Undergraduate Texts in Mathematics

Serge Lang

Undergraduate Algebra

Second Edition

ringer-Verlag
界图书出版公司

Serge Lang

Undergraduate Algebra

Second Edition

Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo Hong Kong
世界图书出版公司
北京・广州・上海・西安

Serge Lang
Department of Mathematics
Yale University
New Haven, CT 06520
U.S.A.

AMS Subject Classification (1980): 13-01, 15-01

Library of Congress Cataloging-in-Publication Data
Lang, Serge, 1927-
Undergraduate algebra / Serge Lang.—2nd ed.
p. cm.—(Undergraduate texts in mathematics)
1. Algebra. I. Title. II. Series.
QA152.2.L36 1990
512.9—dc20 90-9648

Reprinted by World Publishing Corporation, Beijing, 1992
for distribution and sale in The People's Republic of China only
ISBN 7-5062-1390-7

ISBN 0-387-97279-X Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97279-X Springer-Verlag Berlin Heidelberg New York

Undergraduate Texts in Mathematics

Springer Books on Elementary Mathematics by Serge Lang

MATH! Encounters with High School Students
1985, ISBN 96129-1

The Beauty of Doing Mathematics
1985, ISBN 96149-6

Geometry. A High School Course (with G. Murrow), **Second Edition**
1989, ISBN 96654-4

Basic Mathematics
1988, ISBN 96787-7

A First Course in Calculus
1986, ISBN 96201-8

Calculus of Several Variables
1987, ISBN 96405-3

Introduction to Linear Algebra
1986, ISBN 96205-0

Linear Algebra
1987, ISBN 96412-6

Undergraduate Algebra, Second Edition
1990, ISBN 97279-X

Undergraduate Analysis
1983, ISBN 90800-5

Complex Analysis
1985, ISBN 96085-6

Foreword

This book, together with *Linear Algebra*, constitutes a curriculum for an algebra program addressed to undergraduates.

The separation of the linear algebra from the other basic algebraic structures fits all existing tendencies affecting undergraduate teaching, and I agree with these tendencies. I have made the present book self contained logically, but it is probably better if students take the linear algebra course *before* being introduced to the more abstract notions of groups, rings, and fields, and the systematic development of their basic abstract properties. There is of course a little overlap with the book *Linear Algebra*, since I wanted to make the present book self contained. I define vector spaces, matrices, and linear maps and prove their basic properties.

The present book could be used for a one-term course, or a year's course, possibly combining it with *Linear Algebra*. I think it is important to do the field theory and the Galois theory, more important, say, than to do much more group theory than we have done here. There is a chapter on finite fields, which exhibit both features from general field theory, and special features due to characteristic p. Such fields have become important in coding theory.

There is also a chapter on some of the group-theoretic features of matrix groups. Courses in linear algebra usually concentrate on the structure theorems, quadratic forms, Jordan form, etc. and do not have the time to mention, let alone emphasize, the group-theoretic aspects of matrix groups. I find that the basic algebra course is a good place to introduce students to such examples, which mix abstract group theory with matrix theory. The groups of matrices provide concrete examples for the more abstract properties of groups listed in Chapter II.

The construction of the real numbers by Cauchy sequences and null sequences has no standard place in the curriculum, depending as it does on mixed ideas from algebra and analysis. Again, I think it belongs in a basic algebra text. It illustrates considerations having to do with rings, and also with ordering and absolute values. The notion of completion is partly algebraic and partly analytic. Cauchy sequences occur in mathematics courses on analysis (integration theory for instance), and also number theory as in the theory of p-adic numbers or Galois groups.

For a year's course, I would also regard it as appropriate to introduce students to the general language currently in use in mathematics concerning sets and mappings, up to and including Zorn's lemma. In this spirit, I have included a chapter on sets and cardinal numbers which is much more extensive than is the custom. One reason is that the statements proved here are not easy to find in the literature, disjoint from highly technical books on set theory. Thus Chapter X will provide attractive extra material if time is available. This part of the book, together with the Appendix, and the construction of the real and complex numbers, also can be viewed as a short course on the naive foundations of the basic mathematical objects.

If all these topics are covered, then there is enough material for a year's course. Different instructors will choose different combinations according to their tastes. For a one-term course, I would find it appropriate to cover the book up to the chapter on field theory, or the matrix groups. Finite fields can be treated as optional.

Elementary introductory texts in mathematics, like the present one, should be simple and always provide concrete examples together with the development of the abstractions (which explains using the real and complex numbers as examples before they are treated logically in the text). The desire to avoid encyclopedic proportions, and specialized emphasis, and to keep the book short explains the omission of some theorems which some teachers will miss and may want to include in the course. Exceptionally talented students can always take more advanced classes, and for them one can use the more comprehensive advanced texts which are easily available.

New Haven, Connecticut, 1987 S. LANG

Acknowledgments

I thank Ron Infante and James Propp for assistance with the proofreading, suggestions, and corrections.

S.L.

Foreword to the Second Edition

I have added some topics, for various reasons. For instance, I added the Sylow theorems, which have become fashionable and for which there was considerable demand. I have added material on symmetric polynomials, on principal rings and on the Jordan normal form, and on field theory, among other things. However, an undergraduate text such as this one must stop short of encyclopedic proportions. It must be rooted in examples and special cases, accompanying more general results. It must cover several aspects of algebra. Individual instructors will have to make choices.

I have added a number of exercises. All the exercises have been carefully chosen, some to provide routine practice, and some to give basic information about algebraic structures which are used constantly in mathematics. The way to learn them is for students to work them out as part of the course, and all the exercises should be regarded as an essential part of the course. They should all be worked out. Sometimes I have included exercises which are subsequently worked out as formal results in text. This policy is deliberate: to make students think about a result and try to prove it for themselves before it is officially handled in class. I have also tried to indicate more advanced directions and results in several places, referring to more advanced books. Such optional results go beyond the present course but they may stimulate some readers who want to get ahead.

Finally, I have tried on several occasions to put students in contact with genuine research mathematics, by selecting instances of conjectures which can be formulated in language at the level of this course. I have stated more than half a dozen such conjectures, of which the *abc* conjecture provides one spectacular example. Usually students have to wait years before they realize that mathematics is a live activity, sustained by its open problems. I have found it very effective to break down this obstacle whenever possible.

New Haven, Connecticut, 1990 SERGE LANG

Acknowledgment

I thank Keith Conrad for his suggestions and help with the proofreading.

S.L.

Undergraduate Texts in Mathematics

Apostol: Introduction to Analytic Number Theory. Second edition.
Armstrong: Groups and Symmetry.
Armstrong: Basic Topology.
Bak/Newman: Complex Analysis.
Banchoff/Wermer: Linear Algebra Through Geometry.
Brémaud: An Introduction to Probabilistic Modeling.
Bressoud: Factorization and Primality Testing.
Brickman: Mathematical Introduction to Linear Programming and Game Theory.
Cederberg: A Course in Modern Geometries.
Childs: A Concrete Introduction to Higher Algebra.
Chung: Elementary Probability Theory with Stochastic Processes. Third edition.
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Dixmier: General Topology.
Driver: Why Math?
Ebbinghaus/Flum/Thomas: Mathematical Logic.
Edgar: Measure, Topology, and Fractal Geometry.
Fischer: Intermediate Real Analysis.
Fleming: Functions of Several Variables. Second edition.
Foulds: Optimization Techniques: An Introduction.
Foulds: Combinatorial Optimization for Undergraduates.
Franklin: Methods of Mathematical Economics.
Halmos: Finite-Dimensional Vector Spaces. Second edition.
Halmos: Naive Set Theory.
Iooss/Joseph: Elementary Stability and Bifurcation Theory. Second edition.
James: Topological and Uniform Spaces.
Jänich: Topology.
Kemeny/Snell: Finite Markov Chains.
Klambauer: Aspects of Calculus.
Lang: A First Course in Calculus. Fifth edition.
Lang: Calculus of Several Variables. Third edition.
Lang: Introduction to Linear Algebra. Second editon.
Lang: Linear Algebra. Third edition.
Lang: Undergraduate Algebra. Second edition.
Lang: Undergraduate Analysis.
Lax/Burstein/Lax: Calculus with Applications and Computing. Volume 1.
LeCuyer: College Mathematics with APL.
Lidl/Pilz: Applied Abstract Algebra.
Macki/Strauss: Introduction to Optimal Control Theory.
Malitz: Introduction to Mathematical Logic.
Marsden/Weinstein: Calculus I, II, III. Second edition.
Martin: The Foundations of Geometry and the Non-Euclidean Plane.
Martin: Transformation Geometry: An Introduction to Symmetry.
Millman/Parker: Geometry: A Metric Approach with Models.
Owen: A First Course in the Mathematical Foundations of Thermodynamics.
Peressini/Sullivan/Uhl: The Mathematics of Nonlinear Programming.
Prenowitz/Jantosciak: Join Geometries.
Priestly: Calculus: An Historical Approach.

Undergraduate Texts in Mathematics

(continued)

Protter/Morrey: A First Course in Real Analysis.
Protter/Morrey: Intermediate Calculus. Second edition.
Ross: Elementary Analysis: The Theory of Calculus.
Scharlau/Opolka: From Fermat to Minkowski.
Sigler: Algebra.
Simmonds: A Brief on Tensor Analysis.
Singer/Thorpe: Lecture Notes on Elementary Topology and Geometry.
Smith: Linear Algebra. Second edition.
Smith: Primer of Modern Analysis. Second edition.
Stanton/White: Constructive Combinatorics.
Stillwell: Mathematics and Its History.
Strayer: Linear Programming and Its Applications.
Thorpe: Elementary Topics in Differential Geometry.
Troutman: Variational Calculus with Elementary Convexity.
Wilson: Much Ado About Calculus.

Contents

CHAPTER IV

CHAPTER V

CHAPTER VI

CHAPTER VII

CHAPTER VIII

CHAPTER IX

CHAPTER X

CHAPTER I

The Integers

I, §1. TERMINOLOGY OF SETS

A collection of objects is called a **set**. A member of this collection is also called an **element** of the set. It is useful in practice to use short symbols to denote certain sets. For instance, we denote by $\mathbf{Z}$ the set of all integers, i.e. all numbers of the type $0, \pm 1, \pm 2, \ldots$. Instead of saying that x is an element of a set S, we shall also frequently say that x **lies in** S, and write $x \in S$. For instance, we have $1 \in \mathbf{Z}$, and also $-4 \in \mathbf{Z}$.

If S and S' are sets, and if every element of S' is an element of S, then we say that S' is a **subset** of S. Thus the set of positive integers $\{1, 2, 3, \ldots\}$ is a subset of the set of all integers. To say that S' is a subset of S is to say that S' is part of S. Observe that our definition of a subset does not exclude the possibility that $S' = S$. If S' is a subset of S, but $S' \neq S$, then we shall say that S' is a **proper** subset of S. Thus $\mathbf{Z}$ is a subset of $\mathbf{Z}$, and the set of positive integers is a proper subset of $\mathbf{Z}$. To denote the fact that S' is a subset of S, we write $S' \subset S$, and also say that S' is **contained** in S.

If S_1, S_2 are sets, then the **intersection** of S_1 and S_2, denoted by $S_1 \cap S_2$, is the set of elements which lie in both S_1 and S_2. For instance, if S_1 is the set of integers $\geqq 1$ and S_2 is the set of integers $\leqq 1$, then

$$S_1 \cap S_2 = \{1\}$$

(the set consisting of the number 1).

The **union** of S_1 and S_2, denoted by $S_1 \cup S_2$, is the set of elements which lie in S_1 or in S_2. For instance, if S_1 is the set of integers $\leqq 0$

and S_2 is the set of integers $\geqq 0$, then $S_1 \cup S_2 = \mathbf{Z}$ is the set of all integers.

We see that certain sets consist of elements described by certain properties. If a set has no elements, it is called the **empty** set. For instance, the set of all integers x such that $x > 0$ and $x < 0$ is empty, because there is no such integer x.

If S, S' are sets, we denote by $S \times S'$ the set of all pairs (x, x') with $x \in S$ and $x' \in S'$.

We let $\# S$ denote the number of elements of a set S. If S is finite, we also call $\# S$ the **order** of S.

I, §2. BASIC PROPERTIES

The integers are so well known that it would be slightly tedious to axiomatize them immediately. Hence we shall assume that the reader is acquainted with the elementary properties of arithmetic, involving addition, multiplication, and inequalities, which are taught in all elementary schools. Later in this book, the reader will see how one can axiomatize such rules (see, for instance, the chapter on rings for the rules concerning addition and multiplication, and the chapter on ordering for the rules concerning inequalities).

We mention explicitly one property of the integers which we take as an axiom concerning them, and which is called **well-ordering**.

Every non-empty set of integers $\geqq 0$ *has a least element.*

(This means: If S is a non-empty set of integers $\geqq 0$, then there exists an integer $n \in S$ such that $n \leqq x$ for all $x \in S$.)

Using this well-ordering, we shall prove another property of the integers, called induction. It occurs in several forms.

Induction: First Form. *Suppose that for each integer* $n \geqq 1$ *we are given an assertion* $A(n)$, *and that we can prove the following two properties*:

(1) *The assertion* $A(1)$ *is true.*
(2) *For each integer* $n \geqq 1$, *if* $A(n)$ *is true, then* $A(n + 1)$ *is true.*

Then for all integers $n \geqq 1$, *the assertion* $A(n)$ *is true.*

Proof. Let S be the set of all positive integers n for which the assertion $A(n)$ is false. We wish to prove that S is empty, i.e. that there is no element in S. Suppose there is some element in S. By well-ordering, there exists a least element n_0 in S. By assumption, $n_0 \neq 1$, and hence $n_0 > 1$. Since n_0 is least, it follows that $n_0 - 1$ is not in S, in other words the assertion $A(n_0 - 1)$ is true. But then by property (2), we conclude that $A(n_0)$ is also true because

$$n_0 = (n_0 - 1) + 1.$$

This is a contradiction, which proves what we wanted.

Example. We wish to prove that for each integer $n \geqq 1$,

$$A(n): \quad 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

This is certainly true when $n = 1$, because

$$1 = \frac{1(1+1)}{2}.$$

Assume that our equation is true for an integer $n \geqq 1$. Then

$$\begin{aligned} 1 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{n^2 + n + 2n + 2}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Thus we have proved the two properties (1) and (2) for the statement denoted by $A(n+1)$, and we conclude by induction that $A(n)$ is true for all integers $n \geqq 1$.

Remark. In the statement of induction, we could replace 1 by 0 everywhere, and the proof would go through just as well.

The second form is a variation on the first.