Universitext

Igor R. Shafarevich

Discourses on Algebra

代数讲义

Springer

世界图书出版公司
www.wpcbj.com.cn

Igor R. Shafarevich

Discourses on Algebra

Translated from the Russian
by William B. Everett

Springer

图书在版编目（CIP）数据

代数讲义 = Discourses on Algebra：英文/（俄罗斯）沙夫罗维奇主编. —北京：世界图书出版公司北京公司，2009.8

ISBN 978-7-5100-0503-9

Ⅰ. 代… Ⅱ. 沙… Ⅲ. 高等代数—高等学校—教材—英文 Ⅳ. 015

中国版本图书馆 CIP 数据核字（2009）第 100865 号

书　　名： Discourses on Algebra
作　　者： Igor R. Shafarevich

中 译 名： 代数讲义
责任编辑： 高蓉

出 版 者： 世界图书出版公司北京公司
印 刷 者： 三河国英印务有限公司
发　　行： 世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话： 010-64021602，010-64015659
电子信箱： kjb@ wpcbj. com. cn

开　　本： 24 开
印　　张： 12.5
版　　次： 2009 年 08 月
版权登记： 图字：01-2009-0687

书　　号： 978-7-5100-0503-9/O · 719　　**定　　价：** 35.00 元

Igor R. Shafarevich
Mathematical Institute of the
Russian Academy of Sciences
Ul. Gubkina 8
117 966 Moscow, Russia
e-mail: shafar@mech.math.msu.su

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Shafarevic, Igor R.:
Discourses on algebra / Igor R. Shafarevich. Transl. from the Russian by William B. Everett. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Universitext)
ISBN 3-540-42253-6

Originally published as Izbrannye glavy algebry
Matematicheskoe obrazovanie (zhurnal), Moscow 2000

ISBN 3-540-42253-6 Springer-Verlag Berlin Heidelberg New York

Mathematics Subject Classification (2000): 11-XX, 12-XX, 13-XX, 15-XX

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Universitext

Abstract

In this book by a leading Russian mathematician and full member of the Russian Academy of Sciences, Igor Rostislavovich Shafarevich, the elements of algebra as a field of contemporary mathematics are laid out based on material bordering the school program as closely as possible.

The book can be used as enrichment materials for students in grades 9–12 in both ordinary schools and schools with a deeper study of mathematics and the sciences and also as a book for mathematics teachers.

Preface

I wish that algebra would be the Cinderella of our story. In the mathematics program in schools, geometry has often been the favorite daughter. The amount of geometric knowledge studied in schools is approximately equal to the level achieved in ancient Greece and summarized by Euclid in his *Elements* (third century B.C.). For a long time, geometry was taught according to Euclid; simplified variants have recently appeared. In spite of all the changes introduced in geometry courses, geometry retains the influence of Euclid and the inclination of the grandiose scientific revolution that occurred in Greece. More than once I have met a person who said, "I didn't choose math as my profession, but I'll never forget the beauty of the elegant edifice built in geometry with its strict deduction of more and more complicated propositions, all beginning from the very simplest, most obvious statements!"

Unfortunately, I have never heard a similar assessment concerning algebra. Algebra courses in schools comprise a strange mixture of useful rules, logical judgments, and exercises in using aids such as tables of logarithms and pocket calculators. Such a course is closer in spirit to the brand of mathematics developed in ancient Egypt and Babylon than to the line of development that appeared in ancient Greece and then continued from the Renaissance in western Europe. Nevertheless, algebra is just as fundamental, just as deep, and just as beautiful as geometry. Moreover, from the standpoint of the modern division of mathematics into branches, the algebra courses in schools include elements from *several* branches: algebra, number theory, combinatorics, and a bit of probability theory.

The task of this book is to show algebra as a branch of mathematics based on materials closely bordering the course in schools. The book does not claim to be a textbook, although it is addressed to students and teachers. The development presumes a rather small base of knowledge: operations with integers and fractions, square roots, opening parentheses and other operations on expressions involving letter symbols, the properties of inequalities. All these skills are learned by the 9th grade. The complexity of the mathematical considerations increases somewhat as we move through the book. To help the reader grasp the material, simple problems are given to be solved.

The material is grouped into three basic themes—**Numbers**, **Polynomials**, and **Sets**—each of which is developed in several chapters that alternate with the chapters devoted to the other themes.

Certain matters related to the basic text, although they do not use more ideas than are already present, are more complicated and require that the reader keep more facts and definitions in mind. These matters are placed in supplements to the chapters and are not used in subsequent chapters.

For the proofs of assertions given in the book, I chose not the shortest but the most "understandable." They are understandable in the sense that they connect the assertion to be proved with a larger number of concepts and other assertions; they thus clarify the position of the assertion to be proved within the structure of the presented area of mathematics. A shorter proof often appears later, sometimes as a problem to be solved.

At the first acquaintance with mathematics, the history of its development usually retreats into second place. Sometimes it even seems that mathematics was born in the form of a perfected textbook. In fact, mathematics has arisen as the result of the work of uncounted scholars throughout many milleniums. To give some attention to that aspect of mathematics, the dates of the lives of the mathematicians (and physicists) mentioned in the text are listed at the end of the book.

There are quite many formulas. For convenience in referring to them, they are numbered. If I only give the formula number when referring to it, then the formula is in the current chapter. For example, if "multiplying equality (16), we obtain ... " is said in Chap. 2, then the formula with the number (16) in Chap. 2 is meant. If a formula in a different chapter is intended, then the number of the chapter is also given, for example, "using formula (12) in Chap. 1." To help find the necessary chapter, the chapter numbers are printed at the top of every left-hand page. Theorems and lemmas are numbered in order throughout the entire book.

The Foundation for Mathematical Education and Enlightenment and especially S. I. Komarov and V. M. Imaikin helped me greatly in preparing the manuscript. S. P. Demushkin took upon himself the labor of reading the manuscript and made many important comments. I convey my heartfelt gratitude to all of them.

I. R. Shafarevich Moscow, 2000

Added to the English edition:

Finally, I express my cordial gratitude to Bill Everett, who translated this book into English. As far as I can judge, this is beautiful English. However, I am not an expert in this. But certainly, he greatly improved the text as he showed me several mistakes and urged me by his questions to clarify the exposition in some places.

I. R. S. Moscow, 2002

Contents

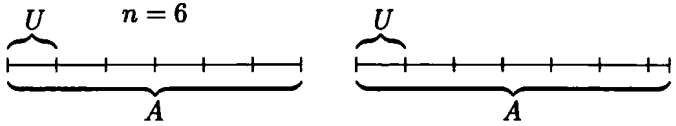
1
Integers

Topic: Numbers

1. $\sqrt{2}$ Is Not Rational

Natural numbers arose as a result of *counting*. An important step in mankind's development of logic was the recognition that two eyes, two persons walking together, and the two oars of a boat have something in common, something expressed in the abstract concept *two*. The next step was taken with difficulty, which is evident because the word *three* in many languages is equivalent to *many* or *too much*. But the concept of an endless series of natural numbers was gradually worked out.

After that it was natural to use numbers not only for *counting* but also for *measuring* lengths, areas, weights, and so on. For definiteness, we discuss measuring the lengths of line segments. We first choose a unit of length: millimeter (mm), centimeter (cm), kilometer (km), light year.... Let the line segment U define the unit of length. When the unit of length is chosen, we can try to use it to measure other line segments. If U is completely placed on a line segment A exactly n times, we say that the length of the line segment A is n (Fig. 1a). But as a rule, some small bit, smaller than the line segment U, remains uncovered (Fig. 1b).



(a) (b)

Fig. 1

Then we can reduce the unit of length, dividing U into m identical smaller segments U'. If U' is completely placed on the line segment A exactly n' times, then the length of A is equal to n'/m (in the original unit of length U).

People in different lands in the course of milleniums used this procedure in different situations until finally the question arose: **Is such a division of the unit of length always possible?** This totally novel question is related to a specific historical epoch; the question came up in the school of Pythagoras in ancient Greece in the sixth or fifth century B.C. The segments A and U are said to be *commensurable* if there exists a segment U' that can be completely placed on the segment U exactly m times and on the segment A exactly n times. Thus, the question is: **Are any two given line segments commensurable?** Or (yet another form of the question), is the length of any given line segment always a rational number n/m (in terms of a specified unit of length)? The answer is **NO!** And it is very easy to give an example of noncommensurable line segments. We consider a square whose side is the unit of length U. Then we take the diagonal of the square to be the line segment A.

Theorem 1. *The side and the diagonal of a square are noncommensurable.*

Before beginning the proof, we state the theorem in another form. We compare the side and diagonal of a square using the famous Pythagorean theorem: the area of the square constructed on the hypotenuse of a right triangle is equal to the sum of the areas of the two squares constructed on the other two sides of the triangle. Or, in other words, the hypotenuse squared is equal to the sum of the two legs squared.

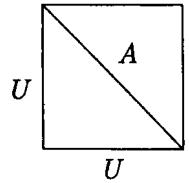


Fig. 2

But the diagonal A of our square is the hypotenuse of an isosceles right triangle whose two legs coincide with the sides U of the square (Fig. 2). Therefore, in our case, $A^2 = 2U^2$, and if A and U are commensurable, that is, if there exists U' such that $A = nU'$ and $U = mU'$, then we would have $(n/m)^2 = 2$, which is to say $n/m = \sqrt{2}$. Thus Theorem 1 can be stated differently.

Theorem 2. *$\sqrt{2}$ is not a rational number.*

We prove the theorem in this form. But first we make one observation. Although we refer to the Pythagorean theorem, we use it in the very special case of an isosceles right triangle. In this case, it is completely obvious.

It immediately follows from the known conditions for the equality of triangles that all five small isosceles right triangles in Fig. 3 are equal. Therefore they have the same area S. But the square constructed on the line segment U consists of two such triangles, and its area is U^2. Therefore $U^2 = 2S$. Analogously, $A^2 = 4S$. Therefore $A^2 = 2U^2$ and $(A/U)^2 = 2$.

Now we can turn to the proof of Theorem 2. Because we want to prove the *impossibility* of representing $\sqrt{2}$ in the form $\sqrt{2} = n/m$, it is natural to use *proof by contradiction*. We suppose that $\sqrt{2} = n/m$, where n and m are natural numbers. We take them to be relatively prime, that is, if they had a common divisor, then it was canceled without changing the value of the fraction n/m. By the definition of a square root, the equality $\sqrt{2} = n/m$ means that $2 = (n/m)^2 = n^2/m^2$. Multiplying both sides by m^2, we obtain the equality

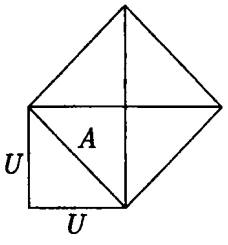


Fig. 3

$$2m^2 = n^2, \tag{1}$$

where n and m are two relatively prime natural numbers.

Because we have the factor 2 in the left-hand side, naturally, the question is tied to the divisibility of natural numbers by 2. Numbers that are divisible by 2 are called *even numbers*, and those not divisible by 2 are called *odd numbers*. By this definition, each even number k can be represented in the form $k = 2l$, where l is a natural number. That is, we have a certain obvious expression for even numbers, while odd numbers are so far defined purely negatively—this expression is impossible for them. But we can easily obtain an obvious expression for odd numbers, too.

Lemma 1. *Each odd number r can be represented in the form $r = 2s + 1$, where s is a natural number or 0. Conversely, each such number is odd.*

The converse assertion is totally obvious: if $r = 2s + 1$ were even, then it would have a representation $r = 2l$, whence

$$2l = 2s + 1, \qquad 2(l - s) = 1.$$

And this assertion is obviously contradictory.

To prove the primary assertion, we note that if the odd number $r \leq 2$, then $r = 1$ and the expression to be found has the form with $s =$

0. And if the odd number $r > 1$, then already $r \geq 3$. Subtracting 2 from it, we obtain the number $r_1 = r - 2 \geq 1$, where r_1 is again odd. If r_1 is still greater than 1, then we again subtract 2 and obtain $r_2 = r_1 - 2$. With this procedure, we obtain a decreasing series of odd numbers $r, r_1, r_2, \ldots$ in which each successive number is 2 less than the preceding number. We can continue this as long as $r_i > 1$. Because natural numbers cannot decrease without limit, we eventually arrive at the case where subtracting 2 is no longer possible, that is, $r_i = 1$. We obtain

$$r_i = r_{i-1} - 2 = r_{i-2} - 2 - 2 = \cdots = r - 2 - 2 - \cdots - 2 = r - 2i = 1.$$

This means that $r = 2i + 1$, which was to be proved. □

We can now introduce a fundamental property of even and odd numbers.

Lemma 2. *The product of two even numbers is even, the product of an even number and an odd number is even, and the product of two odd numbers is odd.*

The first two assertions are obvious from the definition of an even number: if $k = 2l$, then no matter what the second factor m is, even or odd, always $km = 2lm$, which means it is even. But to prove the final assertion, we need Lemma 1. Let k_1 and k_2 be odd numbers. According to Lemma 1, we can represent them in the form

$$k_1 = 2s_1 + 1, \qquad k_2 = 2s_2 + 1,$$

where s_1 and s_2 are natural numbers or 0. Then

$$k_1 k_2 = (2s_1 + 1)(2s_2 + 1) = 4s_1 s_2 + 2s_1 + 2s_2 + 1 = 2s + 1,$$

where $s = 2s_1 s_2 + s_1 + s_2$. We saw that any number of the form $2s + 1$ is odd, and this means that $k_1 k_2$ is odd. □

We note a special case of Lemma 2: *the square of an odd number is odd.*

Now it is completely easy to finish the proof of Theorem 2. We suppose that equality (1) is satisfied, where m and n are relatively prime natural numbers. If n were odd, then by Lemma 2, n^2 would be odd, but it is even according to equality (1). Therefore, n is even and can be represented in the form $n = 2s$. But m and n are relatively prime, which means that m must be odd (otherwise m and n would have the common divisor 2). Substituting the expression for n in equality (1) and dividing by 2, we obtain

$$m^2 = 2s^2,$$

that is, the square of an odd number is even, which contradicts Lemma 2. Theorem 2, and that means Theorem 1 also, is proved. □

We can look at Theorems 1 and 2 from a different point of view, presuming that the result of measuring the length of a line segment (with a given unit of length) is a certain number and that the square root of any positive number is a certain number. Then Theorems 1 and 2 assert that in the case of the diagonal of a square or in the case of $\sqrt{2}$, this certain number is not rational, in other words, it is *irrational*. This is the simplest example of an irrational number. Many irrational numbers exist. We meet some of them later. Probably, the most "well-known" irrational number (after $\sqrt{2}$) is π, the ratio of the circumference of a circle to its diameter. But to prove that π is irrational requires more complex means than we use here, and so we do not prove it in this book.

All numbers both rational and irrational together comprise the real numbers. In one of the following chapters, we try to state more precisely the logical meaning of the concept of a real number. Until then, we continue to use real numbers in the form that they are usually taught in school, not thinking especially about their logical basis.

Why did it take mankind so long to recognize the existence of such a simple, and at the same time important, circumstance as the existence of irrational numbers? The answer is simple—because for any practical purpose, $\sqrt{2}$, for example, can be considered a rational number. We state this assertion in the form of a theorem.

Theorem 3. *No matter how small a number ε is given, it is possible to find a rational number $a = m/n$ such that $a < \sqrt{2}$ and $\sqrt{2} - a < \varepsilon$.*

Because all practical measurements by necessity are taken with a certain accuracy, we can consider that $\sqrt{2}$ is rational with that degree of accuracy; we can say that our *measurement* gives us $\sqrt{2}$ as a rational number.

To prove Theorem 3, we take our "no matter how small" number ε in the form $1/10^n$ with sufficiently large n. We then find a natural number k such that

$$\frac{k}{10^n} \leq \sqrt{2} < \frac{k+1}{10^n}. \tag{2}$$

Then we can let $a = k/10^n$ because $\sqrt{2} - k/10^n < 1/10^n$.

Inequality (2) is equivalent to the inequality

$$\frac{k^2}{10^{2n}} \leq 2 < \frac{(k+1)^2}{10^{2n}}$$

or

$$k^2 \leq 2 \cdot 10^{2n} < (k+1)^2.$$

Because the number n (and therefore the number $2 \cdot 10^{2n}$ also) is a given specific number, there exists the greatest natural number k whose square is not greater than $2 \cdot 10^{2n}$. This k gives the value of a that was needed.

Obviously, the conclusion in Theorem 3 holds not only for the number $\sqrt{2}$ but also for any positive real number x (we restrict ourselves here to positive numbers for simplicity). This becomes obvious if we represent x as a point on the number line, divide the unit of length U into the small segments $U/10^n$, and then cover the number line with these small segments (Fig. 4).

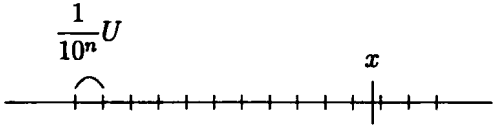


Fig. 4

Then the last mark that is not to the right of x gives the needed rational number. If this mark is the kth mark, then

$$a = \frac{k}{10^n} \leq x \qquad \text{and} \qquad x - a < \frac{1}{10^n}.$$

Theorem 3 is proved. □

But now estimate, please, the depth of the assertion contained in Theorems 1 and 2. This assertion could never be confirmed by any kind of experiment, because an experiment is always conducted with a certain accuracy. And with *any* specified accuracy, $\sqrt{2}$ can be expressed as a rational number! This achievement of pure reason could not appear, even as a result of the accumulation of many milleniums of human experience, until the revolution in mathematics that was accomplished in ancient Greece during the 7th–5th centuries B.C. It is not surprising that in the school of Pythagoras, this knowledge was considered a sacred secret that must be withheld from the uninitiated. But one of the Pythagoreans, Hippas, revealed the secret. According to one legend, the gods punished him for this with death resulting from a shipwreck. A hundred years later, Plato related in the book *Laws* how he, no longer young, was smitten when he learned that it is not always possible "to measure a length with a length." He told of his "disgraceful ignorance."

"It seemed to me that this was characteristic not of a human but of some sort of swine. And I was embarrassed not only for myself but also for all Greeks."

Proved Theorems 1 and 2 can shed light on a question mathematicians often pose: Why are theorems proved? The first answer that comes to mind is to become convinced of the truth of some assertion. But it sometimes happens that the accumulation of particular cases of such verification is so large that the truth of the assertion no longer elicits any doubt (and often elicits the ridicule of physicists who say that mathematicians prove truths that were already beyond doubt). But we saw that sometimes the proof introduces mathematicians to a totally new world of mathematical ideas that would never have been known without the proof.

Problems:

1. Prove that the numbers $\sqrt{6}$ and $\sqrt[3]{2}$ are irrational.
2. Prove that the number $\sqrt{2}+\sqrt{3}$ is irrational.
3. Prove that the number $\sqrt[3]{3}+\sqrt{2}$ is irrational.
4. Find $\sqrt{2}$ to the accuracy of $1/100$.
5. Prove that every natural number can be represented as a sum of terms of the form 2^k such that a given term occurs no more than once. Prove that there is only one such representation for each natural number.

2. The Irrationality of Other Square Roots

It would be interesting now to try generalizing the results we obtained in the previous section. For example, can we use the same method to prove that $\sqrt{3}$ is irrational? It is obviously natural to attempt adapting our previous arguments to the new situation. We must now prove the impossibility of the equality $3 = (n/m)^2$ or

$$3m^2 = n^2, \tag{3}$$

where, as in Sec. 1, we can consider the fraction n/m to be reduced, that is, the natural numbers m and n are relatively prime. Because the factor 3 appears in equality (3), we naturally call upon the property of divisibility by 3. We see how Lemmas 1 and 2 can be adapted to this new case.

Lemma 3. *Each natural number r either is divisible by 3 or can be represented in one of the two forms $r = 3s + 1$ or $r = 3s + 2$, where s is a natural number or 0. Conversely, numbers of the form $3s + 1$ or $3s + 2$ are not divisible by 3.*