by A there is a basis consisting of eigenvectors of T. And P is the change of basis matrix from the old basis to the new basis, while the columns of P are the respective eigenvectors.

If $P = Q$ is an *orthogonal* matrix, then we are in better situation because $Q^{-1} = Q^T$, and we have the presentation $Q^T AQ = D$, which is preferrable since the transpose Q^T is much easier to compute rather than the inverse matrix Q^{-1}.

Also, in geometric language orthogonality of Q means that the old and new bases *are "not very different"*: the lengths and angles of basis vectors are preserved (for example, the new basis may be obtained from the old by some rotations or reflections).

This is the reason why it is desirable to find the matrices A that possess such a diagonalization of type $Q^T AQ = D$, which we call *orthogonal diagonalization*. The matrix and the transformation T defined by it are called *orthogonally diagonalizable*.

The Spectral Theorem gives an amazingly simple classification of such matrices:

Theorem 29.25. *(The Spectral Theorem for real matrices) A real matrix S is orthogonally diagonalizable if and only if it is a symmetric matrix.*

Although Spectral Theorem has no trivial proof, it fortunately provides an incomplicated algorithm for orthogonal diagonalization. If you are not interested in proof technique, you are recommended to skip this proof.

Proof of Theorem 29.25. First, assume a real matrix S is orthogonally diagonalizable, and show it is a symmetric matrix.

If $S = PDP^T$ is the orthogonal diagonalization, then

$$S^T = \left(PDP^T\right)^T = (P^T)^T D^T P^T = PD^T P^T = PDP^T = S$$

(we used the evident fact that $D^T = D$ for diagonal matrix D).

The hard part is to prove sufficiency of Spectral Theorem. We do it using induction by matrix size. For 1×1 matrices it is evident, so assume the statement is true for all $(n-1) \times (n-1)$ matrices.

By Corollary 29.23 S has an eigenvalue λ. Let v_1 be the associated eigenvector. By point 1 of Proposition 11.27 we can add some vectors $v_2, \dots, v_n$ to get a basis $G = \{v_1, \dots, v_n\}$ for V. Convert it to an orthonormal basis $E = \{e_1, \dots, e_n\}$ by the Gram-Schmidt process. Recall that by this process the vector v_1 is being just multiplied by $|v_1|^{-1}$. Thus, e_1 is collinear to v_1, and so it also is an eigenvector. The vector $S(e_1) = \lambda e_1$ in the basis E has the coordinates $[\lambda e_1]_E = (\lambda, 0, \dots, 0)$, and the 1'st column of the matrix $B = [S]_E$ looks like:

$$\begin{bmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Then the matrix B can be written as:

$$B = \left[\begin{array}{c:c} \lambda & w \\ \hdashline \mathbf{0} & C \end{array}\right],$$

where C is a $(n-1) \times (n-1)$ matrix, and w is a row vector in $\mathbb{R}^{n-1}$.

Denote by L the change of basis matrix from the old basis G to new basis E. We have $B = L^{-1} S\, L$, or $B = L^T S\, L$, since L is orthogonal. Thus, $B^T = \left(L^T S\, L\right)^T = L^T S^T\, L = L^T S\, L = B$. We got that B also is symmetric, i.e., in above form of B we have $w = 0$ and C is a symmetric matrix:

$$B = \left[\begin{array}{c:c} \lambda & \mathbf{0} \\ \hdashline \mathbf{0} & C \end{array}\right].$$

By inductive hypothesis C is orthogonally diagonalizable: $R^T C\, R = D'$ for some diagonal matrix D' and some orthogonal matrix R. It remains to take the matrix

$$Q = \left[\begin{array}{c:c} 1 & \mathbf{0} \\ \hdashline \mathbf{0} & R \end{array}\right].$$

as the orthogonal matrix Q to get the diagonalization $Q^T S\, Q = D$. Here D is a diagonal matrix the diagonal of which consists of λ, followed by the diagonal elements of D'. $\square$

We have done all the hard work, and it is relatively easy to build the orthogonal diagonalization promised. Suppose we have a transformation S given by a symmetric matrix S in an orthonormal basis of a real space V. By Spectral Theorem S is diagonalizable (to state this we do not even have to use the criterion on geometric multiplicity or on algebraic multiplicity of sections 24.3 and 24.4).

Let $\lambda_1, \dots, \lambda_k$ be all the distinct eigenvalues of S. We can find a basis $\{v_{s1}, \dots, v_{sn_1}\}$ to each eigenspace E_{λ_s} for each eigenvalue λ_s, $s = 1, \dots, k$ (using null space methods). By the Gram-Schmidt process we can bring each of these bases to respective orthonormal form $\{e_{s1}, \dots, e_{sn_1}\}$. The combined set

$$\{e_{11}, \dots, e_{1n_1}; \ \dots \ ; e_{k1}, \dots, e_{kn_k}\} \tag{29.5}$$

also is orthonormal because the vectors corresponding to *distinct* eigenvalues are orthogonal by Lemma 29.24. According to Lemma 27.2 the set (29.5) is independent, and so it is a basis for V.

Put the vectors of (29.5) by columns to get the respective orthogonal matrix Q. We get the orthogonal diagonalization $Q^T S Q = D$, where $Q^T = Q^{-1}$, and where the diagonal matrix D is formed by eigenvalues $\lambda_1, \dots, \lambda_k$, each λ_s repeated as many times as its geometric multiplicity n_s is.

How to orthogonally diagonalize a real matrix. This algorithm relies on the fact that we know the roots of the characteristic polynomial (see Remark 23.19).

Algorithm 29.26 (Detection of orthogonal diagonalizibility of a real matrix and computation of its orthogonal diagonalization)**.** We are given a real matrix $S \in M_{n,n}(\mathbb{R})$, and we know its eigenvalues $\lambda_1, \dots, \lambda_k$.

► Detect if or not S is orthogonally diagonalizible. If yes, compute its diagonal form D, and write it as $D = Q^T S Q$, where Q is an orthogonal matrix.

1. If S is not symmetric, output: S is not orthogonally diagonalizable. End of the process.
2. Else, output: S is orthogonally diagonalizable.
3. For each $s = 1, \dots, k$ compute a basis $\{v_{s1}, \dots, v_{sn_s}\}$ for null$(S - \lambda_s I)$ using Algorithm 15.2, where $n_s = \dim\big(E_{\lambda_s}\big)$.
4. For each $s = 1, \dots, k$ using the Gram-Schmidt process of Algorithm 27.6 bring $\{v_{s1}, \dots, v_{sn_s}\}$ to an orthonormal basis $\{e_{s1}, \dots, e_{sn_s}\}$.
5. Set the matrix $Q \in M_{n,n}(\mathbb{R})$ with columns consisting of coordinates of vectors: $e_{11}, \dots, e_{1n_1}; \ \dots \ ; e_{k1}, \dots, e_{kn_k}$.
6. Set the diagonal matrix $D \in M_{n,n}(\mathbb{R})$ with entries $\lambda_1, \dots, \lambda_k$ on its diagonal, each λ_s occurring n_s times.
7. Output the equality $D = Q^T S Q$ with matrices Q, D computed above.

Remark 29.27. Let us compare this with Algorithm 24.16 to see how much simpler algorithm we got. In Algorithm 29.26 we deduce orthogonal diagonalizibility of S simply from fact that S is symmetric, whereas in Algorithm 24.16 (steps **1-3**) we have to compute the dimensions of all eigenspaces. Also, in this algorithm we use the transpose Q^T whereas in Algorithm 24.16 (step **8**) we have to compute the inverse matrix P^{-1}. On the other hand, in this algorithm we have to do one extra step: the Gram-Schmidt process.

Example 29.28. Consider the real symmetric matrix

$$S = \begin{bmatrix} 3 & 1 & -1 \\ 1 & 3 & -1 \\ -1 & -1 & 5 \end{bmatrix}.$$

Its characteristic polynomial is

$$f(\lambda) = |S - \lambda I| = -(\lambda - 2)(\lambda - 3)(\lambda - 6),$$

and we have three eigenvalues: $\lambda_1 = 2$, $\lambda_2 = 3$, $\lambda_3 = 6$.

Thus, each eigenspace is 1-dimensional. So let us find eigenbases for each of them.

For $\lambda_1 = 2$ we have

$$S - \lambda_1 I = \begin{bmatrix} 3 & 1 & -1 \\ 1 & 3 & -1 \\ -1 & -1 & 5 \end{bmatrix} - 2 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$=\begin{bmatrix}1&1&-1\\1&1&-1\\-1&-1&3\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&1&0\\0&0&\mathbf{1}\\0&0&0\end{bmatrix}=\mathrm{rref}(S-\lambda_1 I).$$

As the basis for E_{λ_1} take $v_1=(1,-1,0)$.

For $\lambda_2=3$ we have

$$S-\lambda_2 I=\begin{bmatrix}3&1&-1\\1&3&-1\\-1&-1&5\end{bmatrix}-3\cdot\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$=\begin{bmatrix}0&1&-1\\1&0&-1\\-1&-1&2\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&0&-1\\0&\mathbf{1}&-1\\0&0&0\end{bmatrix}=\mathrm{rref}(S-\lambda_2 I).$$

As the basis for E_{λ_2} take $v_2=(-1,-1,-1)$ or, simpler, $v_2=(1,1,1)$.

For $\lambda_3=6$ we have

$$S-\lambda_3 I=\begin{bmatrix}3&1&-1\\1&3&-1\\-1&-1&5\end{bmatrix}-6\cdot\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$=\begin{bmatrix}-3&1&-1\\1&-3&-1\\-1&-1&-1\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&0&\frac12\\0&\mathbf{1}&\frac12\\0&0&0\end{bmatrix}=\mathrm{rref}(S-\lambda_3 I).$$

As the basis for E_{λ_3} take $v_3=(\frac12,\frac12,-1)$ or, simpler, $v_3=(1,1,-2)$.

Since each of three bases consists of one vector only, the Gram-Schmidt process applied to any of them just means that we normalize the vectors: $e_1=(\frac{1}{\sqrt2},-\frac{1}{\sqrt2},0)$, $e_2=(\frac{1}{\sqrt3},\frac{1}{\sqrt3},\frac{1}{\sqrt3})$, $e_3=(\frac{1}{\sqrt6},\frac{1}{\sqrt6},-\frac{2}{\sqrt6})$. So the orthogonal matrix is:

$$Q=\begin{bmatrix}\frac{1}{\sqrt2}&\frac{1}{\sqrt3}&\frac{1}{\sqrt6}\\-\frac{1}{\sqrt2}&\frac{1}{\sqrt3}&\frac{1}{\sqrt6}\\0&\frac{1}{\sqrt3}&-\frac{2}{\sqrt6}\end{bmatrix}=\frac{1}{\sqrt6}\begin{bmatrix}\sqrt3&\sqrt2&1\\-\sqrt3&\sqrt2&1\\0&\sqrt2&-2\end{bmatrix},$$

and the diagonal matrix is:

$$D=\begin{bmatrix}2&0&0\\0&3&0\\0&0&6\end{bmatrix}.$$

The equality $D=Q^TSQ$ is very easy to verify.

Let us do an example in which the eigenspaces are not 1-dimensional, so we will really have to orthigonalize vectors.

Example 29.29. Assume we are given the real symmetric matrix

$$S=\begin{bmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{bmatrix}.$$

The characteristic polynomial is $f(\lambda)=|S-\lambda I|=-\lambda(\lambda-3)^2$, and we have two eigenvalues $\lambda_1=0$, $\lambda_2=3$.

For $\lambda_1=0$ we have

$$S-\lambda_1 I=\begin{bmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{bmatrix}$$

$$\sim\begin{bmatrix}\mathbf{1}&0&-1\\0&\mathbf{1}&-1\\0&0&0\end{bmatrix}=\mathrm{rref}(S-\lambda_1 I).$$

As the basis for E_{λ_1} take $v_1=(-1,-1,-1)$ or, simpler, $v_1=(1,1,1)$.

For $\lambda_2=3$ we have

$$S-\lambda_2 I=\begin{bmatrix}2&-1&-1\\-1&2&-1\\-1&-1&2\end{bmatrix}-3\cdot\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$=\begin{bmatrix}-1&-1&-1\\-1&-1&-1\\-1&-1&-1\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&1&1\\0&0&0\\0&0&0\end{bmatrix}=\mathrm{rref}(S-\lambda_2 I).$$

As the basis for E_{λ_2} take $v_{21}=(1,-1,0)$ and simpler, $v_{22}=(1,0,-1)$.

The Gram-Schmidt process applied to the first basis just means that we normalize the vector v_1 to get $e_1=(\frac{1}{\sqrt3},\frac{1}{\sqrt3},\frac{1}{\sqrt3})$.

Now apply the Gram-Schmidt process to vectors v_{21},v_{22}. We have $h_{21}=v_{21}$, and $e_{21}=(\frac{1}{\sqrt2},-\frac{1}{\sqrt2},0)$. Then

$$h_{22}=v_{22}-\mathrm{proj}_{h_{21}}(v_{22})$$

$$=(1,0,-1)-\tfrac12(1,-1,0)=(\tfrac12,\tfrac12,-1).$$

$$e_{22}=\tfrac{1}{|h_{22}|}h_{22}=(\tfrac{1}{\sqrt6},\tfrac{1}{\sqrt6},-\tfrac{\sqrt2}{\sqrt3}).$$

The orthogonal matrix is:

$$Q=\begin{bmatrix}\frac{1}{\sqrt3}&\frac{1}{\sqrt2}&\frac{1}{\sqrt6}\\\frac{1}{\sqrt3}&-\frac{1}{\sqrt2}&\frac{1}{\sqrt6}\\\frac{1}{\sqrt3}&0&-\frac{\sqrt2}{\sqrt3}\end{bmatrix}=\frac{1}{\sqrt6}\begin{bmatrix}\sqrt2&\sqrt3&1\\\sqrt2&-\sqrt3&1\\\sqrt2&0&-\sqrt4\end{bmatrix},$$

and the diagonal matrix is:

$$D=\begin{bmatrix}0&0&0\\0&3&0\\0&0&3\end{bmatrix}.$$

The equality $D=Q^TSQ$ is easy to verify.

Example 29.30. If a matrix S is *orthogonally* diagonalizable, i.e., $D=Q^TSQ$, then S also is diagonalizable in the *ordinary* sense, i.e., $D=P^{-1}SP$ for some invertible matrix P. We just take $P=Q$ and $P^{-1}=Q^T$.

However, *not every diagonalization of matrix is orthogonal diagonalization*, even if the matrix in question is *symmetric*.

Consider the previous Examples 29.29 for which we already have found the matrices Q and D. The vectors

$$(\tfrac{1}{\sqrt3},\tfrac{1}{\sqrt3},\tfrac{1}{\sqrt3}),\quad(\tfrac{1}{\sqrt2},-\tfrac{1}{\sqrt2},0),\quad(\tfrac{1}{\sqrt6},\tfrac{1}{\sqrt6},-\tfrac{\sqrt2}{\sqrt3})$$

do form an (orthonormal) eigenbasis for $\mathbb{R}^3$. Take some non-zero scalar multiples of those vectors, such as:

$$(3,3,3),\quad(5,-5,0),\quad(4,4,-8).$$

They still are eigenvectors and they still are linearly independent. In this new eigenbasis we have the same matrix D as above, but the invertible matrix this time is:

$$P = \begin{bmatrix} 3 & 5 & 4 \\ 3 & -5 & 4 \\ 3 & 0 & -8 \end{bmatrix}.$$

We have a diagonalization $D = P^{-1}S\,P$ which is *not* orthogonal, and which uses the rather ugly inverse matrix:

$$P^{-1} = \begin{bmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} \\ \frac{1}{10} & -\frac{1}{10} & 0 \\ \frac{1}{24} & \frac{1}{24} & -\frac{1}{12} \end{bmatrix}.$$

Exercises

E.29.1. Detect if each of the following matrices is orthogonal: $A = \left[\begin{smallmatrix} 0 & 2 & 2 \\ 2 & 2 & -2 \\ 2 & -2 & 0 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$, $C = \left[\begin{smallmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right]$. *Hint*: you can use either one of the criterions in Lemma 29.1 or Theorem 29.8.

E.29.2. The transformation T is given on $\mathbb{R}^3$ by the rule $T(x,y,z) = \frac{1}{2}(\sqrt{3}x-y,\ x+\sqrt{3}y,\ 2y-2z)$. **(1)** Find out if T is orthogonal using point 2 of Theorem 29.8. *Hint*: compare the lengths $|v|$ and $|T(v)|$ for an appropriate vector. **(2)** Find out if T is orthogonal using point 3 of Theorem 29.8. *Hint*: build the matrix if T in, say, standard basis.

E.29.3. We are given that a transformation T of a real space V preserves the angles between vectors, i.e., the angle between $T(u)$ and $T(v)$ is equal to the angle between u and v for any $u, v \in V$. Does T also preserve the vector lengths, i.e., does $|T(v)| = |v|$ hold for any $v \in V$? See the remark after Theorem 29.8.

E.29.4. Let P be a projection of $\mathbb{R}^3$ given as $P(x,y,z) = (x,y,0)$. Show that P is *not* orthogonal in two ways: **(1)** Study the matrix of P. **(2)** Apply Theorem 29.8 to P.

E.29.5. A transformation T of the space $\mathbb{R}^3$ has the characteristic polynomial $f(\lambda) = (\lambda+1)(\lambda-1)(\lambda-2)$. Using this information deduce weather T can be an orthogonal transformation.

E.29.6. Compute the QR-factorization of the matrices: **(1)** $A = \left[\begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix}\right]$. **(2)** $B = \left[\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{smallmatrix}\right]$.

E.29.7. We are given the invertible matrix A for which we know its QR-factorization $A = QR$. Given that A is diagonalizable, find the absolute value $|\lambda_1 \cdots \lambda_k|$ of the product of all eigenvalues $\lambda_1, \dots, \lambda_k$ of A. *Hint*: what is the determinant of A?

E.29.8. Detect if the transformation T of the space $\mathbb{R}^3$ is a symmetric transformation, if it is given as **(1)** $T(x,y,z) = \big(x - 2(y+2z),\ z-2x,\ 4x+y+5z\big)$. **(2)** $T = P_1 + P_2$, where P_1 is the projection $P_1(x,y,z) = (0,y,z)$, and P_2 is the projection $P_2(x,y,z) = (x,0,z)$ **(3)** $T = 3R^5$, where R is the reflection $R(x,y,z) = (x,-y,\ z)$.

E.29.9. We are given the transformation $T(x,y,z) = (x-z,\ 5y,\ x+z)$. **(1)** Show that T is *not* orthogonal using Theorem 29.8. I.e., find a vector $v \in \mathbb{R}^3$ such that $|T(v)| \neq |v|$. Or find two vectors $u, v \in \mathbb{R}^3$ such that $T(u) \cdot T(v) \neq u \cdot v$. **(2)** Show that T is *not* symmetric using Theorem 27.19. I.e., find two vectors $u, v \in \mathbb{R}^3$ such that $T(u) \cdot v \neq u \cdot T(v)$.

E.29.10. Compute the orthogonal diagonalization of the matrix $A = \left[\begin{smallmatrix} 3 & 1 & -1 \\ 1 & 3 & 1 \\ -1 & 1 & 3 \end{smallmatrix}\right]$.

E.29.11. Compute the orthogonal diagonalization of the matrix $A = \left[\begin{smallmatrix} 7 & -2 & -2 \\ -2 & 7 & -2 \\ -2 & -2 & 7 \end{smallmatrix}\right]$. *Hint*: Use the solution of the similar Exercise 29.10.

E.29.12. Compute the orthogonal diagonalization of the matrix $A = \left[\begin{smallmatrix} 1 & -2 & 2 \\ -2 & 4 & -4 \\ 2 & -4 & 4 \end{smallmatrix}\right]$. You may use the fact the 0 is one of the eigenvalues of A.

APPENDIX A

Divisibility and the Euclid's Algorithm in $\mathbb{Z}$

A.1. The Euclid's Algorithm and the greatest common divisor in $\mathbb{Z}$

As usual, we denote by $\mathbb{Z}$ the set of integers with operations of addition $x+y$ and multiplication $x \cdot y$ for any $x, y \in \mathbb{Z}$. We say that an integer d *divides* an integer x, or d is a *divisor* of x, or x is a *multiple* of d, if there is an integer c such that $x = d \cdot c$. This is denoted by $d \mid x$, or by $x \vdots d$.

An integer d is a *common divisor* of x and y, if it divides both x and y. Moreover:

Definition A.1. An integer d is a *greatest common divisor* of integers x and y, if d is their common divisor, and every common divisor h of x and y also divides d. I.e.:

1. $d \mid x$ and $d \mid y$;
2. if $h \mid x$ and $h \mid y$, then $h \mid d$.

The greatest common divisor of x and y is denoted by $\gcd(x, y)$. For instance:

$$\gcd(36, 27) = 9, \quad \gcd(-36, 27) = 9, \quad \gcd(-36, -27) = 9.$$

Notice that $\gcd(x, y)$ is not unique for the given x, y. We also have $\gcd(36, 27) = -9$, since -9 and 9 both meet the points of Definition A.1.

Do every two non-zero integers always have a greatest common divisor? And if yes, how to compute it? The answers are given by the Euclid's Algorithm.

Theorem A.2 (Euclid's Theorem)**.** *For any integer x and for a non-zero integer y there exist integers q and r such that*

$$x = qy + r, \tag{A.1}$$

where either $r = 0$, or $r \neq 0$ and $|r| < |y|$.

Proof. If $x = 0$, then (A.1) is trivial for $q = r = 0$. So we suppose x is non-zero. The next trivial case is $|x| < |y|$, when we can take $q = 0$, $r = x$ to get $x = 0 \cdot y + x$.

Thus, suppose $|x| \geq |y| > 0$, and consider two cases: If x and y are both positive or both negative, take q to be the largest positive integer for which $|x| \geq |qy|$ and $|x| < |(q+1)y|$. If one of x and y is positive, and the other is negative, take q to be the least negative integer for which $|x| \geq |qy|$ and $|x| < |(q-1)y|$. Then for both cases we can choose the $r = x - qy$. □

Call (A.1) a *division with remainder*. Here x is the *dividend*, y is the *divisor*, q is the *quotient*, r is the *remainder*.

For the given non-zero integers x and y let us repeatedly apply Euclid's Theorem adding each of the lines below, only if the remainder in previous line is non-zero:

$$\begin{aligned}
x &= qy + r, && \text{where } r = 0 \text{ or } |r| < |y|,\\
y &= q_1 r + r_1, && \text{where } r_1 = 0 \text{ or } |r_1| < |r|,\\
r &= q_2 r_1 + r_2, && \text{where } r_2 = 0 \text{ or } |r_2| < |r_1|,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && \text{where } r_{n-1}{=}0 \text{ or } |r_{n-1}|{<}|r_{n-2}|,\\
r_{n-2} &= q_n r_{n-1} + \boldsymbol{r_n}, && \text{where } r_n = 0 \text{ or } |r_n| < |r_{n-1}|,\\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned} \tag{A.2}$$

Since $|r| > |r_1| > |r_2| > \cdots \geq 0$ are strictly descending, this process cannot go infinitely. It ends at some step, when we finally get $r_{n+1} = 0$. Denote the last non-zero remainder by $d = r_n$, and show that $d = \gcd(x, y)$.

From the last line of (A.2) we get $d \mid r_{n-1}$. Since d divides both r_n and r_{n-1}, we from the line before get $d \mid r_{n-2}$. In similar way we from the line before it get $d \mid r_{n-3}$. Going upwards in (A.2) we eventually get $d \mid y$ and $d \mid x$, i.e., the first point of Definition A.1.

To check the second point of Definition A.1 suppose $h \mid x$ and $h \mid y$. Then by the first line of (A.2) we have $h \mid r$. From the second line we get $h \mid r_1$. Going downwards in (A.2) we eventually get $h \mid d$.

Example A.3. Let us compute $\gcd(1071, 462)$.

$$\begin{aligned}
1071 &= 2 \cdot 462 + 147,\\
462 &= 3 \cdot 147 + 21,\\
147 &= 7 \cdot 21 + 0.
\end{aligned}$$

So $\gcd(1071, 462) = 21$. In the same time $\gcd(-1071, -462) = 21$, $\gcd(1071, 462) = -21$, or $\gcd(1071, -462) = 21$.

Example A.4. Compute $\gcd(53667, 25527)$.

$$\begin{aligned}
53667 &= 2 \cdot 25527 + 2613,\\
25527 &= 9 \cdot 2613 + 2010,\\
2613 &= 1 \cdot 2010 + 603,\\
2010 &= 3 \cdot 603 + 201,\\
603 &= 3 \cdot 201 + 0.
\end{aligned}$$

Therefore $\gcd(53667, 25527) = 201$.

Theorem A.5. *For any non-zero integers x and y there are integers u and v such that*

$$\boldsymbol{ux + vy = d = \gcd(x, y)}. \tag{A.3}$$

Proof. From the system (A.2) we have

$$\begin{aligned}
d = r_n &= r_{n-2} - q_n r_{n-1},\\
r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2}.
\end{aligned}$$

Substituting the value of r_{n-1} into the previous line we get:

$$\begin{aligned}
d &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2})\\
&= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2}.
\end{aligned}$$

This presentation of d uses the remainders r_{n-3} and r_{n-2}, and applying the previous line of (A.2) we will get a presentation of d using r_{n-4} and r_{n-3}. Continuing this process we go upwards in (A.2), and eventually get the presentation $d = ux + vy$. □

The above process of finding the representation (A.3) is called *Extended Euclid's Algorithm*, and the equality (A.3) is sometimes called *Bézout's identity* with *Bézout's coefficients* u, v.

Call two integers x and y *coprime*, if $\gcd(x, y) = 1$.

Corollary A.6. *For any coprime integers x and y there are integers u, v such that:*

$$ux + vy = 1.$$

Example A.7. Using calculations done for integers $x = 1071, y = 462$ in Example A.3 we have:

$$\begin{aligned} 21 &= 462 - 3 \cdot 147 \\ &= 462 - 3(1071 - 2 \cdot 462) \\ &= -3 \cdot 1071 + (1 + 3 \cdot 2)462 \\ &= -3 \cdot 1071 + 7 \cdot 462 \\ &= -3x + 7y. \end{aligned}$$

Example A.8. By Example A.4 we get:

$$\begin{aligned} 201 &= 2010 - 3 \cdot 603 \\ &= 2010 - 3(2613 - 1 \cdot 2010) \\ &= -3 \cdot 2613 + 4 \cdot 2010 \\ &= -3 \cdot 2613 + 4 \cdot (25527 - 9 \cdot 2613) \\ &= 4 \cdot 25527 - 39 \cdot 2613 \\ &= 4 \cdot 25527 - 39(53667 - 2 \cdot 25527) \\ &= -39 \cdot 53667 + 82 \cdot 25527 = -39x + 82y. \end{aligned}$$

A.2. The least common multiple in $\mathbb{Z}$

Call an integer m a *common multiple* of integers x and y, if they both divide m.

Definition A.9. An integer m is a *least common multiple* of integers x and y, if m is their common multiple, and every common multiple l of x and y also is divisible by m. I.e.:

1. $x \mid m$ and $y \mid m$;
2. if $x \mid l$ and $y \mid l$, then $m \mid l$.

The least common multiple of a and b is denoted by $\operatorname{lcm}(x, y)$. For example:

$$\operatorname{lcm}(36, 27) = 108, \ \ \operatorname{lcm}(36, 27) = -108, \ \ \operatorname{lcm}(-36, 27) = 108, \ \ \operatorname{lcm}(-36, -27) = 108.$$

To show that every two non-zero integers always have a greatest common divisor, and to obtain a method of its calculation we need a simple lemma:

Lemma A.10. *If the product xy of integers x, y is divisible by the integer h, and x is coprime with h, then y is divisible by h.*

Proof. By Theorem A.5 we can find $u, v \in \mathbb{Z}$ such that $ux + vh = 1$. Multiplying both sides by y we get:

$$u \cdot xy + vh \cdot y = y.$$

Since $h \mid (u \cdot xy)$ and $h \mid (vh \cdot y)$, we have $h \mid y$. □

Corollary A.11. *If the product xy of integers x, y is divisible by a prime number p, then at least one of x, y also is divisible by p.*

Theorem A.12. *For any non-zero integers x and y their least common multiple exists, and*

$$\gcd(x, y) \cdot \operatorname{lcm}(x, y) = x \cdot y. \tag{A.4}$$

Proof. Since x and y are divisible by $d = \gcd(x, y)$, write $x = dc$ and $y = de$. Denote $m = dce$, and show that $m = \operatorname{lcm}(x, y)$. The first point of Definition A.9, clearly, is satisfied: $m = (dc)e = xe$, i.e., $x \mid m$, and also $m = (de)c = yc$, i.e., $y \mid m$.

To prove the second point take any integer l divisible by x and y. We have $l = xk = dck$ for some k. Since $y = d \cdot e$ divides $l = d \cdot ck$, we have $e \mid ck$. Notice that e and c are coprime, for, if they had a non-trivial common divisor s, then sd would be a common divisor of x and y, not dividing d. Thus, by previous lemma $e \mid ck$ implies $e \mid k$, i.e., $k = eq$ for some q. We have $l = xk = dc \cdot eq = dce \cdot q = mq$. □

(A.4) provides the simple formula to compute the least common multiple for any non-zero integers x and y:

$$\mathbf{lcm}(x, y) = \frac{x \cdot y}{\mathbf{gcd}(x, y)}.$$

Example A.13. We already computed in Example A.3 that $\gcd(1071, 462) = 21$. Therefore we get:

$$\operatorname{lcm}(x, y) = \frac{1071 \cdot 462}{21} = 23562.$$

Example A.14. Since we in Example A.4 have already computed $\gcd(53667, 25527) = 201$, we have:

$$\operatorname{lcm}(x, y) = \frac{53667 \cdot 25527}{201} = 6815709.$$

APPENDIX B

Modular arithmetic in $\mathbb{Z}_m$ and $\mathbb{Z}_p$

B.1. Modular operations in $\mathbb{Z}_m$

Fix any natural number $m \geq 2$, and denote by $\mathbb{Z}_m$ the set

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Call m the *modulus* and define on $\mathbb{Z}_m$ *modular operations* $+_m$ and $\cdot_m$ as follows. For any $x, y \in \mathbb{Z}_m$ divide the sum $x + y$ by m, and define $x +_m y$ to be equal to the remainder of that division (see Appendix A.1). Also, divide the product $x \cdot y$ by m, and define $x \cdot_m y$ to be equal to the remainder of that division.

Example B.1. Let us fix the modulus $m = 5$ and do some modular operations in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. We have $4 +_5 3 = 2$ because $4 + 3 = 7$, and dividing 7 by 5 we get the remainder 2. Also, $3 \cdot_5 3 = 4$ because $3 \cdot 3 = 9$, and dividing 9 by 5 we get the remainder 4.

Next, for the modulus $m = 23$ we have $\mathbb{Z}_{23} = \{0, 1, 2, \ldots, 22\}$. It is easy to compute:

$$17 +_{23} 21 = 15,$$
$$7 \cdot_{23} 16 = 20,$$
$$5 \cdot_{23} 6 \ +_{23} \ 12 \cdot_{23} 6 = 7 +_{23} 3 = 10.$$

Let us see which properties of operations $+_m$ and $\cdot_m$ in $\mathbb{Z}_m$ are similar to properties of ordinary operations $+$ and $\cdot$ with integers in $\mathbb{Z}$ or with real numbers in $\mathbb{R}$.

1. $\mathbb{Z}_m$ is *closed* with respect to $+_m$ and $\cdot_m$, i.e., the sum $x +_m y$ and product $x \cdot_m y$ belong to $\mathbb{Z}_m$ for arbitrary $x, y \in \mathbb{Z}_m$.
2. Operations $+_m$ and $\cdot_m$ are *commutative*, i.e., $x +_m y = y +_m x$ and $x \cdot_m y = y \cdot_m x$.
3. Operations $+_m$ and $\cdot_m$ are *associative*, i.e., $(x +_m y) +_m z = x +_m (y +_m z)$ and also $(x \cdot_m y) \cdot_m z = x \cdot_m (y \cdot_m z)$.
4. There are *trivial* elements for both $+_m$ and $\cdot_m$. Namely, for the additive trivial *zero* element $0 \in \mathbb{Z}_m$ we have $x +_m 0 = x$ for any $x \in \mathbb{Z}_m$. And for the multiplicative trivial *unit* element $1 \in \mathbb{Z}_m$ we have $x \cdot_m 1 = x$ for any $x \in \mathbb{Z}_m$.
5. Operations $+_m$ and $\cdot_m$ are connected by *distributivity* condition, i.e., $x \cdot_m (y +_m z) = x \cdot_m y + x \cdot_m z$.
6. There is an *opposite* element $-x$ for every $x \in \mathbb{Z}_m$, i.e., $x +_m (-x) = 0$. Indeed, just take $-x = m - x$. Say, for $3 \in \mathbb{Z}_5$ we have $-3 = 2$ because $3 +_5 2 = 0$. Unlike the previous properties, this property is for addition only.

A property in which $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{Z}_m$ differ much is the existence of *inverse* for any non-zero element. We know that any non-zero number x has an inverse in $\mathbb{R}$, i.e., there is an x^{-1} such that $x \cdot x^{-1} = 1$. However, in $\mathbb{Z}$ the only two numbers with this property are 1 and -1. The next two examples show that the situation is more mixed in $\mathbb{Z}_m$.

Example B.2. Take $m = 6$ and $x = 3 \in \mathbb{Z}_6$. Then there is no element 3^{-1} in $\mathbb{Z}_6$. We can verify this in two ways.

Firstly, multiplying the element 3 by any of six elements of $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ we never get 1.

Secondly, if the element 3^{-1} existed in $\mathbb{Z}_6$, then multiplying both sides of the equality

$$3^{-1} \cdot_6 3 = 1$$

by 2 we would get:

$$(3^{-1} \cdot_6 3) \cdot_6 2 = 1 \cdot_6 2 = 2,$$

which brings to contradiction with:

$$(3^{-1} \cdot_6 3) \cdot_6 2 = 3^{-1} \cdot_6 (3 \cdot_6 2) = 3^{-1} \cdot_6 0 = 0 \neq 2.$$

Example B.3. On the other hand, taking $m = 5$ we get $\mathbb{Z}_5 = \{0,1,2,3,4\}$ in which *every* non-zero element has an inverse:

$$1^{-1} = 1, \quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4.$$

So in this sense $\mathbb{Z}_5$ is similar to $\mathbb{R}$. Every non-zero element in any them has an inverse.

Agreement B.4. We need some simplification in notation. For briefness we will mostly denote the operations in $\mathbb{Z}_m$ not by $+_m$ and $\cdot_m$ but by just $+$ and $\cdot$, whenever it is clear that we do *modular* operations. Say, writing "$13 + 9 = 5$ and $5 \cdot 11 = 4$ in $\mathbb{Z}_{17}$" we suppose the modular sum $13 +_{17} 9 = 5$ and the modular product $5 \cdot_{17} 11 = 4$.

B.2. Modular inverses in $\mathbb{Z}_p$

The following theorem allows to distinguish those moduli m for which all the non-zero numbers in $\mathbb{Z}_m$ have inverses:

Theorem B.5. *$\mathbb{Z}_m$ contains an inverse $x^{-1} \in \mathbb{Z}_m$ for any non-zero $x \in \mathbb{Z}_m$ if and only if m is a prime.*

Proof. If $m = kl$ is a composite number ($k, l \neq \pm 1$), then there is no k^{-1} in $\mathbb{Z}_m$ because, otherwise, multiplying the equality $k^{-1}k = 1$ by l we would get:

$$(k^{-1}k)\, l = 1 \cdot l = l,$$
$$(k^{-1}k)\, l = k^{-1}(kl) = k^{-1} \cdot 0 = 0$$

which is a contradiction as $l \neq 0$ (compare with above Example B.2).

If $m = p$ is a prime number, then fix any $x = 1, 2, \ldots, p-1$, and notice that p is coprime to x. By Corollary A.6, there are integers u, v such that $up + vx = 1$, that is, $vx - 1$ is divisible by p.

In case $1 < v < p$, we already get that $v = x^{-1}$ in $\mathbb{Z}_p$.

In case $v \leq 0$ or $v \geq p$, just replace v by an integer v' such that $v' \in \{1, \ldots, p-1\}$ and $v' \equiv v (\operatorname{mod} p)$ (i.e., divide v by p and take v' to be the positive remainder obtained). Then $v'x - 1$ still is divisible by p. I.e., we have $v' = x^{-1}$ in $\mathbb{Z}_p$. □

The above proof also shows how to find the inverse x^{-1} of the non-zero $x \in \mathbb{Z}_p$. First construct the equality $up + vx = 1$ by the Extended Euclid's Algorithm (see Theorem A.5 and Corollary A.6). Then:

If $1 < v < p$, just take v as x^{-1}.

If $v \leq 0$, then add to v a multiple kp of p to get a number $v' = v + kp$ such that $1 < v' < p$. Then take v' as x^{-1}.

If $v \geq 0$, then subtract from v a multiple kp of p to get a $v' = v - kp$ such that $1 < v' < p$. Then take v' as x^{-1}.

Example B.6. Let us find 2^{-1} in $\mathbb{Z}_5$ by the method of this proof. Since, evidently,

$$-1\cdot 5+3\cdot 2=1,$$

we have $2^{-1}=3$ (compare with Example B.2).

Example B.7. Find the inverse 4^{-1} of the number 4 in $\mathbb{Z}_{151}$.

Following the steps of the Euclid's Algorithm we have:

$$\begin{aligned} 151 &= 37\cdot 4+3,\\ 4 &= 1\cdot 3+1,\\ 3 &= 3\cdot 1+0. \end{aligned}$$

From where:

$$\begin{aligned} 1 &= 4-1\cdot 3\\ &= 4-(151-37\cdot 4)\\ &= -151+38\cdot 4. \end{aligned}$$

We have $4^{-1}=38$ in $\mathbb{Z}_{151}$, that is, $4\cdot_{151}38=1$.

Example B.8. To see that sometimes computation of an inverse may be a more routine process, and to actually apply the specific case mentioned at the end of proof above, let us find the inverse 62^{-1} in $\mathbb{Z}_{151}$.

By the Euclid's Algorithm:

$$\begin{aligned} 151 &= 2\cdot 62+27,\\ 62 &= 2\cdot 27+8,\\ 27 &= 3\cdot 8+3,\\ 8 &= 2\cdot 3+2,\\ 3 &= 1\cdot 2+1,\\ 2 &= 2\cdot 1+0. \end{aligned}$$

From where:

$$\begin{aligned} 1 &= 3-1\cdot 2\\ &= 3-(8-2\cdot 3)\\ &= -8+3\cdot 3\\ &= -8+3(27-3\cdot 8)\\ &= 3\cdot 27-10\cdot 8\\ &= 3\cdot 27-10(62-2\cdot 27)\\ &= -10\cdot 62+23\cdot 27\\ &= -10\cdot 62+23(151-2\cdot 62)\\ &= 23\cdot 151-56\cdot 62. \end{aligned}$$

In this case $v=-56$ is *not* in $\{1,\dots,150\}$, and we yet have to divide v by 151 (i.e., to add 151 to v):

$$-56=-1\cdot 151+95.$$

Since $95\in\{1,\dots,150\}$, we get $62^{-1}=95$ in $\mathbb{Z}_{151}$, that is, $62\cdot_{151}95=1$.

Theorem B.5 together with six properties listed in previous section show that when $m=p$ is prime number, then the algebraic properties of operations of addition and multiplication in $\mathbb{Z}_p$ are very similar to the properties of the operations in $\mathbb{R}$. In terminology of Section 4.1 both $\mathbb{Z}_p$ and $\mathbb{R}$ are *fields*, and Theorem B.5 can be rephrased as: *$\mathbb{Z}_m$ is a field if and only if $m=p$ is prime*.

This is the reason why in our course we consider $\mathbb{Z}_p$ with prime modulus p mainly: vector spaces are defined on *fields*. So whenever we write $\mathbb{Z}_p$, we consider p to be a *prime* number even if the context.

APPENDIX C

Introduction to complex numbers

C.1. Definition of complex numbers

The appendix is a just quick summary for complex numbers. For detailed introduction we refer to the textbooks cited in Bibliography.

Complex numbers are introduced by a special mathematical symbol called "imaginary unit" and denoted by i. It is a number the square of which is defined to be equal to -1, that is, $i^2 = -1$. Using this symbol the complex numbers x are defined as the sums

$$\boldsymbol{x = a + bi}$$

with $a, b \in \mathbb{R}$ (such as $2+3i$, $6-i$, etc.). Denote the set of complex numbers by $\mathbb{C}$. It is comfortable to present compex numbers on two-dimensional plane, putting the number $x = a + bi$ at the point with coordinates a and b, as shown in Figure C.1 (a).

The number $\mathrm{Re}(x) = a$ is called the *real part* of $x = a + bi$, and $\mathrm{Im}(x) = b$ is called *imaginary part* of x. So we have:

$$x = \mathrm{Re}(x) + \mathrm{Im}(x)\, i.$$

When the imaginary part or the real part of x are zero, we may omit them, and just write, say, 2 instead of $2+0i$, or write $5i$ instead of $0+5i$. Keeping this in mind, the real numbers can also be considered as complex numbers with "missing" imaginary parts, i.e., we can write $\mathbb{R} \subseteq \mathbb{C}$.

The complex number $\bar{x}$ is the *conjugate* of x, if $\mathrm{Re}(\bar{x}) = \mathrm{Re}(x)$ and $\mathrm{Im}(\bar{x}) = -\mathrm{Im}(x)$, that is, $\bar{x} = a - bi$, see Figure C.1 (a).

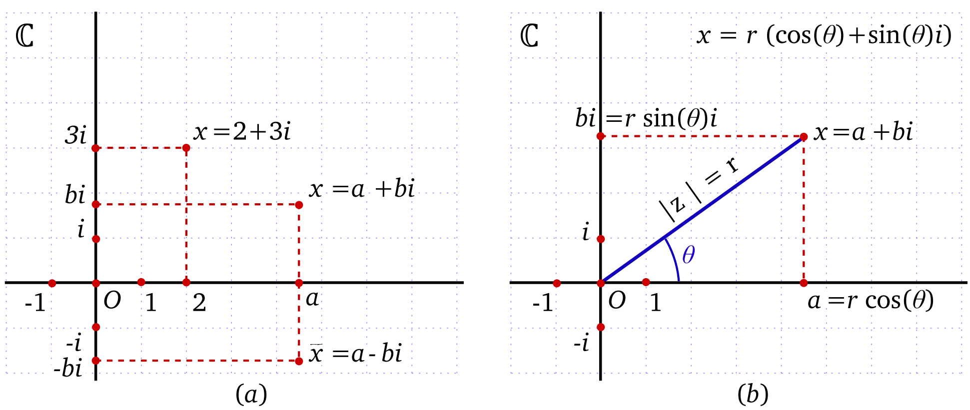


FIGURE C.1. The complex plane $\mathbb{C}$.

Any complex number $x = a + bi \in \mathbb{C}$ has a *modulus* (or absolute value):

$$r = |x| = \sqrt{a^2 + b^2} \in [0, \infty)$$

(the distance of x from the origin O), and an *argument*:

$$\theta = \arg x \in (-\pi, \pi],$$

where θ is the angle formed by the segment $[Ox]$ with the positive real axis (see Figure C.1 (b). Clearly, $r\cos\theta = a$ and $r\sin\theta = b$, and we get the *polar* form (also called the *trigonometric* form, or the *mod-arc* form) of a complex number x:

$$\begin{aligned} x &= a + bi = r\cos\theta + i\, r\sin\theta \\ &= \boldsymbol{r(\cos\theta + i\sin\theta)}. \end{aligned}$$

Example C.1. Here are some complex numbers presented in polar form:

$$\begin{aligned} 1+i &= \sqrt{2}\left(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4}\right), \\ 2-2i &= \sqrt{8}\left(\cos\left(-\tfrac{\pi}{4}\right) + i\sin\left(-\tfrac{\pi}{4}\right)\right), \end{aligned}$$

$$\begin{aligned} 3i &= 3\left(\cos\tfrac{\pi}{2} + i\sin\tfrac{\pi}{2}\right), \\ -3i &= 3\left(\cos\left(-\tfrac{\pi}{2}\right) + i\sin\left(-\tfrac{\pi}{2}\right)\right), \\ 5 &= 5\left(\cos 0 + i\sin 0\right), \\ -5 &= 5\left(\cos\pi + i\sin\pi\right). \end{aligned}$$

C.2. Operations with complex numbers

The *sum* of complex numbers $x = a + bi$ and $x' = a' + b'i$ is defined by

$$x + x' = (a + a') + (b + b')i,$$

which is similar to the rule of vector sum in $\mathbb{R}^2$ (see Figure C.2 (a), compare it with Figure 1.3 in Section 1.1). The *product* of complex numbers $x = a + bi$ and $x' = a' + b'i$ is defined based on the equality $i^2 = -1$ and on distributivity. Namely:

$$\begin{aligned} x \cdot x' &= (a + bi)(a' + b'i) \\ &= aa' + (ba')i + (ab')i + (bb')i^2 = (aa' - bb') + (a'b + ab')i. \end{aligned}$$

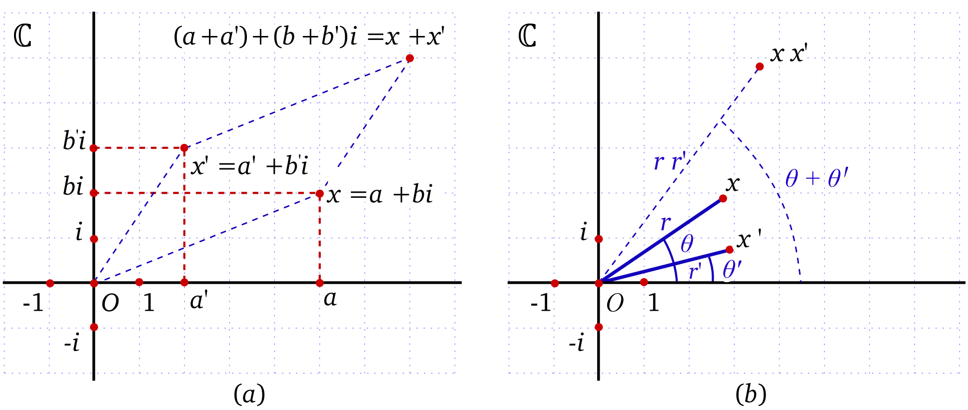


FIGURE C.2. Addition and multiplication of complex numbers.

Example C.2. Here are sums and product of some complex numbers:

$$(2+3i)+(-4+2i)=-2+5i,$$
$$3i+(1+4i)=1+7i,$$
$$(2+3i)\cdot(-4+2i)=-8-12i+4i+6i^2=-14-8i,$$
$$(2+i)\cdot 6i=12i+6i^2=-6+12i.$$

Complex numbers multiplication has a handy geometric interpretation. Take any two complex numbers x and x' in their polar forms $x = r(\cos\theta + i\sin\theta)$ and $x' = r'(\cos\theta' + i\sin\theta')$. Then:

$$x\cdot x' = rr'\big[(\cos\theta\cos\theta' - \sin\theta\sin\theta') + i(\sin\theta\cos\theta' + \cos\theta\sin\theta')\big]$$
$$= rr'\big[\cos(\theta+\theta') + i\sin(\theta+\theta')\big].$$

We get the rule: *multiplying the complex numbers we multiply their moduli and add their arguments*, see Figure C.2 (b).

Example C.3. Consider the product:

$$(1+i)\cdot 3i = \sqrt{2}\cdot 3\big(\cos\tfrac{3}{4}\pi + i\sin\tfrac{3}{4}\pi\big)$$
$$= 3\sqrt{2}\Big(-\tfrac{\sqrt{2}}{2} + i\tfrac{\sqrt{2}}{2}\Big) = -3+3i.$$

Example C.4. This rule can be used to easily find some products of complex numbers with minimum of computation. Take, say, $x_1 = 1+i$, $x_2 = 3i$, $x_3 = -5i$. Let us compute the product $x_1x_2x_3$.

We know that $\arg x_1 = \frac{\pi}{4}$, $\arg x_2 = \frac{\pi}{2}$, $\arg x_3 = -\frac{\pi}{2}$. So by the rule above

$$\arg(x_1x_2x_3) = \tfrac{\pi}{4} + \tfrac{\pi}{2} - \tfrac{\pi}{2} = \tfrac{\pi}{4}.$$

Also, $|x_1| = \sqrt{2}$, $|x_2| = 3$, $|x_3| = 5$. Therefore, $|x_1x_2x_3| = \sqrt{2}\cdot 3\cdot 5 = 15\sqrt{2}$, and we have:

$$x_1x_2x_3 = 15\sqrt{2}(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4}) = \tfrac{15}{2} + i\tfrac{15}{2}.$$

The operation of conjugation $\bar{x}$ is connected with addition, multiplication and with other operations by the following basic rules:

1. $\bar{\bar{x}} = x$,
2. $\overline{x+x'} = \bar{x} + \bar{x}'$,
3. $\overline{x\cdot x'} = \bar{x}\cdot\bar{x}'$,
4. $\bar{x} = x$ if and only if $x \in \mathbb{R}$,
5. if $x = r(\cos\theta + i\sin\theta)$ then $\bar{x} = r(\cos(-\theta) + i\sin(-\theta))$,
6. $x\bar{x} = r^2 = |x|^2$. In particular, $x\bar{x}$ is a real number.

The proof of any of these properties is an easy exercise.

If $x = r(\cos\theta + i\sin\theta)$ is the polar form of the complex number x, then applying the formula of complex numbers multiplication (in polar form) n times we get the *De Moivre's formula*:

$$x^n = r^n(\cos n\theta + i\sin n\theta).$$

This formula also allows to find the roots of complex numbers. Call the complex number $t \in \mathbb{C}$ the *n'th root* of $x \in \mathbb{C}$ if $t^n = x$.

Example C.5. Firstly, notice that the notion of real roots of real numbers is a particular case of the complex roots.

For example, 2 is the 5'th root of 32, and it is the 2'nd root (square root) of 4.

Example C.6. By definition i is a square root of -1. Actually, $-i$ also is a square root of -1. And -1 has no real square roots.

It is easy to verify that $t = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ is a 8'th root of 1.

In general, for any complex number $x = r(\cos\theta + i\sin\theta)$ and for any $n \in \mathbb{N}$ the number of n'th roots of x is equal to n, and all these roots can be found by formula:

$$t_k = \sqrt[n]{r}\left(\cos\frac{\theta + 2\pi k}{n} + i\sin\frac{\theta + 2\pi k}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

When $x = 1$, we get the roots

$$t_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1$$

which form the vertices of a regular n-sided polygon, the center of which is at the origin 0, and one of the vertices of which is fixed on the point $t = 1$ in plane $\mathbb{C}$. In figure below the 6'th roots t_0, t_1, t_2, t_3, t_4, t_5 of 1 form in $\mathbb{C}$ the six vertices of a regular 6-sided polygon:

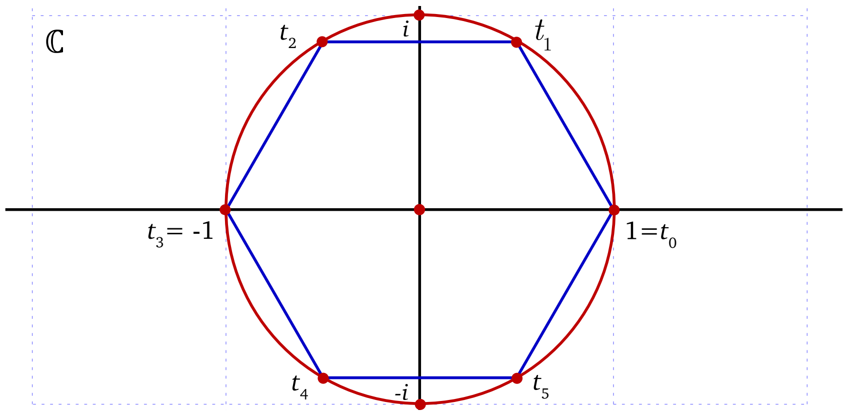


FIGURE C.3. The 6'th roots of 1 form a regular 6-sided polygon in $\mathbb{C}$.

APPENDIX D

Polynomials over fields

D.1. Polynomials and operations with them

You surely are familiar real with polynomials such as $f(x) = 3x^2 + x + 4$ or $f(x) = 5x^4 - 2x^3 + \frac{4}{5}$ as a particular type or real functions $f(x)$.

For any field F this concept can be generalized to polynomials over F as *formal sums* of type:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + x a_{n-1} + a_n, \tag{D.1}$$

where $n \in \mathbb{N} \cup \{0\}$, $a_i \in F$ for $i = 1, \ldots, n$ and $a_0 \neq 0$, if $n \neq 0$. This sum can also be used to define a function $f : F \to F$. Namely, for any $c \in F$ set the value of the function as $f(c) = a_0 c^n + a_1 c^{n-1} + \cdots + a_{n-1} c + a_n$.

The integer n is called the *degree* of $f(x)$, and is denoted as $n = \deg(f(x))$. No degree is defined for the *zero* polynomial $f(x) = 0$. The summands $a_i x^{n-i}$ in (D.1) are called the *terms* of $f(x)$, and the scalars a_i are called the *coefficients* of $f(x)$. The first summand $a_0 x^n$ is called the *leading term* of $f(x)$, and the first coefficient a_0 is called the *leading coefficient* of $f(x)$. Notice why the above requirement $a_0 \neq 0$ is necessary. Without it we would have no reasonable definition for the degree of the polynomial, say, $f(x) = 0x^2 + 3x + 5$. The last term a_n in (D.1) is called the *constant* term of the polynomial. If $f(x) = a_n$, i.e., if it has no terms other than a_n, then $f(x)$ is a *constant polynomial*. For a constant polynomial $f(x)$ we have $\deg(f(x)) = 0$, unleas $f(x)$ is the zero polynomial $f(x) = 0$ which has no degree.

Denote the set of the above defined polynomials by $F[x]$. From this perspective the real polynomials that you know from school form the set $\mathbb{R}[x]$.

Example D.1. In $\mathbb{R}[x]$ we have the polynomial $f(x) = 2x^3 - 4x^2 + x + 2$with degree $\deg(f(x)) = 3$.

Over complex field $\mathbb{C}$ we have the set $\mathbb{C}[x]$ of complex polynomials, such as$f(x) = (1 + i)x^2 + ix + 3$with degree $\deg(f(x)) = 2$.

In $\mathbb{Z}_5[x]$ we have the modular polynomial $f(x) = 3x^4 + x + 1$with degree $\deg(f(x)) = 4$.

We can also consider *binary* polynomials over $\mathbb{Z}_2$. They form the set $\mathbb{Z}_2[x]$ of polynomials the coefficients of which have `true = 1` and `false = 0` values.

By Agreement 10.9 we write the polynomials *in ascending order* of terms as $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, when we consider them *vectors* in polynomial spaces.

Addition of polynomials $f(x), g(x) \in F[x]$ is defined by the familiar rule of adding the coefficients by respective degrees (if $f(x)$ and $g(x) \in F[x]$ have distinct degrees, then we use zeros for the missing terms).

Multiplication of a polynomial $f(x) \in F[x]$ by a scalar $c \in F$ is defined by multiplying all coefficients of $f(x)$ by c.

Multiplication of polynomials $f(x), g(x) \in F[x]$ is defined by multiplying each term of $f(x)$ to each term of $g(x)$, and then collecting the terms of equal degrees to simplify the result.

Example D.2. For polynomials over $\mathbb{R}$ we have:

$$(2x^3 - 4x^2 + x + 2) \ + \ (3x^2 + 3x + 7)$$
$$= 2x^3 - x^2 + 4x + 9.$$
$$4(2x^3 - 4x^2 + x + 2) = (8x^3 - 16x^2 + 4x + 8).$$
$$(2x^3 - 4x^2 + x + 2) \ \cdot \ (x + 2)$$
$$= 2x^4 - 4x^3 + x^2 + 2x + 4x^3 - 8x^2 + 2x + 4$$
$$= 2x^4 - 7x^2 + 4x + 4.$$

Example D.3. For modular polynomials over $\mathbb{Z}_5$ we have:

$$(3x^3 + 4x^2 + 4) \ + \ (2x^2 + 4x + 1)$$
$$= 3x^3 + x^2 + 4x.$$
$$4(3x^3 + 4x^2 + 4) = 12x^3 + x^2 + 1.$$
$$(3x^3 + 4x^2 + 4) \ \cdot \ (2x^2 + 1)$$
$$= x^5 + 3x^4 + 3x^2 + 3x^3 + 4x^2 + 4$$
$$= x^5 + 3x^4 + 3x^3 + 2x^2 + 4.$$

Compare these with examples 10.5 and 10.6, where we define vector spaces of polynomials and of restricted degree polynomials over F.

D.2. The roots of polynomials

In school mathematics we call the number $c \in \mathbb{R}$ a root of the real polynomial $f(x) \in \mathbb{R}[x]$, if $f(c) = 0$. This can be generalized for polynomials over any field F: an element $c \in F$ is a *root* of the polynomial $f(x) \in F[x]$, if $f(c) = a_0 c^n + \cdots + a_n = 0$.

Example D.4. $c = 3$ is a root of $f(x) = x^2 - 6x + 9 \in \mathbb{R}[x]$.

The real polynomial $f(x) = x^2 - 2$ has two roots $c = \pm\sqrt{2}$. But the its analog has no roots in $\mathbb{Q}[x]$.

The complex polynomial $f(x) = ix^2 - 5x - 6i$ has the roots $c = -3i$ and $c = -2i$.

The complex polynomial $f(x) = x^2 + 1$ has two complex roots $c = \pm i$. But the same polynomial considered as a real polynomial (we can do that as both its coefficients are real) has no roots in $\mathbb{R}$.

The polynomial $f(x) = x^2 + 2$ over $\mathbb{Z}_3$ has two roots $c = 1$ and $c = 2$.

Lemma D.5. *The scalar $c \in F$ is a root of the polynomial $f(x) \in F[x]$ if and only if $f(x)$ for some $g(x) \in F[x]$ has the presentation:*

$$\boldsymbol{f(x) = (x - c)g(x).}$$

Proof. One side is evident: if $f(x) = (x - c)g(x)$, then $f(c) = 0 \cdot g(c) = 0$. Prove necessity by induction by degree $n = \deg(f(x))$. The statement is evident for $n = 0, 1$.

Assume $f(x) = a_0 x^n + \cdots + a_n$ has the root c. Clearly:

$$f(x) = a_0 x^n + \cdots + a_n \ - \ a_0 x^{n-1}(x - c) \ + \ a_0 x^{n-1}(x - c). \tag{D.2}$$

The polynomial

$$d(x) = a_0 x^n + \cdots + a_n \ - \ a_0 x^{n-1}(x - c)$$

is of degree less than n because the leading term $a_0 x^n$ is cancelled with $a_0 x^{n-1} \cdot x$. Clearly, $d(c) = 0$ because $f(c) - a_0 c^{n-1}(c - c) = 0 - 0 = 0$. By induction hypotheses $d(x) = (x - c)g_1(x)$ for some $g_1(x) \in F[x]$. By (D.2) we get

$$f(x) = (x - c)g_1(x) + a_0 x^{n-1}(x - c) = (x - c)\big(g_1(x) + a_0 x^{n-1}\big).$$

It remains to set $g(x) = g_1(x) + a_0 x^{n-1}$. $\square$

It may turn out that c is a root for $g(x)$ also, and then $f(x)$ can be presented as $f(x) = (x-c)\cdot(x-c)t(x) = (x-c)^2 t(x)$ for some $t(x) \in F[x]$. Repeating this process we eventually get

$$f(x) = (x-c)^t q(x) \tag{D.3}$$

such that c is *not* a root for $q(x) \in F[x]$. We call t the *multiplicity* of the root c of $f(x)$. When $t = 1$, we call c a *simple* root; and when $t > 1$, we call c a *multiple* root.

Next assume $c_1, \ldots, c_k$ are all the roots of $f(x)$, having multiplicities respectively $t_1, \ldots, t_k$. Choosing $c = c_1$ we rewrite (D.3) as $f(x) = (x-c_1)^{t_1} q_1(x)$. As it is easy to check[1], c_2 is the root of $q_1(x)$, and we have $q_1(x) = (x-c_2)^{t_2} q_2(x)$ for some polynomial $q_2(x)$. Continuing this process we in the k'th step get $q_k(x) = (x-c_k)^{t_k} h(x)$. Thus, we for any $f(x) \in F[x]$ get the decomposition

$$f(x) = (x-c_1)^{t_1} \cdots (x-c_k)^{t_k} h(x) \tag{D.4}$$

where $h(x)$ is a polynomial with *no roots* in F.

Example D.6. Multiplicity of the root $c = 3$ of $f(x) = x^2 - 6x + 9 \in \mathbb{R}[x]$ is 2 because $f(x) = (x-3)^2$.

Both roots $c_{1,2} = \pm\sqrt{2}$ are simple roots for $f(x) = x^2 - 2 \in \mathbb{R}[x]$. But if we consider the similar polynomial on rational field: $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, it will clearly have no roots.

Both roots $c_1 = -3i$ and $c_2 = -2i$ of the complex polynomial $f(x) = ix^2 - 5x - 6i = (x-3i)(x-2i) \in \mathbb{C}[x]$ are simple.

The polynomial $f(x) = x^2 + 1 \in \mathbb{C}[x]$ has two simple roots $c_{1,2} = \pm i$. Whereas considering on real field: $f(x) = x^2 + 1 \in \mathbb{R}[x]$ we get a polynomial with no roots.

$f(x) = x^2 + 2 = (x+1)(x+2) = (x-2)(x-1) \in Z_3[x]$ has two simple roots $c_1 = 1$ and $c_2 = 2$.

Example D.7. The *real* polynomial

$$f(x) = 2x^5 + 12x^4 + 252x^3 - 1376x^2 - 654x + 6084$$

has a root $c_1 = 3$, and so:

$$f(x) = (x-3)(2x^4 + 18x^3 + 306x^2 - 458x - 2028).$$

Since $c_1 = 3$ is a root for the second factor also, we have

$$f(x) = (x-3)^2(2x3 + 24x2 + 378x + 676).$$

Since 3 no longer is a root for the second factor above, $c_1 = 3$ is a root of multiplicity 2.

Since $c_2 = -2$ is a root for the second factor above, we have

$$f(x) = (x-3)^2(x+2)(2x^2 + 20x + 338),$$

which is the decomposition (D.4) for $f(x)$ because the square trinomial $2x^2 + 20x + 338$ has no real roots (just compute $D = b^2 - 4ac = -2304 < 0$). I.e., $c_2 = -2$ is a simple root.

But this square trinomial does have complex roots $c_3 = -5 + 12i$ and $c_4 = -5 - 12i$.

Thus, considering the analog of our polynomial $f(x)$ over *complex* field we get a different decomposition (D.4) for it in $\mathbb{C}[x]$:

$$f(x) = (x-3)^2(x+2)(x+5-12i)(x+5+12i)\,2,$$

where 3 is a root of multiplicity 2, whereas 2, $-5+12i$, $-5-12i$ are simple roots.

Observe that over $\mathbb{R}$ we got a "big" factor $h(x) = 2x^2 + 20x + 338$, whereas over $\mathbb{C}$ we only have a constant $h(x) = 2$. We will see a generalization of this shortly.

A remarkable property of complex numbers is that *an arbitrary non-constant polynomial $f(x) \in \mathbb{C}[x]$ has a root*. Therefore, at each step of the above process the factor $q(x)$ "splits", if it is non-constant. The process ends only when $h(x) = a$ (as in Example D.7, where have had $h(x) = 2$). We get:

[1] Add a reference to UFD

Theorem D.8. *Every non-constant polynomial $f(x) \in \mathbb{C}[x]$ has a complex root. Moreover, the sum of multiplicities of all roots $c_1, \ldots, c_k$ of $f(x)$ is equal to $n = \deg(f(x))$, i.e.:*

$$f(x) = a\,(x - c_1)^{t_1} \cdots (x - c_k)^{t_k} \tag{D.5}$$

This important result also is called *"Fundamental theorem of algebra"*, since it has played key role in historical development of Mathematics.

A field F is called an *algebraically closed* field, if every non-constant polynomial $f(x) \in F[x]$ has a root. It is clear that the analog of Theorem D.8 holds for any algebraically closed field. $\mathbb{C}$ is the only algebraically closed field considered in our course.

In examples above we always were able to write the decomposition (D.4). But this is not aways the case. You certainly know how to compute the roots of any *square* trinomial $ax^2 + bx + c$ using its discriminant. For *cubic* polynomials $ax^3 + bx^2 + cx + d$ the roots can be found by Cardano's formula (see Example 16.11.4 and Proposition 16.12.3 in [ARTIN]). For *quartic* polynomials $ax^4 + bx^3 + cx^2 + dx + e$ the problem of finding the roots can be reduced to Cardano's formula (see Proposition 16.12.3 in [ARTIN]). We do not bring these formulas here (because we are not going to use them actually), and what you need be aware is that for any polynomial of degree at most 4 we are able to find all the roots (if it has roots).

The situation is more complicated for polynomial $f(x)$ of degree greater then or equal to 5. Then $f(x)$ may not be *solvable by radicals*, i.e., (leaving the exact definition of this term aside) the roots of $f(x)$ may not be found whatever formula (inducing addition, multiplication, any powers and any roots) we apply. For example, the roots of *quintic* polynomials $x^5 - 16x + 2$ cannot be found by radicals.

For more information on this topic see Chapter 16, in particular, Theorem 16.12.4 in [ARTIN], or other literature covering *Galois theory*.

APPENDIX E

Permutations

E.1. Definition of permutations, cycles

Definition E.1. A *permutation* is a bijective function on the set $\{1, 2, \ldots, n\}$.

Permutations usually are denoted by lowercase Greek characters σ, τ, π, etc... Say, the following function σ is a permutation on $\{1, 2, 3\}$:

$$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1, \tag{E.1}$$

whereas the function

$$\tau(1) = 2,\ \tau(2) = 2,\ \tau(3) = 1$$

is not a permutation, since it is neither injective nor surjective.

If σ is a permutation on the set $\{1, 2, \ldots, n\}$, then n is called the *degree* of σ. The set of all permutations of degree n is denoted by S_n.

One way to write a permutation is *Cauchy's two-raw notation*:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \tag{E.2}$$

which means: $\sigma(1) = i_1$, $\sigma(2) = i_2$,..., $\sigma(n) = i_n$; or in slightly different manner:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

The permutation given, say, in (E.1) can be written as:

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

In some cases permutations may be written differently: the 1'st raw may not be in the natural order $1, 2, \ldots, n$. For instance, the above permutation σ may also be written as

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

because, in spite of distinct notation, we still have $\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1$ (i.e., σ is the same according to definition of a function). More generally, if $\begin{pmatrix} k \\ i_k \end{pmatrix}$ is a column of σ in (E.2), then $\sigma(k) = i_k$ regardless of the *position* of that column in (E.2). Thus, if needed, we can *swap the columns* without changing permutation.

If the 1'st row of the above notation is fixed (say, in the ascending order $1, 2, \ldots, n$), then the given permutation σ, clearly, is *uniquely* determined by the placement of the numbers $1, 2, \ldots, n$ in the 2'nd row of the permutation. In particulater, $|S_n| = n!$.

Example E.2. S_3 has the following $3! = 6$ permutations:

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}.$$

And S_2 has just $2! = 2$ permutations:

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

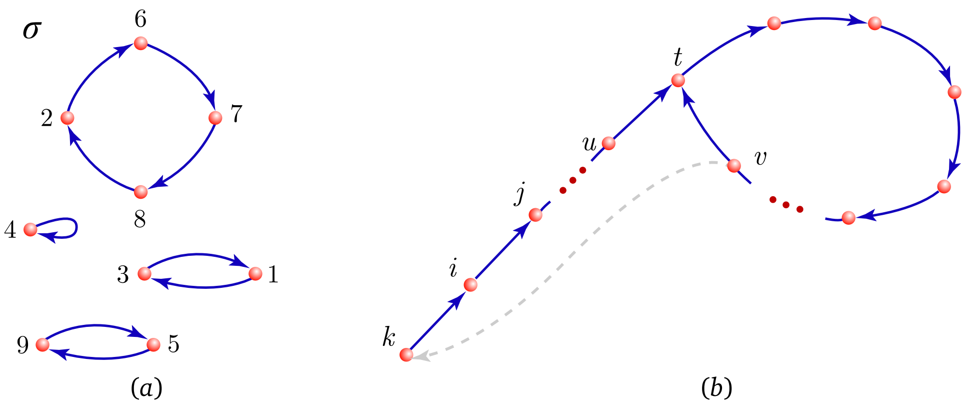


FIGURE E.1. Cycles in permutations.

Lets us start introduction of the *cycles* form of permutations by an example:

Example E.3. We can represent the following permutation σ by Figure E.1 (a):

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 1 & 4 & 9 & 7 & 8 & 2 & 5 \end{pmatrix}$$

Notice that:
$3, 1$ form a cycle of length 2;
$2, 6, 7, 8$ form a cycle of length 4;
4 forms a cycle of length 1;
$9, 5$ form a cycle of length 2.

Having these four cycles we know the permutation σ already. So we can write σ as:

$$\sigma = (31)(2678)(4)(95).$$

Can such a cycles form be found for *any permutation* $\sigma \in S_n$? To show this fix any $k \in \{1, \dots, n\}$ and consecutively construct the elements $\sigma(k) = i$, $\sigma(i) = j$, etc...

$$k \xrightarrow{\sigma} i \xrightarrow{\sigma} j \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} u \xrightarrow{\sigma} t \xrightarrow{\sigma} \cdots$$

as in Figure E.1 (b). In this process we cannot get infinitely many *distinct* numbers, and at some step we get *the first repeated number* t. If $t \neq k$, we get a contradiction, since σ is a bijection, and for distinct elements u, v we cannot have $\sigma(u) = \sigma(v) = t$, as in Figure E.1 (b). Thus, $t = k$, and k is in the cycle $(kij \cdots u)$. Continuing this procedure for other elements of $\{1, 2, \dots, n\}$ we get the remaining cycles also. Thus, each permutation σ can be written in some *cycles form*:

$$\boldsymbol{\sigma = (i_1 \cdots i_k)(j_1 \cdots j_s) \cdots (r_1 \cdots r_l).}$$

Each of the numbers $1, 2, \dots, n$ lies in one and only one of those cycles. $(i_1 \cdots i_k)$ is called a *cycle* of length k. It is clear that the cycles of a permutation may be written in any order, and each cycle may start by any of its elements. Also we often omit the cycles of length 1.

Example E.4. The permutation of Example E.3 can be written as:

$$\begin{aligned}\sigma &= (31)(2678)(4)(95)\\ &= (2678)(4)(31)(95)\\ &= (6782)(4)(13)(59)\\ &= (6782)(13)(59).\end{aligned}$$

The following example shows why it may be comfortable to omit cycles of length 1:

Example E.5. We have:

$$\begin{aligned}\tau &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 9 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1\end{pmatrix}\\ &= (19)(2)(3)(4)(5)(6)(7)(8) = (19).\end{aligned}$$

Since τ actually moves the numbers 1 and 9 *only*, it is simpler to write it just $\tau = (19)$, and to omit the cycles $(2),(3),(4),(5),(6),(7),(8)$ which in this case hold no relevant information, if we in advance agree that numbers not present in $\tau = (19)$ in fact are not moved.

Agreement E.6. Omitting cycles of length 1 may sometimes cause misunderstanding. Say, the permutations $\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 1 & 4 & 5\end{pmatrix}$ and $\tau = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$ may both be written as (13), and in case we are given this cycle (13) only, we cannot figure out which permutation it stands for. To overcome this we agree to state the degree of the given permutation in the context. Say, writing "consider the permutation (13) of degree 5" we mean σ, and writing "take the permutation $(13) \in S_3$" we mean τ.

Remark E.7. We defined permutations as bijections on the sets $\{1, 2, \ldots, n\}$, but it is clear that everything we stated can easily be extended for bijections on any sets $\{a_1, a_2, \ldots, a_n\}$ of n elements, also. Some specific problems do require such generalizations. However, in this brief summary we do not cover them, leaving generalizations as easy exercises for you.

E.2. Products of permutations, transpositions

The product $\sigma\tau$ of permutations $\sigma, \tau \in S_n$ is the *composition* $\sigma \circ \tau$ of these two functions. I.e., if $\tau(i) = j$ and $\sigma(j) = k$, then $\sigma\tau(i) = \sigma\big(\tau(i)\big) = \sigma(j) = k$:

$$i \xrightarrow{\tau} j \xrightarrow{\sigma} k, \qquad i \xrightarrow{\sigma\tau} k.$$

Example E.8. In Cauchy's two-raw notation we have:

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

And if the same presentations are written in cycles form, then

$$(12)(354) \cdot (15423) = (14)(253).$$

Since composition of functions is associative operation for any bijections, we have:

Proposition E.9. *Multiplication is an associative operation in S_n, i.e., for any $\sigma, \tau, \pi \in S_n$ the equality $(\sigma\tau)\pi = \sigma(\tau\pi)$ holds in S_n.*

In S_n denote by (1) the *identity* permutation $(1) = \begin{pmatrix}1 & 2 & \cdots & n\\ 1 & 2 & \cdots & n\end{pmatrix} = (1)(2)\cdots(n)$. Trivial verification shows that:

Proposition E.10. *There is an identity element in S_n, i.e., for any $\sigma \in S_n$ the equalities $\sigma(1) = (1)\sigma = \sigma$ hold in S_n.*

For any $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ denote by $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ the *inverse* permutation for σ. It is easy to verify that:

Proposition E.11. *For any $\sigma \in S_n$ there is its inverse element σ^{-1} such that $\sigma\sigma^{-1} = \sigma^{-1}\sigma = (1)$.*

How the inverse looks like, if the permutation is in its cycles form? For any cycle $(i_1 \cdots i_k)$ we evidently have $(i_1 \cdots i_k)^{-1} = (i_k \cdots i_1)$.

Thus, if $\sigma = (i_1 \cdots i_k)(j_1 \cdots j_s) \cdots (r_1 \cdots r_l)$, then

$$\boldsymbol{\sigma^{-1} = (i_k \cdots i_1)(j_s \cdots j_1) \cdots (r_l \cdots r_1).}$$

The rule $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$ is easy to deduce, whereas more "naturally looking" relation $(\sigma\tau)^{-1} = \sigma^{-1}\tau^{-1}$ does *not* hold, in general.

Example E.12. For the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432), \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

we have:

$$\sigma^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau^{-1} = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

and in cycles form $\sigma^{-1} = (2341)$ and $\tau^{-1} = (43)(21) = (12)(34)$. The equalities $\sigma\sigma^{-1} = (1)$, $\tau\tau^{-1} = (1)$, $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$, and the inequality $(\sigma\tau)^{-1} \neq \sigma^{-1}\tau^{-1}$ can be verified directly.

Remark E.13. Let G be any set, on which an *operation* $\cdot$ is defined, that is, for any $a, b \in G$ their product $a \cdot b$ is given in G. If this operation is associative; if there is an identity element $1 \in G$, i.e., $a \cdot 1 = 1 \cdot a = a$ for any $a \in G$; and if for any $a \in G$ there is an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$, then G together with $\cdot$ is called a *group*, and often is denoted by $\langle G, \cdot \rangle$. Our three propositions above mean that $\langle S_n, \cdot \rangle$ is a group (with respect to the operation $\cdot$ of permutations multiplication). Other examples of groups are easy to construct using numbers, matrices, functions, etc...

Call *transposition* a permutation of the following type:

$$(rs) = \begin{pmatrix} 1 & 2 & \cdots & \boldsymbol{r} & \cdots & \boldsymbol{s} & \cdots & n \\ 1 & 2 & \cdots & \boldsymbol{s} & \cdots & \boldsymbol{r} & \cdots & n \end{pmatrix}.$$

According to Agreement E.6 when we use the transpositions (25) or (35) in, say, S_6, we assume that (25) or (15) map 1 to 1, 6 to 6, etc...

It is easy to verify that any cycle $(i_1 i_2 i_3 \cdots i_k)$ is a product of some transpositions:

$$\boldsymbol{(i_1 i_2 i_3 \cdots i_k) = (i_1 i_k) \cdots (i_1 i_3)(i_1 i_2).} \tag{E.3}$$

And since each permutation is a product of some cycles, we get:

Theorem E.14. *Each permutation can be decomposed to a product of transpositions.*

Example E.15. We have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 2 & 1 & 4 & 6 & 8 & 9 & 7 \end{pmatrix}$$
$$= (13254)(789)$$
$$= (14)(15)(12)(13)(79)(78).$$

Notice how we omitted (6) as it is a cycle of length 1.

Example E.16. Such decompositions are *not* unique. For $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$ we have two decompositions:

$$\sigma = (14)(13)(12),$$
$$\sigma = (12)(13)(13)(14)(13)(24)(12).$$

Although these decompositions are different, they both have *odd* number of transpositions. We will extend this trend in Remark E.27.

E.3. Parity of permutations

Let $\sigma \in S_n$ be a permutation written as:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$

The pair of elements (i_r, i_s) in the 2'nd row of σ is an *inversion*, if $i_r > i_s$ and $r < s$, i.e., the larger number i_r stands to the left from the smaller number i_s.

Example E.17. For the permutation

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

we have the inversions $(2,1)$, $(5,3)$, $(5,4)$ (so i_r and i_s need not be neighbors).

Example E.18. There is an easy way to collect the inversions for larger permutions. For

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 7 & 6 & 5 & 9 & 8 & 4 \end{pmatrix}$$

count the inversions going from the left to the right, ignoring the previously counted inversions. Namely:

- There is only one inversion starting by 2. It is $(2,1)$.
- There is no new inversion starting by 1 because all numbers to the right from 1 are larger than 1. And we do not count $(2,1)$ (evolving 1), since we counted it previously.
- There is no new inversion starting by 3.
- There are 3 new inversions starting by 7: $(7,6)$, $(7,5)$, $(7,4)$.
- Plus 2 new inversions starting by 6: $(6,5)$, $(6,4)$.
- Plus 1 new inversion starting by 5: $(5,4)$.
- Plus 2 new inversions starting by 9: $(9,8)$, $(9,4)$.
- Plus 1 new inversion starting by 8: $(8,4)$.

So we get $1+0+0+3+2+1+2+1 = \mathbf{10}$ inversions in total.

We call a permutation σ an *even* permutation, if the number of its inversions is even, and call σ an *odd* permutation, if the number of its inversions is odd. Introduce the function $\operatorname{sgn}(\sigma)$:

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even,} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

Call $\operatorname{sgn}(\sigma)$ the *sign* of the permutation σ. We also use the term *parity*: "parity of σ is odd", "σ and π are of the same parity", etc... The identity permutation has zero inversions, so it is even.

Example E.19. The permutation of Example E.17 has 3 inversions, and we have:

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

And the permutation of Example E.18 has 10 inversions, and so:

$$\operatorname{sgn}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 7 & 6 & 5 & 9 & 8 & 4 \end{pmatrix} = 1.$$

For identity permutation we have $\operatorname{sgn}((1)) = 1$.

As we mentioned, a permutation might be written so that its first raw is *not* in the natural order $1, 2, \ldots, n$. To compute its sign in such a case we first swap its columns to arrange the first raw in natural order. Then we count the inversions in the 2'nd raw.

Example E.20. Swapping the columns we get

$$\sigma = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

So it has six inversions $(3,1)$, $(3,2)$, $(5,1)$, $(5,4)$, $(5,2)$, $(4,2)$, and $\operatorname{sgn}(\sigma) = 1$.

Lemma E.21. *For any permutation σ and for a transposition (rs) in S_n:*

$$\operatorname{sgn}(\sigma\cdot(rs)) = -\operatorname{sgn}(\sigma)\,.$$

Or, in other words, swapping the entries i_r and i_s in the 2'nd row of σ changes the parity of the permutation:

$$\operatorname{sgn}\begin{pmatrix}1 & \cdots & r & \cdots & s & \cdots & n\\ i_1 & \cdots & i_r & \cdots & i_s & \cdots & i_n\end{pmatrix} = -\operatorname{sgn}\begin{pmatrix}1 & \cdots & r & \cdots & s & \cdots & n\\ i_1 & \cdots & i_s & \cdots & i_r & \cdots & i_n\end{pmatrix}.$$

***Proof*.** It is easy to verify that multiplication by (rs) actually is equivalent to swapping of entries i_r and i_s in the 2'nd row. We prove the second of equivalent statements.

Start by the case when i_r and i_s are neighbours, i.e., swapping the entries we just

$$\text{replace}\quad \sigma = \begin{pmatrix}1 & \cdots & r & s & \cdots & n\\ i_1 & \cdots & i_r & i_s & \cdots & i_n\end{pmatrix}\quad\text{by}\quad \begin{pmatrix}1 & \cdots & r & s & \cdots & n\\ i_1 & \cdots & i_s & i_r & \cdots & i_n\end{pmatrix}.$$

Those inversions of σ which do not evolve i_r or i_s, clearly, are not affected by this swapping. So the number of all such inversions is *not* changed.

If in σ an entry to the left of i_r has (or does not have) an inversion with i_r or with i_s, this fact does not change by the swapping. The same holds for entries to the right of i_s. So the number of all such inversions also is *not* changed.

There remains only one possibility: the possible inversion of i_r and i_s. If (i_r, i_s) *is* an inversion (i.e. $i_r > i_s$), we will lose it after the swapping. If (i_r, i_s) is *not* an inversion, we get one new inversion after we swap i_r and i_s. In either case the total number of inversions is changed by 1 only.

Turn to the case when i_r and i_s are *not* neighbours, and there are, say, t entries between them:

$$\sigma = \begin{pmatrix}1 & \cdots & r & k_1 & k_2 & \cdots & k_t & s & \cdots & n\\ i_1 & \cdots & i_r & i_{k_1} & i_{k_2} & \cdots & i_{k_t} & i_s & \cdots & i_n\end{pmatrix}.$$

Swap i_r with i_{k_1}, then with i_{k_2}, etc... and bring it next to i_s. Then swap i_r with i_s. Then swap i_s with i_{k_t}, then with $i_{k_{t-1}}$, etc... and bring i_s to the *initial* position of i_r.

During this process $t+1+t$ total swaps are done). By the first part of the proof, we changed the sign of the permutation $2t+1$ times, which is an odd number. □

Let us study two special cases of how multiplication by (rs) affects the cycles:

Example E.22. Consider the product:

$$(\mathbf{2}1378\mathbf{6}954)\cdot(\mathbf{26}) = (1378\mathbf{6})(\mathbf{2}954).$$

So multiplication by (26) *splits the cycle to two parts*. (Since we can start/end a cycle by any of its elements, assume it starts by 2).

It is easy to see that, in general:

$$(\boldsymbol{r}\, i_1\cdots i_u \boldsymbol{s}\, j_1\cdots j_v)\cdot(\boldsymbol{r}\,\boldsymbol{s}) = (i_1\cdots i_u \boldsymbol{s})(\boldsymbol{r}\, j_1\cdots j_v).$$

Example E.23. Compute the product:

$$(1495\mathbf{2})(\mathbf{6}837)\cdot(\mathbf{26}) = (\mathbf{2}837\mathbf{6}1495).$$

So multiplication by (26) *merges two cycle into one*. (Since we can start/end a cycle by any of its elements, assume the first ends by 2, and the second starts by 6).

And, in general:

$$(i_1\cdots i_u \boldsymbol{r})(\boldsymbol{s}\, j_1\cdots j_v)\cdot(\boldsymbol{r}\,\boldsymbol{s}) = (\boldsymbol{r}\ j_1\cdots j_v\ \boldsymbol{s}\ i_1\cdots i_u).$$

We got the following rule:

Lemma E.24. *Let the permutation $\sigma \in S_n$ be given in its cycles form:*

$$\sigma = (i_1 \cdots i_k)(j_1 \cdots j_s) \cdots (r_1 \cdots r_l). \tag{E.4}$$

Then for any transposition $(rs) \in S_n$ there are two alternatives:

1. *r and s are inside the same cycle in (E.4), and multiplication of σ by (rs) splits that cycle to two cycles.*
2. *r and s are inside two different cycles in (E.4), and multiplication of σ by (rs) merges those cycles into one cycle.*

***Proof*.** In both cases we can reorder the cycles of σ so that the single cycle (holding both r and s), or two different cycles (holding r or s each) stand at the end of the cycles decomposition. Then multiplication by (rs) acts according to rules of obtained above. □

For a permutation $\sigma \in S_n$ let c be the number of cycles in the cycles form of σ (including the cycles of length 1). Call the difference $d = n - c$ the *decrement* of σ.

We use Lemma E.24 and Lemma E.21 to prove the following helpful theorem:

Theorem E.25. *For any permutation $\sigma \in S_n$ let t be the number of transpositions in a given decomposition of σ, and let $d = n - c$ be the decrament of σ. Then the parity of σ coincides with parity of t and with parity of d.*

Consider an example before we proof Theorem E.25.

Example E.26. We have already counted that

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 7 & 6 & 5 & 9 & 8 & 4 \end{pmatrix}.$$

has 10 inversions. Thus, $\operatorname{sgn}(\sigma) = 1$.

To compute the decrement present this in cycles form:

$$\sigma = (12)(3)(479)(56)(8)$$

(5 cycles, including the cycle of length 1). The decrement is $9 - 5 = 4$, an even number. We again get that $\operatorname{sgn}(\sigma) = 1$ by Theorem E.25.

Go on and present σ by transpositions:

$$\sigma = (12)(49)(47)(56),$$

we get an even number of transpositions (four transpositions). So again $\operatorname{sgn}(\sigma) = 1$ by Theorem E.25.

Remark E.27. Now we can answer the question asked in Example E.16. Transpositions decompositions of a given permutation σ may be *different*, but they all evolve even nuber of transpositions, if $\operatorname{sgn}(\sigma) = 1$; or odd nuber of transpositions, if $\operatorname{sgn}(\sigma) = -1$.

***Proof of Theorem E.25*.** Assume the transpositions decomposition of σ is: $\sigma = (r_1 s_1) \cdots (r_t s_t)$. Then, clearly

$$\sigma = (1) \cdot \sigma = \Big((1)(2) \cdots (n)\Big) \cdot \Big((r_1 s_1)(r_2 s_2) \cdots (r_t s_t)\Big).$$

We can interpret the above product like this:
- first multiply $(1)(2) \cdots (n)$ from the right by $(r_1 s_1)$,
- then multiply the result of previous step by $(r_2 s_2)$,
- ....
- finally, multiply the previous result by $(r_t s_t)$, and get the σ.

The initial permutation $(1)(2) \cdots (n)$ is *even*. And on each of the above steps we by Lemma E.21 change the parity. Arriving to the final step we have changed parity t times and arrived to σ. So party of t coincides with the parity of σ.

To prove the statement about the decrament notice that in the beginning of process we start with an *even* permutation $(1)(2)\cdots(n)$ which has n cycles and an *even* decrament $n-n=0$. Then on each of the above steps we by Lemma E.21 change the parity of the current permutation, and by Lemma E.24 we either merge two cycles into one, or separate a cycle into two, that is, on each step we change the number of cycles by 1, i.e, we change the parity of the decrament of the current permutation.

At the end of the process we have done t steps and arrived to σ which has the decrament $d=n-c$. If t is even, then $d=n-c$ is even, and if t is odd, then $d=n-c$ also is odd. $\square$

Linear Algebra course quizzes with full solutions

Below is the full bank of quizzes and their solutions at all pup quiz surveys held during the Linear Algebra 104 course in the spring semesters of 2016–2019. Each quiz booklet included three exercises from the list below. The students had nearly fifteen minutes to solve them.

Unlike the exercises mentioned at the end of the chapters above, these quizzes cover not all the chapters but just those included in the Linear Algebra 104 course. To see the structure of that course check the Syllabus on page 11.

Quizzes on real spaces, lines and planes

Quiz Q1. In $\mathbb{R}^2$ the line ℓ_1 is passing via the point $P=(5,0)$, and has the direction vector $d=(1,-\sqrt{3})$. The line ℓ_2 is given by its parametric form $\begin{cases} x=2t \\ y=2\sqrt{3}\,t \end{cases}$. Write the general form of ℓ_1. Does the origin $O=(0,0)$ belong to ℓ_2? Find the size of the angle OMP where M is the intersection point of ℓ_1 and ℓ_2.
Solution: As a normal vector for ℓ_1 we can take the vector $n=(\sqrt{3},1)$, since $d\perp n$. The general equation of ℓ_1 is $3x+y-5\sqrt{3}=0$. The origin $O=(0,0)$ belongs to ℓ_2 as we get that point for $t=0$. As direction vector for ℓ_2 we can take, say, $k=(1,\sqrt{3})$. One side of the triangle OMP is on Ox. The direction vectors are forming $-\frac{\pi}{3}$ and $\frac{\pi}{3}$ angles with Ox. So the angle OMP also is $\frac{\pi}{3}$. Or we can directly compute $\frac{1-3}{\sqrt{(1+3)(1+3)}}=-\frac{1}{2}$, and take the *positive* angle $\frac{\pi}{3}$.

Quiz Q2. We know that the planes $\mathcal{P}_1$ and $\mathcal{P}_2$ are parallel in $\mathbb{R}^3$. $\mathcal{P}_1$ is passing via the points $A=(1,\,2,\,0)$, $B=(1,\,3,\,-1)$, $C=(0,\,1,\,3)$. Build the general equation for $\mathcal{P}_2$, if you know that $\mathcal{P}_2$ contains the point $M=(1,2,3)$.
Solution: As direction vectors for $\mathcal{P}_1$ we can take $d=\overrightarrow{AB}=(0,\,1,\,-1)$ and $k=\overrightarrow{AC}=(-1,\,-1,\,3)$. Their cross product $n=d\times k=(2,\,1,\,1)$ is a normal vector for *both* planes. As position for $\mathcal{P}_2$ take $p=\overrightarrow{OM}=(1,\,2,\,3)$. From the normal form $n\cdot v=n\cdot p$ we get the general equation $2x+y+z-7=0$.

Quiz Q3. In $\mathbb{R}^3$ the plane $\mathcal{P}_1$ is given by its position vector $p=(1,0,3)$ and by two direction vectors $d=(0,2,1)$ and $k=(1,0,0)$. About the plane $\mathcal{P}_2$ we know that its normal vector is $h=2d$, and it passes via $A=(2,0,3)$. Write the general equations of both planes. Combining these two equations we get a system of two linear equations. Deduce if that system has a solution by comparing the normal vectors of $\mathcal{P}_1$ and $\mathcal{P}_2$ *only*.
Solution: As a normal vector for $\mathcal{P}_1$ we take $n=d\times k=(0,1,-2)$. From the normal form $n\cdot v=n\cdot p$ we get the general equation $y-2z+6=0$. Since $h=2d$ is collinear to d, we can take d as a normal vector for $\mathcal{P}_2$, and $A=(2,0,3)$ as a position. We get the

equation $2y+z-3=0$. The system consisting of these two equations has a solution because $\mathcal{P}_1$ and $\mathcal{P}_2$ are not parallel (as their normal vectors are not *collinear*).

Quiz Q4. The plane $\mathcal{P}$ is given in $\mathbb{R}^3$ by general equation $2x-y+3z=1$. Find the parametric form of the line ℓ that passes via $A=(1,5,0)$ and is perpendicular to $\mathcal{P}$. Explain your answer.

Solution: As a normal for $\mathcal{P}$ take $n=(2,-1,3)$. Then n is a direction for ℓ, and $p=\overrightarrow{OA}=(1,5,0)$ is a position for ℓ. So the equations of the parametric form are: $x=1+2t$, $y=5-t$, $z=3t$.

Quiz Q5. The plane $\mathcal{P}$ in $\mathbb{R}^3$ is parallel to the vector $v=(1,2,-1)$, and is passing via the points $A=(2,1,0)$, $B=(1,0,1)$. Find the parametric form of the line ℓ which is passing via the point $M=(1,3,0)$, and is perpendicular to $\mathcal{P}$. Explain your answer.

Solution: As direction vectors for $\mathcal{P}$ take $\overrightarrow{AB}=(-1,-1,1)$ and $v=(1,2,-1)$. The cross product $\overrightarrow{AB}\times v=(-1,0,-1)$ is orthogonal to $\mathcal{P}$ and, thus, is a direction vector for ℓ. I.e., the parametric form is: $x=1-t$, $y=3$, $z=-t$.

Quiz Q6. The rectangle $ABCD$ (listed counter-clockwise) is given in $\mathbb{R}^2$ by its three vertices $A=(7,2)$, $B=(4,1)$, $C=(6,-5)$. Find a parametric form of the line ℓ passing via D, and orthogonal to $\overrightarrow{CA}$. Explain your answer.

Solution: Since $\overrightarrow{BA}=(3,1)$, $\overrightarrow{BC}=(2,-6)$, we have the position vector for ℓ as: $\overrightarrow{OD}=\overrightarrow{BA}+\overrightarrow{BC}+\overrightarrow{OB}=(3,1)+(2,-6)+(4,1)=(9,-4)$. Since $\overrightarrow{CA}=(1,7)$, as a direction vector for ℓ we can take $d=(7,-1)$. Thus, the parametric form is $x=9+7t$, $y=-4-t$.

Quiz Q7. The triangle ABC is given in $\mathbb{R}^2$ as follows. We know the point $A=(1,2)$. Also $\overrightarrow{AB}=2w$ where $w=(-1,3)$ And the vector $\overrightarrow{AC}$ is equal to the projection of the vector $v=(4,2)$ on the vector $u=(2,2)$. Find the vertices B and C.

Solution: $\overrightarrow{AB}=2w=(-2,6)$. Then, $\overrightarrow{OB}=\overrightarrow{OA}+\overrightarrow{AB}=(1,2)+(-2,6)=(-1,8)$. So $B=(-1,8)$. Also, $\overrightarrow{AC}=\operatorname{proj}_u v=\frac{u\cdot v}{u\cdot u}u=\frac{12}{8}(2,2)=\frac{3}{2}(2,2)=(3,3)$. Thus, $\overrightarrow{OC}=\overrightarrow{OA}+\overrightarrow{AC}=(1,2)+(3,3)=(4,5)$. So $C=(4,5)$.

Quiz Q8. In $\mathbb{R}^3$ the plane $\mathcal{P}$ is given by its three points $O=(0,0,0)$, $A=(2,1,0)$, $B=(1,0,1)$. Find the distance d from $\mathcal{P}$ to the point $M=(0,6,0)$. Explain your answer.

Solution: As directions for $\mathcal{P}$ take $u=\overrightarrow{OA}=(2,1,0)$, $v=\overrightarrow{OB}=(1,0,1)$. Their cross product is the normal $n=u\times v=(1,-2,-1)$. Then $\operatorname{proj}_n\overrightarrow{OM}=\frac{-12}{6}(1,-2,-1)=(-2,4,2)$. So $d=|(-2,4,2)|=\sqrt{24}$.

Quiz Q9. We have a triangle in $\mathbb{R}^2$ given by its three vertices $A=(0,1)$, $B=(2,1)$, $C=(3,0)$. Using vector operations find the height h from the vertex C to the base AB. Explain your answer.

Solution: Denote $u=\overrightarrow{AB}=(2,0)$ and $v=\overrightarrow{AC}=(3,-1)$. Then h is equal to length of vector $\operatorname{proj}_u(v)-v=\frac{6}{4}(2,0)-(3,-1)=(0,1)$. Therefore $h=1$.

Quiz Q10. In $\mathbb{R}^3$ we are given the points $A=[6,8,0]$ and $B=[4,6,-2]$. Find the distance d from the midpoint M of the segment AB from the plane $\mathcal{P}$ given by the general equation $x+2y-z-8=0$. Explain your answer.

Solution: $M=\left[\frac{6+4}{2},\frac{8+6}{2},\frac{0-2}{2}\right]=[5,7,-1]$. As normal vector for $\mathcal{P}$ take $n=[1,2,-1]$. To find a position vector p for $\mathcal{P}$ assign $x=0, y=0$, and get $0+2\cdot 0-z-8=0$, i.e., $z=-8$ and $p=[0,0,-8]$. Then d is equal to the length of projection of $v=$

$\overrightarrow{OM} - p = (5,7,7)$ on n. We have $\text{proj}_n(v) = \frac{n \cdot v}{n \cdot n} n = \frac{5+14-7}{1+4+1} n = 2[1,2,-1] = [2,4,-2]$. So $d = \|[2,4,-2]\| = \sqrt{24}$.

Quizzes on complex and modular fields and spaces

Quiz Q11. Write the polar form of the complex number $x = 5\sqrt{3}+5\,i$. Using DeMoavre's formula compute the power $y = x^{301}$. Find the conjugate $\bar{y}$ of y.
Solution: $x = 5\sqrt{3} + 5\,i = 10\frac{\sqrt{3}}{2} + 10\frac{1}{2}i = 10(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = 10(\cos\frac{\pi}{6} + \sin\frac{\pi}{6}i)$. Thus $y = x^{301} = 10^{301}(\cos\frac{301\cdot\pi}{6} + \sin\frac{301\cdot\pi}{6}i) = 10^{301}(\cos\frac{\pi}{6} + \sin\frac{\pi}{6}i) = 10^{301}\frac{\sqrt{3}}{2} + 10^{301}\frac{1}{2}\,i$. The conjugate is $\bar{y} = 10^{301}\frac{\sqrt{3}}{2} - 10^{301}\frac{1}{2}\,i$.

Quiz Q12. For a complex number $x \in \mathbb{C}$ we are given $|x| = r = 2$ and $\arg(x) = \frac{\pi}{6}$. Compute the number $z = x^{30}$. What are the real part and the imaginary part of z? Find the inverses of x and of z.
Solution: We have $x = 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}) = 2(\frac{\sqrt{3}}{2} + i\frac{1}{2}) = \sqrt{3} + i$. By DeMoavre's formula $z = x^{30} = 2^{30}(\cos\frac{30\cdot\pi}{6} + i\sin\frac{30\cdot\pi}{6}) = 2^{30}(\cos(5\pi) + i\sin(5\pi)) = -2^{30}$. The real part of z is -2^{30}, the imaginary part is 0. The inverse of z is $-\frac{1}{2^{30}}$. The inverse of $x =$ is $\frac{1}{\sqrt{3}+i} = \frac{1}{\sqrt{3}+i} \cdot \frac{\sqrt{3}-i}{\sqrt{3}-i} = \frac{\sqrt{3}-i}{4} = \frac{\sqrt{3}}{4} - \frac{1}{4}i$.

Quiz Q13. Write the complex numbers $x = 2-2i$ and $y = -\sqrt{3}-i$ in their polar forms. Using the obtained polar forms compute the product $t = \bar{x}\,y\,x$. Explain your answer.
Solution: We have $x = \sqrt{8}\,(\cos(-\frac{\pi}{4}) + i\,\sin(-\frac{\pi}{4}))$ and $y = 2\,(\cos(-\frac{5\pi}{6}) + i\,\sin(-\frac{5\pi}{6}))$. And for the conjugate: $\bar{x} = \sqrt{8}\,(\cos(\frac{\pi}{4}) + i\,\sin(\frac{\pi}{4}))$. The modulus of t is $\sqrt{8}\cdot 2\cdot\sqrt{8} = 16$. The argument of t is $-\frac{\pi}{4} - \frac{5\pi}{6} + \frac{\pi}{4} = -\frac{5\pi}{6}$. Thus $t = 16\,(\cos(-\frac{5\pi}{6}) + i\,\sin(-\frac{5\pi}{6})) = -8\sqrt{3} - 8i$.

Quiz Q14. The complex number $x \in \mathbb{C}$ is given by its modulus $r = 1$ and argument $\theta = -\frac{\pi}{3}$. Using DeMoavre's formula compute the power $t = x^{61}$. Then compute the vector $\frac{1}{t}v$, if $v = (1+i, -i) \in \mathbb{C}^2$. Explain your answer.
Solution: $|t^{61}| = 1^{61} = 1$ and the argument of t^{61} is $-\frac{\pi}{3}\cdot 61 = -\frac{\pi}{3}\cdot 60 - \frac{\pi}{3}$. Thus, $t^{61} = t = \frac{1}{2} - \frac{\sqrt{3}}{2}i$. Since $\frac{1+i}{\frac{1}{2}-\frac{\sqrt{3}}{2}i} = 2\frac{1+i}{1-\sqrt{3}i} = 2\frac{1+i}{1-\sqrt{3}i}\cdot\frac{1+\sqrt{3}i}{1+\sqrt{3}i} = \frac{1-\sqrt{3}}{2} + \frac{1+\sqrt{3}}{2}i$ and $\frac{i}{\frac{1}{2}-\frac{\sqrt{3}}{2}i} = 2\frac{i}{1-\sqrt{3}i} = 2\frac{i}{1-\sqrt{3}i}\cdot\frac{1+\sqrt{3}i}{1+\sqrt{3}i} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$, we have $\frac{1}{t}v = \frac{1}{2}\big(1-\sqrt{3}+(1+\sqrt{3})i,\ \sqrt{3}+i\big)$.

Quiz Q15. Write all the 5'th complex roots of 1, i.e., all the values of $\sqrt[5]{1}$ in polar form, and present them graphically. Of them choose the root t with largest *positive* argument, and find its inverse t^{-1} and its conjugate $\bar{t}$. Explain your answer.
Solution: There are five roots: $\cos(\frac{2\pi}{5}k) + i\sin(\frac{2\pi}{5}k)$ with $k = 1,2,3,4,5$. They are forming the vertices of the regular 5-angle with radius 1 on $\mathbb{C}$. The root with largest positive argument is achieved for $k = 2$, i.e., $t = \cos(\frac{4\pi}{5}) + i\sin(\frac{4\pi}{5})$. Its inverse and conjugate are equal: $t^{-1} = \bar{t} = \cos(\frac{4\pi}{5}) - i\sin(\frac{4\pi}{5}) = \cos(-\frac{4\pi}{5}) + i\sin(-\frac{4\pi}{5})$.

Quiz Q16. List all the 3'rd complex roots of 1. Of these roots find the root t for which $\arg t \in (\frac{\pi}{2}, \pi)$. Explain your answer.
Solution: There are *three* roots $t_k = \cos\big(\frac{2\pi}{3}k\big) + i\,\sin\big(\frac{2\pi}{3}k\big)$, where $k = 0,1,2$. Their arguments are: 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$. So the only option is $t = t_1 = \cos\big(\frac{2\pi}{3}\big) + i\,\sin\big(\frac{2\pi}{3}\big)$.

Quiz Q17. We are given the complex vector $v = (5, 5i, 10-5i) \in \mathbb{C}^3$ and the scalar $a = 2+i$. Find the inverse a^{-1} and calculate the vector $-a^{-1}\,v$.
Solution: $a^{-1} = \frac{1}{2+i} = \frac{1}{2+i}\cdot\frac{2-i}{2-i} = \frac{2-i}{5}$. Then we have $-a^{-1}\,v = -\frac{2-i}{5}(5,\, 5i,\, 10-5i) = (-2+i, -1-2i, -3+4i)$.

Quiz Q18. We are given the complex number $x = 1+i$ and a complex vector $\vec{v} = (2,-i) \in \mathbb{C}^2$. Compute the vector $\vec{w} = x^{20}\,\vec{v}$. Explain your answer.
Solution: The polar form of x is $x = r(\cos\theta + i\sin\theta) = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})$. Thus, $z^{20} = (\sqrt{2})^{20}(\cos\frac{20\cdot\pi}{4} + i\sin\frac{20\cdot\pi}{4}) = 2^{10}(\cos(5\pi) + i\sin(5\pi)) = -2^{10}$. Therefore, $\vec{w} = (-2^{11}, 2^{10}i)$.

Quiz Q19. Find the inverse x^{-1}, and compute the vector $x^{-1}\vec{v}$ in $\mathbb{C}^3$, if we know that $|x| = \sqrt{2}$, $\arg(x) = \frac{\pi}{4}$, $\vec{v} = (3, 0, 2i)$. Explain your answer.
Solution: Since $|x| = \sqrt{2}$ and $\arg(x) = \frac{\pi}{4}$, then $x = 1+i$. We have $x^{-1} = \frac{1}{1+i} = \frac{1}{1+i}\frac{1-i}{1-i} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i$. Thus, $x^{-1}\vec{v} = (\frac{1}{2} - \frac{1}{2}i)(3, 0, 2i) = (\frac{3}{2} - \frac{3}{2}i,\ 0,\ 1+i)$.

Quiz Q20. In the space $\mathbb{Z}_7^2$ we are given the vectors $u = (3,6)$ and $v = (5,2)$. Find a vector $w \in \mathbb{Z}_7^2$ such that $3w + u = 5v$. Explain your answer.
Solution: We have $3w = 5v - u = 5(5,2) - (3,6) = (4,3) - (3,6) = (1,4)$. Thus, $w = 3^{-1}(1,4) = 5(1,4) = (5,6)$. ($3^{-1} = 5$ because $7 = 2\cdot 3 + 1$, i.e., $1\cdot 7 - 2\cdot 3 = 1$ and so $3^{-1} = -2 + 7 = 5$.)

Quiz Q21. We are given the decomposition $7\cdot 67 - 13\cdot 36 = 1$. In modular space $\mathbb{Z}_{67}^2$ find a vector u such that $36u = (24,54) - (22,53)$. Explain your answer.
Solution: Since $-13 \notin \mathbb{Z}_{67}$, we have $36^{-1} = -13 + 67 = 54 \in \mathbb{Z}_{67}$. Therefore $36u = (24,54) - (22,53) = (2,1)$ and so $u = 36^{-1}(2,1) = 54(2,1) = (41,54)$.

Quiz Q22. Find a such value for the number $a \in \mathbb{Z}_5$ for which the vector $u = (a,1)$ is collinear to the vector $v = 2^{-1}\big((4,2) + (3,4)\big)$, e.g., $u = cv$ for some scalar $c \in \mathbb{Z}_5$. Explain your answer.
Solution: Clearly, $2^{-1} = 3$ in $\mathbb{Z}_5$. Thus, $v = 3\big((4,2) + (3,4)\big) = 3(2,1) = (1,3)$. Comparing the second coordinates of *collinear* vectors u and v we see that $1 = c\cdot 3$, i.e., $c = 3^{-1} = 2$. Thus, $a = 2\cdot 1 = 2$, i.e., $u = (2,1) = 2v$.

Quiz Q23. Find the inverse a^{-1}, and compute the vector $a^{-1}\vec{v} + \vec{u}$ in $\mathbb{Z}_5^3$ if $a = 2$, $\vec{u} = (3,0,2)$, $\vec{v} = (4,1,4)$. Explain your answer.
Solution: In the field $\mathbb{Z}_5$ we have $a^{-1} = 2^{-1} = 3$. Then $3(4,1,4) + (3,0,2) = (2,3,2) + (3,0,2) = (0,3,4)$.

Quiz Q24. In the space $\mathbb{Z}_7^2$ list all the vectors v that are collinear to the vector $w = (2,4)$ (i.e., those vectors v which are of form $v = c\,w$ for $c \in \mathbb{Z}_7$). Explain your answer.
Solution: As $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$, the collinear vectors are: $0\,(2,4) = (0,0)$, $1\,(2,4) = (2,4)$, $2\,(2,4) = (4,1)$, $3\,(2,4) = (6,5)$, $4\,(2,4) = (1,2)$, $5\,(2,4) = (3,6)$, $6\,(2,4) = (5,3)$.

Quiz Q25. In modular space $\mathbb{Z}_5^3$ we are given the vectors $u = (2,1,0)$ and $v = (4,3,2)$. Calculate the vector $w = 3^{-1}u - 4v$. Explain your answer.
Solution: Since in the field $\mathbb{Z}_5$ we have $3^{-1} = 2$, then $w = 3^{-1}(2,1,0) - 4(4,3,2) = 2(2,1,0) - 4(4,3,2) = (4,2,0) - (1,2,3) = (3,0,2)$.

Quiz Q26. We already know the equality $6\cdot 37 - 17\cdot 13 = 1$. Using it calculate the vector $w = 13^{-1}(2,\,3) - 3(11,\,15)$ in the modular space $\mathbb{Z}_{37}^2$.

Solution: Since -17 is negative, $13^{-1} = -17+37 = 20$. Then $20(2,3) - 3(11,15) = (3,23) - (33,8) = (7,15)$.

Quiz Q27. In the space $\mathbb{Z}_5^3$ find a vector v such that $v + (2,3,1) = (3,2,1)$. Also find a vector u such that $3u = (4,1,0)$. Explain your answer.
Solution: If $v + (2,3,1) = (1,2,0)$, then $v = (3,2,1) - (2,3,1) = (1,4,0)$. Also, since in $\mathbb{Z}_5$ we have $3^{-1} = 2$, we from $3u = (4,1,0)$ have $u = 3^{-1}(4,1,0) = 2(4,1,0) = (3,2,0)$.

Quizzes on linear equations, matrices, row-equivalence

Quiz Q28. Write the augmented matrix of the system $\begin{cases} x_3 = 1 \\ x_1 + 2x_2 = 1 \\ 2x_1 + 4x_2 + x_3 = 3 \end{cases}$. Bring $\bar{A}$ to a row-echelon form, and based on it detect if the system is consistent. Indicate which are the free and pivot variables.
Solution: $\bar{A} = \begin{bmatrix} 0&0&1&1 \\ 1&2&0&1 \\ 2&4&1&3 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&1 \\ 0&0&1&1 \\ 2&4&1&3 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&1 \\ 0&0&1&1 \\ 0&0&1&1 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&1 \\ 0&0&1&1 \\ 0&0&0&0 \end{bmatrix} = R$. The system is consistent, since the last column of R contains no pivot, i.e., $\operatorname{rank}(A) = 2 = \operatorname{rank}(\bar{A})$. x_1, x_3 are pivot variables, x_2 is a free variable.

Quiz Q29. In $\mathbb{R}^3$ we are given two planes. We know the normal vector $n = (1,2,1)$ and the position $p = (1,0,0)$ for $\mathcal{P}_1$. And we know $\mathcal{P}_2$ has the general form $2x+4y+3z-5 = 0$. Compose a system consisting of general equations of $\mathcal{P}_1$ and of $\mathcal{P}_2$. Find out if the system has a solution using a row-echelon form of its augmented matrix.
Solution: The general form of $\mathcal{P}_1$ is $x + 2y + z = n \cdot p = 1$. The system is $\begin{cases} x+2y+z = 1 \\ 2x+4y+3z = 5 \end{cases}$. For its augmented matrix we have $\bar{A} = \begin{bmatrix} 1&2&1&1 \\ 2&4&3&5 \end{bmatrix} \sim \begin{bmatrix} 1&2&1&1 \\ 0&0&1&4 \end{bmatrix}$. So the system is consistent because its last column contains no pivot.

Quiz Q30. We are given two real matrices $A = \begin{bmatrix} 1&1&0&1 \\ 0&1&2&2 \\ 0&2&4&6 \end{bmatrix}$ and $B = \begin{bmatrix} 1&1&0&1 \\ 0&1&2&2 \\ 0&2&4&4 \end{bmatrix}$. Detect if they are row-equivalent or not. (You may use systems of linear equations, or the reduced row-echelon forms.)
Solution: Bring to row-echelon form: $A \sim \begin{bmatrix} 1&1&0&1 \\ 0&1&2&2 \\ 0&0&0&2 \end{bmatrix}$, $B \sim \begin{bmatrix} 1&1&0&1 \\ 0&1&2&2 \\ 0&0&0&0 \end{bmatrix}$. The first is augm. matrix for an *inconsistent*, and the second is augm. matrix for a *consistent* system, and so $A \not\sim B$. Else, check $\operatorname{rref}(A) \neq \operatorname{rref}(B)$, and so $A \not\sim B$.

Quiz Q31. Find out which ones of these real matrices are row-equivalent $A = \begin{bmatrix} 1&3&0 \\ 0&0&1 \\ 2&6&0 \end{bmatrix}$, $B = \begin{bmatrix} 1&3&0 \\ 1&3&1 \\ 0&0&0 \end{bmatrix}$, $C = \begin{bmatrix} 2&2&2&2 \\ 4&4&4&7 \end{bmatrix}$. Also find the ranks of these matrices. *Hint*: first compare their sizes.
Solution: C is not row-equivalent to A or B since it is of different size. Compute $A = \begin{bmatrix} 1&3&0 \\ 0&0&1 \\ 2&6&0 \end{bmatrix} \sim \begin{bmatrix} 1&3&0 \\ 0&0&1 \\ 0&0&0 \end{bmatrix} = \operatorname{rref}(A)$ and $B = \begin{bmatrix} 1&3&0 \\ 1&3&1 \\ 0&0&0 \end{bmatrix} \sim \begin{bmatrix} 1&3&0 \\ 0&0&1 \\ 0&0&0 \end{bmatrix} = \operatorname{rref}(B)$. Since $\operatorname{rref}(A) = \operatorname{rref}(B)$, we have $A \sim B$. Also, from $\operatorname{rref}(A)$ and $\operatorname{rref}(B)$ it is clear that $\operatorname{rank}(A) = \operatorname{rank}(B) = 2$. Since $C = \begin{bmatrix} 2&2&2&2 \\ 4&4&4&7 \end{bmatrix} \sim \begin{bmatrix} 2&2&2&2 \\ 0&0&0&3 \end{bmatrix}$, we have $\operatorname{rank}(C) = 2$.

Quiz Q32. A system of real linear equations is given by its augmented matrix $\bar{A} = \begin{bmatrix} 0&0&1&0&2 \\ 1&2&0&0&0 \\ 0&0&0&2&6 \end{bmatrix}$. Solve the system by Gauss-Jordan method. Apply Theorem 7.19 for this system.
Solution: Find the $\operatorname{rref}(\bar{A})$ as follows: $\bar{A} = \begin{bmatrix} 0&0&1&0&2 \\ 1&2&0&0&0 \\ 0&0&0&2&6 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&0&0 \\ 0&0&1&0&2 \\ 0&0&0&2&6 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1}&2&0&0&0 \\ 0&0&\mathbf{1}&0&2 \\ 0&0&0&\mathbf{1}&3 \end{bmatrix} = \operatorname{rref}(\bar{A})$. So the system is consistent. We get $\begin{cases} x_1 = -2x_2 \\ x_3 = 2 \\ x_4 = 3. \end{cases}$ Assigning $x_2 = \alpha$ we have the general

solution $\{(-2\alpha,\ \alpha,\ 2,\ 3)\ |\ \alpha\in\mathbb{R}\}$. By Theorem 7.19 the system is consistent because $\operatorname{rank}(A)=\operatorname{rank}(\bar{A})=3$.

Quiz Q33. We are given the system of real equations $\begin{cases} x_1+3x_2+x_4 & =0\\ x_3+x_4 & =2\\ 2x_1+6x_2+2x_4 & =0\end{cases}$. Bring $\bar{A}$ to a reduced row-echelon form, and solve the system by the Gauss-Jordan method (write the solution as a set).
Solution: $\bar{A}=\begin{bmatrix}1&3&0&1&0\\0&0&1&1&2\\2&6&0&2&0\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&3&0&1&0\\0&0&\mathbf{1}&1&2\\0&0&0&0&0\end{bmatrix}=\operatorname{rref}(\bar{A})$. The system is consistent, since the last column contains no pivot, i.e., $\operatorname{rank}(A)=2=\operatorname{rank}(\bar{A})$. x_1,x_3 are pivot variables, x_2,x_4 are free variables. In $\begin{cases}x_1 = -3x_2-x_4\\ x_3 = 2-x_4\end{cases}$ we set $x_2=\alpha,\ \ x_4=\beta$. Then the general solution is $\{(-3\alpha-\beta,\ \alpha,\ 2-\beta,\ \beta)\,|\,\alpha,\beta\in\mathbb{R}\}$.

Quiz Q34. We have a system of real linear equations $AX=B$ with the augmented matrix $\bar{A}=\begin{bmatrix}1&2&0&3&0&0\\0&0&1&3&0&0\\0&0&1&3&1&1\end{bmatrix}$. Find if the system is consistent. If yes, find its general solution. Explain your answer.
Solution: $\bar{A}=\begin{bmatrix}2&4&0&4&0&0\\0&0&1&3&0&0\\0&0&1&3&1&1\end{bmatrix}\sim\begin{bmatrix}2&4&0&4&0&0\\0&0&1&3&0&0\\0&0&0&0&1&1\end{bmatrix}\sim\begin{bmatrix}1&2&0&2&0&0\\0&0&1&3&0&0\\0&0&0&0&1&1\end{bmatrix}=\operatorname{rref}(\bar{A})$. So $AX=B$ is consistent. We get $\begin{cases}x_1 = -2x_2-2x_4\\ x_3 = -3x_4\\ x_5 = 1\end{cases}$ Assigning $x_2=\alpha$ and $x_4=\beta$ we have the general solution $\{[-2\alpha-2\beta,\ \ \alpha,\ \ -3\beta,\ \beta,\ \ 1]\ |\ \alpha,\ \beta\in\mathbb{R}\}$.

Quiz Q35. We are given two matrices $A=\begin{bmatrix}1&1&0\\0&0&1\\0&1&3\end{bmatrix}$ and $B=\begin{bmatrix}2&0&0\\0&1&0\\0&1&0\end{bmatrix}$. Using any method find out if they are row-equivalent or not. Explain your answer.
Solution: We have $A\sim\begin{bmatrix}1&1&0\\0&1&3\\0&0&1\end{bmatrix}\sim\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}\sim\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$, and $B\sim\begin{bmatrix}2&0&0\\0&1&0\\0&0&0\end{bmatrix}\sim\begin{bmatrix}1&0&0\\0&1&0\\0&0&0\end{bmatrix}$. Since $\operatorname{rref}(A)\neq\operatorname{rref}(B)$, then $A\not\sim B$.

Quiz Q36. The reduced row-echelon form of the augmented matrix $\bar{A}$ of the system of linear equations $AX=B$ is $\operatorname{rref}(\bar{A})=\begin{bmatrix}1&3&0&5&0&0\\0&0&1&2&0&0\\0&0&0&0&1&1\end{bmatrix}$. Detect if or not the system is consistent, list its pivot and free variables. Find $\operatorname{rank}(A)$ of the matrix of system. Explain your answer.
Solution: The system is consistent since $\operatorname{rank}(A)=\operatorname{rank}(\bar{A})=3$ (or since the last column of $\bar{A}$ is *not* pivot). The pivot variables are x_1,x_3,x_5. The free variables are x_2,x_4.

Quiz Q37. The reduced row-echelon form $\operatorname{rref}(\bar{A})$ of the augmented matrix $\bar{A}$ of a system of lin. equations is $\operatorname{rref}(\bar{A})=\left[\begin{array}{cccccc|c}1&3&0&1&0&2\\0&0&1&2&0&0\\0&0&0&0&1&2\end{array}\right]$. Find if the system is consistent, and if yes, compute its general solution.
Solution: It is consistent since $\operatorname{rank}(A)=\operatorname{rank}(\bar{A})=3$ (i.e., the last column isn't pivot).
We have $\begin{cases}x_1=2-3x_2-x_4\\ x_3=-2x_4\\ x_5=2\end{cases}$.
From here setting $x_2=\alpha,\ \ x_4=\beta$ we get the solution $(2-3\alpha-\beta,\ \ \alpha,\ \ -2\beta,\ \ \beta,\ \ 2)$, $\alpha,\beta\in\mathbb{R}$.

Quiz Q38. Write the augmented matrix of the following system of linear equations, and bring it to a row-echelon form: $\begin{cases}x_1+2x_2 & =1\\ x_1+2x_2+x_3 & =0\\ x_3 & =1\end{cases}$. Then deduce from that from if the system is consistent.
Solution: $\bar{A}=\begin{bmatrix}1&2&0&1\\1&2&1&0\\0&0&1&1\end{bmatrix}\sim\begin{bmatrix}1&2&0&1\\0&0&1&-1\\0&0&1&1\end{bmatrix}\sim\begin{bmatrix}1&2&0&1\\0&0&1&-1\\0&0&0&2\end{bmatrix}$. The system is inconsistent because $\operatorname{rank}(A)=2\neq3=\operatorname{rank}(\bar{A})$.

Quizzes on matrix algebra

Quiz Q39. We have the real matrices $A = [2 \ \ 1 \ \ 0]$ and $B = [1 \ \ 0 \ \ 2]$. Compute the matrix $N = A^T \cdot B$. Find the rank of N. Suppose N is the augmented matrix of some system of linear equations. Is that system consistent?
Solution: We get $N = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix}$. Its row-echelon from is computed as $N = \begin{bmatrix} 2 & 0 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 2 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. That is, $\operatorname{rank}(N) = 1$. The system is consistent because the last column of N contains no pivot. Or, by Theorem 7.19 we have $\operatorname{rank} \begin{bmatrix} 2 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \operatorname{rank} \begin{bmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} = 1$.

Quiz Q40. We are given the complex row matrices $A = [2i \ \ 3 \ \ 0]$ and $B = [-i \ \ 0 \ \ 1]$ in $M_{1,3}(\mathbb{C})$. Compute the matrix $M = 2(A^T \cdot B)$. Deduce without any row-elimination, if $\operatorname{rank}(M)$ may be equal to 3.
Solution: We have $M = 2 \cdot \begin{bmatrix} 2i \\ 3 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} -i & 0 & 1 \end{bmatrix} = 2 \cdot \begin{bmatrix} 2 & 0 & 2i \\ -3i & 0 & 3 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 4i \\ -6i & 0 & 6 \\ 0 & 0 & 0 \end{bmatrix}$. Since the 3'rd row of M is zero, its row-echelon form may contain *at most* 2 non-zero rows, i.e., $\operatorname{rank}(M) \neq 3$.

Quiz Q41. We are given the matices $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$. Compute $M = A \cdot B^T + I_2$, and then find $\operatorname{rank}(M)$. Explain your answer.
Solution: We have $A \cdot B^T = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$. Therefore, $M = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}$. The matrix M already is in row-echelon form, and it has two non-zero rows. I.e., $\operatorname{rank}(M) = 2$.

Quiz Q42. We are given the matix $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. Complete the matrix operations $2A \cdot A^T$.
Solution: We have $2A = \begin{bmatrix} 0 & 0 & 2 \\ 2 & 4 & 0 \\ 0 & 2 & 0 \end{bmatrix}$. Therefore $2A \cdot A^T = \begin{bmatrix} 0 & 0 & 2 \\ 2 & 4 & 0 \\ 0 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 10 & 4 \\ 0 & 4 & 2 \end{bmatrix}$.

Quiz Q43. We are given the matices $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. Compute $(AB)^T + I_3$.
Solution: We have $AB = \begin{bmatrix} 0 & 2 & 2 \\ 2 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$. Thus $(AB)^T + I_3 = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 2 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$.

Quiz Q44. We are given the matrix $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix}$. Based on *definitions* of elementary matrices detect if A is an elementary matrix. Compute the power A^{100} using the result you found. Explain your answer.
Solution: Since A is obtained from I_3 by element. operat. of 3'rd type, A is an element. matrix of the 3'rd type. Its action corresponds to $R3 + 2R1$. Applying this transformation for 100 times is the same as $R3 + 200R1$. Therefore, $A^{100} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 200 & 0 & 1 \end{bmatrix}$.

Quiz Q45. Using the *definition* of elementary matrices indicate if $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix}$ is an elementary matrix (if yes, of which type?). Compute the power A^{10} *without using the row-by-column multiplication rule*.
Solution: A is an elementary matrix of 3'rd type as it is obtained from I using $R3 + 5 \cdot R1$. Thus, A^{10} is equivalent to repeated application of $R3 + 5 \cdot R1$ for 10 times, i.e., to $R3 + 50 \cdot R1$. Thus $A^{10} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 50 & 0 & 1 \end{bmatrix}$.

Quiz Q46. We know that $A \in M_{3,3}(\mathbb{R})$ is a product of three matrices M, N, K from $M_{3,3}(\mathbb{R})$. We also know that $\operatorname{rank}(M) = 3$, $\operatorname{rref}(N) = I_3$, and K is the elementary matrix corresponding to $R2 + 7R3$. From this information deduce if or not A is invertible. Also, find $\operatorname{rref}(A)$.

Solution: From the theorem on equivalent conditions for invertible matrices we get that M, N, K are invertible. So their product also is invertible. Thus, $\operatorname{rref}(A) = I_3$ by the same theorem.

Quiz Q47. We are given $A = \begin{bmatrix} 1&0&0\\0&0&0\\0&0&1 \end{bmatrix}$, $B = \begin{bmatrix} 1&0&0\\0&1&1\\0&0&1 \end{bmatrix}$, $C = \begin{bmatrix} 1&0&0\\1&1&0\\0&1&1 \end{bmatrix}$, $D = \begin{bmatrix} 0&0&2\\0&1&0\\1&0&0 \end{bmatrix}$. For each of them explain if it is an elementary matrix using the definitions of elementary matrices. Interpreting the elementary matrices by elementary operations calculate the matrix B^{2019} and find $\operatorname{rref}\big(B^{2019}\big)$.
Solution: A, C, D are not elementary, since they cannot be obtained from I_3 by only one elementary operation. B is elementary, and it corresponds to $R2 + R3$. Applying this 2019 times we add to the 2'nd row the 3'rd row 2019 times, i.e., $R2 + 2019 \cdot R3$. Thus, $B^{2019} = \begin{bmatrix} 1&0&0\\0&1&2019\\0&0&1 \end{bmatrix}$. Since B^{2019} is invertible, we get $\operatorname{rref}\big(B^{2019}\big) = I_3$.

Quiz Q48. The matrix $A \in M_{3,3}(\mathbb{R})$ is a product $A = E_1E_2E_3$ of elementary matrices. E_1 corresponds to $3 \cdot R1$, and E_2 corresponds to $R1 \longleftrightarrow R3$, and E_3 corresponds to $R2+2R1$. Find the inverse A^{-1}.
Solution: $E_1 = \begin{bmatrix} 3&0&0\\0&1&0\\0&0&1 \end{bmatrix}$, $E_2 = \begin{bmatrix} 0&0&1\\0&1&0\\1&0&0 \end{bmatrix}$, $E_3 = \begin{bmatrix} 1&0&0\\2&1&0\\0&0&1 \end{bmatrix}$. Thus, $E_1^{-1} = \begin{bmatrix} \frac{1}{3}&0&0\\0&1&0\\0&0&1 \end{bmatrix}$, $E_2^{-1} = \begin{bmatrix} 0&0&1\\0&1&0\\1&0&0 \end{bmatrix}$, $E_3^{-1} = \begin{bmatrix} 1&0&0\\-2&1&0\\0&0&1 \end{bmatrix}$. So $A^{-1} = E_3^{-1}E_2^{-1}E_1^{-1} = \begin{bmatrix} 1&0&0\\-2&1&0\\0&0&1 \end{bmatrix}\begin{bmatrix} 0&0&1\\0&1&0\\1&0&0 \end{bmatrix}\begin{bmatrix} \frac{1}{3}&0&0\\0&1&0\\0&0&1 \end{bmatrix} = \begin{bmatrix} 0&0&1\\0&1&-2\\1&0&0 \end{bmatrix}\begin{bmatrix} \frac{1}{3}&0&0\\0&1&0\\0&0&1 \end{bmatrix} = \begin{bmatrix} 0&0&1\\0&1&-2\\\frac{1}{3}&0&0 \end{bmatrix}$. We need not find A to get the A^{-1}.

Quiz Q49. The matrix $A \in M_{3,3}(\mathbb{R})$ is a product of 20 elementary matrices. Find $\operatorname{rank}(A)$. Is A invertible?
Solution: Each elementary matrix is invertible, and the product of invertible matrices is invertible. The rank of an invertible matrix is equal to its degree. In this case $\operatorname{rank}(A)$ is equal to 3.

Quiz Q50. We are given the matrix $A \in M_{3,3}(\mathbb{R})$. We know that $\operatorname{rank}(A) = 3$. Is A invertible? Does A have a transpose? What is $\operatorname{rref}(A)$? Explain your answer.
Solution: A is of degree $n = 3$, and is rank is equal to its degree: $\operatorname{rank}(A) = 3$. By theorem on equivalent conditions for square matrices A is invertible, and $\operatorname{rref}(A) = I_3$. A has a transpose since *any* matrix has a transpose.

Quiz Q51. Indicate if the matrix $A = \begin{bmatrix} 1&0&2\\0&1&1\\0&1&2 \end{bmatrix}$ is invertible, and compute it, in case A is an invertible matrix.
Solution: We have $[A \mid I] = \left[\begin{array}{ccc|ccc} 1&0&2&1&0&0\\0&1&1&0&1&0\\0&1&2&0&0&1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1&0&2&1&0&0\\0&1&1&0&1&0\\0&0&1&0&-1&1 \end{array}\right]$. Since $\operatorname{rank}[A \mid I\,] = 3$, then A is invertible. $[A \mid I\,] \sim \left[\begin{array}{ccc|ccc} 1&0&0&1&2&-2\\0&1&0&0&2&-1\\0&0&1&0&-1&1 \end{array}\right]$. Therefore $A^{-1} = \begin{bmatrix} 1&2&-2\\0&2&-1\\0&-1&1 \end{bmatrix}$.

Quiz Q52. Compute the inverse of the matrix $A = \begin{bmatrix} 1&0&1\\0&1&0\\0&1&1 \end{bmatrix}$ by the Gauss-Jordan method.
Solution: $[A \mid I] = \left[\begin{array}{ccc|ccc} 1&0&1&1&0&0\\0&1&0&0&1&0\\0&1&1&0&0&1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1&0&1&1&0&0\\0&1&0&0&1&0\\0&0&1&0&-1&1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1&0&0&1&1&-1\\0&1&0&0&1&0\\0&0&1&0&-1&1 \end{array}\right] = [I \mid A^{-1}]$. Therefore $A^{-1} = \begin{bmatrix} 1&1&-1\\0&1&0\\0&-1&1 \end{bmatrix}$.

Quiz Q53. Find out if the matrix $A = \begin{bmatrix} 2&0&0\\1&0&1\\0&1&2 \end{bmatrix} \in M_{3,3}(\mathbb{Z}_3)$ is invertible, and compute the inverse by the Gauss-Jordan method, if yes. Deduce from from your results (with no new row-eliminations) what is $\operatorname{rref}(A)$. *Hint*: A is over $\mathbb{Z}_3$, so all operations are *modular*.

Solution: Firstly, $[A \mid I] = \left[\begin{array}{ccc|ccc} 2&0&0&1&0&0\\ 1&0&1&0&1&0\\ 0&1&2&0&0&1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 2&0&0&1&0&0\\ 0&0&1&1&1&0\\ 0&1&2&0&0&1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 2&0&0&1&0&0\\ 0&1&2&0&0&1\\ 0&0&1&1&1&0 \end{array}\right]$. We get that rank$[A \mid I] = 3$, that is, A is an invertible matrix. Next, $[A \mid I] \sim \left[\begin{array}{ccc|ccc} 1&0&0&2&0&0\\ 0&1&2&0&0&1\\ 0&0&1&1&1&0 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1&0&0&2&0&0\\ 0&1&0&1&1&1\\ 0&0&1&1&1&0 \end{array}\right]$. Thus, $A^{-1} = \begin{bmatrix} 2&0&0\\ 1&1&1\\ 1&1&0 \end{bmatrix}$. Finally, $\mathrm{rref}(A) = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix} = I$ because A is an invertible matrix.

Quiz Q54. $A \in M_{3,3}(\mathbb{R})$ is a product $A = E_1E_2E_3E_4$ of four elementary matrices which respectively correspond to four elementary operations: $R3 \longleftrightarrow R1$, $R2 + R1$, $-5 \cdot R1$, $R3 - 5R1$. Find the matrices E_1, E_2, E_3, E_4. Then find the inverses $E_1^{-1}, E_2^{-1}, E_3^{-1}, E_4^{-1}$. Deduce if A is invertible. If yes, present A^{-1} as a product of four elementary matrices.
Solution: $E_1 = \begin{bmatrix} 0&0&1\\ 0&1&0\\ 1&0&0 \end{bmatrix}$, $E_2 = \begin{bmatrix} 1&0&0\\ 1&1&0\\ 0&0&1 \end{bmatrix}$, $E_3 = \begin{bmatrix} -5&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix}$, $E_4 = \begin{bmatrix} 1&0&0\\ 0&1&0\\ -5&0&1 \end{bmatrix}$. Then $F_1 = E_1^{-1} = E_1$, $F_2 = E_2^{-1} = \begin{bmatrix} 1&0&0\\ -1&1&0\\ 0&0&1 \end{bmatrix}$, $F_3 = E_3^{-1} = \begin{bmatrix} -\frac{1}{5}&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix}$, $F_4 = E_4^{-1} = \begin{bmatrix} 1&0&0\\ 0&1&0\\ 5&0&1 \end{bmatrix}$. In these notations: $A^{-1} = F_4F_3F_2F_1$.

Quizzes on spaces, subspaces, bases

Quiz Q55. In matrix space $M_{2,2}(\mathbb{R})$ we are given $U = \left\{\begin{bmatrix} a&b\\ c&d \end{bmatrix} \mid a+b=0,\ c \cdot d > 0\right\}$. Determine if U is a subspace of $M_{2,2}(\mathbb{R})$. Explain your answer.
Solution: U is *not* a subspace. The condition $c \cdot d > 0$ means that *both* entries in the 2'nd row are positive *or* negative. The sum of two matrices with this property may *not* have this property. $\begin{bmatrix} 1&-1\\ -3&-1 \end{bmatrix} + \begin{bmatrix} 1&-1\\ 2&2 \end{bmatrix} = \begin{bmatrix} 2&-2\\ -1&1 \end{bmatrix} \notin U$.

Quiz Q56. In the space $\mathbb{C}^3$ we are given a subset defined as $U = \{(x, y, z) \mid x = 2y,\ z^2 = y\}$. Determine if U is a subspace of $\mathbb{C}^3$. Explain your answer.
Solution: U is *not* a subspace as it does *not* meet the conditions of the second definition of subspace. Say, $v = (2, 1, -1)$ is in U, but $3v = 3(2, 1, -1) = (6, 3, -3)$ is not in U, as $(-3)^2 \neq 3$.

Quiz Q57. In the real polynomial space $V = \mathcal{P}_4$ we are given a subset W of all polynomils $f(x) = a + bx + cx^4$ for which $(a + b + c)^2 < 5$. Find two linearly independent vectors in W. Determine if W is a subspace of V.
Solution: As two linearly independent vectors take any non-collinear polynomials in W, say, $f_1(x) = x^4$, $f_2(x) = x$. U is *not* a subspace. $f(x) = x + x^4 \in W$, but $3f(x) = 3x + 3x^4 \notin W$.

Quiz Q58. In the polynomial space $V = \mathcal{P}_3$ we are given a subset $U = \{ax + bx^3 \mid a, b \in \mathbb{R}\}$. Determine if U is a subspace of V. Are *all* the polynomials of U of degree 3? Explain your answer.
Solution: U is a subspace, as $(ax + bx^3) + (a'x + b'x^3) = (a + a')x + (b + b')x^3$ and $c \cdot (ax + bx^3) = (c \cdot a)x + (c \cdot b)x^3$ also are in U. *Not* all polynomials of U are of degree 3, as $f(x) = 0$ has *no degree*, and $f(x) = x$ has degree 1.

Quiz Q59. In the matrix space $V = M_{2,3}(\mathbb{R})$ we are given the subset $W = \left\{\begin{bmatrix} a&0&3a\\ 0&2a&0 \end{bmatrix} \mid a \in \mathbb{R}\right\}$. Using any definition of subspace determine if W is a subspace of V. If yes, find a basis for W. Explain your answer.
Solution: Sum of matrices of above type is of the same type: $\begin{bmatrix} a&0&3a\\ 0&2a&0 \end{bmatrix} + \begin{bmatrix} a'&0&3a'\\ 0&2a'&0 \end{bmatrix} = \begin{bmatrix} a''&0&3a''\\ 0&2a''&0 \end{bmatrix}$, where $a'' = a + a'$. For any $c \in \mathbb{R}$ we have $c \cdot \begin{bmatrix} a&0&3a\\ 0&2a&0 \end{bmatrix} = \begin{bmatrix} a'&0&3a'\\ 0&2a'&0 \end{bmatrix}$

where $a' = ca$. So W is a subspace. As a basis for W take $M = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 0 \end{bmatrix}$. It is linearly independent because $M \neq 0$. And it is a spanning set because $\begin{bmatrix} a & 0 & 3a \\ 0 & 2a & 0 \end{bmatrix} = a \cdot M$ for any a.

Quizzes on change of basis in spaces

Quiz Q60. Let E be the standard basis in $\mathbb{R}^3$. Vectors of the basis $G = \{g_1, g_2, g_3\}$ of V are not given, but we know the change of basis matrix $P_{GE} = \begin{bmatrix} 0&1&0 \\ 1&0&1 \\ 2&0&1 \end{bmatrix}$. Find the coordinates $[v]_E$ of the vector $v \in V$, if $[v]_G = (2,3,0)$.
Solution: Since $P_{EG} = P_{GE}^{-1}$, we compute $\begin{bmatrix} 0&1&0&1&0&0 \\ 1&0&1&0&1&0 \\ 2&0&1&0&0&1 \end{bmatrix} \sim \begin{bmatrix} 1&0&1&0&1&0 \\ 0&1&0&1&0&0 \\ 2&0&1&0&0&1 \end{bmatrix} \sim \begin{bmatrix} 1&0&1&0&1&0 \\ 0&1&0&1&0&0 \\ 0&0&-1&0&-2&1 \end{bmatrix} \sim \begin{bmatrix} 1&0&0&0&-1&1 \\ 0&1&0&1&0&0 \\ 0&0&1&0&2&-1 \end{bmatrix} = [I_3 \,|\, P_{EG}]$. Then $[v]_E = P_{EG}[v]_G = (-3,2,6)$.

Quiz Q61. In the space $V = \mathbb{R}^3$ we have two bases $G = \{g_1, g_2, g_3\}$ and $H = \{h_1, h_2, h_3\}$. The coordinates of their vectors in the standard basis E are: $g_1 = \begin{bmatrix} 0\\4\\1 \end{bmatrix}$, $g_2 = \begin{bmatrix} 1\\2\\4 \end{bmatrix}$, $g_3 = \begin{bmatrix} 0\\2\\1 \end{bmatrix}$, and $h_1 = \begin{bmatrix} 1\\2\\1 \end{bmatrix}$, $h_2 = \begin{bmatrix} 0\\2\\0 \end{bmatrix}$, $h_3 = \begin{bmatrix} 0\\0\\1 \end{bmatrix}$. Find the coordinates of the vector $v \in \mathbb{R}^3$ in the basis H, if its coordinates in the basis G are $[3,0,1]$.
Solution: Bring $[H \,|\, G]$ to the reduced row-echelon form. $[H \,|\, G] \sim \begin{bmatrix} 1&0&0&0&1&0 \\ 2&2&0&4&2&2 \\ 1&0&1&1&4&1 \end{bmatrix} \sim \begin{bmatrix} 1&0&0&0&1&0 \\ 0&1&0&2&0&1 \\ 0&0&1&1&3&1 \end{bmatrix} = [I \,|\, P_{HG}]$. Thus, $P_{HG} = \begin{bmatrix} 0&1&0 \\ 2&0&1 \\ 1&3&1 \end{bmatrix}$, and so $[v]_H = P_{HG} \cdot [v]_G = \begin{bmatrix} 0&1&0 \\ 2&0&1 \\ 1&3&1 \end{bmatrix} \begin{bmatrix} 3\\0\\1 \end{bmatrix} = \begin{bmatrix} 0\\7\\4 \end{bmatrix}$.

Quiz Q62. In $V = \mathbb{R}^3$ we are given two bases: the first basis E consists of vectors $e_1 = [0,1,0]$, $e_2 = [1,0,1]$, $e_3 = [0,0,1]$; and the second basis G consists of vectors $g_1 = [0,0,1]$, $g_2 = [2,1,2]$, $g_3 = [1,1,0]$. Compute the appropriate change of basis matrix, and using it find the coordinates $[v]_E$ of the vector $v \in V$ in basis E, if we know that its coordinates in basis G are $[v]_G = [0,1,1]$.
Solution: Bring the block matrix $[E \,|\, G] = \begin{bmatrix} 0&1&0&0&2&1 \\ 1&0&0&0&1&1 \\ 0&1&1&1&2&0 \end{bmatrix}$ to the reduced row-echelon form. $[E \,|\, G] \sim \begin{bmatrix} 1&0&0&0&1&1 \\ 0&1&0&0&2&1 \\ 0&1&1&1&2&0 \end{bmatrix} \sim \begin{bmatrix} 1&0&0&0&1&1 \\ 0&1&0&0&2&1 \\ 0&0&1&1&0&-1 \end{bmatrix} = [I \,|\, P_{EG}]$. So $P_{EG} = \begin{bmatrix} 0&1&1 \\ 0&2&1 \\ 1&0&-1 \end{bmatrix}$, and we have $[v]_E = P_{EG} \cdot [v]_G = \begin{bmatrix} 0&1&1 \\ 0&2&1 \\ 1&0&-1 \end{bmatrix} \begin{bmatrix} 0\\1\\1 \end{bmatrix} = \begin{bmatrix} 2\\3\\-1 \end{bmatrix}$.

Quiz Q63. In $\mathbb{R}^3$ we are given the standard basis E and the basis $G = \{g_1, g_2, g_3\}$, where $g_1 = [1,0,0]$, $g_2 = [2,0,1]$, $g_3 = [1,1,0]$. Find the change of basis matrices P_{EG} and P_{GE}. Can $P_{EG} \cdot P_{GE}$ be presented as a product of *elementary* matrices?
Solution: Since E is standard, $P_{EG} = \begin{bmatrix} 1&2&1 \\ 0&0&1 \\ 0&1&0 \end{bmatrix}$. Compute P_{GE} by $[G \,|\, E] = [G \,|\, I_3] = \begin{bmatrix} 1&2&1&1&0&0 \\ 0&0&1&0&1&0 \\ 0&1&0&0&0&1 \end{bmatrix} \sim \begin{bmatrix} 1&2&1&1&0&0 \\ 0&1&0&0&0&1 \\ 0&0&1&0&1&0 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&1&-1&0 \\ 0&1&0&0&0&1 \\ 0&0&1&0&1&0 \end{bmatrix} \sim \begin{bmatrix} 1&0&0&1&-1&-2 \\ 0&1&0&0&0&1 \\ 0&0&1&0&1&0 \end{bmatrix} = [I_3 \,|\, P_{GE}]$, that is, $P_{GE} = \begin{bmatrix} 1&-1&-2 \\ 0&0&1 \\ 0&1&0 \end{bmatrix}$. Since $P_{EG} \cdot P_{GE} = I$, it is an identity (and invertible) matrix, which clearily is an elementary matrix.

Quiz Q64. In the space $\mathbb{R}^2$ we are given two bases $E = \{\begin{bmatrix} 2\\0 \end{bmatrix}, \begin{bmatrix} 4\\1 \end{bmatrix}\}$ and $G = \{\begin{bmatrix} 0\\3 \end{bmatrix}, \begin{bmatrix} 2\\1 \end{bmatrix}\}$. Find the coordinates $[v]_E$ of the vector $v \in \mathbb{R}^2$ in basis E, if we know its coordinates $[v]_G = [1,5]$ in basis G.
Solution: Bring the matrix $[E \,|\, G] = \begin{bmatrix} 2&4&0&2 \\ 0&1&3&1 \end{bmatrix}$ to the reduced row-echelon form. $[E \,|\, G] \sim \begin{bmatrix} 1&2&0&1 \\ 0&1&3&1 \end{bmatrix} \sim \begin{bmatrix} 1&0&-6&-1 \\ 0&1&3&1 \end{bmatrix} = [I \,|\, P_{EG}]$. So $P_{EG} = \begin{bmatrix} -6&-1 \\ 3&1 \end{bmatrix}$, and therefore $[v]_E = P_{EG} \cdot [v]_G = \begin{bmatrix} -6&-1 \\ 3&1 \end{bmatrix} \begin{bmatrix} 1\\5 \end{bmatrix} = \begin{bmatrix} -11\\8 \end{bmatrix}$.

Quiz Q65. In $\mathbb{R}^3$ we are given the standard basis E and the basis $G = \{g_1, g_2, g_3\}$, where $g_1 = (1,1,0)$, $g_2 = (1,2,0)$, $g_3 = (0,1,1)$. Find the change of basis matrices P_{EG} and P_{GE}. Which is the product $P_{EG} \cdot P_{GE}$?
Solution: Since E is standard, $P_{EG} = \left[\begin{smallmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right]$. Compute P_{GE} by $[G \,|\, E] = [G \,|\, I_3] = \left[\begin{smallmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 0 & 0 & 2 & -1 & 1 \\ 0 & 1 & 0 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{smallmatrix}\right] = [I_3 \,|\, P_{GE}]$, that is, $P_{GE} = \left[\begin{smallmatrix} 2 & -1 & 1 \\ -1 & 1 & -1 \\ 0 & 0 & 1 \end{smallmatrix}\right]$. And $P_{EG} \cdot P_{GE} = I$ since $P_{EG}^{-1} = P_{GE}$.

Quizzes on matrix computation methods in spaces

Quiz Q66. In $\mathbb{R}^3$ we are given the set of vectors $\{v_1, v_2, v_3, v_4\}$, where $v_1 = (1,-2,0)$, $v_2 = (-1,1,1)$, $v_3 = (0,-2,2)$, $v_4 = (0,-1,1)$. Find a basis for the span of this set, indicate its dimension. Detect if the subset $\{v_1, v_2, v_4\}$ is linearly independent or not.
Solution: We have $\left[\begin{smallmatrix} 1 & -1 & 0 & 0 \\ -2 & 1 & -2 & -1 \\ 0 & 1 & 2 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & -1 \\ 0 & 1 & 2 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & -2 & -1 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. Since the pivots are in the first two columns, a basis for $\operatorname{span}(v_1, v_2, v_3, v_4)$ is $\{v_1, v_2\}$. Dimension is 2. $\{v_1, v_2, v_4\}$ is linearly dependent since v_4 is the combination of $\{v_1, v_2\}$.

Quiz Q67. Select a *maximal* linearly independent subsystem of vectors: $v_1 = [1,-1,0]$, $v_2 = [-2,2,0]$, $v_3 = [0,2,1]$, $v_4 = [2,2,2]$. Is the span of these four vectors equal to $\mathbb{R}^3$?
Solution: Compose $A = \left[\begin{smallmatrix} 1 & -2 & 0 & 2 \\ -1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 \end{smallmatrix}\right]$. Bring A to row-echelon form $A \sim \left[\begin{smallmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. Since the pivots are in 1'st and 3'rd columns, a maximal linearly independent subsystem is v_1, v_3. Since the span is 2-dimensional it is *not* equal to $\mathbb{R}^3$?

Quiz Q68. In the space $V = \mathcal{P}_2$ we are given five polynomials $f_1(x) = 1 + x^2$, $f_2(x) = 2 + x + 2x^2$, $f_3(x) = 1 + 3x + x^2$, $f_4(x) = 2 + 5x + 2x^2$, $f_5(x) = 3 + 5x^2$. Find a maximal linearly independent subset S of the set of these polynomials. Detect if the subset S is a basis for V.
Solution: In V fix a basis $E = \{1,\ x,\ x^2\}$ and defining a coordinate system $\phi_E : V \to \mathbb{R}^3$ find the coordinates of our polynomials. Putting them by columns we get the matrix $A = [f_1\ f_2\ f_3\ f_4\ f_5] = \left[\begin{smallmatrix} 1 & 2 & 1 & 2 & 3 \\ 0 & 1 & 3 & 5 & 0 \\ 1 & 2 & 1 & 2 & 5 \end{smallmatrix}\right]$ with row-echelon form $A \sim \left[\begin{smallmatrix} 1 & 2 & 1 & 2 & 3 \\ 0 & 1 & 3 & 5 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{smallmatrix}\right]$. Pivots are in 1'st, 2'nd, 5'th columns. A maximal linearly independent subsystem is $S = \{f_1(x),\ f_2(x),\ f_5(x)\}$. Since the space V also is 3-dimensional, S is a basis for V.

Quiz Q69. Detect if the following system of matrix vectors of $M_{2,2}(\mathbb{R})$ is linearly dependent: $M_1 = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 1 \end{smallmatrix}\right]$, $M_2 = \left[\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right]$, $M_3 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 4 \end{smallmatrix}\right]$, $M_4 = \left[\begin{smallmatrix} 1 & 4 \\ 5 & 2 \end{smallmatrix}\right]$. Is their span U equal to $M_{2,2}(\mathbb{R})$?
Solution: By coordinate map $M_{2,2}(\mathbb{R}) \to \mathbb{R}^4$ present matrices as vectors, and compose a new matrix $A = \left[\begin{smallmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 4 \\ 1 & 4 & 5 & 2 \end{smallmatrix}\right]$ putting them by rows. Then $A \sim \left[\begin{smallmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 2 & 2 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right]$. The system is dependent, and $U \neq M_{2,2}(\mathbb{R})$.

Quiz Q70. Select a maximally independent subset of the following set of polynomial vectors: $f_1(x) = 4$, $f_2(x) = 3 + x + x^3$, $f_3(x) = 1 + x + x^3$, $f_4(x) = 1 + x^2 + 3x^3$.

Solution: By the map $\mathcal{P}_3 \to \mathbb{R}^4$ compose $A = \begin{bmatrix} 4&3&1&1\\ 0&1&1&0\\ 0&0&0&1\\ 0&1&1&3 \end{bmatrix}$. Bring A to row-echelon form $A \sim \begin{bmatrix} 4&3&1&1\\ 0&1&1&0\\ 0&0&0&1\\ 0&0&0&3 \end{bmatrix} \sim \begin{bmatrix} \mathbf{4}&3&1&1\\ 0&\mathbf{1}&1&0\\ 0&0&0&\mathbf{1}\\ 0&0&0&0 \end{bmatrix}$. Since the pivots are in 1'st, 2'nd and 4'th columns, a maximal lin. independent subsystem is $f_1(x)$, $f_2(x)$, $f_4(x)$.

Quiz Q71. Find the span $U = \operatorname{span}(v_1, v_2, v_3, v_4)$ of vectors $v_1 = (1,2,1,2)$, $v_2 = (2,4,5,4)$, $v_3 = (1,2,1,3)$, $v_4 = (0,0,0,2)$, i.e., compute its basis. Which is the dimension of U?

Solution: Using the coordinates of vectors as columns compose the matrix $A = \begin{bmatrix} 1&2&1&2\\ 2&4&5&4\\ 1&2&1&3\\ 0&0&0&2 \end{bmatrix}$. Bring it ro row-echelon form $A \sim \begin{bmatrix} 1&2&1&2\\ 0&0&3&0\\ 1&2&1&3\\ 0&0&0&2 \end{bmatrix} \sim \begin{bmatrix} 1&2&1&2\\ 0&0&3&0\\ 0&0&0&1\\ 0&0&0&2 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1}&2&1&2\\ 0&0&\mathbf{3}&0\\ 0&0&0&\mathbf{1}\\ 0&0&0&0 \end{bmatrix} = R$. So $\dim(U) = 3$, and as a basis for U take the first three rows of R.

Quiz Q72. Find $W = \operatorname{span}(v_1, v_2, v_3, v_4)$ of vectors $v_1 = (1,0,-1,0)$, $v_2 = (0,1,0,2)$, $v_3 = (1,1,0,0)$, $v_4 = (2,2,-1,2)$, i.e., compute its basis. Is W equal to $\mathbb{R}^4$? Find a 2-dimensional subspace in W which contains v_1.

Solution: Putting coordinates of vectors as columns we have $A = \begin{bmatrix} 1&0&1&2\\ 0&1&1&2\\ -1&0&0&-1\\ 0&2&0&2 \end{bmatrix}$. Bring it to row-echelon form $A \sim \begin{bmatrix} 1&0&1&2\\ 0&1&1&2\\ 0&0&1&1\\ 0&2&0&2 \end{bmatrix} \sim \begin{bmatrix} 1&0&1&2\\ 0&1&1&2\\ 0&0&1&1\\ 0&0&-2&-2 \end{bmatrix} \sim \begin{bmatrix} 1&0&1&2\\ 0&1&1&2\\ 0&0&1&1\\ 0&0&0&0 \end{bmatrix}$. So $\dim(W) = 3$, and W is not equal to $\mathbb{R}^4$. As a basis for W take the first three vectors v_1, v_2, v_3. As a 2-dimensional subspace in W take $\operatorname{span}(v_1, v_2)$.

Quizzes on null spaces and on general solutions of $AX = B$ by null space

Quiz Q73. Find the nullity and a basis for the null space of $A = \begin{bmatrix} 2&4&0&4\\ 0&0&1&3\\ 1&2&1&5 \end{bmatrix}$. Using nullity($A$) tell what is rank($A$). Find a vector $B \in \mathbb{R}^3$ for which the system $AX = B$ is consistent.

Solution: First find the rref(A) as $\begin{bmatrix} 2&4&0&4\\ 0&0&1&3\\ 1&2&1&5 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 1&2&1&5 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 0&0&1&3 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 0&0&0&0 \end{bmatrix}$. So nullity($A$) $= 2$, and null(A) has a basis $e_1 = \begin{bmatrix} 2\\ -1\\ 0\\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 2\\ 0\\ 3\\ -1 \end{bmatrix}$. We have rank($A$) $= 4 -$ nullity(A) $= 4 - 2 = 2$. As B take any vector linearly dependent on the 1'st and 3'rd columns of A. Say, take $B = (2,1,2)$.

Quiz Q74. Find a basis for the null space of the matrix $A = \begin{bmatrix} 2&4&0&6&0\\ 0&0&1&4&0\\ 1&2&1&7&1 \end{bmatrix}$. Deduce from nullity($A$) what is the rank of A. Find which is the dimension of the space of solutions of the homogeneous system of linear equations $AX = O$?

Solution: First find the rref(A) as $A \sim \begin{bmatrix} 2&4&0&6&0\\ 0&0&1&4&0\\ 1&2&1&7&1 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&3&0\\ 0&0&1&4&0\\ 0&0&0&0&1 \end{bmatrix}$. So nullity($A$) $= 2$, and null(A) has a basis $e_1 = (2, \mathbf{-1}, 0, \mathbf{0}, 0)$, $e_2 = (3, \mathbf{0}, 4, \mathbf{-1}, 0)$. Then rank($A$) $= 5 -$ nullity(A) $= 5 - 2 = 3$. The solutions $AX = O$ have dimension 2.

Quiz Q75. Find the null space and nullity of $A = \begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 1&2&1&5 \end{bmatrix}$. Using nullity($A$) tell what is rank($A$).

Solution: Compute the rref(A) by $\begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 1&2&1&5 \end{bmatrix} \sim \begin{bmatrix} 1&2&0&2\\ 0&0&1&3\\ 0&0&1&3 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1}&2&0&2\\ 0&0&\mathbf{1}&3\\ 0&0&0&0 \end{bmatrix}$. Null space null($A$) has a basis $e_1 = \begin{bmatrix} 2\\ -1\\ 0\\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 2\\ 0\\ 3\\ -1 \end{bmatrix}$. We have nullity($A$) $= 2$. Since rank(A) + nullity(A) $= 4$, we have rank(A) $= 4 - 2 = 2$.

Quiz Q76. The rref of the augmented matrix of the system $AX = B$ is $\text{rref}(\bar{A}) = \begin{bmatrix} \mathbf{1} & 5 & 0 & 9 & 8 \\ 0 & 0 & \mathbf{1} & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Write the general solution of $AX = B$ in form $\alpha_1 e_1 + \cdots + \alpha_{n-r} e_{n-r} + v_0$, where $e_1, \ldots, e_{n-r}$ is the basis of null(A).
Solution: There are two non-pivot columns in A: the 2'nd and 4'th. So $\dim(\text{null}(A)) = 2$. As a basis $\{e_1, e_2\}$ of null(A), and as a single solution v_0 of $AX = B$ take: $e_1 = \begin{bmatrix} 5 \\ -1 \\ 0 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 9 \\ 0 \\ 6 \\ -1 \end{bmatrix}$, $v_0 = \begin{bmatrix} 8 \\ 0 \\ 7 \\ 0 \end{bmatrix}$.

Quiz Q77. Find the general solution of the system of linear equations $AX = B$ in the form $\text{null}(A) + v_0 = \alpha_1 e_1 + \cdots + \alpha_{n-r} e_{n-r} + v_0$, if we know that the reduced row-echelon form of the augmented matrix $\bar{A}$ is $\begin{bmatrix} \mathbf{1} & 3 & 0 & -2 & 1 \\ 0 & 0 & \mathbf{1} & -5 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. What is nullity$(A)$ of the coefficient matrix A? What is rank$(\bar{A})$ of the augmented matrix $\bar{A}$?
Solution: There are two non-pivot columns in A: the 2'nd and 4'th. So nullity$(A) = 2$. We have rank$(\bar{A}) = 2$. As a basis $\{e_1, e_2\}$ of null(A), and as a single solution v_0 of $AX = B$ take: $e_1 = \begin{bmatrix} 3 \\ -1 \\ 0 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 2 \\ 0 \\ 5 \\ -1 \end{bmatrix}$, $v_0 = \begin{bmatrix} 1 \\ 0 \\ 2 \\ 0 \end{bmatrix}$.

Quiz Q78. We are given the system $\begin{cases} 2x_1 + 4x_2 + 6x_4 = 2 \\ x_3 + 2x_4 = 3 \\ x_1 + 2x_2 + x_3 + 5x_4 = 4 \end{cases}$. Detect if it is consistent. If yes, find a basis for the null space of the coefficient matrix A, and present the general solution of the system in the form null$(A) + v_0$.
Solution: $\bar{A} = \begin{bmatrix} 2 & 4 & 0 & 6 & 2 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 1 & 5 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 1 & 5 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Since rank$(A)$ = rank$(\bar{A})$, the system is consistent. The last matrix is in rref form. As basis for take $e_1 = (2, \mathbf{-1}, 0, \mathbf{0})$, $e_2 = (3, \mathbf{0}, 2, \mathbf{-1})$. A solution of $AX = B$ is $v_0 = (1, \mathbf{0}, 3, \mathbf{0})$. The general solution is null$(A) + v_0 = \text{span}(e_1, e_2) + v_0$.

Quizzes on subspace calculus

Quiz Q79. In $V = \mathbb{R}^3$ we are given two subspaces U and W. For U we have its basis $\{u_1, u_2\}$ where $u_1 = (2, 0, 1)$, $u_2 = (0, 2, 0)$. And W is the plane passing by O, with two direction vectors $w_1 = (-4, -6, -2)$, $w_2 = (0, 0, 1)$. Find a basis for the intersection $U \cap W$ by any method. Deduce weather $U + W$ is equal to V.
Solution: $[A \,|\, -B] = \begin{bmatrix} 2 & 0 & 4 & 0 \\ 0 & 2 & 6 & 0 \\ 1 & 0 & 2 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. The null space of $[A \,|\, -B]$ is 1-dimensional, and its basis vector is, say, $(2, 3, \mathbf{-1}, 0)$. So as a basis for 1-dimensional intersection $U \cap W$ we take $2u_1 + 3u_2 = (4, 6, 2)$, or $(2, 3, 1)$. Since $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W) = 2 + 2 - 1 = 3$, we have $U + W = V$.

Quiz Q80. U and W are subspaces in $\mathbb{R}^4$. We have $U = \text{span}(u_1, u_2)$, where $u_1 = (2, 0, 0, 2)$, $u_2 = (1, 1, 1, 1)$, and we know W has a basis consisting of vectors $w_1 = (0, 3, 3, 0)$, $w_2 = (2, 4, 8, 2)$. Find out if $\{u_1, u_2\}$ is a basis for U. Compute a basis for the sum $U + W$. From this deduce the dimension of $\dim(U \cap W)$ without any new matrix operations.
Solution: u_1, u_2 are independent (not collinear), and $\{u_1, u_2\}$ is a basis. $[u_1\ u_2\ w_1\ w_2] = \begin{bmatrix} 2 & 1 & 0 & 2 \\ 0 & 1 & 3 & 4 \\ 0 & 1 & 3 & 8 \\ 2 & 1 & 0 & 2 \end{bmatrix} \sim \begin{bmatrix} 2 & 1 & 0 & 2 \\ 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Thus, $U + W$ has a basis $\{u_1,\ u_2,\ w_2\}$. Since $\dim(U + W) = 3$, $\dim(U \cap W) = \dim(U) + \dim(W) - \dim(U + W) = 2 + 2 - 3 = 1$.

Quiz Q81. Vectors $u_1 = (1,0,1)$, $u_2 = (1,2,3)$, $u_3 = (3,2,5)$, $u_4 = (0,1,2)$, $u_5 = (2,0,2)$ are given in $\mathbb{R}^3$. Find a maximal independent subset of the set $S = \{u_1, u_2, u_3, u_4, u_5\}$. Find the dimension of span(S). Indicate the dimension of the sum $U+W$, where $U = \text{span}(u_1, u_2)$ and $W = \text{span}(u_3, u_4, u_5)$. Does U contain W?
Solution: We have $A = \left[\begin{smallmatrix} 1&1&3&0&2\\ 0&2&2&1&0\\ 1&3&5&2&2 \end{smallmatrix}\right]$. Bringing to row-echelon form $A \sim \left[\begin{smallmatrix} 1&1&3&0&2\\ 0&2&2&1&0\\ 0&2&2&2&0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&3&0&2\\ 0&2&2&1&0\\ 0&0&0&1&0 \end{smallmatrix}\right]$ we get the maximal linearly independent vectors $S = \{u_1, u_2, u_4\}$. Also, $\dim(U+W) = 3$. The subspace U does not contain W.

Quizzes on linear transformations

Quiz Q82. Let T be a transformation of the space $\mathbb{R}^3$ given by the rules $T(e_1) = (1,0,2)$, $T(e_2) = (-1,1,-1)$, $T(e_3) = e_2 + e_3$, where $E = \{e_1, e_2, e_3\}$ is the standard basis in $\mathbb{R}^3$. Find the nullity of T, and compute the kernel of T by finding a basis for it. Find dim(range (T)) using the above computed results.
Solution: We have $A = [T] = [T(e_1)\ T(e_2)\ T(e_3)] = \left[\begin{smallmatrix} 1&-1&0\\ 0&1&1\\ 2&-1&1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&0&1\\ 0&1&1\\ 0&0&0 \end{smallmatrix}\right] = \text{rref}(A)$. So $\text{rank}(A) = 2$. Therefore, $\text{nullity}(T) = 3-2 = 1$. And a basis vector for $\ker(T) = \text{null}(A)$ is $e = \left[\begin{smallmatrix} 1\\ 1\\ -1 \end{smallmatrix}\right]$. We have $\dim(\text{range}(T)) = 3 - \text{nullity}(T) = 2$.

Quiz Q83. In polynomial space $\mathcal{P}_2$ with the basis $E = \{1, x, x^2\}$ a transformation T is given by the rule $T(f(x)) = f'(x) + f''(x)$. Find a basis for $\ker(T)$ using the null space of $A = [T]_E$. Deduce from here the dimension of range(T).
Solution: We have $[T(1)]_E = [0]_E = (0,0,0)$, $[T(x)]_E = [1]_E = (1,0,0)$, $[T(x^2)]_E = [2x+2]_E = (2,2,0)$. So $A = [T]_E = \left[\begin{smallmatrix} 0&1&2\\ 0&0&2\\ 0&0&0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 0&1&0\\ 0&0&1\\ 0&0&0 \end{smallmatrix}\right]$. Then null($A$) has a single basis vector $(-1,0,0)$ or $(1,0,0)$. I.e., $\ker(T)$ consists of all constant polynomials. Next, $\dim\big(\text{range}(T)\big) = \text{rank}(T) = 3-1 = 2$.

Quiz Q84. The transformation $T : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ is defined as $T(x,y,z) = (4x+2y+z,\ x+y+2z)$. Compute rank($T$), and find a basis for the range of T. Tell what is the nullity of T using rank(T).
Solution: $A = [T] = \left[\begin{smallmatrix} 4&2&1\\ 1&1&2 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 4&2&1\\ 0&3&3 \end{smallmatrix}\right]$. Then $\text{rank}(A) = \text{rank}(T) = 2$. As basis for range($T$) we can take $\{\left[\begin{smallmatrix} 4\\ 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2\\ 1 \end{smallmatrix}\right]\}$. Or, since $\mathbb{Z}_5^2$ is 2-dimensional, we have $\text{range}(T) = \mathbb{Z}_5^2$, and we could also take *any* basis of $\mathbb{Z}_5^2$. Also $\text{nullity}(A) = \text{nullity}(T) = 3-2 = 1$.

Quiz Q85. The transformation T of the space $\mathbb{R}^3$ is given as $T(x,y,z) = (x+y,\ x+z,\ 2x+y+z)$. Find the nullity of T, compute the kernel of T by finding a basis for it.
Solution: We have $A = [T] = \left[\begin{smallmatrix} 1&1&0\\ 1&0&1\\ 2&1&1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&0\\ 0&-1&1\\ 2&1&1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&0\\ 0&-1&1\\ 0&-1&1 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&0\\ 0&1&-1\\ 0&0&0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&0&1\\ 0&1&-1\\ 0&0&0 \end{smallmatrix}\right] = \text{rref}(A)$. Therefore $\text{nullity}(T) = 3-2 = 1$. As a basis for $\ker(T) = \text{null}(A)$ we can take $e = \left[\begin{smallmatrix} 1\\ -1\\ -1 \end{smallmatrix}\right]$ or $e = \left[\begin{smallmatrix} -1\\ 1\\ 1 \end{smallmatrix}\right]$.

Quiz Q86. A transformation T is defined on $\mathbb{R}^3$ by $T(x,y,z) = (x+y+2z,\ 2x+y+4z,\ 2y)$. Find the rank of T, compute the range of T by calculating a basis for it.
Solution: $A = [T] = \left[\begin{smallmatrix} 1&1&2\\ 2&1&4\\ 0&2&0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&2\\ 0&-1&0\\ 0&2&0 \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} 1&1&2\\ 0&-1&0\\ 0&0&0 \end{smallmatrix}\right]$. The last matrix is in ref form with pivots in 1'st and 2'nd columns. Thus, as a basis for $\text{range}(T) = \text{col}(A)$ we can take $e_1 = \left[\begin{smallmatrix} 1\\ 2\\ 0 \end{smallmatrix}\right]$, $e_2 = \left[\begin{smallmatrix} 1\\ 1\\ 2 \end{smallmatrix}\right]$. And $\text{rank}(T) = \text{rank}(A) = 2$.

Quiz Q87. Two transformations T and S are defined on the space $\mathbb{R}^3$ by their matrices $A=[T]=\begin{bmatrix}1&0&2\\0&3&1\\0&0&1\end{bmatrix}$ and $B=[S]=\begin{bmatrix}2&1&0\\0&2&1\\0&0&1\end{bmatrix}$. Find the matrix of composition ST. Determine if T, S or ST are invertible. Explain your answers.
Solution: The matrix of ST is $C=B\cdot A=[ST]=\begin{bmatrix}2&3&5\\0&6&3\\0&0&1\end{bmatrix}$. Each of the matrices A,B,C has a non-zero determinant (this is evident using triangle rule). So any of transformations T, S and ST are invertible.

Quiz Q88. T is given on $\mathbb{R}^3$ by $A=[T]=\begin{bmatrix}1&2&0\\1&3&0\\0&0&2\end{bmatrix}$, and S is given by rules $S(e_1)=(1,3,0)$, $S(e_2)=(1,2,0)$, $S(e_3)=3e_3$ ($E=\{e_1,e_2,e_3\}$ is the standard basis). Find the matrices of $T+S$ and ST. Is the transformation $(3\cdot ST)^{100}$ invertible?
Solution: $B=[S]=\begin{bmatrix}1&1&0\\3&2&0\\0&0&3\end{bmatrix}$. The matrix of $T+S$ is $A+B=\begin{bmatrix}2&3&0\\4&5&0\\0&0&5\end{bmatrix}$. The matrix of ST is $BA=\begin{bmatrix}2&5&0\\5&12&0\\0&0&6\end{bmatrix}$. The determinants of A and B are non-zero (Laplace expansion by 3'rd column). So the determinant of $(3\cdot BA)^{100}$ also is non-zero.

Quiz Q89. In the real polynomial space $\mathcal{P}_2$ we are given two transformations defined by $T(f(x))=f'(x)$ and $S(f(x))=2f(x)$. Find the matrix of transformation $T+S$ in the basis $E=\{1,\ x,\ x^2\}$.
Solution: Since $T(1)=0$, $T(x)=1$, $T(x^2)=2x$, the matrix of T is $[T]_E=\begin{bmatrix}0&1&0\\0&0&2\\0&0&0\end{bmatrix}$. Next, since $S(1)=2$, $S(x)=2x$, $S(x^2)=2x^2$, the matrix of S is $[S]_E=\begin{bmatrix}2&0&0\\0&2&0\\0&0&2\end{bmatrix}$. Thus, $[T+S]_E=[T]_E+[S]_E=\begin{bmatrix}2&1&0\\0&2&2\\0&0&2\end{bmatrix}$.

Quizzes on eigenvalues eigenspaces

Quiz Q90. T is a transformation of $\mathbb{R}^3$ given by the rules $T\begin{bmatrix}2\\0\\0\end{bmatrix}=\begin{bmatrix}4\\6\\0\end{bmatrix}$, $T\begin{bmatrix}0\\1\\0\end{bmatrix}=\begin{bmatrix}3\\2\\0\end{bmatrix}$, $T\begin{bmatrix}0\\0\\3\end{bmatrix}=\begin{bmatrix}0\\0\\15\end{bmatrix}$. Detect if $\lambda=5$ is an eigenvalue for T. If yes, find a basis for the eigenspace E_5.
Solution: We have $A=[T]=\begin{bmatrix}2&3&0\\3&2&0\\0&0&5\end{bmatrix}$. So $\lambda=5$ is an eigenvalue, as $T(e_3)=5e_3$. Then $A-5I=\begin{bmatrix}-3&3&0\\3&-3&0\\0&0&0\end{bmatrix}\sim\begin{bmatrix}1&-1&0\\0&0&0\\0&0&0\end{bmatrix}$. So $\dim(E_5)=\text{nullity}(A-5I)=3-1=2$. As basis for E_5 take $\left\{\begin{bmatrix}-1\\-1\\0\end{bmatrix},\begin{bmatrix}0\\0\\-1\end{bmatrix}\right\}$ or, a little prettier, $\left\{\begin{bmatrix}1\\1\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\end{bmatrix}\right\}$.

Quiz Q91. The transformation T of $\mathbb{R}^3$ is given by its matrix $A=\begin{bmatrix}3&1&0\\1&3&0\\0&0&4\end{bmatrix}$. We already know that $\lambda=4$ is an eigenvalue of T. Detect its geometric multiplicity and find a basis for the eigenspace E_4.
Solution: We have $A-4I=\begin{bmatrix}-1&1&0\\1&-1&0\\0&0&0\end{bmatrix}\sim\begin{bmatrix}1&-1&0\\0&0&0\\0&0&0\end{bmatrix}=\text{rref}(A-4I)$. So $\dim(E_4)=\text{nullity}(A-4I)=3-1=2$. As basis for E_4 take the basis $e_1=\begin{bmatrix}-1\\-1\\0\end{bmatrix}$, $e_2=\begin{bmatrix}0\\0\\-1\end{bmatrix}$ or the basis $g_1=\begin{bmatrix}1\\1\\0\end{bmatrix}$, $g_2=\begin{bmatrix}0\\0\\1\end{bmatrix}$.

Quiz Q92. A transformation $T:\mathbb{R}^3\to\mathbb{R}^3$ is given by is matrix $A=[T]=\begin{bmatrix}3&1&0\\1&3&0\\0&0&2\end{bmatrix}$. Write the characteristic polynomial $f(\lambda)$ of T, find its roots, and for each root indicate its (algebraic) multiplicity.

Solution: We have $f(\lambda) = \det\begin{bmatrix} 3-\lambda & 1 & 0 \\ 1 & 3-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{bmatrix} = (2-\lambda)\cdot(-1)^{3+3}\cdot\det\begin{bmatrix} 3-\lambda & 1 \\ 1 & 3-\lambda \end{bmatrix} = (2-\lambda)((3-\lambda)^2-1) = (2-\lambda)(\lambda^2-6\lambda+8)$. $d = (-6)^2-4\cdot 8 = 4$. The roots of $\lambda^2-6\lambda+8$ are $\frac{6+2}{2} = 4$ and $\frac{6-2}{2} = 2$. Therefore $f(\lambda) = -(\lambda-2)^2(\lambda-4)$.

Quiz Q93. The transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ is given by the rules: $T\begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 8 \\ 6 \\ 0 \end{bmatrix}$, $T\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -3 \\ -2 \\ 0 \end{bmatrix}$, $T\begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \\ -2 \end{bmatrix}$. Find the eigenvalues of T using the characteristic polynomial $f(\lambda)$. Indicate the *algebraic* multiplicity of each eigenvalue.
Solution: $[T] = \begin{bmatrix} 4 & -3 & 1 \\ 3 & -2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$. By Laplace expansion: $f(\lambda) = \begin{vmatrix} 4-\lambda & -3 & 1 \\ 3 & -2-\lambda & 1 \\ 0 & 0 & 2-\lambda \end{vmatrix} = (2-\lambda)\,(-1)^{3+3} \cdot \begin{vmatrix} 4-\lambda & -3 \\ 3 & -2-\lambda \end{vmatrix} = (2-\lambda)\big((4-\lambda)(-2-\lambda)+9\big) = (2-\lambda)(\lambda^2-2\lambda+1) = (2-\lambda)(\lambda-1)^2$. The algebraic multiplicity of 2 is 1, and alg. multiplicity of 1 is 2.

Quiz Q94. A transformation T is given by its matrix $A = \begin{bmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$. We are given that $\lambda = 5$ is an eigenvalue of T. Detect its geometric multiplicity and find a basis for the eigenspace E_5.
Solution: We have $A-5I = \begin{bmatrix} 3-5 & 2 & 0 \\ 2 & 3-5 & 0 \\ 0 & 0 & 5-5 \end{bmatrix} = \begin{bmatrix} -2 & 2 & 0 \\ 2 & -2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} -2 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A-5I)$. Thus, $\dim(E_5) = \text{nullity}(A-5I) = 3-1 = 2$. As basis for E_5 take $e_1 = \begin{bmatrix} -1 \\ -1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$ or, equivalently, $e_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

Quiz Q95. $T : \mathbb{R}^3 \to \mathbb{R}^3$ is defined by its matrix $A = [T] = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$. We know that one of its eigenvalues is $\lambda = 3$. Compute eigenspace E_3 by finding a basis for it. Which is the geometric multiplicity of 3?
Solution: $A-\lambda I = A-3I = \begin{bmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Then $A-3I \sim \begin{bmatrix} -1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} \mathbf{1} & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \text{rref}(A-3I)$. The geom. multiplicity of 3 is $3-1 = 2$. As a basis for E_3 we can take $e_1 = \begin{bmatrix} -1 \\ -1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$ or, equivalently, $e_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

Quiz Q96. The transformation $T : \mathbb{R}^3 \to \mathbb{R}^3$ is given as $T(x, y, z) = (3x+2y,\ 2x+3y,\ 5z)$. Write the characteristic polynomial $f(\lambda)$ of T. Find all the eigenvalues of T, and for each eigenvalue indicate its algebraic multiplicity.
Solution: $A = [T] = \begin{bmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$. We have $f(\lambda) = \begin{vmatrix} 3-\lambda & 2 & 0 \\ 2 & 3-\lambda & 0 \\ 0 & 0 & 5-\lambda \end{vmatrix} = (5-\lambda)\cdot(-1)^{3+3}\cdot \begin{vmatrix} 3-\lambda & 2 \\ 2 & 3-\lambda \end{vmatrix} = (5-\lambda)((3-\lambda)^2-4) = (5-\lambda)(\lambda^2-6\lambda+5)$. The roots of $\lambda^2-6\lambda+5$ are $\frac{6+4}{4} = 5$ and $\frac{6-4}{2} = 1$. So $f(\lambda) = -(\lambda-5)^2(\lambda-1)$. Alg. multiplicities are 2 and 1.

Quizzes on similar matrices and diagonalization

Quiz Q97. Using any method detect if any of these matrices are similar: $A = \begin{bmatrix} 1 & 1 & 3 \\ 1 & 1 & 4 \\ 1 & 1 & 5 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 6 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 3 \end{bmatrix}$.
Solution: $\det(A)$ is zero (it has equal columns), so it is not similar to B or C, determinants of which are non-zero by triangle rule. Also B and C are not similar because A has eigenvalues $1, 6$, whereas B has eigenvalues $1, 2, 3$.

Quiz Q98. We are given two matrices $A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & 4 \end{bmatrix}$. The third matrix C is unknown, but we are given that $\text{rank}(C) = 3$, and $Cv = 5v$ for some non-zero vector v. Detect which ones of the matrices A, B, C may be similar.

Solution: We have $\det(A) = 0$, $\det(B) = 2 \cdot 3 \cdot 4 = 24 \neq 0$. Also $\det(C) \neq 0$ because $\operatorname{rank}(C) = 3$. So A is *not* similar to B or to C. Next, B and C are not similar because the eigenvalues of B are $\lambda = 2, 3, 4$ only, whereas C has the eigenvalue $\lambda = 5$.

Quiz Q99. In standard basis E of $\mathbb{R}^2$ the transformation T has the matrix $A = [T]_E = \begin{bmatrix} -1 & 6 \\ -1 & 4 \end{bmatrix}$, and the transformation S has the matrix $C = [S]_E = \begin{bmatrix} 5 & 5 \\ 0 & 5 \end{bmatrix}$. Find the matrix $B = [T]_G$ of T in the basis $G = \left\{ \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix} \right\}$. Then detect which of the matrices A, B, C are *similar* to each other.
Solution: We have the change of basis matrix $P = P_{EG} = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$. Compute its inverse by $\begin{bmatrix} 2 & 3 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 1 & -2 \end{bmatrix}$. Thus, $P^{-1} = \begin{bmatrix} -1 & 3 \\ 1 & -2 \end{bmatrix}$ and $B = P^{-1}AP = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. From here we see that the eigenvalues of T are 2 and 1. The matrices A and B are similar as $B = P^{-1}AP$. But C is *not* similar to them as it has the eigenvalue 5.

Quiz Q100. We have $A = \begin{bmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$, and we know $|A - \lambda I| = -(\lambda - 1)(\lambda - 5)^2$. We also know that E_1 has the basis $\left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix} \right\}$, and E_5 has basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$. Find diagonalization $P^{-1}AP = D$ using algebraic multiplicities (don't calculate P^{-1}).
Solution: 1 and 5 have algebr. multiplicities 1 and 2. Their sum $1 + 2 = 3$ is euqal to $\dim(V)$. According to given bases the geom. multip. of 1 and 5 are equal to their algebr. multiplicities. So diagonalization is possible. $P = \begin{bmatrix} -1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix}$.

Quiz Q101. For the transformation T of $\mathbb{R}^3$ we know that $T(1,1,1) = (2,2,2)$, and that the eigenspace E_3 of T has two linearly independent vectors $v = (2,4,3)$ and $w = (1,0,5)$ Is this information enough to find the diagonalization $P^{-1}AP = D$ for A? If yes, find the matrices D and P.
Solution: From $T(1,1,1) = (2,2,2)$ it follows that $\lambda_1 = 2$ is an eigenvalue for eigenvector $u = (1,1,1)$, and so $\dim(E_2) \geq 1$. Since $\dim(E_3) \geq 2$, we have $\dim(E_2) + \dim(E_3) \geq 3 = \dim(\mathbb{R}^3)$, i.e., diagonalization is possible, and $\dim(E_2) = 1$, $\dim(E_3) = 2$. As P take $[u\ v\ w] = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 4 & 0 \\ 1 & 3 & 5 \end{bmatrix}$, and as the diagonal matrix take $D = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$.

Quiz Q102. For the transformation T of $\mathbb{R}^3$ given by the matrix $A = \begin{bmatrix} 3 & -2 & 1 \\ 4 & -3 & 1 \\ 0 & 0 & -1 \end{bmatrix}$ we already know that its eigenvalues are $\lambda_1 = 1$ and $\lambda_2 = -1$. We also know that E_1 is spanned by a single vector $(1,1,0)$. Find an eigenbasis for E_{-1}, and deduce if A is diagonalizable. If yes, write the diagonalization of A. (Computation of the *inverse* P^{-1} is *not* required!)
Solution: We already know that the geometric multiplicity of $\lambda_1 = 1$ is 1. Next, $A - \lambda_2 I = A + I = \begin{bmatrix} 4 & -2 & 1 \\ 4 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{4} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. As basis for E_{-1} take the vector $\left(-\frac{1}{2}, -1, 0\right)$ or, better, $(1,\ 2,\ 0)$, *and* the vector $\left(\frac{1}{4},\ 0,\ -1\right)$ or, better, $(1,\ 0,\ -4)$. The sum of geometric multiplicities is $1 + 2 = 3 = \dim(\mathbb{R}^3)$, so T is diagonalizable. We have $D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ and $P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 0 & 0 & -4 \end{bmatrix}$.

Quizzes on inner product spaces

Quiz Q103. Find an orthonormal basis for $\mathbb{R}^3$ by Gram–Schmidt process using $v_1 = (1,1,0)$, $v_2 = (0,0,2)$, $v_3 = (0,1,-1)$.

Solution: $h_1 = v_1 = (1,1,0)$. We can take $h_2 = v_2 = (0,0,2)$ because $v_2 \perp v_1$. Next $h_3 = v_3 - \frac{1}{2}h_1 - \frac{-2}{4}h_2 = (-\frac{1}{2},\frac{1}{2},0)$. After normalization we have $e_1 = (\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$, $e_2 = (0,0,1)$, $e_3 = (-\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0)$.

Quiz Q104. In the space $V = \mathbb{R}^3$ we are given the line ℓ which passes by O, and has the direction vector $d = (1,1,1)$. Build an *orthonormal* basis $\{e_1,e_2,e_3\}$ for V such that e_1 belongs to ℓ. *Hint*: you may use the Gram-Schmidt process.
Solution: Take any basis of V with first vector d. The Gram-Schmidt process just scales the first vector. Say $v_1 = d = (1,1,1)$, $v_2 = (0,1,0)$, $v_3 = (0,0,1)$. Then: $e_1 = \frac{1}{\sqrt{3}}(1,1,1)$, $e_2 = \frac{1}{\sqrt{6}}(-1,\sqrt{4},-1)$, $e_3 = \frac{1}{\sqrt{2}}(-1,0,1)$.

Quiz Q105. We are given a real matrix $Q = \begin{bmatrix} 1/2 & 0 & -\sqrt{3}/2 \\ 0 & 1 & 0 \\ \sqrt{3}/2 & 0 & 1/2 \end{bmatrix}$. Find out if Q is orthogonal in two ways. First, compare the columns of Q. Second, use the product matrix Q^TQ. Is the matrix Q^2 also orthogonal?
Solution: If v_1,v_2,v_3 are columns of Q, then $|v_i| = 1$ and $v_i \cdot v_j$ for $i \neq j$. So Q is orthogonal. The same follows from $Q^TQ = I$. Since Q preserves the lengths Q^2 also preserves the lengths, and is orthogonal. Or compute $(QQ)^TQQ = Q^TQ^TQQ = Q^TIQ = I$.

Quiz Q106. A transformation S is given on $V = \mathbb{R}^3$ by $S(x,y,z) = \big(\sqrt{3}x+z,\ -2y,\ -x+\sqrt{3}z\big)$. And the transformation T is defined as $T = \frac{1}{2}\cdot S$. Detect if T is *orthogonal* transformation. Is there a non-zero $v \in V$ for which $T(v) = \sqrt{3}\,v$?
Solution: $A = [T] = \frac{1}{2}[S] = \frac{1}{2}\begin{bmatrix} \sqrt{3} & 0 & 1 \\ 0 & -2 & 0 \\ -1 & 0 & \sqrt{3} \end{bmatrix}$. Then $A^TA = \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} = I_3$, and so T is orthogonal. Therefore all the eigenvalues of T are 1 or -1. Thus, for we may *never* have $T(v) = \sqrt{3}\,v$.

Quiz Q107. T is a transformation given on $\mathbb{R}^3$ by the rule $T(x,y,z) = \Big(2x-4y,\ \ 4(z-x),\ \ 4y-2z\Big)$. By any method detect if T is a *symmetric* transformation. 6 and -6 are eigenvalues of T. Let u be an eigenvector associated to 6, and v be an eigenvector associated to -6. Can you find the dot product $u \cdot v$ *without* actually computing the vectors u,v?
Solution: The matrix $Q = [T] = \begin{bmatrix} 2 & -4 & 0 \\ -4 & 0 & 4 \\ 0 & 4 & -2 \end{bmatrix}$ is symmetric, so T is a symmetric transformation. Thus, the eigenvectors associated to *different* eigenvectors 6 and -6 are orthogonal, i.e., $u \cdot v = 0$.

Quiz Q108. A real transformation S is given by ts matrix $S = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$. Without any calculations deduce that S is *diagonalizable*. We also know that S has eigenvalues $\lambda_1 = 5$, $\lambda_2 = -1$, such that E_5 is spanned by $u = (1,1,1)$, and E_{-1} is spanned by the vectors $v = (-1,1,0)$ and $w = (-1,0,1)$. Find the *orthogonal* diagonalization of S.
Solution: S is even *orthogonally* diagonalizable, as S is *symmetric*. By Gram-Schmidt process an orthonormal basis for E_5 is formed by $e_1 = \frac{1}{\sqrt{3}}u = \frac{1}{\sqrt{3}}(1,1,1)$. Applying Gram-Schmidt to $\{v,w\}$ we get $e_2 = \frac{1}{\sqrt{2}}(-1,1,0)$, $e_3 = \big(-\frac{1}{\sqrt{6}},\frac{1}{\sqrt{6}},\frac{\sqrt{2}}{\sqrt{3}}\big) = \frac{1}{\sqrt{6}}(-1,1,\sqrt{4})$.

So $D = \begin{bmatrix} 5 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$ and $Q = \begin{bmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{\sqrt{2}}{\sqrt{3}} \end{bmatrix} = \frac{1}{\sqrt{6}}\begin{bmatrix} \sqrt{2} & -\sqrt{3} & -1 \\ \sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & 0 & \sqrt{4} \end{bmatrix}$.

Solutions and hints to selected exercises

Part 1. Introduction to Vectors, Spaces and Fields.

E.1.5. No, because $v = au$ is impossible, as $2 \neq a \cdot 0$. If $u = av$, then $0 = a \cdot 2$, i.e., $a = 0$. But then we wound have $3 = 0 \cdot x = 0$. **E.1.9.** **(1)** $\overrightarrow{OA} = u + v + w = (0, 4, \sqrt{8})$. **(2)** The length is $\sqrt{0 + 16 + 8} = \sqrt{24}$. **(3)** $\mathrm{proj}_u(\overrightarrow{OA}) = \frac{u \cdot \overrightarrow{OA}}{u \cdot u} u = \frac{8}{8} u = (2, 2, 0)$ (this also is clear geometrically, as projection of the diagonal of a *cube* on one of the edges is equal to that edge). **(4)** $\mathrm{proj}_{\overrightarrow{OA}}(\overrightarrow{OC}) = \frac{\overrightarrow{OA} \cdot \overrightarrow{OC}}{\overrightarrow{OA} \cdot \overrightarrow{OA}} \overrightarrow{OA} = \frac{1}{6} \overrightarrow{OA} = \left(0, \frac{4}{6}, \frac{\sqrt{8}}{6}\right) = \left(0, \frac{2}{3}, \frac{\sqrt{2}}{3}\right)$. So the distance is $\sqrt{1 + \frac{1}{9} + \frac{2}{9}} = \frac{\sqrt{12}}{3}$. **E.1.10.** $|\mathrm{proj}_u(v)| = \left|\frac{u \cdot v}{u \cdot u} u\right| = \left|\frac{u \cdot v}{u \cdot u}\right| \cdot |u| = \left|\frac{u \cdot v}{u \cdot u}\right| \cdot \sqrt{u \cdot u} = \frac{|u \cdot v|}{\sqrt{u \cdot u}}$. By Cauchy-Schwartz inequality this is less than equal to $\frac{1}{\sqrt{u \cdot u}} \sqrt{(u \cdot u)(v \cdot v)} = \sqrt{v \cdot v} = |v|$. **E.1.11.** **(1)** Yes. For any orthogonal vectors $u \cdot v = 0 < 4$. **(2)** No. By Cauchy-Schwarz inequality $|u \cdot v| \le |u| \cdot |v| < 2 \cdot 2 = 4$. **E.1.12.** **(1)** To find C denote $u = \overrightarrow{AC}$. Clearly, $u = \overrightarrow{AB} + \overrightarrow{AD} = (230, 230, 0)$. It is easy to see, that the first two coordinates of M are $230/2 = 115$. However, let us compute this by projection also. Since the third coordinate of M clearly is 147, and since the first two coordinates of M are equal (due to symmetry), we can denote $M = (c, c, 147)$ and $v = \overrightarrow{AM} = (c, c, 147)$. Since the projection of v on u is $\frac{1}{2}u$, we have $\frac{1}{2}u = \mathrm{proj}_u(v) = \frac{u \cdot v}{u \cdot u} u = \frac{230 \cdot c \cdot 2}{230^2 \cdot 2}(230, 230, 0) = (c, c, 0)$, i.e., $c = \frac{230}{2} = 115$ and $M = (115, 115, 147)$. **(2)** The length of the side CM is $\sqrt{2 \cdot 115^2 + 147^2} = \sqrt{48059} \approx 219.22$. Alternatively, notice that $|CM| = |AM|$. **(3)** The distance from D to BM is equal to the distance $|BD - \mathrm{proj}_{\overrightarrow{BM}}(\overrightarrow{BD})|$. We have $\overrightarrow{BD} = (-230, 230, 0)$ and $\mathrm{proj}_{\overrightarrow{BM}}(\overrightarrow{BD}) \approx (-126.59, -126.59, 161.81)$. The distance is ≈ 146.991. *"For every joy there is a price to be paid"* (ancient Egyptian proverb). **E.1.13.** Consider vectors formed by the given coordinates: $u = (x_1, \dots, x_n)$ and $v = (y_1, \dots, y_n)$. Square both sides of the Cauchy-Schwarz inequality: $|u \cdot v|^2 \le |u|^2 \cdot |v|^2$. But $|u \cdot v|^2 = \left(\sum_{i=1}^n x_i y_i\right)^2$, $|u|^2 = \sum_{i=1}^n x_i^2$ and $|v|^2 = \sum_{i=1}^n y_i^2$. **E.1.14.** **(1)** Let $u = (x_1, \dots, x_n)$ and $u = (y_1, \dots, y_n)$. Then $(au) \cdot v = ax_1y_1 + \dots + ax_ny_n = a(x_1y_1 + \dots + x_ny_n) = a(u \cdot v)$. **(2)** By Proposition 1.6 we have $u \cdot (av) = (av) \cdot u = a(v \cdot u) = a(u \cdot v)$. **(3)** By Proposition 1.6 we have $u \cdot (v + w) = (v + w) \cdot u = v \cdot u + w \cdot u = u \cdot v + u \cdot w$. **E.2.1.** **(1)** Take the direction vector $d = \overrightarrow{AB} = (-1, -2)$ and the position vector $p = \overrightarrow{OA} = (-1, 3)$. **(2)** Notice that the normal $-2v$ defines the same line as the normal v. **(3)** Since the direction vector of ℓ_1 is $d = (-1, -2)$, it has a normal vector $n = (2, -1)$. Denote $w = \overrightarrow{OC} - p = (1, 0)$. The distance from C to ℓ_1 is equal to the length of the projection $\mathrm{proj}_n(w) = \frac{n \cdot w}{n \cdot n} n = \frac{2}{5}(2, -1)$. I.e., it is equal to $\frac{2}{5}\sqrt{4 + 1} = \frac{2}{\sqrt{5}}$. **E.2.2.** The general form of ℓ is $3x - y + 1 = 0$. **(1)** ℓ_1 and ℓ both have the same normal vector n, which according to the general form is $n = (3, -1)$. **(2)** As a normal vector for ℓ_2 we may take any vector orthogonal to n, for example, $(1, 3)$. **E.2.3.** **(2)** The lines ℓ_1 and ℓ_2 have the direction vectors $d_1 = \overrightarrow{AB} = (-2, -1)$ and $d_2 = \overrightarrow{AC} = (3, c - 2)$ respectively. They are perpendicular if and only if $0 = d_1 \cdot d_2 = -2 \cdot 3 - (c - 2) = -4 - c$, i.e., $c = -4$, and $C = (4, -4)$. **(3)** The parametric form of ℓ_2 can be written using the direction vector $d_2 = (3, -6)$ and the position vector $\overrightarrow{OA}$. For the normal form we can take any vector orthogonal to d_2, for example, $n = (6, 3)$. **E.2.4.** As direction vectors we can respectively take $d_1 = (1, \tan(\alpha_1))$ and $d_2 = (1, \tan(\alpha_2))$. **(1)** The vectors d_1 and d_2 are collinear if and only if $\tan(\alpha_1) = \tan(\alpha_2)$. **(2)** The vectors d_1 and d_2 are orthogonal if and only if $0 = d_1 \cdot d_2 = 1 + \tan(\alpha_1) \cdot \tan(\alpha_2)$, i.e., $k_1 \cdot k_2 = -1$. **E.2.5.** **(1)** The vector $\overrightarrow{BC} = (4, -4)$ also is a direction vector. Moreover, we can take the *collinear* direction vector $d = (1, -1)$ for simplicity! The position vector is $p = (4, 5)$. The vector form is $v = p + td$ for the obtained vectors p, d. The parametric form is $\begin{cases} x = 4 + t \\ y = 5 - t \end{cases}$. Taking the normal vector $n = (1, 1)$ we get the normal form $n \cdot v = n \cdot p$. Then $1 \cdot x + 1 \cdot y = 9$, i.e., the normal form is $x + y - 9 = 0$. **(2)** The midpoint M of the segment AB is $\left(\frac{4+0}{2}, \frac{5+3}{2}\right) = (2, 4)$. The normal vector is $n = \overrightarrow{AC} = (0, -6)$. The direction vector is $d = (6, 0)$. Write the four forms like in previous point, using these vectors. The general form is $4x + 2y - 16 = 0$ or, equivalently, $2x + y - 8 = 0$. **(3)** We get the system $\begin{cases} x + y - 9 \ = 0 \\ 2x + y - 8 = 0 \end{cases}$. It has a solution, since the lines ℓ_1 and ℓ_2 are *not* parallel, and so they have an intersection. Since the intersection is *one* point only, the system has *one* solution. **E.2.6.** **(1)** As direction vectors for $\mathcal{P}$ we can take $d = \overrightarrow{AB} = (-1, 1, 0)$ and $k = \overrightarrow{AC} = (0, 2, -1)$. A vector orthogonal to d and k is the cross product $n = d \times k = (-1, -1, -2)$. For simplicity replace it by $n = (1, 1, 2)$. The required forms can be written using n and the position vector, say, $p = \overrightarrow{OA} = (2, -1, 1)$. **(2)** The angle between v and n is $\frac{\pi}{2}$, since $v \cdot n = -2 + 0 + 2 = 0$. Thus, $\alpha = 0$. **E.2.7.** **(2)** As a normal vector n for $\mathcal{P}_3$ we can take the cross product of the normal vectors of $\mathcal{P}_1$ and $\mathcal{P}_2$, i.e., $n = (1, 2, -1) \times (1, 0, 1) = (2, -2, -2)$ or, better, $(-1, 1, 1)$. **E.2.8.** **(1)** As normal vector for both $\mathcal{Q}$ and $\mathcal{P}$ we can take $n = (2, 3, -1)$. As position vector take $p = \overrightarrow{OA} = (2, 0, 3)$. To find the direction vectors d, k for $\mathcal{Q}$ we just need three points on $\mathcal{P}$. They will be found if we find three points M, N, K on $\mathcal{P}$, and then set $d = \overrightarrow{MN}$, $k = \overrightarrow{MK}$. This is easy to do, if we assign some values to variables x, y and then find the z from $2x + 3y - z + 1 = 0$ (just avoid the case when M, N, K are on the same line). Having these vectors find the four forms. **(2)** As position vector for $\mathcal{R}$ take $p = \overrightarrow{OB} = (0, 2, 1)$. We readily have the direction vectors $d = u$, $k = w$. And as normal vector take the vector product $n = u \times w$. Having these vectors find the four forms. **(3)** *Hint*: the normal vectors are not collinear in this case. So the planes have intersection, and the system has a solution. Since the intersection is a line, the system has infinitely many solutions. **E.2.10.** **(1)** Denote $u = \overrightarrow{AB} = (0, 2, 0)$ and $v = \overrightarrow{AC} = (0, 2, -3)$. Then $\operatorname{proj}_u(v) = \frac{4}{4}(0, 2, 0) = (0, 2, 0)$. So $h = \sqrt{(-3)^2} = 3$. **(2)** The area is $\frac{1}{2}h|u| = 3$. We may now notice that ABC is a right angled triangle. **E.2.11.** First find the point D. If $u = \overrightarrow{BA} = (-2, 1, 0)$ and $u = \overrightarrow{BC} = (-2, 2, -3)$, then $\overrightarrow{OD} = \overrightarrow{OB} + (u + v) = (-2, -3, -1)$. **(1)** Having the point $D = (-2, -3, -1)$ we can compute the parametric forms using the position vector $\overrightarrow{OD}$ and the direction vectors $\overrightarrow{DA} = (2, -2, 3)$ and $\overrightarrow{DC} = (2, -1, 0)$. **(2)** The angle α can be obtained by $\cos\alpha = \frac{4+2}{\sqrt{4+4+9}\sqrt{2+1}} = \frac{6}{\sqrt{85}}$. **E.2.12.** **(2)** The cross product w computed for point (1) is a normal vector for $\mathcal{P}$. The point L can be found as the head of the vector $\overrightarrow{AD} + \frac{1}{2}\overrightarrow{DM}$. **E.2.13.** **(1)** As direction vectors for ℓ_1 and ℓ_2 respectively take $d_1 = \overrightarrow{AB} = (1, 1, 2)$ and $d_2 = \overrightarrow{CD} = (2, 2, 6)$. As position vectors take $p_1 = (1, 3, 1)$ and $p_2 = (0, -1, -4)$. Then the parametric form of ℓ_1 consists of three equations: $x = 1 + t$, $y = 3 + t$, $z = 1 + 2t$ (we denote the parametric variable by t). And the parametric form of ℓ_2 will consist of three equations: $x = 2r$, $y = -1 + 2r$, $z = -4 + 6r$ (we denote the parameter by r, not by t since we use this in second point). **(2)** The vector $n = \overrightarrow{MN}$ has the *shortest* length, when its length is equal to the distance between ℓ_1 and ℓ_2. And then n is orthogonal to ℓ_1 and ℓ_2, that is, n is orthogonal to d_1 and d_2. Let us find such an n. Since $n = \overrightarrow{MN}$, then $n = (2r - (1 + t),\ -1 + 2r - (3 + t),\ -4 + 6r - (1 + 3t)) = (2r - t - 1,\ 2r - t - 4,\ 6r - 2t - 5)$. By the way, form this it follows that ℓ_1 and ℓ_2 are *not* intersecting, since n is non-zero (its first and second coordinates $2r - t - 1$ and $2r - t - 4$ may never *simultaneously* become 0 for *any* choice of parameters t, r). $n \cdot d_1 = 0$ means $(2r - t - 1) + (2r - t - 4) + (6r - 2t - 5) \cdot 2 = -6t + 16r - 15 = 0$. And $n \cdot d_2 = 0$ means $(2r - t - 1) \cdot 2 + (2r - t - 4) \cdot 2 + (6r - 2t - 5) \cdot 6 = -16t + 44r - 40 = 0$, which is equivalent to $-4t + 11r - 10 = 0$. This system of two linear equations in two variables is easy to solve to get $t = -\frac{5}{2}$, $r = 0$. Thus, $M = (-\frac{3}{2}, \frac{1}{2}, -4)$ and $N = (0, -1, -4)$, which means,

$|n| = \sqrt{\left(-\frac{3}{2}\right)^2 + \left(\frac{3}{2}\right)^2} = \frac{3}{\sqrt{2}}$. **E.3.2.** **(1)** $c^3 = 2-11i$, and $u-v = (2+2i,\ -4+4i,\ -1+i)$. Then $c^3(u-v) = (26-18i,\ 36+52i,\ 9+13i)$. **(2)** Compute taking into account that $\frac{c}{d} = 3+i$. **(3)** Compute taking into account that $\frac{(u+v)}{c} = \frac{1}{c}(u+v)$, and that $\frac{1}{c} = (2-i)^{-1} = \frac{2}{5} + i\frac{1}{5}$. **E.3.3.** **(1)** $c^2 + d = (1-i)^2 - 2 + i = -2 - i$, and $(-2-i)^{-1} = \frac{1}{-2-i} = \frac{1}{-2-i} \cdot \frac{-2+i}{-2+i} = -\frac{2}{5} + \frac{1}{5}i$. Also $cu + v = (1-i)[1+3i, 2-i] + [5i, 2-i] = [4+2i, 1-3i] + [5i, 2-i] = [4+7i, 3-4i]$. Therefore, $w = \left(-\frac{2}{5} + \frac{1}{5}i\right)[4+7i, 3-4i] = [-3-2i, -\frac{2}{5}+\frac{11}{5}i]$. **E.3.4.** **(1)** If $x_k = a_k + b_k i$, then $\bar{x}_k = a_k - b_k i$. Then $x_k + \bar{x}_k = 2a_k$ which is a real number. **(2)** $x_k - \bar{x}_k = 2b_k i$ which is a real number *only* if $b_k = 0$. I.e., $v - \bar{v} \in \mathbb{R}^n$ holds only if $v \in \mathbb{R}^n$. **E.3.5.** **(1)** There are six roots. See Figure C.3. **E.3.6.** **(2)** The half of u is $2^{-1}u$. Since in $\mathbb{Z}_3$ we have $2^{-1} = 2$ (because $2 \cdot_3 2 = 1$), then $2^{-1}u = 2[2,1,0,1] = [1,2,0,2]$. **E.3.7.** **(2)** Since $\mathbb{Z}_5 = \{0,1,2,3,4\}$ has only a few elements, it is simpler to directly check which one of the four non-zero elements is the inverse of 4. We get $4 \cdot_5 4 = 1$. **E.3.8.** **(1)** $14\left[\begin{smallmatrix}97\\53\end{smallmatrix}\right] = \left[\begin{smallmatrix}150\\138\end{smallmatrix}\right]$. **(2)** $-v = -\left[\begin{smallmatrix}97\\53\end{smallmatrix}\right] = \left[\begin{smallmatrix}151-97\\151-53\end{smallmatrix}\right] = \left[\begin{smallmatrix}54\\98\end{smallmatrix}\right]$. **(3)** By Example B.8 we already know that $62^{-1} = 95$. Thus, $\frac{v}{62} = 62^{-1}v = 95\left[\begin{smallmatrix}97\\53\end{smallmatrix}\right] = \left[\begin{smallmatrix}4\\52\end{smallmatrix}\right]$. **(4)** By Euclid's Algorithm we get $31 \cdot 151 - 72 \cdot 65 = 1$. Dividing -72 by 151 we get $-72 = -1 \cdot 151 + 79$, i.e., $65^{-1} = 79$ in $\mathbb{Z}_{151}$. Thus, $\frac{v}{65} = 65^{-1}v = 79\left[\begin{smallmatrix}97\\53\end{smallmatrix}\right] = \left[\begin{smallmatrix}113\\110\end{smallmatrix}\right]$. **E.3.9.** **(1)** Take, say, $v_1 = (1,2,0)$, $v_2 = 2v_1 = (2,1,0)$, $v_3 = 0v_1 = (0,0,0)$. **(2)** Take, say, $v_1 = (1,0,0)$, $v_2 = (0,1,0)$, $v_3 = (0,0,2)$. **E.3.10.** **(1)** $u + v = (1,1,1,0,0)$. **(2)** The truth table of operation $\mathtt{XOR}$ *coincides with addition rule in* $\mathbb{Z}_2$ because $0 \,\mathtt{XOR}\, 0 = 0$, $0 \,\mathtt{XOR}\, 1 = 1$, $1 \,\mathtt{XOR}\, 0 = 1$, $1 \,\mathtt{XOR}\, 1 = 0$. Therefore $w = u + v$. **E.4.1.** **(1)** If such $0'$ exists, then $0 + 0' = 0$. On the other hand $0 + 0' = 0'$ by point 3 in Definition 4.1. So $0 = 0'$. **(2)** In analogy with the previous point, $1 \cdot 1' = 1$ and $1 \cdot 1' = 1'$. **E.4.2.** F^n has p^n elements since a vector is a sequence of length n, in which each entry accepts p values. **E.4.3.** By the hint given in exercise we have $(a + b\sqrt{2})(\frac{a}{r} - \frac{b}{r}\sqrt{2}) = \frac{1}{r}(a + b\sqrt{2})(a - b\sqrt{2}) = \frac{r}{r} = 1$. So any non zero $a + b\sqrt{2}$ has an inverse $\frac{a}{r} - \frac{b}{r}\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. Also, $\mathbb{Q}(\sqrt{2})$ contains the zero element $0 = 0 + 0\sqrt{2}$, and the identity element $1 = 1 + 0\sqrt{2}$. The remaining axioms Definition 4.1 hold in $\mathbb{Q}(\sqrt{2})$ because they hold in $\mathbb{R}$, in general. **E.4.4.** $+_4$ clearly satisfies points 1-4 of Definition 4.1. $*$ is defined to be commutative. Associativity and distributivity are easy to check. As inverses we can take: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$. **E.4.5.** **(1)** By the hint to Exercise 4.3 $a^{-1} = \frac{2}{r} - \frac{1}{r}\sqrt{2} = 1 - \frac{\sqrt{2}}{2}$, since $r = 2^2 - 2 \cdot 1^2 = 2$. Then $u + bv = [3\sqrt{2}, -1] + 3\sqrt{2}\,[1 - \sqrt{2}, \sqrt{2}] = [-6 + 6\sqrt{2},\ 5]$. Thus, $w = \frac{u+bv}{a} = (1 - \frac{\sqrt{2}}{2})[-6 + 6\sqrt{2},\ 5] = [-12 + 9\sqrt{2},\ 5 - \frac{5}{2}\sqrt{2}]$. **E.4.6.** **(1)** Yes. The operaation is *closed* because the sum and product of two elements of type $a + b\sqrt{3}$ also is of this type. The inverse is calculated using the fact that $r = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2 \in \mathbb{Q}$. Thus, $(a + b\sqrt{3})^{-1} = \frac{a}{r} - \frac{b}{r}\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. **(2)** No. Because the product of two elements of type $a + b\sqrt{2} + c\sqrt{3}$ may no longer be an element of *that* type. Example: $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$, but $\sqrt{6} \neq a + b\sqrt{2} + c\sqrt{3}$ for whatever $a, b, c \in \mathbb{Q}$. **E.4.7.** $\mathbb{R}(x)$ is a field. The points 1., 2., 5., 6., 9. of Definition 4.1 hold for any functions. As additive identity for point 3. take $\frac{0}{1} = \frac{0}{q(x)}$. As multiplicative identity for point 7. take $\frac{1}{1} = \frac{q(x)}{q(x)}$. As the opposite for $f(x) = \frac{p(x)}{q(x)}$ of point 4. take $-f(x) = \frac{-p(x)}{q(x)}$. And if $f(x) = \frac{p(x)}{q(x)}$ is *non-zero* then $p(x)$ is *non-zero*, and we can take the inverse $f^{-1}(x) = \frac{q(x)}{p(x)}$ for point 8.

Part 2. Systems of Linear Equations.

E.5.2. **(2)** To get a different series of elementary operations start by swapping any two rows during the process. If the final row you get still is $0 = 1$, then just apply say, $2 \cdot R3$, i.e., multiply the 3'rd row by 2. **E.5.4.** **(1)** Take any collinear vectors n_1, n_2, n_3, and choose non-intersecting planes. **(2)** Take any non-zero, pairwise non-collinear vectors n_1, n_2, n_3 the heads of which do *not* belong to a plane passing by O. **(3)** Take any non-zero, pairwise non-collinear vectors n_1, n_2, n_3 the heads of which *do* belong to a plane plane passing by O. **E.5.6.** **(1)** Yes. The intersection of any lines in $\mathbb{R}^2$ or planes in $\mathbb{R}^3$ may be either empty set, or a point, or a line, or a plane. So if it contains more then one point, it is a line or a plane. **(2)** No. A space F^n on a *finite* field F has $|F|^n$ elements, i.e., it is a finite set. So the solutions of any system with n variables also are finite, since each of them is a vector in F^n. Say, the system with two equations $x + 2y = 1$, $2x + y = 2$ has exactly *three* solutions on $\mathbb{Z}_3$ which are: $(0,2)$, $(2,1)$, $(1,0)$. **E.6.6**. A matrix may have different row-echelon forms. We bring just some of them. **(1)** A row-echelon form is $\begin{bmatrix} \mathbf{1} & 0 & 0 & 1 \\ 0 & \mathbf{1} & -2 & 0 \\ 0 & 0 & 0 & \mathbf{-2} \end{bmatrix}$. The pivots are marked in bold. **(2)** A row-echelon form is $\begin{bmatrix} \boldsymbol{i} & 3 \\ 0 & \boldsymbol{i} \\ 0 & 0 \end{bmatrix}$. The pivots are marked in bold. **(3)** A row-echelon form is $\begin{bmatrix} \mathbf{1} & 2 & 4 \\ 0 & \mathbf{1} & 2 \\ 0 & 0 & \mathbf{1} \end{bmatrix}$. The pivots are marked in bold. **E.6.7**. Notice that the fourth matrix already is in row-echelon form. And to bring the fifth matrix to row-echelon form one should just replace all elements below $a_{11} = 1$ by 0. **E.6.9**. **(2)** There are a few ways to get a matrix which is *not* row-equivalent to A. For example, if we take a matrix O in $M_{3,4}(\mathbb{R})$ consisting of zeros only, then we cannot arrive to A starting from O because none of elementary operations alters O. Another way: consider the system of linear equations for which A is an augmented matrix. Then choose another system of three linear equations in four variables, which has another solution (or has no solution, at all). Then the augmented matrix of this new system will not be row-equivalent to A. **E.6.10**. **(1)** These four elementary operations just swap the first two rows. So we could replace them by a single operation $R1 \leftrightarrow R2$. **(2)** In analogy with previous part, any elementary operation $Ri \leftrightarrow Rj$ can be replaced by four operations $Rj + Ri$, $Ri - Rj$, $Rj + Ri$, $(-1)\cdot Ri$. **E.7.1**. **(3)** The general solution is $\left(\frac{2}{3}\alpha + \frac{1}{3}\beta + 1,\ -\frac{4}{3}\alpha - \frac{2}{3}\beta,\ \frac{4}{3}\alpha - \frac{4}{3}\beta,\ \alpha,\ \beta\right)$ for any $\alpha, \beta \in \mathbb{R}$. **(4)** The system has a unique solution $\left(\frac{3}{10}, 0, -1, -\frac{1}{10}\right)$. **E.7.2**. The augmented matrix is: $\bar{A} = \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 2 & 4 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 & 0 & 4 \end{bmatrix}$. Bring to row-echelon form: $\bar{A} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & -2 & -2 & -2 & -2 \\ 0 & 0 & 0 & 2 & 2 & 0 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & -3 & 3 \\ 0 & 0 & 0 & 2 & 2 & 0 & 4 \end{bmatrix} \sim$ $\begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & -3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & -3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. The respective system is $\begin{cases} x_1 + 2x_2 + x_3 + x_4 + x_5 + x_6 = 2 \\ -2x_4 - 2x_5 + x_6 = -5 \\ -3x_6 = 3. \end{cases}$ The pivot columns are the 1'st , 4'th, 6'th columns. The non-pivot columns are the 2'nd , 3'rd, 5'th columns. $\begin{cases} x_1 + x_4 + x_6 = 2 - 2x_2 - x_3 - x_5 \\ -2x_4 + x_6 = -5 + 2x_5 \\ -3x_6 = 3. \end{cases}$ Assigning $x_2 = x_3 = x_5 = 0$ we get the system $\begin{cases} x_1 + x_4 + x_6 = 2 \\ -2x_4 + x_6 = -5 \\ -3x_6 = 3. \end{cases}$ From where $x_6 = -1$, $x_4 = 2$, $x_1 = 1$, and the single solution we look for is $(1, 0, 0, 2, 0, -1)$. Assigning parametric values $x_2 = \alpha$, $x_3 = \beta$, $x_5 = \gamma$ we get the system $\begin{cases} x_1 + x_4 + x_6 = 2 - 2\alpha - \beta - \gamma \\ -2x_4 + x_6 = -5 + 2\gamma \\ -3x_6 = 3. \end{cases}$ I.e., $x_6 = -1$, $x_4 = 2 - \gamma$, $x_1 = 1 - 2\alpha - \beta$, and the general solution of the system is $\{(1 - 2\alpha - \beta,\ \alpha,\ \beta,\ 2 - \gamma,\ \gamma,\ -1) \mid \alpha, \beta, \gamma \in \mathbb{R}\}$. **E.7.4**. We computed the row-echelon form $\bar{A} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & -2 & -2 & -2 & -2 \\ 0 & 0 & 0 & 2 & 2 & 0 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & -3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Bringing it to reduced row-echelon form: $\sim$ $\begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & -2 & -2 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 0 & 3 \\ 0 & 0 & 0 & -2 & -2 & 0 & -4 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 0 & 3 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \mathrm{rref}(\bar{A})$. The respective system is $\begin{cases} x_1 + 2x_2 + x_3 = 1 \\ x_4 + x_5 = 2 \\ x_6 = -1. \end{cases}$ The pivot columns are the 1'st , 4'th, 6'th columns. The non-pivot columns are the 2'nd , 3'rd, 5'th columns. Moving the free variables to the right-hand side, and assigning parametric values $x_2 = \alpha$, $x_3 = \beta$, $x_5 = \gamma$ we get the system $\begin{cases} x_1 = 1 - 2\alpha - \beta \\ x_4 = 2 - \gamma \\ x_6 = -1. \end{cases}$ And the general solution is $\{(1 - 2\alpha - \beta,\ \alpha,\ \beta,\ 2 - \gamma,\ \gamma,\ -1) \mid \alpha, \beta, \gamma \in \mathbb{R}\}$. $\mathrm{rank}(\bar{A}) = 3$. This can be explained by the fact that the row-echelon form (or the reduced row-echelon form has) three non-zero rows. This *also* follows from the fact the fact that the row-echelon form (or the reduced row-echelon form has) three pivots. By Theorem 7.19 this system is consistent because $\mathrm{rank}(A) = \mathrm{rank}(\bar{A})$, since the row-echelon form (or the reduced row-echelon form) of A also has three non-zero rows. **E.7.5**. The first system has the unique solution $(-\frac{1}{3+i}, -\frac{6}{3+i}, \frac{3}{3+i}) = \left(-\frac{3}{10} + \frac{i}{10}, -\frac{18}{10} + \frac{6i}{10}, \frac{9}{10} - \frac{3i}{10}\right) \in \mathbb{C}^3$. The second system has the unique solution $(1, 1, 0) \in \mathbb{Z}_3^3$. **E.7.6**. For each $\bar{A}$ we have computed its reduced row-echelon form $\mathrm{rref}\big(\bar{A}\big)$. Take any matrix B which is in reduced row-echelon form, but is distinct from $\mathrm{rref}\big(\bar{A}\big)$ in at least one entry. **E.7.9**. Ranks of augmented matrices for Exercise E.7.1 respectively are 3 and 4. The rank of both augmented matrices for Exercise E.7.5 is 3. **E.7.12**. **(1)** $\mathrm{rref}(A) = \mathrm{rref}(B) = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, $\mathrm{rref}(C) = \begin{bmatrix} 1 & 2 & \frac{4}{3} & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. So the only row-equivalent matrices are $A \sim B$. **(2)** By previous calculations we have $\mathrm{rank}(A) = \mathrm{rank}(B) = 3$, $\mathrm{rank}(C) = 2$.

Part 3. Matrix Algebra.

E.8.2. Let $X=\begin{bmatrix}2&1\\1&3\end{bmatrix}$, $X'=\begin{bmatrix}1&1\\2&3\end{bmatrix}$, $W=\begin{bmatrix}2&3\\1&2\end{bmatrix}$, $W'=\begin{bmatrix}1&2\\1&1\end{bmatrix}$, $Y=Z=O=\begin{bmatrix}0&0\\0&0\end{bmatrix}$. Then $A\cdot B=\left[\begin{array}{c:c}X&O\\ \hdashline O&W\end{array}\right]\cdot\left[\begin{array}{c:c}X'&O\\ \hdashline O&W'\end{array}\right]=\left[\begin{array}{c:c}X\cdot X'&O\\ \hdashline O&W\cdot W'\end{array}\right]$. **E.8.3.** It is impossible to calculate $(A^T+C)^T+B$ because A^T+C is a 4×3 matrix, $(A^T+C)^T$ is a 3×4 matrix which cannot be added to the 3×3 matrix B. The other three operations are doable. **E.8.7.** G is the inverse of B. **E.9.2.** **(1)** $\begin{bmatrix}1&0&0\\0&1&0\\-2&0&1\end{bmatrix}$. **(2)** $\begin{bmatrix}1&-3&0\\0&1&0\\0&0&1\end{bmatrix}$. **(3)** $\begin{bmatrix}1&0&0\\0&4&0\\0&0&1\end{bmatrix}$. **(4)** $\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}$. **(5)** The operation is $R2+R1$ so we have $\begin{bmatrix}1&0&0\\1&1&0\\0&0&1\end{bmatrix}$. **(6)** The operation again is $R2+R1$ so we have the same matrix as in previous point. **(7)** The last row is the 3'rd row. So we have $\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$. **E.9.3.** **(1)** E_1 corresponds to swapping of the 2'nd and 3'rd lines. Applying this operation twice changes nothing in the matrix. So $E_1^{10}=I$, $E_1^{11}=E_1$. Next, E_2 corresponds to multiplication of the 3'rd row by 5. So E_2^3 corresponds to application of this operation three times. I.e. $E_2^3=\begin{bmatrix}1&0&0\\0&1&0\\0&0&125\end{bmatrix}$. Finally, E_3 corresponds to adding to the 2'nd row the 1'st row times -3. Applying this operation for 10 times just adds to the 2'nd row the 1'st row times -30. So we have $E_3^{10}=\begin{bmatrix}1&0&0\\-30&1&0\\0&0&1\end{bmatrix}$. **E.9.7.** **(1)** $\operatorname{rank}(A)=3$ and $\operatorname{rank}(B)=2$. **(2)** By point 5 of Theorem 9.10 $\operatorname{rref}(A)=I$ and $\operatorname{rref}(B)\neq I$ (since $\operatorname{rank}(B)\neq3$). **(3)** Use point 6 of Theorem 9.10. **(4)** Reduction of A to $\operatorname{rref}(A)$ takes 7 elementary operations: $R3+(-1)R1$, $\frac12R2$, $R3+(-1)R2$, $2R3$, $R2+(-\frac12)R3$, $R1+(-2)R3$, $R1+(-1)R2$. The respective elementary matrices are: $E_1=\begin{bmatrix}1&0&0\\0&1&0\\-1&0&1\end{bmatrix}$, $E_2=\begin{bmatrix}1&0&0\\0&1/2&0\\0&0&1\end{bmatrix}$, $E_3=\begin{bmatrix}1&0&0\\0&1&0\\0&-1&1\end{bmatrix}$, $E_4=\begin{bmatrix}1&0&0\\0&1&0\\0&0&2\end{bmatrix}$, $E_5=\begin{bmatrix}1&0&0\\0&1&-1/2\\0&0&1\end{bmatrix}$, $E_6=\begin{bmatrix}1&0&-2\\0&1&0\\0&0&1\end{bmatrix}$, $E_7=\begin{bmatrix}1&-1&0\\0&1&0\\0&0&1\end{bmatrix}$. Thus, $E_7E_6E_5E_4E_3E_2E_1\cdot A=\operatorname{rref}(A)=I$. So we get the presentation $A=F_1F_2F_3F_4F_5F_6F_7$, where $F_i=E_i^{-1}$ for $i=1,\ldots,7$. That is, $F_1=\begin{bmatrix}1&0&0\\0&1&0\\1&0&1\end{bmatrix}$, $F_2=\begin{bmatrix}1&0&0\\0&2&0\\0&0&1\end{bmatrix}$, $F_3=\begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix}$, $F_4=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1/2\end{bmatrix}$, $F_5=\begin{bmatrix}1&0&0\\0&1&1/2\\0&0&1\end{bmatrix}$, $F_6=\begin{bmatrix}1&0&2\\0&1&0\\0&0&1\end{bmatrix}$, $F_7=\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}$. **E.9.8.** $A^{-1}=\begin{bmatrix}1&1&-3\\0&1&-2\\-1&-2&6\end{bmatrix}$, $B^{-1}=\begin{bmatrix}-i&0\\-2&i\end{bmatrix}$, $C^{-1}=\begin{bmatrix}0&1\\1&1\end{bmatrix}$. **E.9.9.** **(1)** $\operatorname{rank}(A)=2\neq3$ so A is not invertible. $\operatorname{rank}(B)=1\neq3$ so B is not invertible. $\operatorname{rank}(C)=3$ so C is invertible. **(2)** The elementary operations are: $C=\begin{bmatrix}0&1&0\\1&2&0\\2&0&3\end{bmatrix}\overset{R1\leftrightarrow R2}{\sim}\begin{bmatrix}1&2&0\\0&1&0\\2&0&3\end{bmatrix}\overset{R3-2R1}{\sim}\begin{bmatrix}1&2&0\\0&1&0\\0&-4&3\end{bmatrix}\overset{R3+4R2}{\sim}$ $\begin{bmatrix}1&2&0\\0&1&0\\0&0&3\end{bmatrix}\overset{\frac13\cdot R3}{\sim}\begin{bmatrix}1&2&0\\0&1&0\\0&0&1\end{bmatrix}\overset{R1-2R2}{\sim}\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$. The respective elementary matrices are $E_1=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$, $E_2=\begin{bmatrix}1&0&0\\0&1&0\\-2&0&1\end{bmatrix}$, $E_3=\begin{bmatrix}1&0&0\\0&1&0\\0&4&1\end{bmatrix}$, $E_4=\begin{bmatrix}1&0&0\\0&1&0\\0&0&\frac13\end{bmatrix}$, $E_5=\begin{bmatrix}1&-2&0\\0&1&0\\0&0&1\end{bmatrix}$. So we have $E_5\,E_4\,E_3\,E_2\,E_1\cdot C=\operatorname{rref}(C)=I$ (and $\operatorname{rref}(C)=I$ because C is invertible). **(3)** The respective inverses are $F_1=E_1^{-1}=E_1$, $F_2=E_2^{-1}=\begin{bmatrix}1&0&0\\0&1&0\\2&0&1\end{bmatrix}$, $F_3=E_3^{-1}=\begin{bmatrix}1&0&0\\0&1&0\\0&-4&1\end{bmatrix}$, $F_4=E_4^{-1}=\begin{bmatrix}1&0&0\\0&1&0\\0&0&3\end{bmatrix}$, $F_5=E_5^{-1}=\begin{bmatrix}1&2&0\\0&1&0\\0&0&1\end{bmatrix}$. We have the presentation $A=F_1\,F_2\,F_3\,F_4\,F_5$.

Part 4. Abstract Vector Spaces.

E.10.1. No, some points of Definition 10.1 do not hold (such as the 3'rd or 8'th). **E.10.2.** **(1)** Yes. **(2)** No. **(3)** Yes. **E.10.3.** **(1)** Yes. **(2)** Yes. **(3)** No. **E.10.4.** **(1)** Yes. **(2)** No, because a product $af(x)$ may *not* belong to V if a is an irrational number. **E.10.5.** Yes. **E.10.7.** **(1)** Yes. **(2)** No. **(3)** No. **E.10.8.** We have $-v+v=(-v+v)+\vec0=(-v+v)+\big[-v+\big(-(-v)\big)\big]=\big[(-v+v)+(-v)\big]+\big(-(-v)\big)=\big[-v+\big(v+(-v)\big)\big]+\big(-(-v)\big)=(-v+\vec0)+\big(-(-v)\big)=-v+\big(-(-v)\big)=\vec0$. Using the already proven part we get $\vec0+v=\big(v+(-v)\big)+v=v+\big((-v)+v\big)=v+\vec0=v$. **E.10.9.** Below we are going to prove all the points of Proposition 10.10 *without* using the commutativity axiom 1 of vector space Definition 10.1. We use Exercise E.10.8. Point 1. Suppose the trivial vector $\vec0$ is *not* unique, i.e., there is another vector $0'$ meeting the requirements of Definition 10.1. Then $\vec0=\vec0+0'=0'$ (by our supposition, by axiom 3 and by Exercise E.10.8). Contradiction. Point 2. Suppose the opposite vector $-v$ is *not* unique for certain $v\in V$, i.e., there is another vector v' meeting the requirements of Definition 10.1. Then $v+(-v)=\vec0=v+v'$ (by our supposition). Adding to both sides from the left the vector $-v$ we get $-v=v'$ (by axioms 2, 4, 3 and Exercise E.10.8). Contradiction. Point 3. Since $\vec0+\vec0=\vec0$ by axiom 3, then $-\vec0=\vec0$ by point 2. Next, by Exercise E.10.8 we have $-v+v=\vec0$. From here and from point 2 it follows that $-(-v)=v$. Point 4. Since $0v=(0+0)v=0v+0v$, we can add $-0v$ to both sides of this equality to get $\vec{0}=0v+(-0v)=(0v+0v)+(-0v)=0v+\big(0v+(-0v)\big)=0v+\vec{0}=0v$. (we used the axioms 2, 4, 3). Similarly, since $a\vec{0}=a(\vec{0}+\vec{0})=a\vec{0}+a\vec{0}$, we can add $-(a\vec{0})$ to both sides of this equality to get $\vec{0}=a\vec{0}+\big(-(a\vec{0})\big)=(a\vec{0}+a\vec{0})+\big(-(a\vec{0})\big)=a\vec{0}+\Big(a\vec{0}+\big(-(a\vec{0})\big)\Big)=a\vec{0}+\vec{0}=a\vec{0}$ (we used the axioms 2, 4, 3). Point 5. $av+(-a)v=(a-a)v=0v=\vec{0}$ by point 4. Then by point 2 we have $(-a)v=-(av)$. Similarly, $av+a(-v)=a\big(v+(-v)\big)=a\vec{0}=\vec{0}$ by point 4, and $a(-v)=-(av)$ by point 2. Taking here $a=1$ we have $-v=(-1)v$. Point 6. $-(u+v)=(-1)(u+v)=(-1)u+(-1)v=-u+(-v)=-u-v$ by point 5 and axiom 5. Point 7. $a(u-v)=a\big(u+(-v)\big)=au+a(-v)=au+(-av)=au-av$ by point 5 and axiom 5. **E.10.10**. By axioms 3, 2, Exercise E.10.8 and point 6 of Proposition 10.10 (we can use Proposition 10.10 because in Exercise E.10.9 we proved it *without* using axiom 1 of Definition 10.1) we have $v+u=(v+u)+\vec{0}=(v+u)+\big[-(u+v)+(u+v)\big]=\big[(v+u)+\big(-(u+v)\big)\big]+(u+v)=\big[(v+u)+\big(-u+(-v)\big)\big]+(u+v)$. It remains to notice that $\big[(v+u)+\big(-u+(-v)\big)\big]=\big((v+u)+(-u)\big)+(-v)=\big(v+(u+(-u))\big)+(-v)=(v+\vec{0})+(-v)=v+(-v)=\vec{0}$. Thus, $v+u=\vec{0}+(u+v)=u+v$. **E.10.11**. To show that axiom 8 is necessary it is enough to suggest a system that satisfies the remaining seven axioms, but which is *not* a vector space according to Definition 10.1. Take the field $F=\mathbb{R}$, the set $V=\mathbb{R}^3$, and define addition $u+v$ of elements of V in the traditional way, just like vectors in the *real space* $\mathbb{R}^3$. And for any $a\in F$ and $v\in V$ define $av=\vec{0}$. Then the axioms 1–4 hold here by default (they do not evolve multiplication by a scalar). And the axioms 5–7 are trivial to verify. Axiom 8 evidently fails. **E.11.1**. Yes, v is a linear combination. Not unique. This answers are easy to obtain by solving a system of lin. equations. **E.11.2**. **(1)** No. **(2)** No. **(3)** Yes. **E.11.4**. **(2)** Take $v_1=(1,0,0)$, $v_2=(0,1,0)$, $v_2=v_1+v_2$. **E.11.5**. Denote by w_1,w_2,w_3 the last (4'th) column vectors of each of these matrices. The vectors $w_1=[-7,0,0]$, $w_2=[0,-7,0]$, $w_3=[0,0,-7]$ are independent. **E.11.6**. **(1)** The span is a plane passing by Oz axis and forming 45° angle with xOz. **(3)** The span is $\mathcal{P}_2$. **E.11.7**. $\operatorname{span}(U)=U$ and $\operatorname{span}(V)=V$. **E.11.8**. Assume the contrary: $F[X]=\operatorname{span}(h_1(x),\dots,h_n(x))$ is spanned by finitely many polynomials $h_1(x),\dots,h_n(x)$ of degrees, say, $d_1,\dots,d_n$. Let d me the maximum of these degrees, and let $f(x)$ be *any* polynomial of degree higher than d. Any linear combination of $h_1(x),\dots,h_n(x)$ has a degree strictly less than d, so it cannot be equal to $f(x)$. **E.11.9**. **(1)** Yes. **(2)** No (is not a spanning set). **(3)** No (is not linearly independent). **E.11.10**. $\vec{0}$ evidently has a presentation $\vec{0}=0u_1+\cdots+0u_m$. By the requirement of the exercise this presentation is *unique*. I.e., if we take any other coefficients, then the respective combination will not be zero. **E.11.12**. **(1)** $\dim(V)=2$. **(2)** $\dim(V)=2$. **(3)** $\dim(\mathbb{C})=2$, if $\mathbb{C}$ is considered as vector space over $\mathbb{R}$. **E.11.13**. The matrices M_1,M_2,M_3,M_4 are not a spanning set for $M_{2,2}(\mathbb{R})$ because the entry a_{21} is zero in all of them. They are not linearly independent because their span is 3-dimensional, and four vectors cannot be independent in a 3-dimensional space. Three polynomials f_1,f_2,f_3 are linearly independent, but they are not a spanning set for $\mathcal{P}_3(\mathbb{R})$ because $\dim(\mathcal{P}_3(\mathbb{R}))=4$. Also, $\dim(\operatorname{span}(f_1,f_2,f_3))=3$. **E.12.3**. Take $g_1=(3,0,0)$, $g_2=(0,4,0)$, $g_3=(0,0,-5)$. **E.13.1**. $P_{EG}=\begin{bmatrix}1&0&0\\3&2&1\\1&1&1\end{bmatrix}$, $P_{GE}=\begin{bmatrix}1&0&0\\-2&1&-1\\1&-1&2\end{bmatrix}=P_{EG}^{-1}$. **E.13.2**. $P_{EG}\cdot P_{GE}=P_{GE}\cdot P_{EG}=I$ by Theorem 13.4. **E.13.3**. $u=[u]_G=P_{GE}\cdot[u]_E=(1,1,4)$ and $v=[v]_G=P_{GE}\cdot[v]_E=(2,-5,4)$. **E.13.4**. Bring the matrix $[E\,|\,G]=\begin{bmatrix}2&0&1&2\\3&4&4&2\end{bmatrix}$ to the form $\operatorname{rref}[E\,|\,G]=[I\,|\,P_{EG}]=\begin{bmatrix}1&0&3&1\\0&1&0&1\end{bmatrix}$ to get $P_{EG}=\begin{bmatrix}3&1\\0&1\end{bmatrix}$. **E.13.5**. **(1)** Since E is the *standard* basis, $P_{EG}=[g_1\ g_2\ g_3]=\begin{bmatrix}-1&2&0\\0&2&-1\\1&-1&0\end{bmatrix}$, and $P_{EH}=[h_1\ h_2\ h_3]=\begin{bmatrix}1&0&1\\0&1&0\\2&3&1\end{bmatrix}$. **(2)** We have $[G\mid I]=\begin{bmatrix}-1&2&0&1&0&0\\0&2&-1&0&1&0\\1&-1&0&0&0&1\end{bmatrix}\sim\begin{bmatrix}1&0&0&1&0&2\\0&1&0&1&0&1\\0&0&1&2&-1&2\end{bmatrix}=[I\mid P_{GE}]$. I.e. $P_{GE}=\begin{bmatrix}1&0&2\\1&0&1\\2&-1&2\end{bmatrix}$ **(3)** $[u]_G=P_{GE}\cdot[u]_E=\begin{bmatrix}1&0&2\\1&0&1\\2&-1&2\end{bmatrix}\begin{bmatrix}3\\1\\2\end{bmatrix}=\begin{bmatrix}7\\5\\9\end{bmatrix}$ and $[v]_G=P_{GE}\cdot[u]_E=\begin{bmatrix}1&0&2\\1&0&1\\2&-1&2\end{bmatrix}\begin{bmatrix}1\\0\\3\end{bmatrix}=\begin{bmatrix}7\\4\\8\end{bmatrix}$. **(4)** $[w]_E=P_{EG}\cdot[w]_G=[g_1\ g_2\ g_3]\cdot[w]_G=\begin{bmatrix}-1&2&0\\0&2&-1\\1&-1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\1\\-1\end{bmatrix}$. **(5)** $[G\mid H]=\begin{bmatrix}-1&2&0&1&0&1\\0&2&-1&0&1&0\\1&-1&0&2&3&1\end{bmatrix}\sim\begin{bmatrix}1&0&0&5&6&3\\0&1&0&3&3&2\\0&0&1&6&5&4\end{bmatrix}=\operatorname{rref}[G\mid H]=[I\mid P_{GH}]$. Alternatively, P_{GH} can be computed as $P_{GH}=P_{GE}\cdot P_{EH}=\begin{bmatrix}1&0&2\\1&0&1\\2&-1&2\end{bmatrix}\begin{bmatrix}1&0&1\\0&1&0\\2&3&1\end{bmatrix}=\begin{bmatrix}5&6&3\\3&3&2\\6&5&4\end{bmatrix}$.

Part 5. Matrix Computations in Spaces.

E.14.2. **(1)** Form the matrix A putting the coordinates of u_1, u_2, u_3, u_4 as rows of A. Row echelon form of A has just two non-zero rows. So $\dim(U) = 2$ and $U \neq \mathbb{R}^4$. **(2)** Row-echelon form of matrix formed by coordinates of v_1, v_2, v_3 has three non-zero rows. So $\dim(U) = 3$ and $U \neq V = \mathbb{R}^5$. **(3)** Row-echelon form of matrix formed by coordinates of w_1, w_2, w_3, w_4 has two non-zero rows (don't forget that the calculations are over $\mathbb{Z}_5$). So $\dim(U) = 2$. Since $\dim(V) = \dim\big(\mathbb{Z}_5^3\big) = 3$, we have $U \neq V$. **E.14.3.** By coordinate map $\phi_E : \mathcal{P}_3(\mathbb{R}) \to \mathbb{R}^4$ we put in correspondence to our three polynomials the vectors $[f_1(x)]_E = [1,2,-1]$, $[f_2(x)]_E = [0,1,1]$, $[f_3(x)]_E = [-1,1,0]$. The respectice matrix $A = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 1 \\ -1 & 1 & 0 \end{bmatrix}$ has a row-echelon form $R = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Since $\operatorname{rank}(R) = 3$, the vectors $f_1(x), f_2(x), f_3(x)$ are linearly independent. Since they all are in $\mathcal{P}_2(\mathbb{R})$ (which is 3-dimensional), we have $U = \operatorname{span}(f_1(x), f_2(x), f_3(x)) = \mathcal{P}_2(\mathbb{R})$. **E.14.4.** **(2)** Using the coordinate map $\phi_E : M_{2,2}(\mathbb{R}) \to \mathbb{R}^4$ we buld the matrix $A = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 2 & 2 & 4 \\ 1 & 1 & 3 & 4 \end{bmatrix}$. Its row-echelon form is $R = \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Since $\operatorname{rank}(R) = 2$, the vectors v_1, v_2, v_3 are linearly dependent. **E.14.7.** In Exercise E.14.4 we saw that three vectors v_1, v_2, v_3 are linearly dependent. To see which ones of them form a maximal linearly independent subset put the coordinates by columns to get the matrix $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 2 & 2 & 3 \\ 2 & 4 & 4 \end{bmatrix}$. Its row-echelon form is $R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Since the pivots are the 1'st and 2'nd columns, as a maximal linearly independent system we can take v_1, v_2. **E.14.8.** In Exercise E.14.3 we have shown that $f_1(x), f_2(x), f_3(x)$ are linearly independent. So the maximal linearly independent subset also is $f_1(x), f_2(x), f_3(x)$. **E.14.9.** By Algorithm 14.29 we get $u = 2v_1 + v_2 - v_3$. **E.14.10.** **(1)** $\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} 2 & -1 & 1 \\ -4 & 2 & -2 \\ 1 & 0 & 2 \\ 0 & -2 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, from where we can take the basis $e_1 = (1, -\frac{1}{2}, \frac{1}{2})$, $e_2 = (0,1,3)$, $e_3 = (0,0,1)$ for $\operatorname{span}(v_1, v_2, v_3, v_4)$. The vector $e_1 = (1, -\frac{1}{2}, \frac{1}{2})$ can be replaced by $e_1 = (2,-1,1)$. **(2)** Since we got *three* basis vectors for $\operatorname{span}(v_1, v_2, v_3, v_4)$, we have that this span is 3-dimensional. Since $V = \mathbb{R}^3$ also is 3-dimensional, we have $\operatorname{span}(v_1, v_2, v_3, v_4) = V$. **(3)** No, from the results of point 1 and 2, and from Algorithm 14.19 we can only deduce a basis for the row space, but not *which ones* of the spanning vectors are independent. **(4)** The vectors v_1, v_2, v_3 are linearly dependent because $\begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{bmatrix} 2 & -1 & 1 \\ -4 & 2 & -2 \\ 1 & 0 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{bmatrix}$ (the last row is totally zero). **(5)** $[v_1 v_2 v_3 v_4] = \begin{bmatrix} 2 & -4 & 1 & 0 \\ -1 & 2 & 0 & -2 \\ 1 & -2 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & \frac{1}{2} & 0 \\ 0 & 0 & 1 & -4 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. The pivot are in columns $1,3,4$. So as a maximal linearly independed vectors we may take v_1, v_3, v_4. Yes, they span the same subspace as the basis e_1, e_2, e_3 found in point 1. **(6)** Bring to redeuced row-echelon form: $[v_1 v_2 v_3 v_4\, u] = \begin{bmatrix} 2 & -4 & 1 & 0 & 7 \\ -1 & 2 & 0 & -2 & 7 \\ 1 & -2 & 2 & 1 & 7 \end{bmatrix} \sim \begin{bmatrix} 1 & -2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 5 \\ 0 & 0 & 0 & 1 & -4 \end{bmatrix}$. From where we have $u = v_1 + 5v_3 - 4v_4$. **E.14.11.** **(1)** $\begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ 1 & 1 & 4 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = R$, and as a basis for U we can take the non-zero rows of R, i.e., $e_1 = (1,0,2,1)$, $e_2 = (0,1,2,0)$, $e_3 = (0,0,1,-1)$. We have $\dim(U) = 3$, so $U \neq V$. **(2)** We have $\begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ 1 & 1 & 4 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$, and the vectors u_1, u_2, u_3 are linearly dependent. Therefore, $\operatorname{span}(u_1, u_2, u_3) \neq U$. **(3)** We compute $[u_1 u_2 u_3 u_4] = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 2 & 2 & 4 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Since the pivots are in 1'st, 2'nd and 4'th columns, a maximal independent subset is $\{u_1, u_2, u_4\}$. It spans the same subspace. **E.14.12.** **(2)** We have $[e_1\, e_2\, e_3\, w] = \begin{bmatrix} 2 & 0 & 1 & 4 \\ 1 & 1 & 0 & 3 \\ 0 & 2 & 1 & 6 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{bmatrix}$, from where we get $[w]_E = (1,2,2)$. **E.14.14.** **(1)** Using Algorithm 14.24 we find that $v_1 = 2u_1 + 3u_2$ and $v_2 = u_1 - 2u_2$. **(2)** Therefore $\operatorname{row}(A) = \operatorname{row}(B)$ because $\operatorname{row}(B) \subseteq \operatorname{row}(A)$ by the previous point, and $\operatorname{row}(A)$, $\operatorname{row}(B)$ *both* are of dimension 2. **(3)** Since $\operatorname{row}(A) = \operatorname{row}(B)$, then by Theorem 14.15 we have $A \sim B$. **(4)** We have found that $v_1 = 2u_1 + 3u_2$ and $v_2 = u_1 - 2u_2$. Thus, using the steps of proof for Theorem 14.15 we get v_1 by applying the elementary operations $2 \cdot R1$, $R1 + 3R2$ to the matrix A. Doing this we get a new matrix $C = \begin{bmatrix} v_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} -1 & 3 & 7 \\ -1 & 1 & 1 \end{bmatrix}$. Using Algorithm 14.24 we find $v_2 = \frac{1}{2}v_1 - \frac{7}{2}u_2$. Therefore, to get v_2 from the rows of the matrix C we perform the elementary operations $v_2 = \frac{1}{2}v_1 - \frac{7}{2}u_2$. We get v_2 by applying the elementary operations $\frac{1}{2} \cdot R2$, $R2 - \frac{7}{2}R2$ to the matrix C. Thus the final chain of elementary operations reducing A to B is $2\cdot R1,\ R1+3R2,\ \frac{1}{2}\cdot R2,\ R2-\frac{7}{2}R2$. **(5)** Since $\mathrm{row}(A)=\mathrm{row}(B)$, then by Theorem 14.15 we have $\mathrm{rref}(A)=\mathrm{rref}(B)$. **(6)** Bring A and B to their reduced row-echelon forms. By previous point that will be the same matrix $\mathrm{rref}(A)=\mathrm{rref}(B)$. Thus, we can take the operations used to go from B to D, and use the reverses of the same operations, written in the reverse order. We don't write the details here because such calculations were done earlier. **E.15.1**. Since $\mathrm{rref}(A)=\begin{bmatrix}\mathbf{1}&-2&0&0&-1\\0&0&\mathbf{1}&0&0\\0&0&0&\mathbf{1}&1\end{bmatrix}$, $U=\mathrm{null}(A)$ is 2-dimensional. As a basis of U we can take $e_1=\begin{bmatrix}-2\\-1\\0\\0\\0\end{bmatrix}$, $e_2=\begin{bmatrix}-1\\0\\0\\1\\-1\end{bmatrix}$. **E.15.2**. See solution steps for Exercise E.15.3. **E.15.3**. Since $\mathrm{rref}(\bar{A})=\begin{bmatrix}\mathbf{1}&0&-1&-1&0&-5\\0&\mathbf{1}&0&1&0&12\\0&0&0&0&\mathbf{1}&-8\end{bmatrix}$, the subspace of solutions of the homogeneous system is 2-dimensional, and a basis for it is $e_1=\begin{bmatrix}-1\\0\\-1\\0\\0\end{bmatrix}$, $e_2=\begin{bmatrix}-1\\1\\0\\-1\\0\end{bmatrix}$. As a single solution of the system we can take $v_0=\begin{bmatrix}-5\\12\\0\\0\\-8\end{bmatrix}$. Then the general solution of the system is $\alpha_1e_1+\alpha_2e_2+v_0$ with $\alpha_1,\alpha_2\in\mathbb{R}$. **E.15.5**. **(1)** Since $A=\begin{bmatrix}-2&2&0&2&0\\1&-1&1&0&3\\0&0&1&-1&1\end{bmatrix}\sim\begin{bmatrix}1&-1&0&0&1\\0&0&1&0&2\\0&0&0&1&1\end{bmatrix}=\mathrm{rref}(A)$, we have $\mathrm{nullity}(A)=2$ (because $\mathrm{null}(A)$ has *two* non-pivot columns). **(2)** Since nullity of A is 2, the rank of A is $n-\mathrm{nullity}(A)=5-2=3$. **(3)** Using the non-pivot columns of the matrix $\mathrm{rref}(A)$ found in point (1) we have $e_1=\begin{bmatrix}-1\\-1\\0\\0\\0\end{bmatrix}$, $e_2=\begin{bmatrix}1\\0\\2\\1\\-1\end{bmatrix}$ (we can repace e_1 by $-e_1$ to avoid the "$-$" sign). **(4)** Yes, the system $AX=B$ is consistent because $\mathrm{rank}(A)=3$. Since the augmented matrix $\bar{A}$ cannot have more than 3 linearly independent rows, $\mathrm{rank}(\bar{A})=3=\mathrm{rank}(A)$. **(5)** We have $\bar{A}=\begin{bmatrix}-2&2&0&2&0&2\\1&-1&1&0&3&3\\0&0&1&-1&1&4\end{bmatrix}\sim\begin{bmatrix}1&-1&0&0&1&-1\\0&0&1&0&2&4\\0&0&0&1&1&0\end{bmatrix}=\mathrm{rref}(\bar{A})$. We already know the vectors e_1, e_2 from the point (3). To find a solution v_0 use the last column of $\mathrm{rref}(\bar{A})$. We have $v_0=\begin{bmatrix}-1\\0\\4\\0\\0\end{bmatrix}$. The general solution is $\mathrm{null}(A)+v_0=\mathrm{span}(e_1,e_2)+v_0=\{\alpha e_1+\beta e_2+v_0\mid\alpha,\beta\in\mathbb{R}\}$. **E.16.1**. By Algorithm 16.1 we have $U=W$. **E.16.3**. **(1)** Define the matrices A and B consisting of the coordinates of the vectors A_1,A_2,A_3 and B_1,B_2 respectively: $A=\begin{bmatrix}1&-1&0\\0&1&1\\-1&1&0\\0&2&2\end{bmatrix}$ and $B=\begin{bmatrix}-1&0\\3&3\\1&1\\6&0\end{bmatrix}$. In order to find a basis for $U+W$ we need the row-echelon form of the block matrix $[A|B]$. However, since in the next step we are going to find $U\cap W$, we need the *reduced* row-echelon form of $[A|-B]$, to shorten the calculations let us in the first step find the row-echelon form of $[A|-B]$ (we can do that since $\mathrm{span}(B_1,B_2)=\mathrm{span}(-B_1,-B_2)$). We have $[A|-B]=\begin{bmatrix}1&-1&0&1&0\\0&1&1&-3&-3\\-1&1&0&-1&-1\\0&2&2&-6&0\end{bmatrix}\sim\begin{bmatrix}1&-1&0&1&0\\0&1&1&-3&-3\\0&0&0&0&1\\0&0&0&0&0\end{bmatrix}$. So $\dim(U+W)=3$, and $U+W$ has a basis $\{A_1,A_2,B_2\}$. It also is clear from here that A_3 is a linear combination of A_1 and A_2, and we can drop the third column of our matrix before we calculate the *reduced* row echelon form. $\begin{bmatrix}1&-1&1&0\\0&1&-3&-3\\0&0&0&1\\0&0&0&0\end{bmatrix}\sim\begin{bmatrix}\mathbf{1}&0&-2&0\\0&\mathbf{1}&-3&0\\0&0&0&\mathbf{1}\\0&0&0&0\end{bmatrix}$. As a basis for 1-dimensional null space take the single vector $e=\begin{bmatrix}-2\\-3\\-1\\0\end{bmatrix}$. It is simpler to use its *last* two coordinates (rather than the *first* two coordinates) to find a single basis vector for the 1-dimensional intersection $U\cap W$. Namely, the vector $-1\cdot B_1+0\cdot B_2$. Clearly, the first coefficient -1 can be ignored in this case, and as a basis for $U\cap W$ we may take $\{B_1\}$. **(2)** By Theorem 16.14 we have $3=\dim(U+W)=\dim(U)+\dim(W)-\dim(U\cap W)=2+2-1$. By Theorem 16.21 the sum $U+W$ is *not* direct since $U\cap W$ is not zero. **E.16.4**. No. **E.16.7**. **(1)** As a basis for U we get a maximal linearly independent subset of $\{u_1,u_2,u_3,u_4\}$, namely, the subset $\{u_1,u_3\}$. So $\dim(U)=2$. Clearly, $\dim(V)=1$. Since the bases for W and Y are given directly, we have $\dim(W)=3$ and $\dim(Y)=2$. Since the only two subspaces with equal dimensions are U,Y, we apply the algorithm for this pair *only*. We have $\begin{bmatrix}u_1\\u_3\end{bmatrix}=\begin{bmatrix}1&0&0&1\\1&1&0&0\end{bmatrix}\sim\begin{bmatrix}1&0&0&1\\0&1&0&-1\end{bmatrix}$ and $\begin{bmatrix}5&2&0&3\\2&1&0&1\end{bmatrix}\sim\begin{bmatrix}1&0&0&1\\0&1&0&-1\end{bmatrix}$. Thus, $U=Y$, and all *other* subspaces are *not* equal to each other. **(2)** None of U,V or Y may contain W because they have lower dimension than W. Using the algorithm we get that W contains Y

as a subspace. Since $U = Y$, we get that W contains U. Since the basis vector u_4 of V is in U, we get that W also contains V as a subspace. **E.16.8**. **(1)** Compute, say, the basis $\{u_1, u_2, w_2\}$ for $U + W$. Since $\dim(U + W) = 3$, we have that $U + W$ is equal to $\mathbb{R}^3$. By Theorem 15.12 we have that the dimension of the intersection $U \cap W$ is $2+2-3 = 1$. So, yes, it is a *line*. **(2)** As a maximal linearly independent subset of $\{w_1, w_2, w_3\}$ we can take $\{w_1, w_2\}$. Therefore, we have $[A \mid -B] = \left[\begin{smallmatrix} 0 & 2 & -2 & 0 \\ 1 & 0 & -2 & 0 \\ 1 & 1 & -3 & -1 \end{smallmatrix}\right]$. To get a basis for its null space compute the reduced row-echelon form $\left[\begin{smallmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$. Its null space is 1-dimensional, and has a basis vector $\left[\begin{smallmatrix} -2 \\ -1 \\ -1 \\ 0 \end{smallmatrix}\right]$ or, equivalently, $\left[\begin{smallmatrix} 2 \\ 1 \\ 1 \\ 0 \end{smallmatrix}\right]$. Using its first two coordinates $2, 1$ we get a basis vector for the line $U \cap W$ as $2u_1 + u_2 = (2, 2, 3)$. Now let us apply the free columns method. As some row-echelon form for $[A \mid -B]$ take, say, $\left[\begin{smallmatrix} 1 & 0 & -2 & 0 \\ 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$. Then we have the matrix $C = [0\ 1]$ which already is in reduced row-echelon form. Its nullity is 1, and as a basis vector of its null space we take $e = \left[\begin{smallmatrix} -1 \\ 0 \end{smallmatrix}\right]$ or, equivalently $e = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$. Using its coordinates $1, 0$ we get a basis vector for the line $U \cap W$ as $1 \cdot w_1 + 0 \cdot w_2 = (2, 2, 3)$. **E.16.11**. **(1)** Take $U_1 = \operatorname{span}(x^3)$, $U_2 = \operatorname{span}(x^2)$, $U_3 = \operatorname{span}(x)$, $U_4 = \operatorname{span}(1)$. **(2)** Take $U_1 = \operatorname{span}(x^3)$, $U_2 = \operatorname{span}(x^3 + x^2)$, $U_3 = \operatorname{span}(x^3 + x)$, $U_4 = \operatorname{span}(x^3 + 1)$. **E.16.12**. No, because the sum of dimensions of these *four* subspaces must be equal to $3 = \dim(\mathbb{R}^3)$.

Part 6. Determinants and their Applications.

E.17.4. **(1)** No, because the matrix multiplication is *not* commutative, and the products, say, $E_1E_2E_3$ and $E_3E_1E_2$ may be different. **(2)** Yes, because regardless the order of E_1, E_2, E_3 in factorization, we have $\det(A) = \det(E_1) \cdot \det(E_2) \cdot \det(E_3)$. **E.17.5**. $\det(M^{-1}) = (\det M)^{-1} = (-2)^{-1} = -0.5$; $\det(L^{-1}) = (\det L)^{-1} = (1)^{-1} = 1$; $\det(K^T) = \det K = -5$; $\det(M\,M^{-1}M^T\,M) = (-2)(-2)^{-1}(-2)(-2) = 4$. **E.18.1**. $\det(A) = 15$, $\det(B) = -2i$, $\det(C) = 2$. **E.18.4**. **(1)** If we in A start by operations $C1 \leftrightarrow C3$, $C2 \leftrightarrow C3$, then there will remain only *one* non-zero entry below the diagonal. If we in B start by operations $C1 \leftrightarrow C4$, $R1 \leftrightarrow R4$, then there will remain only *two* non-zero entry below the diagonal. **(2)** Expand A by the 3'rd column and B by the 4'th column. We have $\det(A) = 2(-1)^{1+3}A_{1,3} = 2\left|\begin{smallmatrix} 1 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{smallmatrix}\right| = 2 \cdot 1(-1)^{1+1}\left|\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right| = 2(2-1) = 2$. Next, we have $\det(B) = 3(-1)^{4+4}A_{4,4} = 3\left|\begin{smallmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \end{smallmatrix}\right| = 3\left|\begin{smallmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & \frac{1}{2} \end{smallmatrix}\right| = 3 \cdot 2(-1)^{1+1}\left|\begin{smallmatrix} 1 & 2 \\ 1 & \frac{1}{2} \end{smallmatrix}\right| = 6 \cdot (-\frac{3}{2}) = -9$. **E.19.1**. Since $d = \det(A) = \left|\begin{smallmatrix} 1 & 2 & 1 \\ 3 & 1 & 2 \\ 1 & 3 & 1 \end{smallmatrix}\right| = 1 \neq 0$, the system has a unique solution which can be calculated by Cramer's Rule. We have $d_1 = \det(A_1) = \left|\begin{smallmatrix} 3 & 2 & 1 \\ 1 & 1 & 2 \\ 4 & 3 & 1 \end{smallmatrix}\right| = -2$, $d_2 = \det(A_2) = \left|\begin{smallmatrix} 1 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 4 & 1 \end{smallmatrix}\right| = 1$, $d_3 = \det(A_3) = \left|\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 1 \\ 1 & 3 & 4 \end{smallmatrix}\right| = 3$. The unique solution is: $\left(\frac{-2}{1}, \frac{1}{1}, \frac{3}{1}\right) = (-2, 1, 3)$. **E.19.2**. $\det(A) = 6$. Thus v_1, v_2, v_3, v_4 are linearly independent according to Lemma 19.3, and A is invertible by Corollary 14.14. **E.19.4**. **(1)** Since $\det(A) = 2 \neq 0$, the rows of A are linearly independent. Since $\det(B) = -9 \neq 0$, the columns of B are linearly independent. **(2)** Since $\det(A) \neq 0$ and $\det(B) \neq 0$, the matrices A and B are invertible. Hence A^{100} and B^{1000} also are invertible. Therefore, $\dim(\mathrm{col}(\mathrm{A}^{100})) = \dim(\mathrm{row}(\mathrm{B}^{1000})) = 4$.

Part 7. Linear Transformations.

E.20.1. **(1)** T is a linear transformation. **(2)** T is *not* a linear transformation since the condition, say, $T(2v) = 2T(v)$ fails for $v = (1, 1)$. **(3)** T is a linear transformation. **E.20.3**. For the first two points we use standard bases. **(1)** $[T]_E = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 3 \\ 3 & 0 \end{smallmatrix}\right]$. **(2)** $[T]_E = \left[\begin{smallmatrix} 0 & 2 & 2 \\ 3 & 0 & 0 \end{smallmatrix}\right]$. **(3)** In the basis $E = \{1, x, x^2\}$ we have $[T]_E = \left[\begin{smallmatrix} 0 & 3 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{smallmatrix}\right]$. **E.20.4**. **(1)** Since $T(1, 0) = T(e_1)$, we know the vector $T(e_1) = (3, 2, 1)$. Next $T(e_2) = T(0, 1) = T((1, 1) - (1, 0)) = (-1, 0, 1) - (3, 2, 1) = (-4, -2, 0)$. Therefore, $A = [T] = [T(e_1)\ T(e_2)] = \left[\begin{smallmatrix} 3 & -4 \\ 2 & -2 \\ 1 & 0 \end{smallmatrix}\right]$. **(2)** We have $T(e_1) = T(1, 0, 0) = (1, 0, -1)$, $T(e_2) = T(0, 1, 0) = (0, 0, 1)$, $T(e_3) = T(0, 0, 1) = (1, 3, 0)$. Therefore, $A = [T] = [T(e_1)\ T(e_2)\ T(e_3)] = \left[\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 0 & 3 \\ -1 & 1 & 0 \end{smallmatrix}\right]$. **(3)** We have $T(e_1) = T(1, 0, 0) = (0, 1, 0)$, $T(e_2) = T(0, 1, 0) = (0, 1, 0)$, $T(e_3) = T(0, 0, 1) = (0, 1, 0)$. Therefore, $A = [T] = [T(e_1)\ T(e_2)\ T(e_3)] = \left[\begin{smallmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right]$. **(4)**

We have $T(e_1) = T(1) = 3$ with coordinates $(3,0,0,0)$. $T(e_2) = T(x) = 3x+1$ with coordinates $(1,3,0,0)$. $T(e_3) = T(x^2) = 3x^2+2x$ with coordinates $(0,2,3,0)$. $T(e_4) = T(x^3) = 3x^3 + 3x^2$ with coordinates $(0,0,3,3)$. Therefore, $A = [T] = [T(e_1)\ T(e_2)\ T(e_3)\ T(e_4)] = \begin{bmatrix} 3&1&0&0\\0&3&2&0\\0&0&3&3\\0&0&0&3 \end{bmatrix}$.

E.20.8. **(1)** Since $P = P_{EG} = \begin{bmatrix} 1&-1\\1&1 \end{bmatrix}$ and its inverse is $P^{-1} = P_{GE} = \begin{bmatrix} \frac{1}{2}&\frac{1}{2}\\-\frac{1}{2}&\frac{1}{2} \end{bmatrix}$, we have $[T]_G = P^{-1}\begin{bmatrix} 0&1\\2&1 \end{bmatrix}P = \begin{bmatrix} 2&0\\1&-1 \end{bmatrix}$. **(2)** $[S]_E = P\begin{bmatrix} 3&2\\0&1 \end{bmatrix}P^{-1} = \begin{bmatrix} 1&2\\0&3 \end{bmatrix}$. **E.20.9**. **(1)** We have $T(g_1) = (3,0,1) = 3g_1 + 10g_2 - 3g_3$, $T(g_2) = (0,2,0) = -2g_1 - 12g_2 + 4g_3$, $T(g_3) = (2,6,0) = -4g_1 - 30g_2 + 10g_3$. Putting these coefficients by columns we get the matrix $B = [T]_G = \begin{bmatrix} 3&-2&-4\\10&-12&-30\\-3&4&10 \end{bmatrix}$. **(2)** Clearly, $A = [T]_E = \begin{bmatrix} 1&1&0\\0&0&2\\1&-1&0 \end{bmatrix}$. We have $P = P_{EG} = \begin{bmatrix} 2&0&1\\1&0&1\\0&1&3 \end{bmatrix}$ and $P^{-1} = \begin{bmatrix} 1&-1&0\\3&-6&1\\-1&2&0 \end{bmatrix}$. Thus $B = P^{-1}AP = \begin{bmatrix} 3&-2&-4\\10&-12&-30\\-3&4&10 \end{bmatrix}$. **E.20.10**. **(1)** We have $T\begin{bmatrix} 1\\0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2\\4 \end{bmatrix} = \begin{bmatrix} 1\\2 \end{bmatrix}$ and $T\begin{bmatrix} 0\\1 \end{bmatrix} = T\begin{bmatrix} 1\\1 \end{bmatrix} - T\begin{bmatrix} 1\\0 \end{bmatrix} = \begin{bmatrix} 6\\2 \end{bmatrix} - \begin{bmatrix} 1\\2 \end{bmatrix} = \begin{bmatrix} 5\\0 \end{bmatrix}$. Thus, $A = [T]_E = \begin{bmatrix} 1&5\\2&0 \end{bmatrix}$. Clearly, $P = P_{EG} = \begin{bmatrix} -2&1\\3&-1 \end{bmatrix}$. Then $P^{-1} = \begin{bmatrix} 1&1\\3&2 \end{bmatrix}$, and $B = [T]_G = P^{-1}AP = \begin{bmatrix} 9&-2\\31&-8 \end{bmatrix}$. **(2)** On the other hand, from $A = \begin{bmatrix} 1&5\\2&0 \end{bmatrix}$ we have the form $T(x,y) = (x+5y,\ 2x)$. From there $T(g_1) = T\begin{bmatrix} -2\\3 \end{bmatrix} = \begin{bmatrix} 13\\-4 \end{bmatrix}$ and $T(g_2) = T\begin{bmatrix} 1\\-1 \end{bmatrix} = \begin{bmatrix} -4\\2 \end{bmatrix}$. It is easy to compute that $\begin{bmatrix} 13\\-4 \end{bmatrix} = 9g_1 + 31g_2$ and $\begin{bmatrix} -4\\2 \end{bmatrix} = -2g_1 - 8g_2$. Then we again get $B = [T]_G = \big[[T(g_1)]_G\ [T(g_2)]_G\big] = \begin{bmatrix} 9&-2\\31&-8 \end{bmatrix}$. **E.21.2**. $\ker(T)$ is equal to the subspace U of constant polynomials. Indeed, $\ker(T) \subseteq U$ since for any non-constant polynomial $f(x)$ we have $T(f(x)) = 2f'(x) + f''(x) \neq 0$. And evidently $U \subseteq \ker(T)$. range(T) is equal to the subspace $\mathcal{P}_1(\mathbb{R})$. Indeed, for any $g(x) = ax + b \in \mathcal{P}_1(\mathbb{R})$ we have a polynomial $f(x) \in P_2(\mathbb{R})$ such that $T(f(x)) = g(x)$. Take $f(x) = \frac{1}{2}\int g(x)dx + \int\big[\int g(x)dx\big]dx$. Also, evidently range$(T) \subseteq \mathcal{P}_1(\mathbb{R})$. **E.21.3**. The matrix of T in basis $E = \{1, x, x^2\}$ is $A = [T]_E = \begin{bmatrix} 0&2&2\\0&0&4\\0&0&0 \end{bmatrix}$. Then rref$(A) = \begin{bmatrix} 0&1&0\\0&0&1\\0&0&0 \end{bmatrix}$, from where rank$(T) = 2$ and nullity$(T) = 3 - 2 = 1$. The basis for $\ker(T)$ is obtained using the first (free) column of rref(A), i.e., $\ker(T)$ is the subspace of constant polynomials (we get this using $\begin{bmatrix} -1\\0\\0 \end{bmatrix}$ and Algorithm 15.2). The basis vectors $e_1(x) = 2$ and $e_2(x) = 2+4x$ for range(T) are obtained using the two last columns of A (see Algorithm 21.9). It is easy to see that the polynomials $e_1(x) = 2$ and $e_2(x) = 2+4x$ span $\mathcal{P}_1(\mathbb{R})$. **E.22.1**. **(2)** The matrix of $2T+S$ is $2A+B = \begin{bmatrix} 4&0&1\\0&5&0\\0&1&1 \end{bmatrix}$. **(3)** The matrix of ST^2 is $BA^2 = \begin{bmatrix} 0&0&0\\0&3&0\\0&1&0 \end{bmatrix}$. **(4)** T and S are not invertible since their matrices have zero determinant. $2T+S$ is invertible since $\det(2A+B) = 20 \neq 0$. The product ST^2 also is not invertible. **E.22.2**. The transformation has the matrix $A = \begin{bmatrix} 0&3&0&0\\2&0&0&0\\0&0&0&1\\0&0&2&0 \end{bmatrix}$. Since rank$(A) = 4$, the transformation T is invertible. **E.22.3**. Each invertible matrix has a non-zero determinant. The determinant of any product of such matrices also is non-zero. **E.22.4**. **(1)** Since $S = (T^2)^{-1}$, we have $B = (A^2)^{-1}$, and so $B = \begin{bmatrix} 1&-1&-0\\0&1&-1\\0&-1&2 \end{bmatrix}$. By definition $C = \begin{bmatrix} 1&-1&0\\0&1&1\\1&0&1 \end{bmatrix}$. **(2)** $[LST] = CBA = \begin{bmatrix} 1&0&-2\\0&1&0\\1&1&-2 \end{bmatrix}$, $[TSL] = ABC = \begin{bmatrix} 0&-1&-1\\1&0&1\\-1&1&0 \end{bmatrix}$, $[S^{-1}] = B^{-1} = \begin{bmatrix} 1&2&1\\0&2&1\\0&1&1 \end{bmatrix}$. **(3)** L^{100} is not invertible because $\det(C) = 0$ and, thus, also $\det(C^{100}) = 0$. The transformation $(TS)^{100}$ is invertible because T and S are invertible. Also, $TS = T(T^2)^{-1} = T^{-1}$. We could also notice that $\det((TS)^{100}) \neq 0$. $(100\,T)^{-1}$ is invertible because T is invertible. **E.22.5**. *Hints*: $[R] = \frac{1}{2}\begin{bmatrix} \sqrt{3}&-1\\1&\sqrt{3}\\&&2 \end{bmatrix}$, $[S] = \begin{bmatrix} 0&0&2\\1&-1&0\\1&0&0 \end{bmatrix}$, $[P] = \begin{bmatrix} 1&0&0\\0&1&0\\0&0&0 \end{bmatrix}$. Since R^6 rotates V around Oz by $180°$, i.e., it sends e_1 to $-e_1$ and e_2 to $-e_2$, it is immediately clear that $[R^6] = \begin{bmatrix} -1&0&0\\0&-1&0\\0&0&1 \end{bmatrix}$. It is easy to figure out that $P^{120} = P$ and $R^{12} = I$.

Part 8. Eigenvectors and Diagonalization.

E.23.1. **(3)** Only $w = (0,2,0)$ is an eigenvector. **E.23.2**. The only eigenvalue is $\lambda = 0$. As an eigenvector we can take any non-zero constant function, since $T(c) = (-5)\cdot c' = 0 = \lambda \cdot c$. **E.23.3**. $\det(A - \lambda I) = -\lambda^3 + 7\lambda^2 - 14\lambda + 8$, and its roots (eigenvalues) are $\{1,2,4\}$. $\det(B - \lambda I) = -\lambda^3 + 7\lambda^2 - 16\lambda + 12$, and its roots (eigenvalues) are $\{2,3\}$. $\det(C - \lambda I) = -\lambda^3 + 8\lambda^2 - 21\lambda + 18$, and its roots (eigenvalues) are $\{2,3\}$. **E.23.4**. **(1)** T has *three* distinct eigenvalues $1,2,4$. Each is of geometric multiplicity 1. The eigenspace E_1 has the basis $\{v_1\}$ with $v_1 = (-2,1,1)$. The eigenspace E_2 has the basis $\{v_2\}$ with $v_2 = (-2,1,2)$. The eigenspace E_4

has the basis $\{v_3\}$ with $v_3 = (0,1,0)$. **(2)** T has eigenvalues $2,3$. Of which 2 has geometric multiplicity two, and 3 has geometric multiplicity one. The eigenspace E_2 has the basis $\{v_1,v_2\}$ with $v_1 = (0,1,0)$, $v_2 = (-1,0,1)$. The eigenspace E_3 has the basis $\{v_3\}$ with $v_3 = (-1,2,0)$. **(3)** T has eigenvalues $2,3$. Each has geometric multiplicity one. The eigenspace E_2 has the basis $\{v_1\}$ with $v_1 = (-1,2,0)$. The eigenspace E_3 has the basis $\{v_2\}$ with $v_2 = (0,1,0)$. **E.23.5.** **(1)** $A = \begin{bmatrix} 1&0&0&0\\ 1&2&0&0\\ 0&0&1&0\\ 0&0&-1&3 \end{bmatrix}$. **(2)** Only v_1 is an eigenvector for $\lambda = 1$. **(3)** The characteristic polynomial is $f(\lambda) = |A-\lambda I| = (1-\lambda)^2(2-\lambda)(3-\lambda)$ (there is no need to open the brackets, as we need the roots only). The roots, i.e., the eigenvalues are $\lambda = 1,\ 2,\ 3$. **(4)** Detect a basis for eigenspace E_1. We have $A-\lambda I = A - I = \begin{bmatrix} 0&0&0&0\\ 1&1&0&0\\ 0&0&0&0\\ 0&0&-1&2 \end{bmatrix} \sim \begin{bmatrix} 1&1&0&0\\ 0&0&1&-2\\ 0&0&0&0\\ 0&0&0&0 \end{bmatrix} = \operatorname{rref}(A-I)$. Thus, the geometric multiplicity of $\lambda = 1$ is $\dim(E_1) = \operatorname{nullity}(A-I) = 4-2 = 2$. Using $\operatorname{rref}(A-I)$ we can find a basis for $E_1 = \operatorname{null}(A-I)$ as follows: $v_1 = (1,-1,0,0)$ and $v_2 = (0,0,2,1)$. The geometric multiplicity of $\lambda = 2$ is 1. As the basis vector for E_2 take $u = (0,1,0,0)$. The geometric multiplicity of $\lambda = 3$ is 1. As the basis vector for E_3 take $w = (0,0,0,1)$. **E.23.6.** **(1)** The third row of the matrix of T is $\begin{bmatrix} 0\\0\\5 \end{bmatrix}$, i.e., T just scales the vector $e_3 = \begin{bmatrix} 0\\0\\1 \end{bmatrix}$ by 5 times. So e_3 is an eigenvector, $\lambda = 5$ is an eigenvalue for T. Clearly, $S(d) = d$ (d is not affected by the rotation). So for S the vector d is an eigenvector, $\lambda = 1$ is an eigenvalue. From $L(x,y,z) = (2x-z,\ 3y,\ -x+2z)$ it is evident that if the first and third coordinates of a vector are zero, then the vector is scaled by 3 times by L. Say, $e_2 = \begin{bmatrix} 0\\1\\0 \end{bmatrix}$ is an eigenvector, $\lambda = 3$ is an eigenvalue for L. **(2)** The characteristic polynomial for T is $f_1(\lambda) = -\lambda^3 + 9\lambda^2 - 15\lambda - 25$. The characteristic polynomial for S is $f_2(\lambda) = -\lambda^3 + 1$. The characteristic polynomial for L is $f_3(\lambda) = -\lambda^3 + 7\lambda^2 - 15\lambda + 9$. **(3)** These polynomials are *cubic*, but you can reduce the solution to *quadratic* equations, if you notice that for each polynomial you have one root already. For example, we know that 5 is a root for $f_1(\lambda)$, since it is an eigenvalue for T. So we can divide $f_1(\lambda)$ by $\lambda - 5$ to get $f_1(\lambda) = (\lambda-5)(-\lambda^2+4\lambda+5)$. Solving the *quadratic* equation $-\lambda^2 + 4\lambda + 5 = 0$ we get its roots $\lambda = -1$ and $\lambda = 5$ (i.e., 5 is a root of multiplicity 2 for $f_1(\lambda)$). $f_2(\lambda)$ has only one root $\lambda = 1$ (of multiplicity 1). $f_3(\lambda)$ has the roots $\lambda = 1,3$ (where 3 is a root of multiplicity 2). **(4)** Answers only are given (please do the actual calculations using null spaces). For T we have the eigenvalues $\lambda = -1,5$. There are two eigenspaces: $E_{-1} = \operatorname{span}\big((-1,1,0)\big)$ and $E_5 = \operatorname{span}\big((1,1,0),\,(0,0,1)\big)$ (the geometric multiplicities are 1 and 2). For S we have the eigenvalue $\lambda = 1$. There is an only eigenspace: $E_1 = \operatorname{span}\big((1,1,1)\big)$, i.e., the line ℓ (the geometric multiplicity is 1). For L we have the eigenvalues $\lambda = 1,3$. There are two eigenspaces: $E_1 = \operatorname{span}\big((1,0,1)\big)$ and $E_3 = \operatorname{span}\big((0,1,0),\,(-1,0,1)\big)$ (the geometric multiplicities are 1 and 2). **E.24.1.** A is not similar to the others since it is of rank 2, while the others are of rank 3. B is not similar to the others since it is the only one with determinant -5. The matrices C and D both have the same rank 3 and the same determinant 30. However, their characteristic polynomials and eigenvalues are not the same. **E.24.3.** In answer to point (1) of Exercise E.23.4 we saw that T has three distinct eigenvalues $1,2,4$ each is of geometric multiplicity one. We also computed $v_1 = (-2,1,1)$, $v_2 = (-2,1,2)$, $v_3 = (0,1,0)$ each forming a basis for respective eigenspace. Since $V = \mathbb{R}^3$ is 3-dimensional, $G = \{v_1,v_2,v_3\}$ is a basis for V, and in G the transformation T has the diagonal form $D = \begin{bmatrix} 1&0&0\\ 0&2&0\\ 0&0&4 \end{bmatrix}$. The change of basis matrix $P = P_{EG}$ for presentation $D = P^{-1}AP$ is the matrix $P = \begin{bmatrix} -2&-2&0\\ 1&1&1\\ 1&2&0 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}$. **(2)** In answer to point (2) of Exercise E.23.4 we saw that T has eigenvalues $2,3$ of which 2 is of geometric multiplicity two, and 3 is of geometric multiplicity one. E_2 has a basis consisting of $v_1 = (0,1,0)$, $v_2 = (-1,0,1)$. And E_3 has a basis consisting of $v_3 = (-1,2,0)$. Since $V = \mathbb{R}^3$ is 3-dimensional, $G = \{v_1,v_2,v_3\}$ is a basis for V, and in G the transformation T has the diagonal form $D = \begin{bmatrix} 2&0&0\\ 0&2&0\\ 0&0&3 \end{bmatrix}$. The change of basis matrix $P = P_{EG}$ for presentation $D = P^{-1}BP$ is the matrix $P = \begin{bmatrix} 0&-1&-1\\ 1&0&2\\ 0&1&0 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}$. **(3)** In answer to point (3) of Exercise E.23.4 we saw that T has eigenvalues $2,3$, each with geometric multiplicity one. E_2 has the basis consisting of $v_1 = (-1,2,0)$. The eigenspace E_3 has the basis $\{v_2\}$ with $v_2 = (0,1,0)$. Since the sum 2 of their geometric multiplicities is less than $3 = \dim(V)$, the transformation T is *not* diagonalizable, i.e., there is no presentation $D = P^{-1}CP$. **E.24.4.** **(1)** characteristic polynomial is $\det(A - \lambda I) = -\lambda^3 + 7\lambda^2 - 14\lambda + 8 = -(\lambda-1)(\lambda-2)(\lambda-4)$, and its roots are $\{1,2,4\}$. Each has algebraic *and* geometric multiplicity one. Their sum is $1+1+1 = 3 = \dim(V)$. So A is digitalizable. **(2)** $\det(B-\lambda I) = -\lambda^3 + 7\lambda^2 - 16\lambda + 12 = -(\lambda-2)^2(\lambda-3)$, and its roots are $\{2,3\}$. The root 2 has algebraic *and* geometric multiplicity two. The root 3 has algebraic *and* geometric multiplicity one. Their sum is $2+1 = 3 = \dim(V)$. So B is digitalizable. **(3)** $\det(C-\lambda I) = -\lambda^3 + 8\lambda^2 - 21\lambda + 18 = -(\lambda-2)(\lambda-3)^2$, and its roots are $\{2,3\}$. The root 3 has algebraic multiplicity two, *but* its geometric multiplicity is one. So C is *not* digitalizable. We could establish the same differently, each root has algebraic multiplicity one, and $1+1 \neq 3$. Thus C is *not* digitalizable. **E.24.5.** **(1)** For A we have $f(\lambda) = -\lambda^3 + 12\lambda^2 - 45\lambda + 50$. Roots are easy to find, as we know that one of them is 5 (to see this use Laplace expansion by the 3'rd column of $A - \lambda I$). We have $f(\lambda) = -(\lambda-2)(\lambda-5)^2$. So the eigenvalues are $\lambda_1 = 2$ and $\lambda_2 = 5$. For B we have $f(\lambda) = -\lambda^3 + 4\lambda^2 - 9\lambda + 10$. Roots are easy to find, as we know that one of them is 2. We have $f(\lambda) = -(\lambda-2)(\lambda^2 - 2\lambda + 5)$. So the only eigenvalue is $\lambda_1 = 2$. For C we have $f(\lambda) = -\lambda^3 + 8\lambda^2 - 13\lambda + 6$. Roots are easy to find, as we know that one of them is 1. We have $f(\lambda) = -(\lambda-6)(\lambda-1)^2$. So the eigenvalues are $\lambda_1 = 6$ and $\lambda_2 = 1$. **(2)** For A we have $\dim(E_2) = 1$ and $\dim(E_5) = 1$. Since $1+1 < 3 = \dim(\mathbb{R}^3)$, the matrix A is *not* diagonalizable. For B we have $\dim(E_2) = 1$. Since $1 < 3 = \dim(\mathbb{R}^3)$, the matrix B is *not* diagonalizable. For C we have $\dim(E_6) = 1$ and $\dim(E_1) = 2$. Since $1+2 = 3 = \dim(\mathbb{R}^3)$, the matrix C is *diagonalizable*. **(3)** For A we have that the geometric multiplicity of $\lambda_2 = 5$ is 1, and its algebraic multiplicity is 2. Since $1 < 2$, the matrix A is *not* diagonalizable. Usage of algebraic multiplicity *may* help to shorten the calculations, because after we obtain $1 < 2$, then the geometric multiplicity of $\lambda_1 = 2$ need *not* be computed. For B we have that the algebraic multiplicity of $\lambda_1 = 2$ is 1 (no row-echelon operations are needed to see this). Since $1 \neq 3$, the matrix B is *not* diagonalizable. Usage of algebraic multiplicity really helped to shorten the calculations, because after we obtain $f(\lambda) = -(\lambda-2)(\lambda^2-2\lambda+5)$, no further calculations are needed. For C we have that the geometric *and* algebraic multiplicities of $\lambda_1 = 6$ both are 1 (no row-echelon operations are needed to see this). The geometric *and* algebraic multiplicities of $\lambda_2 = 1$ both are 2 (we need row-echelon operations to find the geometric multiplicity). Since $1+2 = 3$, the matrix C is diagonalizable. Usage of algebraic multiplicity did *not* help much in this case. **(4)** As single basis vector for E_6 take $v = (0,-1,2)$. As basis vectors for E_1 take $u_1 = (3,1,0)$ and $u_2 = (-1,0,1)$ (we can find them as a basis for a null space for $C - 1 \cdot I$). In the eigenbasis $G = \{v, u_1, u_2\}$ we have the diagonal matrix $A = \begin{bmatrix} 6&0&0\\ 0&1&0\\ 0&0&1 \end{bmatrix}$. The change of basis matrix is $P = [v \mid u_1 \mid u_2] = \begin{bmatrix} 0&3&-1\\ -1&1&0\\ 2&0&1 \end{bmatrix}$. We have $P^{-1}CP = D$. **E.24.6.** **(1)** We have $A = \begin{bmatrix} 3&0&0\\ 0&5&2\\ 0&-3&0 \end{bmatrix}$. The characteristic polynomial is $f_1(\lambda) = -\lambda^3 + 8\lambda^2 - 21\lambda + 18 = -(\lambda-2)(\lambda-3)^2$, and the eigenvalues are 2 and 3 (this factorization of $f_1(\lambda)$ is easy to find as we already know A has the eigenvalue 3, we can divide $f_1(\lambda)$ by $\lambda - 3$ to get the remaining quadratic polynomial $-(\lambda-2)(\lambda-3)$). The sum of their geometric multiplicities is $1+2 = 3$, so A is diagonalizable. Next, $B = \begin{bmatrix} 2&-1&1\\ 1&2&0\\ 0&0&2 \end{bmatrix}$. The characteristic polynomial is $f_2(\lambda) = -\lambda^3 + 6\lambda^2 - 13\lambda + 10 = (\lambda-2)(-\lambda^2 + 4\lambda - 5)$, and the only real eigenvalue is 2 (this factorization of $f_2(\lambda)$ is easy to find as we already know B has the eigenvalue 2). Its geometric multiplicities is 1, so A is not diagonalizable. **(2)** Diagonalization is possible for A only. E_2 has the basis $\{(0,-2,3)\}$ and E_3 has the basis $\{(1,0,0),\ (0,-1,1)\}$. So $D = \begin{bmatrix} 2&0&0\\ 0&3&0\\ 0&0&3 \end{bmatrix}$ and $P = \begin{bmatrix} 0&1&0\\ -2&0&-1\\ 3&0&1 \end{bmatrix}$. **(3)** B has only only eigenvalue 2, and its algebraic multiplicity is 1. So the sum of algebraic multiplicities cannot be 3, that is, non-diagonalizability of B follows from this fact, already. No row-elimination operations are needed. **E.24.7.** A is *not* diagonalizable because it has only one eigenvalue $\lambda = 7$ of algebraic multiplicity 2. So the sum of algebraic multiplicities cannot be 4. Next, since $f_2(\lambda) = (\lambda-1)(\lambda+1)(\lambda-2)(\lambda+3)$, the matrix B has four eigenvalues $\lambda = 1, -1, 2, -3$. Each of algebraic multiplicity 1. On the other hand, since each eigenspace is non-zero, its dimension is not 0. The only option we have is that the dimensions of each eigenspace E_1, E_{-1}, E_2, E_{-3} is equal to 1. Since $1+1+1+1 = 4$, B is diagonalizable, and $D = \begin{bmatrix} 1&0&0&0\\ 0&-1&0&0\\ 0&0&2&0\\ 0&0&0&-3 \end{bmatrix}$.

E.25.3. **(1)** There are 8 invariant subspaces. In notation of Example 25.9 these subspaces are: $\{0\}$, U, W, R, $U\oplus W$, $U\oplus R$, $W\oplus R$, $U\oplus W\oplus R=\mathbb{R}^5$. **(2)** When, say, φ is a multiple of π, then U in turn is brakes down to a direct sum of two one-dimensional invariant subspaces. **E.25.4.** The characteristic polynomial of T is $f(\lambda)=\lambda^4$ with only one root $\lambda=0$ (see Example 23.22). As a respective eigenvector v for eigenvalue $\lambda=0$ we can take any non-trivial constant polynomial $v=f(x)=c\neq 0$ (see Example 23.5). Hence for $N=A-0I=T$ we have $\ker(N)=E_0=\operatorname{span}(c)$. The square N^2 has the rank 2 and nullity 2 (see Example 22.6). As easy calculations show the cube N^3 has rank 1 and nullity 3, and N^4 is the identically zero transformation which has rank 0 and nullity 4. So we have the sequence (25.3) as: $\ker(N)\subset\ker\big(N^2\big)\subset\ker\big(N^3\big)\subset\ker\big(N^4\big)=\ker\big(N^5\big)=\cdots$. That is, $r=4$, and the algebraic multiplicity 4 of $\lambda=0$ is achieved by $\dim\big(\big(\ker\big(N^4\big)\big)\big)$. So the decomposition $V=G_\lambda\oplus R$ in this case is $\mathcal{P}_3(\mathbb{R})=\mathcal{P}_3(\mathbb{R})\oplus\{0\}$. **E.25.5.** The characteristic polynomial is $f(\lambda)=(\lambda-3)^2(\lambda+2)^2$ from where we get the eigenvalues $\lambda_1=3$ and $\lambda_2=-2$ both of algebraic multiplicity 2. For $\lambda_1=3$ we have $\operatorname{rank}(N)=3$ and $\operatorname{rank}\big(N^2\big)=2$. I.e., $r=2$, and the algebraic multiplicity is achieved by $\dim\big(\big(\ker\big(N^2\big)\big)\big)=4-\operatorname{rank}\big(N^2\big)=2$. As a basis for $G_{\lambda_1}=G_3=\ker\big(N^2\big)$ we may take the vectors $u_1=(0,0,1,0)$ and $u_2=(1,-2,0,2)$. For $\lambda_2=-2$ we also have $\operatorname{rank}(N)=3$ and $\operatorname{rank}\big(N^2\big)=2$. I.e., $r=2$, and the algebraic multiplicity again is achieved by $\dim\big(\big(\ker\big(N^2\big)\big)\big)=4-\operatorname{rank}\big(N^2\big)=2$. As a basis for $G_{\lambda_2}=G_{-2}=\ker\big(N^2\big)$ we may take the vectors $v_1=(0,1,-2,0)$ and $v_2=(0,0,0,1)$. So the decomposition (25.6) is $\mathbb{R}^4=\operatorname{span}(u_1,u_2)\oplus\operatorname{span}(v_1,v_2)$.

Part 9. Inner Product Spaces and Orthogonality.

E.27.2. **(1)** You need drop the vector v_3. **(2)** Multiply each vector by the inverse of its length. **(3)** Yes, because the transpose of an orthogonal matrix is orthogonal. **E.27.3.** The Gram-Schmidt process outputs the vectors $e_1=(\frac{1}{\sqrt2},0,-\frac{1}{\sqrt2},0)$, $e_2=(0,1,0,0)$, $e_3=(0,0,0,-1)$, $e_4=(\frac{1}{\sqrt2},0,\frac{1}{\sqrt2},0)$. **E.27.4.** By Gram-Schmidt process we get $e_1=\big(\frac{1}{\sqrt2},0,-\frac{1}{\sqrt2}\big)$, $e_2=\big(\frac{1}{\sqrt6},\frac{\sqrt2}{\sqrt3},\frac{1}{\sqrt6}\big)$, $e_3=\big(\frac{1}{\sqrt3},\frac{1}{\sqrt3},\frac{1}{\sqrt3}\big)$. **E.29.3.** Consider the scaling transformation $T(x,y)=(2x,2y)$ on $\mathbb{R}^2$. Does it preserve the angles between vectors? **E.29.4.** (1) The transfarmation has the matrix $\left[\begin{smallmatrix}1&0&0\\0&1&0\\0&0&0\end{smallmatrix}\right]$ which is *not* an orthogonal matrix. (2) By Theorem 29.8 this is not an orthogonal transformation as it is *not* preserving the lengths of vectors, such as, the vector $v=(0,0,1)$ which is mapped to the zero vector. **E.29.5.** T is *not* an orthogonal transformation because $f(\lambda)$ has the toot 2, so T has the eigenvalue $\lambda=2$. Whereas all the eigenvalues of real orthogonal transformations are 1 or -1. **E.29.6.** (1) The Gram-Schmidt process brings the columns $v_1=\left[\begin{smallmatrix}1\\1\end{smallmatrix}\right]$ and $v_2=\left[\begin{smallmatrix}2\\0\end{smallmatrix}\right]$ to the orthonormal vectors $e_1=\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{1}{\sqrt2}\end{bmatrix}$ and $e_2=\begin{bmatrix}\frac{1}{\sqrt2}\\-\frac{1}{\sqrt2}\end{bmatrix}$. That is $Q=\begin{bmatrix}\frac{1}{\sqrt2}&\frac{1}{\sqrt2}\\\frac{1}{\sqrt2}&-\frac{1}{\sqrt2}\end{bmatrix}=\frac{1}{\sqrt2}\left[\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right]$. Then $R=Q^TR=\frac{1}{\sqrt2}\left[\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right]\left[\begin{smallmatrix}1&2\\1&0\end{smallmatrix}\right]=\frac{1}{\sqrt2}\left[\begin{smallmatrix}2&2\\0&2\end{smallmatrix}\right]=\begin{bmatrix}\sqrt2&\sqrt2\\0&\sqrt2\end{bmatrix}$. **E.29.10.** The characteristic polynomial of A is $|A-\lambda I|=-(\lambda-1)(\lambda-4)^2$, and the eigenvalues are $\lambda_1=1$, $\lambda_2=4$ (the second is a root of multiplicity two). Thus, the diagonal matrix is $D=\left[\begin{smallmatrix}1&0&0\\0&4&0\\0&0&4\end{smallmatrix}\right]$. As respective eigenvectors we compute $v_1=(1,-1,1)$ as a basis for eigenspace E_1, then $v_2=(1,1,0)$ and $v_3=(-1,0,1)$ as a basis for eigenspace E_4. We already can take the matrix $P=\left[\begin{smallmatrix}1&1&-1\\-1&1&0\\1&0&1\end{smallmatrix}\right]=[v_1\ v_2\ v_3]$ and have the diagonalization $D=P^{-1}AP$. However, this is not yet an *orthogonal* diagonalization. To find it bring by the Gram-Schmidt process the set $\{v_1,v_2,v_3\}$ to an orthonormal set $\{e_1,e_2,e_3\}$, where $e_1=(\frac{1}{\sqrt3},-\frac{1}{\sqrt3},\frac{1}{\sqrt3})$, $e_2=(\frac{1}{\sqrt2},\frac{1}{\sqrt2},0)$, $e_3=(-\frac{1}{\sqrt6},\frac{1}{\sqrt6},\frac{\sqrt2}{\sqrt3})$. Composing the orthogonal matrix

$$Q=\begin{bmatrix}\frac{1}{\sqrt3}&\frac{1}{\sqrt2}&-\frac{1}{\sqrt6}\\-\frac{1}{\sqrt3}&\frac{1}{\sqrt2}&\frac{1}{\sqrt6}\\\frac{1}{\sqrt3}&0&\frac{\sqrt2}{\sqrt3}\end{bmatrix}=[e_1\ e_2\ e_3]$$

we get the orthogonal diagonalization $D=Q^TAQ$. **E.29.11.** The diagonal form is $D=\left[\begin{smallmatrix}3&0&0\\0&9&0\\0&0&9\end{smallmatrix}\right]$. The respective eigenbasis is $v_1=(1,1,1)$, $v_2=(-1,1,0)$,

$v_3 = (-1, 0, 1)$. Normalizing v_1 we get $e_1 = (\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}})$. Orthonormalizing $\{v_2, v_3\}$ by Gram-Schmidt we get $e_2 = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)$, $e_3 = (-\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{\sqrt{2}}{\sqrt{3}})$. Therefore $Q = \begin{bmatrix} \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & 0 & \frac{\sqrt{2}}{\sqrt{3}} \end{bmatrix}$, and we have the orthogonal diagonalization $Q^T A Q = D$. **E.29.12**. The characteristic polynomial is $f(\lambda) = -\lambda^3 + 9\lambda^2 = -\lambda^2(\lambda - 9)$. The geometric multiplicity of 0 is 2, geometric multiplicity of 9 is 1. Using null spaces we compute the respective eigenbasis vectors $v_1 = (2, 1, 0)$, $v_2 = (-2, 0, 1)$ for E_0 and $u_1 = (1, -2, 2)$ for E_9. By Gram-Schmidt process we get $e_1 = \frac{1}{\sqrt{5}}(2, 1, 0)$, $e_2 = \frac{1}{3\sqrt{5}}(-2, 4, 5)$ for E_0, and $e_3 = \frac{1}{3}(1, -2, 2)$ for E_9. The diagonal form is $D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 9 \end{bmatrix}$. And the orthogonal matrix is $Q = \begin{bmatrix} \frac{2}{\sqrt{5}} & -\frac{2}{3\sqrt{5}} & \frac{1}{3} \\ \frac{1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & -\frac{2}{3} \\ 0 & \frac{5}{3\sqrt{5}} & \frac{2}{3} \end{bmatrix} = \frac{1}{3\sqrt{5}} \begin{bmatrix} 6 & -2 & \sqrt{5} \\ 3 & 4 & -2\sqrt{5} \\ 0 & 5 & 2\sqrt{5} \end{bmatrix}$. We get the orthogonal diagonalization $Q^T A Q = D$.

Index

Bibliography

Bibliography for Linear Algebra

[AXLER] Axler, Sheldon, *Linear Algebra Done Right*, 3rd ed, Springer, Undergraduate Texts in Mathematics (2016).

[BRETSCHER] Bretscher, Otto, *Linear algebra with applications*, 5th ed, Pearson Education, Inc. (2013).

[CURTIS] Curtis, Charles W., *Linear algebra. An introductory approach*, 3rd ed, Undergraduate texts in mathematics, Springer-Verlag, New York Berlin Heidelberg Tokyo (1974).

[HALMOS] Halmos, Paul R. *Finite-dimensional vector spaces*, reprint of the 2nd ed, Undergraduate Texts in Mathematics. New York - Heidelberg - Berlin: Springer-Verlag. VIII (1974).

[HEFFERON] Hefferon, Jim, *Linear algebra*, Joshua - Saint Michael's College (2014).

[HOFFMAN&KUNZE] Hoffman, Kenneth M.; Kunze, Ray, *Linear Algebra*, 2nd ed, Prentice-Hall, Inc., Englewood Cliffs, New Jersey (1971).

[LAY] Lay, David C., *Linear algebra and its applications*, 4th ed, Addison-Wesley (2012).

[LEON] Leon, Steven J. *Linear algebra with applications*, 9th ed, Pearson (2015).

[MALTSEV] Maltsev, Anatoliy I., *Foundations of linear algebra*, 3rd ed, Nauka, Moscow (1970).

[ROBINSON] Robinson, Derek J. S., *A Course in Linear Algebra with Applications*, 2nd ed, World Scientific (2006).

[POOLE] Poole, David, *Linear Algebra, A Modern Introduction*, 4th ed, Cengage Learning (2015).

[STRANG] Strang, Gilbert, *Introduction to linear algebra*, 5th ed, Wellesley, MA: Wellesley-Cambridge Press (2016).

Bibliography for Abstract Algebra

[ARTIN] Artin, Michael, *Algebra*, 2nd ed, Pearson (2010).

[DUMMIT&FOOTE] Dummit, David S.; Foote, Richard M., *Abstract Algebra*, 3rd ed, John Wiley & Sons, Inc. (2004).

[HUNGERFORD] Hungerford, Thomas W., *Algebra*, Springer, Graduate texts in mathematics (1974).

[LANG] Lang, Serge, *Algebra*, 3rd ed, Springer, Graduate texts in mathematics (2002).

[KOSTRIKIN] Kostrikin, Alexei I. *Foundations of algebra*, 2rd ed, Fizmatgiz, Moscow (2004).

[ROTMAN] Rotman, Joseph, *Advanced Modern Algebra*, AMS, Graduate texts in mathematics (2010).

[VAN DER WAERDEN] van der Waerden, Bartel Leendert, *Algebra*, Springer, Graduate texts in mathematics (1970).