

国外数学名著系列

(影印版) 2

Igor R. Shafarevich

Basic Notions of Algebra

代数学基础



科学出版社

www.sciencep.com

图字:01-2005-6732

Igor R. Shafarevich: Basic Notions of Algebra

© Springer-Verlag Berlin Heidelberg 2005

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the People's Republic of China only and not for export therefrom.

本书英文影印版由德国施普林格出版公司授权出版。未经出版者书面许可,不得以任何方式复制或抄袭本书的任何部分。本书仅限在中华人民共和国销售,不得出口。版权所有,翻印必究。

图书在版编目(CIP)数据

代数学基础=Basic Notions of Algebra/(俄罗斯)沙法列维奇(Shafarevich, I. R.)著. —影印版. —北京:科学出版社,2006

(国外数学名著系列)

ISBN 7-03-016691-4

I. 代… II. 沙… III. 代数-英文 IV. 015

中国版本图书馆 CIP 数据核字(2005)第 154387 号

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

中国科学院印刷厂印刷

科学出版社发行 各地新华书店经销

*

2006年1月第 一 版 开本:B5(720×1000)

2006年1月第一次印刷 印张:16 3/4

印数:1—3 000 字数:316 000

定价:48.00 元

(如有印装质量问题,我社负责调换(科印))

《国外数学名著系列》(影印版)专家委员会

(按姓氏笔画排序)

丁伟岳 王 元 石钟慈 冯克勤 严加安 李邦河
李大潜 张伟平 张继平 杨 乐 姜伯驹 郭 雷

项目策划

向安全 林 鹏 王春香 吕 虹 范庆奎 王 璐

执行编辑

范庆奎

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来,需要数学家淡泊名利并付出更艰苦地努力。另一方面,我们也要从客观上为数学家创造更有利的发展数学事业的外部环境,这主要是加强对数学事业的支持与投资力度,使数学家有较好的工作与生活条件,其中也包括改善与加强数学的出版工作。

从出版方面来讲,除了较好较快地出版我们自己的成果外,引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说,施普林格(Springer)出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书,使我国广大数学家能以较低的价格购买,特别是在边远地区工作的数学家能普遍见到这些书,无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权,一次影印了 23 本施普林格出版社出版的数学书,就是一件好事,也是值得继续做下去的事情。大体上分一下,这 23 本书中,包括基础数学书 5 本,应用数学书 6 本与计算数学书 12 本,其中有些书也具有交叉性质。这些书都是很新的,2000 年以后出版的占绝大部分,共计 16 本,其余的也是 1990 年以后出版的。这些书可以使读者较快地了解数学某方面的前沿,例如基础数学中的数论、代数与拓扑三本,都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点,基础数学类的书以“经典”为主,应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家,例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士,曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然,23 本书只能涵盖数学的一部分,所以,这项工作还应该继续做下去。更进一步,有些读者面较广的好书还应该翻译成中文出版,使之有更大的读者群。

总之,我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持,并盼望这一工作取得更大的成绩。

王 元

2005 年 12 月 3 日

Basic Notions of Algebra

I.R. Shafarevich

Translated from the Russian
by M. Reid

Contents

Preface	4
§ 1. What is Algebra?	6
The idea of coordinatisation. Examples: dictionary of quantum mechanics and coordinatisation of finite models of incidence axioms and parallelism.	
§ 2. Fields	11
Field axioms, isomorphisms. Field of rational functions in independent variables; function field of a plane algebraic curve. Field of Laurent series and formal Laurent series.	
§ 3. Commutative Rings	17
Ring axioms; zerodivisors and integral domains. Field of fractions. Polynomial rings. Ring of polynomial functions on a plane algebraic curve. Ring of power series and formal power series. Boolean rings. Direct sums of rings. Ring of continuous functions. Factorisation; unique factorisation domains, examples of UFDs.	
§ 4. Homomorphisms and Ideals	24
Homomorphisms, ideals, quotient rings. The homomorphisms theorem. The restriction homomorphism in rings of functions. Principal ideal domains; relations with UFDs. Product of ideals. Characteristic of a field. Extension in which a given polynomial has a root. Algebraically closed fields. Finite fields. Representing elements of a general ring as functions on maximal and prime ideals. Integers as functions. Ultraproducts and nonstandard analysis. Commuting differential operators.	
§ 5. Modules	33
Direct sums and free modules. Tensor products. Tensor, symmetric and exterior powers of a module, the dual module. Equivalent ideals and isomorphism of modules. Modules of differential forms and vector fields. Families of vector spaces and modules.	
§ 6. Algebraic Aspects of Dimension	41
Rank of a module. Modules of finite type. Modules of finite type over a principal ideal domain. Noetherian modules and rings. Noetherian rings and rings of finite type. The case of graded rings. Transcendence degree of an extension. Finite extensions.	

§ 7. The Algebraic View of Infinitesimal Notions	50
Functions modulo second order infinitesimals and the tangent space of a manifold. Singular points. Vector fields and first order differential operators. Higher order infinitesimals. Jets and differential operators. Completions of rings, p -adic numbers. Normed fields. Valuations of the fields of rational numbers and rational functions. The p -adic number fields in number theory.	
§ 8. Noncommutative Rings	61
Basic definitions. Algebras over rings. Ring of endomorphisms of a module. Group algebra. Quaternions and division algebras. Twistor fibration. Endomorphisms of n -dimensional vector space over a division algebra. Tensor algebra and the non-commuting polynomial ring. Exterior algebra; superalgebras; Clifford algebra. Simple rings and algebras. Left and right ideals of the endomorphism ring of a vector space over a division algebra.	
§ 9. Modules over Noncommutative Rings	74
Modules and representations. Representations of algebras in matrix form. Simple modules, composition series, the Jordan-Hölder theorem. Length of a ring or module. Endomorphisms of a module. Schur's lemma	
§ 10. Semisimple Modules and Rings	79
Semisimplicity. A group algebra is semisimple. Modules over a semisimple ring. Semisimple rings of finite length; Wedderburn's theorem. Simple rings of finite length and the fundamental theorem of projective geometry. Factors and continuous geometries. Semisimple algebras of finite rank over an algebraically closed field. Applications to representations of finite groups.	
§ 11. Division Algebras of Finite Rank	90
Division algebras of finite rank over \mathbb{R} or over finite fields. Tsen's theorem and quasi-algebraically closed fields. Central division algebras of finite rank over the p -adic and rational fields.	
§ 12. The Notion of a Group	96
Transformation groups, symmetries, automorphisms. Symmetries of dynamical systems and conservation laws. Symmetries of physical laws. Groups, the regular action. Subgroups, normal subgroups, quotient groups. Order of an element. The ideal class group. Group of extensions of a module. Brauer group. Direct product of two groups.	
§ 13. Examples of Groups: Finite Groups	108
Symmetric and alternating groups. Symmetry groups of regular polygons and regular polyhedrons. Symmetry groups of lattices. Crystallographic classes. Finite groups generated by reflections.	
§ 14. Examples of Groups: Infinite Discrete Groups	124
Discrete transformation groups. Crystallographic groups. Discrete groups of motion of the Lobachevsky plane. The modular group. Free groups. Specifying a group by generators and relations. Logical problems. The fundamental group. Group of a knot. Braid group.	
§ 15. Examples of Groups: Lie Groups and Algebraic Groups	140
Lie groups. Toruses. Their role in Liouville's theorem.	
A. Compact Lie Groups	143
The classical compact groups and some of the relations between them.	
B. Complex Analytic Lie Groups	147
The classical complex Lie groups. Some other Lie groups. The Lorentz group.	
C. Algebraic Groups	150
Algebraic groups, the adèle group. Tamagawa number.	

§ 16. General Results of Group Theory	151
Direct products. The Wedderburn-Remak-Schmidt theorem. Composition series, the Jordan-Hölder theorem. Simple groups, solvable groups. Simple compact Lie groups. Simple complex Lie groups. Simple finite groups, classification.	
§ 17. Group Representations	160
A. Representations of Finite Groups	163
Representations. Orthogonality relations.	
B. Representations of Compact Lie Groups	167
Representations of compact groups. Integrating over a group. Helmholtz-Lie theory. Characters of compact Abelian groups and Fourier series. Weyl and Ricci tensors in 4-dimensional Riemannian geometry. Representations of $SU(2)$ and $SO(3)$. Zeeman effect.	
C. Representations of the Classical Complex Lie Groups	174
Representations of noncompact Lie groups. Complete irreducibility of representations of finite-dimensional classical complex Lie groups.	
§ 18. Some Applications of Groups	177
A. Galois Theory	177
Galois theory. Solving equations by radicals.	
B. The Galois Theory of Linear Differential Equations (Picard-Vessiot Theory)	181
C. Classification of Unramified Covers	182
Classification of unramified covers and the fundamental group	
D. Invariant Theory	183
The first fundamental theorem of invariant theory	
E. Group Representations and the Classification of Elementary Particles	185
§ 19. Lie Algebras and Nonassociative Algebra	188
A. Lie Algebras	188
Poisson brackets as an example of a Lie algebra. Lie rings and Lie algebras.	
B. Lie Theory	192
Lie algebra of a Lie group.	
C. Applications of Lie Algebras	197
Lie groups and rigid body motion.	
D. Other Nonassociative Algebras	199
The Cayley numbers. Almost complex structure on 6-dimensional submanifolds of 8-space. Nonassociative real division algebras.	
§ 20. Categories	202
Diagrams and categories. Universal mapping problems. Functors. Functors arising in topology: loop spaces, suspension. Group objects in categories. Homotopy groups.	
§ 21. Homological Algebra	213
A. Topological Origins of the Notions of Homological Algebra ...	213
Complexes and their homology. Homology and cohomology of polyhedrons. Fixed point theorem. Differential forms and de Rham cohomology; de Rham's theorem. Long exact cohomology sequence.	
B. Cohomology of Modules and Groups	219
Cohomology of modules. Group cohomology. Topological meaning of the cohomology of discrete groups.	
C. Sheaf Cohomology	225
Sheaves; sheaf cohomology. Finiteness theorems. Riemann-Roch theorem.	

§ 22. <i>K</i> -theory	230
A. Topological <i>K</i> -theory	230
Vector bundles and the functor $\mathcal{V}_{ec}(X)$. Periodicity and the functors $K_n(X)$. $K_1(X)$ and the infinite-dimensional linear group. The symbol of an elliptic differential operator. The index theorem.	
B. Algebraic <i>K</i> -theory	234
The group of classes of projective modules. K_0 , K_1 and K_n of a ring. K_2 of a field and its relations with the Brauer group. <i>K</i> -theory and arithmetic.	
Comments on the Literature	239
References	244
Index of Names	249
Subject Index	251

Preface

This book aims to present a general survey of algebra, of its basic notions and main branches. Now what language should we choose for this? In reply to the question 'What does mathematics study?', it is hardly acceptable to answer 'structures' or 'sets with specified relations'; for among the myriad conceivable structures or sets with specified relations, only a very small discrete subset is of real interest to mathematicians, and the whole point of the question is to understand the special value of this infinitesimal fraction dotted among the amorphous masses. In the same way, the meaning of a mathematical notion is by no means confined to its formal definition; in fact, it may be rather better expressed by a (generally fairly small) sample of the basic examples, which serve the mathematician as the motivation and the substantive definition, and at the same time as the real meaning of the notion.

Perhaps the same kind of difficulty arises if we attempt to characterise in terms of general properties any phenomenon which has any degree of individuality. For example, it doesn't make sense to give a definition of the Germans or the French; one can only describe their history or their way of life. In the same way, it's not possible to give a definition of an individual human being; one can only either give his 'passport data', or attempt to describe his appearance and character, and relate a number of typical events from his biography. This is the path we attempt to follow in this book, applied to algebra. Thus the book accommodates the axiomatic and logical development of the subject together with more descriptive material: a careful treatment of the key examples and of points of contact between algebra and other branches of mathematics and the natural sciences. The choice of material here is of course strongly influenced by the author's personal opinions and tastes.

As readers, I have in mind students of mathematics in the first years of an undergraduate course, or theoretical physicists or mathematicians from outside algebra wanting to get an impression of the spirit of algebra and its place in mathematics. Those parts of the book devoted to the systematic treatment of notions and results of algebra make very limited demands on the reader: we presuppose only that the reader knows calculus, analytic geometry and linear algebra in the form taught in many high schools and colleges. The extent of the prerequisites required in our treatment of examples is harder to state; an acquaintance with projective space, topological spaces, differentiable and complex analytic manifolds and the basic theory of functions of a complex variable is desirable, but the reader should bear in mind that difficulties arising in the treatment of some specific example are likely to be purely local in nature, and not to affect the understanding of the rest of the book.

This book makes no pretence to teach algebra: it is merely an attempt to talk about it. I have attempted to compensate at least to some extent for this by giving a detailed bibliography; in the comments preceding this, the reader can find references to books from which he can study the questions raised in this book, and also some other areas of algebra which lack of space has not allowed us to treat.

A preliminary version of this book has been read by F.A. Bogomolov, R.V. Gamkrelidze, S.P. Dëmushkin, A.I. Kostrikin, Yu.I. Manin, V.V. Nikulin, A.N. Parshin, M.K. Polyvanov, V.L. Popov, A.B. Roiter and A.N. Tyurin; I am grateful to them for their comments and suggestions which have been incorporated in the book.

I am extremely grateful to N.I. Shafarevich for her enormous help with the manuscript and for many valuable comments.

Moscow, 1984

I.R. Shafarevich

I have taken the opportunity in the English translation to correct a number of errors and inaccuracies which remained undetected in the original; I am very grateful to E.B. Vinberg, A.M. Volkhonskii and D. Zagier for pointing these out. I am especially grateful to the translator M. Reid for innumerable improvements of the text.

Moscow, 1987

I.R. Shafarevich

§ 1. What is Algebra?

What is algebra? Is it a branch of mathematics, a method or a frame of mind? Such questions do not of course admit either short or unambiguous answers. One can attempt a description of the place occupied by algebra in mathematics by drawing attention to the process for which Hermann Weyl coined the unpronounceable word 'coordinatisation' (see [H. Weyl 109 (1939), Chap. I, § 4]). An individual might find his way about the world relying exclusively on his sense organs, sight, feeling, on his experience of manipulating objects in the world outside and on the intuition resulting from this. However, there is another possible approach: by means of *measurements*, subjective impressions can be transformed into objective marks, into numbers, which are then capable of being preserved indefinitely, of being communicated to other individuals who have not experienced the same impressions, and most importantly, which can be operated on to provide new information concerning the objects of the measurement.

The oldest example is the idea of *counting* (coordinatisation) and *calculation* (operation), which allow us to draw conclusions on the number of objects without handling them all at once. Attempts to 'measure' or to 'express as a number' a variety of objects gave rise to fractions and negative numbers in addition to the whole numbers. The attempt to express the diagonal of a square of side 1 as a number led to a famous crisis of the mathematics of early antiquity and to the construction of irrational numbers.

Measurement determines the points of a line by real numbers, and much more widely, expresses many physical quantities as numbers. To Galileo is due the most extreme statement in his time of the idea of coordinatisation: 'Measure everything that is measurable, and make measurable everything that is not yet so'. The success of this idea, starting from the time of Galileo, was brilliant. The creation of analytic geometry allowed us to represent points of the plane by pairs of numbers, and points of space by triples, and by means of operations with numbers, led to the discovery of ever new geometric facts. However, the success of analytic geometry is mainly based on the fact that it reduces to numbers not only points, but also curves, surfaces and so on. For example, a curve in the plane is given by an equation $F(x, y) = 0$; in the case of a line, F is a linear polynomial, and is determined by its 3 coefficients: the coefficients of x and y and the constant term. In the case of a conic section we have a curve of degree 2, determined by its 6 coefficients. If F is a polynomial of degree n then it is easy to see that it has $\frac{1}{2}(n+1)(n+2)$ coefficients; the corresponding curve is determined by these coefficients in the same way that a point is given by its coordinates.

In order to express as numbers the roots of an equation, the complex numbers were introduced, and this takes a step into a completely new branch of mathematics, which includes elliptic functions and Riemann surfaces.

For a long time it might have seemed that the path indicated by Galileo consisted of measuring 'everything' in terms of a known and undisputed collec-

tion of numbers, and that the problem consists just of creating more and more subtle methods of measurements, such as Cartesian coordinates or new physical instruments. Admittedly, from time to time the numbers considered as known (or simply called numbers) turned out to be inadequate: this led to a 'crisis', which had to be resolved by extending the notion of number, creating a new form of numbers, which themselves soon came to be considered as the unique possibility. In any case, as a rule, at any given moment the notion of number was considered to be completely clear, and the development moved only in the direction of extending it:

'1, 2, many' \Rightarrow natural numbers \Rightarrow integers
 \Rightarrow rationals \Rightarrow reals \Rightarrow complex numbers.

But matrixes, for example, form a completely independent world of 'number-like objects', which cannot be included in this chain. Simultaneously with them, quaternions were discovered, and then other 'hypercomplex systems' (now called algebras). Infinitesimal transformations led to differential operators, for which the natural operation turns out to be something completely new, the Poisson bracket. Finite fields turned up in algebra, and p -adic numbers in number theory. Gradually, it became clear that the attempt to find a unified all-embracing concept of number is absolutely hopeless. In this situation the principle declared by Galileo could be accused of intolerance; for the requirement to 'make measurable *everything* which is not yet so' clearly discriminates against anything which stubbornly refuses to be measurable, excluding it from the sphere of interest of science, and possibly even of reason (and thus becomes a *secondary quality* or *secunda causa* in the terminology of Galileo). Even if, more modestly, the polemic term 'everything' is restricted to objects of physics and mathematics, more and more of these turned up which could not be 'measured' in terms of 'ordinary numbers'.

The principle of coordinatisation can nevertheless be preserved, provided we admit that the set of 'number-like objects' by means of which coordinatisation is achieved can be just as diverse as the world of physical and mathematical objects they coordinatise. The objects which serve as 'coordinates' should satisfy only certain conditions of a very general character.

They must be individually distinguishable. For example, whereas all points of a line have identical properties (the line is homogeneous), and a point can only be fixed by putting a finger on it, numbers are all individual: 3, $7/2$, $\sqrt{2}$, π and so on. (The same principle is applied when newborn puppies, indistinguishable to the owner, have different coloured ribbons tied round their necks to distinguish them.)

They should be sufficiently abstract to reflect properties common to a wide circle of phenomena.

Certain fundamental aspects of the situations under study should be reflected in *operations* that can be carried out on the objects being coordinatised: addition, multiplication, comparison of magnitudes, differentiation, forming Poisson brackets and so on.

We can now formulate the point we are making in more detail, as follows:

Thesis. *Anything which is the object of mathematical study (curves and surfaces, maps, symmetries, crystals, quantum mechanical quantities and so on) can be 'coordinatised' or 'measured'. However, for such a coordinatisation the 'ordinary' numbers are by no means adequate.*

Conversely, when we meet a new type of object, we are forced to construct (or to discover) new types of 'quantities' to coordinatise them. The construction and the study of the quantities arising in this way is what characterises the place of algebra in mathematics (of course, very approximately).

From this point of view, the development of any branch of algebra consists of two stages. The first of these is the birth of the new type of algebraic objects out of some problem of coordinatisation. The second is their subsequent career, that is, the systematic development of the theory of this class of objects; this is sometimes closely related, and sometimes almost completely unrelated to the area in connection with which the objects arose. In what follows we will try not to lose sight of these two stages. But since algebra courses are often exclusively concerned with the second stage, we will maintain the balance by paying a little more attention to the first.

We conclude this section with two examples of coordinatisation which are somewhat less standard than those considered up to now.

Example 1. The Dictionary of Quantum Mechanics. In quantum mechanics, the basic physical notions are 'coordinatised' by mathematical objects, as follows.

Physical notion	Mathematical notion
State of a physical system	Line φ in an ∞ -dimensional complex Hilbert space
Scalar physical quantity	Self-adjoint operator
Simultaneously measurable quantities	Commuting operators
Quantity taking a precise value λ in a state φ	Operator having φ as eigenvector with eigenvalue λ
Set of values of quantities obtainable by measurement	Spectrum of an operator
Probability of transition from state φ to state ψ	$ (\varphi, \psi) $, where $ \varphi = \psi = 1$

Example 2. Finite Models for Systems of Incidence and Parallelism Axioms. We start with a small digression. In the axiomatic construction of geometry, we often consider not the whole set of axioms, but just some part of them; to be

+	0	1
0	0	1
1	1	0

Fig. 3

×	0	1
0	0	0
1	0	1

Fig. 4

$$A = (0, 0), \quad B = (0, 1), \quad C = (1, 0), \quad D = (1, 1).$$

It is easy to check that the lines of the geometry are then defined by the linear equations:

$$AB: 1X = 0; \quad CD: 1X = 1; \quad AD: 1X + 1Y = 0;$$

$$BC: 1X + 1Y = 1; \quad AC: 1Y = 0; \quad BD: 1Y = 1.$$

In fact these are the only 6 nontrivial linear equations which can be formed using the two quantities 0 and 1.

The construction for the geometry of Figure 2 is similar, but slightly more complicated: suppose that we divide up all integers into 3 sets U , V and W as follows:

U = integers divisible by 3,

V = integers with remainder 1 on dividing by 3,

W = integers with remainder 2 on dividing by 3.

The operations on the symbols U , V , W is defined as in the first example; for example, a number in V plus a number in W always gives a number in U , and so we set $V + W = U$; similarly, the product of two numbers in W is always a number in V , so we set $W \cdot W = V$. The reader can easily write out the corresponding addition and multiplication tables.

It is then easy to check that the geometry of Figure 2 is coordinatised by our quantities U , V , W as follows: the points are

$$A = (U, U), \quad B = (U, V), \quad C = (U, W), \quad D = (V, U), \quad E = (V, V),$$

$$F = (V, W), \quad G = (W, U), \quad H = (W, V), \quad I = (W, W);$$

and the lines are again given by all possible linear equations which can be written out using the three symbols U , V , W ; for example, AFH is given by $VX + VY = U$, and DCH by $VX + WY = V$.

Thus we have constructed finite number systems in order to coordinatise finite geometries. We will return to the discussion of these constructions later.

Already these few examples give an initial impression of what kind of objects can be used in one or other version of 'coordinatisation'. First of all, the collection of objects to be used must be rigorously delineated; in other words, we must

indicate a set (or perhaps several sets) of which these objects can be elements. Secondly, we must be able to operate on the objects, that is, we must define *operations*, which from one or more elements of the set (or sets) allow us to construct new elements. For the moment, no further restrictions on the nature of the sets to be used are imposed; in the same way, an operation may be a completely arbitrary rule taking a set of k elements into a new element. All the same, these operations will usually preserve some similarities with operations on numbers. In particular, in all the situations we will discuss, $k = 1$ or 2 . The basic examples of operations, with which all subsequent constructions should be compared, will be: the operation $a \mapsto -a$ taking any number to its negative; the operation $b \mapsto b^{-1}$ taking any nonzero number b to its inverse (for each of these $k = 1$); and the operations $(a, b) \mapsto a + b$ and ab of addition and multiplication (for each of these $k = 2$).

§2. Fields

We start by describing one type of 'sets with operations' as described in §1 which corresponds most closely to our intuition of numbers.

A *field* is a set K on which two operations are defined, each taking two elements of K into a third; these operations are called *addition* and *multiplication*, and the result of applying them to elements a and b is denoted by $a + b$ and ab . The operations are required to satisfy the following conditions:

Addition:

Commutativity: $a + b = b + a$;

Associativity: $a + (b + c) = (a + b) + c$;

Existence of zero: there exists an element $0 \in K$ such that $a + 0 = a$ for every a (it can be shown that this element is unique);

Existence of negative: for any a there exists an element $(-a)$ such that $a + (-a) = 0$ (it can be shown that this element is unique).

Multiplication:

Commutativity: $ab = ba$;

Associativity: $a(bc) = (ab)c$;

Existence of unity: there exists an element $1 \in K$ such that $a1 = a$ for every a (it can be shown that this element is unique);

Existence of inverse: for any $a \neq 0$ there exists an element a^{-1} such that $aa^{-1} = 1$ (it can be shown that for given a , this element is unique).

Addition and multiplication:

Distributivity: $a(b + c) = ab + ac$.

Finally, we assume that a field does not consist only of the element 0 , or equivalently, that $0 \neq 1$.

These conditions taken as a whole, are called the *field axioms*. The ordinary identities of algebra, such as

$$(a + b)^2 = a^2 + 2ab + b^2$$

or

$$a^{-1} - (a + 1)^{-1} = a^{-1}(a + 1)^{-1}$$

follow from the field axioms. We only have to bear in mind that for a natural number n , the expression na means $a + a + \cdots + a$ (n times), rather than the product of a with the number n (which may not be in K).

Working over an arbitrary field K (that is, assuming that all coordinates, coefficients, and so on appearing in the argument belong to K) provides the most natural context for constructing those parts of linear algebra and analytic geometry not involving lengths, polynomial algebras, rational fractions, and so on.

Basic examples of fields are the field of rational numbers, denoted by \mathbb{Q} , the field of real numbers \mathbb{R} and the field of complex numbers \mathbb{C} .

If the elements of a field K are contained among the elements of a field L and the operations in K and L agree, then we say that K is a *subfield* of L , and L an *extension* of K , and we write $K \subset L$. For example, $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Example 1. In §1, in connection with the 'geometry' of Figure 1, we defined operations of addition and multiplication on the set $\{0, 1\}$. It is easy to check that this is a field, in which 0 is the zero element and 1 the unity. If we write 0 for 0 and 1 for 1, we see that the multiplication table of Figure 4 is just the rule for multiplying 0 and 1 in \mathbb{Q} , and the addition table of Figure 3 differs in that $1 + 1 = 0$. The field constructed in this way consisting of 0 and 1 is denoted by \mathbb{F}_2 . Similarly, the elements U, V, W considered in connection with the geometry of Figure 2 also form a field, in which $U = 0, V = 1$ and $W = -1$. We thus obtain examples of fields with a finite number (2 or 3) of elements. Fields having only finitely many elements (that is, finite fields) are very interesting objects with many applications. A finite field can be specified by writing out the addition and multiplication tables of its elements, as we did in Figures 3–4. In §1 we met such fields in connection with the question of the realisation of a certain set of axioms of geometry in a finite set of objects; but they arise just as naturally in algebra as realising the field axioms in a finite set of objects. A field consisting of q elements is denoted by \mathbb{F}_q .

Example 2. An algebraic expression obtained from an unknown x and arbitrary elements of a field K using the addition, multiplication and division operations, can be written in the form

$$\frac{a_0 + a_1x + \cdots + a_nx^n}{b_0 + b_1x + \cdots + b_mx^m}, \quad (1)$$

where $a_i, b_i \in K$ and not all $b_i = 0$. An expression of this form is called a *rational*

fraction, or a *rational function* of x . We can now consider it as a function, taking any x in K (or any x in L , for some field L containing K) into the given expression, provided only that the denominator is not zero. All rational functions form a field, called the *rational function field*; it is denoted by $K(x)$. We will discuss certain difficulties connected with this definition in §3. The elements of K are contained among the rational functions as 'constant' functions, so that $K(x)$ is an extension of K .

In a similar way we define the field $K(x, y)$ of rational functions in two variables, or in any number of variables.

An *isomorphism* of two fields K' and K'' is a 1-to-1 correspondence $a' \leftrightarrow a''$ between their elements such that $a' \leftrightarrow a''$ and $b' \leftrightarrow b''$ implies that $a' + b' \leftrightarrow a'' + b''$ and $a'b' \leftrightarrow a''b''$; we say that two fields are *isomorphic* if there exists an isomorphism between them. If L' and L'' are isomorphic fields, both of which are extensions of the same field K , and if the isomorphism between them takes each element of K into itself, then we say that it is an *isomorphism over K* , and that L' and L'' are *isomorphic over K* . An isomorphism of fields K' and K'' is denoted by $K' \cong K''$. If L' and L'' are finite fields, then to say that they are isomorphic means that their addition and multiplication tables are the same; that is, they differ only in the notation for the elements of L' and L'' . The notion of isomorphism for arbitrary fields is similar in meaning.

For example, suppose we take some line a and mark a point O and a 'unit interval' OE on it; then we can in a geometric way define addition and multiplication on the directed intervals (or vectors) contained in a . Their construction is given in Figures 5-6. In Figure 5, b is an arbitrary line parallel to a and U an arbitrary point on it, $OU \parallel AV$ and $VC \parallel UB$; then $OC = OA + OB$. In Figure 6, b is an arbitrary line passing through O , and $EU \parallel BV$ and $VC \parallel UA$; then $OC = OA \cdot OB$.

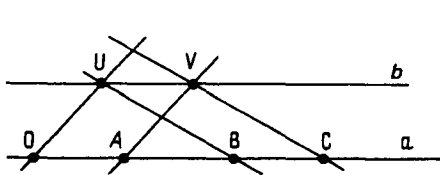


Fig. 5

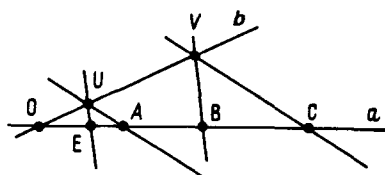


Fig. 6

With this definition of the operations, intervals of the line form a field P ; to verify all the axioms is a sequence of nontrivial geometric problems. Taking each interval into a real number, for example an infinite decimal fraction (this is again a process of measurement!), we obtain an isomorphism between P and the real number field \mathbb{R} .