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

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 □. 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.

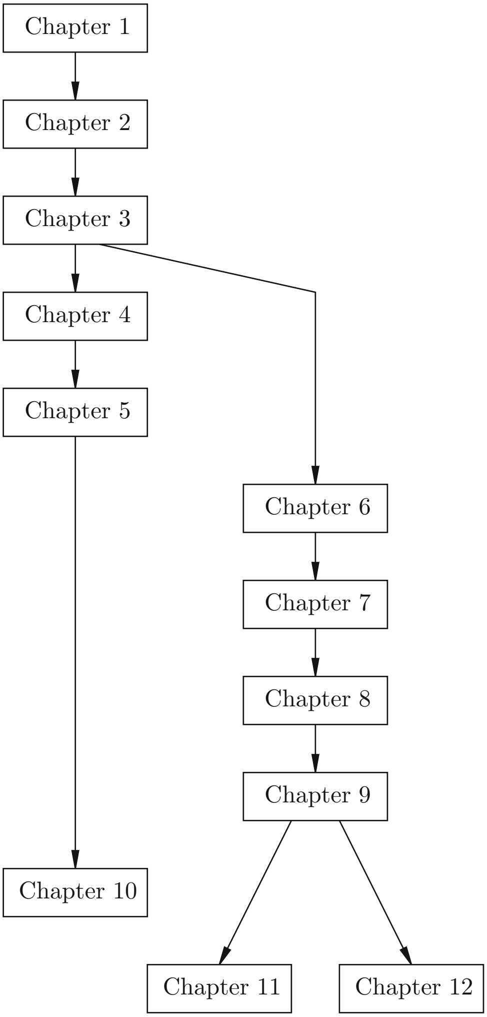
We use the Python programming language for illustration of the considered algorithms. This allows us to familiarize readers with implementation at the initial stage of study. Python was selected because it is a universal and widely used general-purpose programming language, suitable for the successful 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 Sergei Kurgalin
Voronezh, Russia Sergei Borzunov
July 2019

Contents

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
$\varnothing$	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
$\{a_1, a_2, \ldots, a_n\}$	The set consisting of the elements $a_1, a_2, \ldots, a_n$
$\sum\limits_{i=1}^{n} a_i$	The sum $a_1 + a_2 + \cdots + a_n$
$\prod\limits_{i=1}^{n} a_i$	The product $a_1 a_2 \ldots a_n$
$A = (a_{ij})$	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
$\operatorname{tr} A$	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
$M^{i_1,i_2,\ldots,i_k}_{j_1,j_2,\ldots,j_k}$	Minor of the k-th order (see page 59)
$\operatorname{rk} A$	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
$\lvert z \rvert$	Modulus of the complex number z
$\arg z$	Argument of the complex number
Z^{H}	Hermitian conjugate matrix
$\lvert \psi \rangle$	Quantum state
$\lvert 0 \rangle, \lvert 1 \rangle$	Basic quantum states of the qubit
$\sigma_1, \sigma_2, \sigma_3$	Pauli matrices
$\boldsymbol{x} = [x_1, \ldots, x_n]^{T}$	Vector of the n-dimensional space $\mathbb{R}^{n}$
$\mathbf{0}$	Zero vector
$\lVert \boldsymbol{x} \rVert$	Euclidean norm of the vector $\boldsymbol{x}$
$X_{\text{gen.}}$	General solution of a homogeneous system of linear equations
$X_{\text{spec.}}$	Specific solution of a non-homogeneous system of linear equations
$\operatorname{Pr}_{L} \boldsymbol{a}$	Projection of the vector $\boldsymbol{a}$ onto the line L (see page 256)
$\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$	Normalized vectors of the Cartesian coordinate system
$\boldsymbol{a} \perp \boldsymbol{b}$	Orthogonality of the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$
$(\boldsymbol{a} \cdot \boldsymbol{b})$	Scalar or inner product of vectors
$\boldsymbol{a} \times \boldsymbol{b}$	Vectorial or outer product of vectors
$(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$	Scalar triple product
$\boldsymbol{a} \times (\boldsymbol{b} \times \boldsymbol{c})$	Vector triple product
$\operatorname{abs}(x)$	Absolute value of the real number x
$\operatorname{sgn}(x)$	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
$\mathcal{A}(\boldsymbol{x}, \boldsymbol{y})$	Bilinear form
$\omega(\boldsymbol{x})$	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