

Algebra and Geometry with Python

Sergei Kurgalin • Sergei Borzunov

Algebra and Geometry with Python

 Springer

Sergei Kurgalin
Digital Technologies Department
Voronezh State University
Voronezh, Russia

Sergei Borzunov
Digital Technologies Department
Voronezh State University
Voronezh, Russia

ISBN 978-3-030-61540-6

ISBN 978-3-030-61541-3 (eBook)

<https://doi.org/10.1007/978-3-030-61541-3>

© Springer Nature Switzerland AG 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The rapid development of computing places special demands on the training of young specialists in this field. The complexity of the problems that must be solved to satisfy the needs of science, technology, industry and the economy also grows, simultaneously with the rapid growth in the power of modern computer systems. In this connection, we believe that it is essential that computing specialists have fundamental knowledge about the development of the related mathematical frameworks and about how to create methods for solving the above problems.

Algebra and geometry are deemed important areas whose ideas and results are actively used in the development of information systems, as well as in software developed for business projects. The basic notions of algebra are numerical matrices and the methods for working with matrix algorithms. They may be used extensively in scientific and technical problems and in the game industry. The rapid development of game technologies, as well as augmented and alternative reality technologies, means that we must pay special attention to university courses in analytical geometry and linear algebra, pattern properties in 3D space and fast algorithms for working with two- and three-dimensional objects.

Another promising area of application for linear algebra algorithms that has seen rapid development in recent years is Big Data. Analysis of extremely large arrays requires not only knowledge and use of the known methods, but it also issues the challenge to develop new approaches and high-performance algorithms.

This textbook is an introduction to linear algebra and analytical geometry for higher-education students in the natural sciences. It is based on the courses Algebra and Geometry, Analytical Geometry and Fundamental and Computer Algebra, which are taught to first-year students of the Faculty of Computer Sciences at the Voronezh State University. The teaching is meant for theoretical training, as a supplement to the existing textbooks, for practical and laboratory classes, and also for self-study. Going forward, the terms “Algebra” and “Linear Algebra” will be considered equivalent, as well as “Geometry” and “Analytical Geometry”.

The authors have attempted to lay the material down in the most comprehensible form while not sacrificing strictness in definitions and theorems. The statements (theorems, properties) are accompanied with proofs, or references to specialist literature for advanced study of the materials.

The fundamentals of algebra and geometry are presented in the form most suitable for future specialists in computing. We have considered the basic algorithms for working with matrices, vectors and systems of linear equations. The theoretical material contains solutions of most types of problems and is supplemented with plenty of analysed examples. The end of an example is designated by the symbol \square . Each chapter ends with problems for self-study. Many of them are provided not only with full answers but also with detailed solutions. The asterisk sign (*) marks the advanced (enhanced complexity) problems.

Apart from the sections traditionally included in algebra and geometry courses, one of the chapters is devoted to the mathematical fundamentals of the modern section of cryptography, namely elliptic curve cryptography. The availability of this chapter will be a connecting link between the mathematical courses and methods applied in practice by the application software developers.

The section about quantum computing is devoted to one of the examples of the application of algebra. It demonstrates that the notions of linear algebra are used for constructing new algorithms, whose computation capacity exceeds the existing ones considerably.

Let us briefly summarize the content of this textbook. The first four chapters are devoted to classical divisions of linear algebra; they consider matrices and determinants, and systems of linear equations; definitions are given for the notion of vector space and the fundamental solution of a homogeneous system. The next few chapters introduce the fundamentals of vector algebra and the coordinate method on a plane and in a 3D space. The following subjects are considered: vectors in three-dimensional space, the equation of a line on a plane, the equation of a plane in space and the equation of a line in space. Second-order curves are analysed. Material on elliptic curves is usually not included in a “traditional” algebra and geometry course. However, its presence in this book, in our opinion, contributes to a deeper understanding of the methods of linear algebra and analytical geometry and provides an example of the implementation of such methods for solving problems in theoretical and practical cryptography.

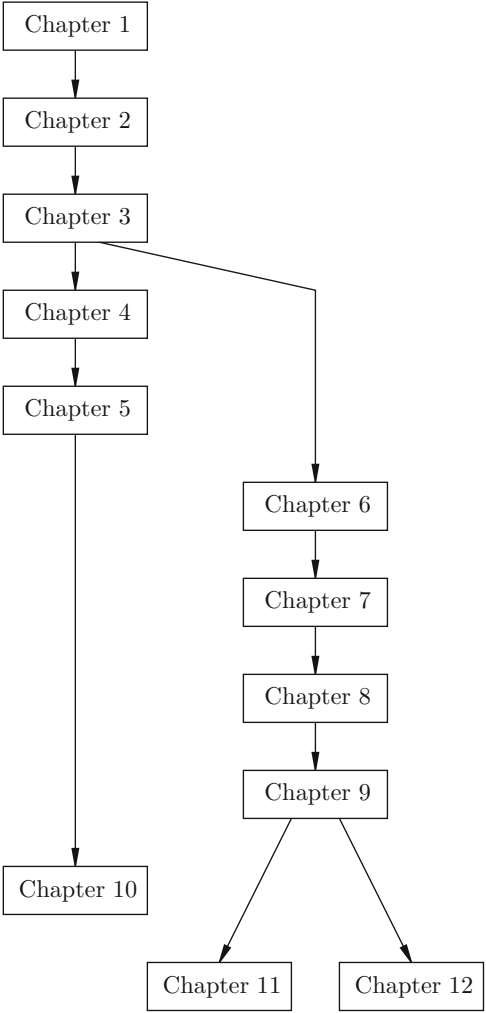
We use the Python programming language for illustration of the considered algorithms. This allows us to familiarize readers with implementation at the initial stage of study. Python was selected because it is a universal and widely used general-purpose programming language, suitable for the successful realization of numerical algorithms; Python is a continuously evolving language; and many of its realizations are open source. Python has the necessary tools to automatically check for the errors that might appear in the program code in the process of its creation. The availability of a great number of additional libraries (such as *NumPy*, *SciPy*, *pandas*) substantially expands the programmer’s capabilities. Thus, this language is quite suitable for teaching linear algebra and analytical geometry algorithms.

As the time of writing, the version of Python known as “Python 2” is still being used in many significant projects and in the literature. However, official support for Python 2 is diminishing and is scheduled to end. So, we use the latest major version, “Python 3”, in this book. Note that there are significant differences between Python 2 and Python 3; however, extended support documentation and tools are available for conversion between the two major versions. Refer to the official Python webpage (<https://www.python.org/>) for more details.

The book offers a list of training literature on linear algebra and analytical geometry, which may be used for a more detailed study on the issues touched upon in this textbook.

The appendices contain reference information, including basic operators in Python and C, trigonometric formulae and the Greek alphabet. These reduce the necessity to address reference literature.

Below you can see the chart of the chapter information dependence in the form of an oriented graph reflecting the preferable order of covering the academic material. For instance, after having studied Chaps. 1, 2 and 3, you can move to one of the two chapters, Chap. 4 or Chap. 6, the contents of which are relatively independent. After Chap. 9, we think Chaps. 11 and 12 can be mastered in any order.



The chapter dependency chart

Acknowledgements

The authors express sincere gratitude to their colleagues for useful discussions and critical remarks. Very useful to the improvement of the text were the valuable remarks of Artem Atanov, Alexey Bukhovets, Tatiana Churakova, Andrei Fediakov, Evgenii Kiselev, Alexander Loboda, Pavel Lukin, Peter Meleshenko, Leonid Minin, Mikhail Semenov and Sergei Zapryagaev.

Enormous help at all stages of working on this book was provided by the experts at Springer. We are especially grateful to editors Aliaksandr Birukou, Ronan Nugent and Wayne Wheeler in collaboration with whom we have been fruitfully working on this and our previous books. Checking of the program code located in the book was performed with the assistance of students of the Faculty of Computer Sciences, Voronezh State University—Anna Danilova, Artem Konovskoy, Nikolai Paukov, Margarita Tepliakova, Vladimir Ushakov and Sergei Zaitsev.

The manuscript of this book was used as the basic teaching for the students at the Voronezh State University, for several semesters. Their interest and enthusiasm had a positive influence on the content of the training course. We thank all the students who took the course in algebra and geometry, and for helping to eradicate some of the misprints and mistakes found in the first versions of the manuscript. Great help in checking the solutions and answers to the problems and exercises was rendered by students Pavel Burdyug, Dmitry Demianov, Kirill Ganigin, Elizaveta Koroteyeva, Zakhar Korsakov, Denis Makushin, Pavel Nekrasov, Natalya Salova, Anna Tsybulskaia, Dmitry Tynyanyy and Anna Yankevich.

Of course, all other mistakes remaining in the text are exclusively on the authors' conscience.

Sergei Kurgalin is especially grateful to Olga Kurgalina and Alexander Shirokov for their constant support during the work on the book.

Voronezh, Russia
Voronezh, Russia
July 2019

Sergei Kurgalin
Sergei Borzunov

Contents

1	Matrices and Matrix Algorithms	1
1.1	Matrices and Operations with Them	1
1.2	Concept of Algorithm, Correctness of Algorithms	12
1.3	Estimation of Algorithm Efficiency	13
1.4	Primitive Matrix Operations in Python	15
1.4.1	NumPy Library	18
1.5	Matrix Algorithms in the Graph Theory	18
	Review Questions	23
	Problems	24
	Answers and Solutions	31
2	Matrix Algebra	43
2.1	Determinant of a Matrix: Determinants of the Second and Third Order	43
2.2	Determinants of the n -th order: Minors	45
2.3	General Properties of Determinants: Elementary Transformations of a Matrix	48
2.4	Inverse Matrix	50
2.5	Integer Powers of a Matrix	52
2.5.1	Mathematical Induction Method	53
2.6	Functions of Matrices	56
2.6.1	Exponent and Logarithm	57
2.7	Matrix Rank	59
	Review Questions	65
	Problems	65
	Answers and Solutions	77
3	Systems of Linear Equations	123
3.1	Cramer's Rule	124
3.2	Inverse Matrix Method	126
3.3	Gaussian Elimination	128
3.4	Fundamental System of Solutions of Homogeneous Systems	137

3.5	General Solution of the Non-homogeneous System of Equations	142
	Review Questions	145
	Problems	146
	Answers and Solutions	150
4	Complex Numbers and Matrices	173
4.1	Arithmetic Operations with Complex Numbers	173
4.2	Fundamental Theorem of Algebra.....	178
4.3	Cardano Formula	178
4.4	Complex Coefficient Matrices	180
4.4.1	Hermitian Matrices	180
4.4.2	Unitary Matrices	182
4.5	Fundamentals of Quantum Computing.....	183
4.5.1	Pauli Matrices and Dirac Matrices	185
4.5.2	Basic Operations with Qubits	186
	Review Questions	191
	Problems	192
	Answers and Solutions	201
5	Vector Spaces.....	217
5.1	Linear Dependence of Vectors in the Space \mathbb{R}^n	218
5.2	Basis in the Space \mathbb{R}^n	219
5.3	Euclidean Vector Space	223
5.4	Eigenvalues and Eigenvectors of a Matrix	225
	Review Questions	231
	Problems	231
	Answers and Solutions	236
6	Vectors in a Three-Dimensional Space	255
6.1	Cartesian Coordinate System	256
6.2	Scalar Product of Vectors	258
6.3	Vector Product of Vectors	260
6.3.1	Properties of the Vector Product	260
6.4	Scalar Triple Product.....	263
6.4.1	Properties of Scalar Triple Product	263
6.5	Vector Triple Product	265
	Review Questions	266
	Problems	266
	Answers and Solutions	268
7	Equation of a Straight Line on a Plane	277
7.1	Slope-Intercept Form of the Equation of a Straight Line.....	277
7.2	General Equation of a Straight Line.....	278
7.3	Slope-Intercept Form of the Equation of a Straight Line Through a Given Point	279
7.4	Equation of a Straight Line Through Two Given Points	280

7.5	Angle Between Two Straight Lines	281
7.6	Intercept Form of the Equation of a Straight Line	282
7.7	Normal (Symmetric) Form of the Equation of a Line	283
7.8	Line Segments	287
	Review Questions	290
	Problems	290
	Answers and Solutions	293
8	Equation of a Plane in Space	307
8.1	Equation of a Plane That Is Orthogonal to the Specified Vector and Passes Through the Specified Point.....	307
8.2	General Equation of a Plane	308
8.3	Intercept Form of the Equation of a Plane	309
8.4	Normal Equation of a Plane	310
8.5	Equation of a Plane That Passes Through the Specified Point Parallel to the Two Specified Vectors	311
8.6	Equation of the Plane That Passes Through the Three Specified Points	312
8.7	Angle Between Two Planes	312
8.8	Distance from a Point to a Plane.....	313
8.9	Pencil of Planes.....	313
	Review Questions	314
	Problems	314
	Answers and Solutions	315
9	Equation of a Line in a Space	321
9.1	Equation of a Line That Passes Through the Specified Point Parallel to the Specified Vector	321
9.2	Equation of a Line That Passes Through the Two Specified Points	323
9.3	Angle Between Two Lines	323
9.4	Angle Between a Line and a Plane	324
9.5	Condition of Two Lines' Belonging to a Plane	326
	Review Questions	328
	Problems	328
	Answers and Solutions	330
10	Bilinear and Quadratic Forms	335
10.1	Bilinear Forms.....	335
10.2	Quadratic Forms.....	337
10.3	Bringing the Quadratic Form to the Canonical Form.....	339
	10.3.1 Lagrange's Method of Separating Perfect Squares.....	340
	10.3.2 Jacobi Method	343
	Review Questions	344
	Problems	345
	Answers and Solutions	346

11	Curves of the Second Order	357
11.1	Ellipse	357
11.2	Hyperbola	360
11.3	Parabola	362
11.4	Degenerate Curves	363
11.4.1	Imaginary Ellipse	363
11.4.2	Pair of Intersecting Lines	364
11.4.3	Pair of Imaginary Intersecting Lines	364
11.4.4	Pair of Parallel Lines	364
11.4.5	Pair of Imaginary Parallel Lines	365
11.4.6	Pair of Coincident Lines	365
11.5	Algorithms for Computing the Coordinates of the Tangent Points of Second Order Curve and the Straight Line	365
	Review Questions	368
	Problems	369
	Answers and Solutions	370
12	Elliptic Curves	383
12.1	Operation of Multiplication of the Elliptic Curve Points	384
12.1.1	Addition of a Point and \mathcal{O}	386
12.1.2	Addition of Two Different Points	386
12.1.3	Addition of Two Opposite Points	388
12.1.4	Duplication of a Point	388
12.2	Elliptic Curves with Rational Points	392
12.3	Implementation of the Addition Algorithm	394
	Review Questions	399
	Problems	399
	Answers and Solutions	401
A	Basic Operators in Python and C	407
B	Trigonometric Formulae	411
C	The Greek Alphabet	413
	References	415
	Index	419

Notation

\mathbb{N}	The set of natural numbers
\mathbb{Z}	The set of integers
\mathbb{Q}	The set of rational numbers
\mathbb{R}	The set of real numbers
\mathbb{C}	The set of complex numbers
\mathbb{R}^n	n -dimensional vector space
\emptyset	The empty set
$A \Rightarrow B$	Logical consequence, or implication
$A \Leftrightarrow B$	Logical equivalence
$\forall x(P(x))$	For all x , the statement $P(x)$ is true
$\exists x(P(x))$	There exists such x that the statement $P(x)$ is true
A and B	Conjunction of logical expressions A and B
A or B	Disjunction of logical expressions A and B
$A \equiv B$	Equivalency
$\{a_1, a_2, \dots, a_n\}$	The set consisting of the elements a_1, a_2, \dots, a_n
$\sum_{i=1}^n a_i$	The sum $a_1 + a_2 + \dots + a_n$
$\prod_{i=1}^n a_i$	The product $a_1 a_2 \dots a_n$
$A = (a_{ij})$	Matrix formed by the elements a_{ij}
A^T	Matrix transposed relative to A
I	Identity matrix
O	Zero matrix
δ_{ij}	Kronecker delta
$[A, B]$	Commutator of the matrices A and B
$\text{tr } A$	Trace of the matrix A
$O(g(n))$	Class of functions growing not faster than the function $g(n)$
$G(V, E)$	G is a graph with vertex set V and edge set E
$d(v)$	Degree of vertex v of a graph
$D(V, E)$	D is a directed graph with vertex set V and edge set E

$d^+(v)$	Out-degree of vertex v in a digraph
$d^-(v)$	In-degree of vertex v in a digraph
$\lfloor x \rfloor$	Floor function of x , i. e., the greatest integer less than or equal to the real number x (see definition on page 78)
M_{ij}	Additional minor of the matrix element placed at the intersection of the i -th row and the j -th column
$A_{ij} = (-1)^{i+j} M_{ij}$	Cofactor of the element a_{ij}
A^{-1}	Inverse of the matrix A
$M_{j_1, j_2, \dots, j_k}^{i_1, i_2, \dots, i_k}$	Minor of the k -th order (see page 59)
$\text{rk } A$	Rank of the matrix A
e^A or $\exp A$	Exponential of the matrix A
$\ln A$	Logarithm of the matrix A
$i = \sqrt{-1}$	Imaginary unit
z^*	Complex number conjugate of the complex number z
$ z $	Modulus of the complex number z
$\arg z$	Argument of the complex number
Z^H	Hermitian conjugate matrix
$ \psi\rangle$	Quantum state
$ 0\rangle, 1\rangle$	Basic quantum states of the qubit
$\sigma_1, \sigma_2, \sigma_3$	Pauli matrices
$\mathbf{x} = [x_1, \dots, x_n]^T$	Vector of the n -dimensional space \mathbb{R}^n
$\mathbf{0}$	Zero vector
$\ \mathbf{x}\ $	Euclidean norm of the vector \mathbf{x}
$X_{\text{gen.}}$	General solution of a homogeneous system of linear equations
$X_{\text{spec.}}$	Specific solution of a non-homogeneous system of linear equations
$\text{Pr}_L \mathbf{a}$	Projection of the vector \mathbf{a} onto the line L (see page 256)
$\mathbf{i}, \mathbf{j}, \mathbf{k}$	Normalized vectors of the Cartesian coordinate system
$\mathbf{a} \perp \mathbf{b}$	Orthogonality of the vectors \mathbf{a} and \mathbf{b}
$(\mathbf{a} \cdot \mathbf{b})$	Scalar or inner product of vectors
$\mathbf{a} \times \mathbf{b}$	Vectorial or outer product of vectors
$(\mathbf{a}, \mathbf{b}, \mathbf{c})$	Scalar triple product
$\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$	Vector triple product
$\text{abs}(x)$	Absolute value of the real number x
$\text{sgn}(x)$	Sign of the real number x
μ	Normalizing factor (see pages 285 and 311)
δ	Deviation of a point from a line or a plane
$\mathcal{A}(\mathbf{x}, \mathbf{y})$	Bilinear form
$\omega(\mathbf{x})$	Quadratic form
ε	Eccentricity of a curve of the second order
Γ	Elliptic curve with real points
Ξ	Elliptic curve with rational points
\mathcal{O}	Point at infinity of an elliptic curve
$A \oplus B$	The sum of two points A and B on an elliptic curve