



M. F. Gilmullin, "Why Do We Need Algebra? The Mathematician's Bible," *Mathematics with Mansur*, Feb. 3, 2025. [Online]. Available: <https://history-math.org/publications/hm-tt-ea92383ab5d3-en/>.

ESSAY

Why Do We Need Algebra? The Mathematician's Bible

A new book by Mansur Gilmullin, *The Mathematician's Bible: Foundations of Higher and Linear Algebra*, has appeared. What does it cover, and why do we need algebra?

Mansur Gilmullin · 03.02.2025 · EN

[Read this article on the journal website](#)



Author Mansur Gilmullin with the print run of his book *The Mathematician's Bible: Foundations of Higher and Linear Algebra* (2024) · [Source](#)

In December 2024, we shared the welcome [news of the publication of a new book](#) by Mansur Gilmullin, *The Mathematician's Bible: Foundations of Higher and Linear Algebra*. You can find it on the publisher's Ridero.ru website by searching for "[Gilmullin, The Mathematician's Bible](#)". Here we take a closer look at the book's contents and explain why we need algebra.

About algebra

The term “algebra” is traced to Muhammad al-Khwarizmi’s (c. 787–850, Baghdad) treatise *Hisab al-jabr wa-l-muqabala* (“Calculation by Completion and Balancing”). The book became known through a Latin translation, and the word *al-jabr* (algebra) came to stand for the entire science of algebra, which until the XIX century was the science of solving equations. *Al-jabr* means “completion”: moving subtracted terms to the other side of an equation.



Muhammad al-Khwarizmi (c. 787–850) on a special USSR stamp with a face value of 4 kopecks, issued on 6 September 1989 for the 1200th anniversary of his birth, together with the title page of his book *Hisab al-jabr wa-l-muqabala* · [Source](#)

Today mathematics is undergoing “algebraization”: algebraic ideas and methods are spreading through both theoretical and applied mathematics. The natural sciences of the XX century greatly extended algebra’s applications. Almost all the methods of linear algebra, for example, have become tools for formulating fundamental laws of nature and algorithms for solving applied problems.

Algebraic methods are also very useful for modelling economic problems and designing the architecture of modern computers. Number-theoretic algorithms have gained new life with the development of computer algebra and its applications, including algorithmic complexity analysis and cryptography.

Modern algebra is defined as the science of algebraic systems: sets equipped with operations and relations on their elements. Classical algebra studies problems that reduce to solving algebraic equations. It, too, forms part of modern algebra.

Why we need algebra

Behind the abstract exterior of most algebraic theories lie concrete theoretical or practical problems. In their time, these problems prompted the creation of new theories and provided tools for solving new problems.

The complex interaction between the theoretical and applied aspects of mathematics, particularly algebra, justifies the concentric approach adopted here: we return several times to the concepts introduced, each time at a different level.

Let us formulate several applied problems in mathematical modelling that motivate the study of algebra's theoretical methods, using *[The Mathematician's Bible](#)*.

Encryption methods

Many modern methods of encrypting information rest on algebra, specifically the theory of congruences presented in chapter 10. RSA, for example — an abbreviation of the surnames Rivest, Shamir and Adleman, 1978 — is a popular public-key cryptographic algorithm based on the computational difficulty of factoring large semiprimes into prime factors. These are positive integers expressible as the product of two primes.

RSA is a system suitable for encryption, decryption and digital signatures. Its principal tools are Euler's totient function and Fermat's little theorem, based on it: $a^{p-1} \equiv 1 \pmod{p}$. Fermat's little theorem is also a central tool in the theory of finite rings and fields, discussed in chapter 8.

Algebra thus helps solve applied problems in information theory.

Reducing data dimensionality

One of the main ways to reduce the dimensionality of data while losing as little information as possible is principal component analysis (PCA). Although Karl Pearson invented the method back in 1901, its applications continue to grow each year: data compression, image processing, econometrics and bioinformatics.

The method is now used in data science and machine learning. Data analysis usually involves constructing a simplified model that describes the real situation as accurately as possible. An object's statistical features are often strongly dependent on one another, making their simultaneous inclusion redundant. More often, however, these dependencies are less strict and less obvious. Knowing the dependencies and correlations allows several features of an object to be expressed through a single feature. Information loss cannot be avoided, but PCA helps minimize it.

Computing the principal components reduces to decomposing the empirical covariance matrix of the data and calculating its eigenvectors and eigenvalues: $Mx = \lambda x$. These are discussed in chapter 7.

Algebra thus helps solve statistical problems.

Elliptic curves

Elliptic curves have served as a basis for cryptosystems since the mid-80s of the last century, and as a tool for certain number-theoretic problems, including factorization and primality testing. Andrew Wiles also used them in number theory in his proof of Fermat's last theorem. These concepts are covered in chapters 8–10. Historically, the term “elliptic curve” derives from “elliptic integral”, demonstrating the connection between algebraic methods and mathematical analysis.

If the field's characteristic is neither 2 nor 3, including fields of characteristic zero such as number fields, a change of coordinates reduces the general equation of an elliptic curve to the canonical form $y^2 = x^3 + ax + b$, called Weierstrass normal form.

Today elliptic-curve cryptosystems are used in key technologies underpinning modern internet security, cryptocurrencies and digital currencies, and algorithms for generating and verifying electronic digital signatures.

Data mining

A fundamental problem in analysing big data is to simplify the data's structure while preserving as much relevant information as possible. Approaches to this problem are usually divided into methods for reducing the dimensionality of the data space and methods of classification and clustering.

Big-data mining methods commonly use algorithms for multiplying AB and inverting A^{-1} square matrices of large order. They also use new algebraic systems, such as bigroup algebras, and noncommutative $ab \neq ba$ and nonassociative $(ab)c \neq a(bc)$ algebraic structures. These basic concepts are discussed in chapters 2, 4 and 5.

Combining algebraic and geometric approaches with methods from topological, linear and computer algebra therefore helps develop effective algorithms for solving difficult problems across scientific and applied fields through artificial intelligence (AI).

The algebra course in The Mathematician's Bible

Since the 90s of the XX century, university algebra syllabuses have continually changed. Different degree programmes place different requirements on graduates, according to their future professions.

Programmes offered over the years at teacher-training, economics and technical universities have combined introductory algebra, general and linear algebra, and number theory.

For teacher-training programmes in mathematics, computer science and physics, for example, the course's main purpose is to study the fundamental algebraic systems and develop the algebraic culture future teachers need to understand fully the aims and tasks of school mathematics and supplementary mathematics education.

For information technology programmes, the subject aims to provide basic knowledge of algebra and an understanding of its concepts and methods, its place within computer science, and its use in applications.

The course can be used in modules, consulting the sections required by a particular degree programme. The concentric presentation of its principal concepts and methods supports this: different chapters revisit them from different perspectives, in greater detail or at a more general level.

Course structure

The course can broadly be viewed as four closely connected parts.

The first, introductory part of algebra (chapters 1–2) covers:

- elements of set theory and logic;
- binary relations (equivalence, order and functional relations);
- introductory material on algebras and algebraic systems (groups, rings and fields);
- the main number systems (positive integers and mathematical induction; the algebraic and trigonometric forms of complex numbers).

Elements of set theory and mathematical logic are presented informally and subsequently play a substantial role in the algebra course. The introductory material on algebras and algebraic systems — groups, rings and fields — in chapter two is developed further in later chapters through a broader range of new examples.

The second part (chapters 3–4) presents basic linear algebra: arithmetic vector spaces, linear dependence, the basis and rank of a system of vectors, matrices and their ranks, and systems of linear equations. It introduces vector spaces over a field, their bases and dimensions, subspaces and affine subspaces. Chapter 4 covers matrix operations, the calculation of determinants and their applications. The determinant of a matrix of arbitrary order is defined through permutations.

Chapter 5 presents the whole classical theory of groups, drawing on examples constructed in earlier chapters. This in turn underpins everything that follows. First, chapters 6–7 extend linear algebra to operations on subspaces, Euclidean spaces and isomorphisms of spaces. The theory of linear operators proceeds as far as the calculation of eigenvalues and eigenvectors. Examples of linear algebras, of linear operators and of matrices arise naturally.

The third part (chapters 8–10) begins with classical ring theory (chapter 8), moving from examples of rings, subrings and ideals to factorization. This provides the setting for the theory of divisibility and congruences in the rings of integers and polynomials. The number-theoretic questions arising here are closely related to the school curriculum and can provide a basis for school elective courses. Divisibility theory is supplemented by arithmetic functions, positional number representations and continued fractions. Congruence theory is supplemented by number-theoretic applications: residue theory, Euler's totient function, divisibility tests and the period length of an infinite decimal expansion.

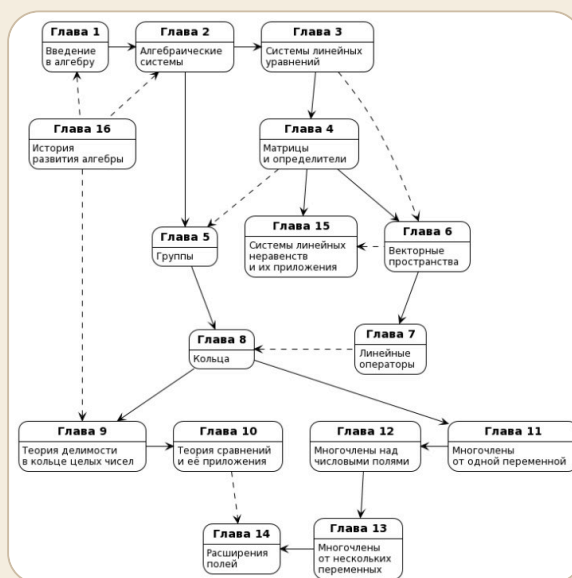
The final chapters 11–13 study polynomial rings in one and several variables. Chapter 12 addresses the subject of classical algebra: solving algebraic equations over the principal number fields. Classical algebra concludes with chapter 14, which presents field extensions and their applications in school mathematics: irrationality, transcendence, solvability of equations by radicals, and compass-and-straightedge construction problems.

The last chapter, 15, is devoted to systems of linear inequalities — the main concepts, consequences and a criterion for inconsistency — and elements of linear programming: standard and canonical problems, dual problems, the simplex method and the transportation problem. These topics can be treated as examples of applications of linear algebra.

The course concludes with an additional chapter, “The History of Algebra”. We believe that when studying algebra, as with any scientific theory or academic subject, its history should be brought into the discussion. The chapter presents a periodization of algebra’s development based on changes in how its subject was understood. Its material can be incorporated appropriately into a systematic exposition of algebra or its individual parts.

All chapters are divided into sections. Definitions, theorems and corollaries are not numbered; where a reference is needed, an explanation identifies the relevant statement. Examples accompany every concept and algorithm. Almost all theorem statements are proved, although the proofs may be skipped on a first reading. Bear in mind, however, that proofs often also provide methods for solving practical problems.

The general course plan has been outlined above; the dependencies and connections between chapters can be shown in the diagram below.



Chapter dependencies in the algebra course in *The Mathematician’s Bible: Foundations of Higher and Linear Algebra* (2024) · [Source](#)

Using this diagram, a reader with the necessary background can begin with any chapter and choose a personal route through the material. Dashed arrows indicate alternative routes and connections between chapters through their theories and examples.

The book's bibliography has also been assembled with teaching needs in mind. The listed literature may come from any year of publication. Other suitable sources naturally exist, and readers can find them independently.



A mock-up of the printed book by M. F. Gilmullin, The Mathematician's Bible: Foundations of Higher and Linear Algebra (2024). Find it on the publisher's Ridero.ru website by searching for "Гильмуллин Библия математика" · [Source](#)

Modern algebra plays the same role as language in a person's communication with the outside world. To appreciate how important it is to learn algebra's language, try doing without it when studying mathematics independently. We wish every reader success in developing a taste for algebra. May algebra mediate between spirit and matter!