

# Graduate Texts in Mathematics

**Serge Lang**

**Algebra**

**Revised Third Edition**

代數

第3版

Springer-Verlag

世界圖書出版公司

Serge Lang

# Algebra

Revised Third Edition

Springer

世界图书出版公司

书 名: Algebra Revised Third Edition  
作 者: Serge Lang  
中译名: 代数 第3版  
出 版 者: 世界图书出版公司北京公司  
印 刷 者: 北京世图印刷厂  
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: 010-64015659, 64038347  
电子信箱: kjsk@vip.sina.com  
开 本: 24 印 张: 39  
出版年代: 2004 年 11 月  
书 号: 7-5062-7184-2/O · 502  
版权登记: 图字:01-2004-5053  
定 价: 126.00 元

世界图书出版公司北京公司已获得 Springer-Verlag 授权在中国大陆  
独家重印发行。

Serge Lang  
Department of Mathematics  
Yale University  
New Haven, CT 96520  
USA

*Editorial Board*

S. Axler  
Mathematics Department  
San Francisco State  
University  
San Francisco, CA 94132  
USA  
axler@sfsu.edu

F.W. Gehring  
Mathematics Department  
East Hall  
University of Michigan  
Ann Arbor, MI 48109  
USA  
fgehring@  
math.lsa.umich.edu

K.A. Ribet  
Mathematics Department  
University of California,  
Berkeley  
Berkeley, CA 94720-3840  
USA  
ribet@math.berkeley.edu

---

Mathematics Subject Classification (2000): 13-01, 15-01, 16-01, 20-01

---

Library of Congress Cataloging-in-Publication Data

Algebra / Serge Lang.—Rev. 3rd ed.

p. cm. — (Graduate texts in mathematics ; 211)

Includes bibliographical references and index.

ISBN 0-387-95385-X (alk. paper)

1. Algebra. I. Title. II. Series.

QA154.3.L3 2002

512—dc21

2001054916

Printed on acid-free paper.

This title was previously published by Addison-Wesley, Reading, MA 1993.

© 2002 Springer-Verlag New York, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

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.

Springer-Verlag is a part of *Springer Science+Business Media*

*springeronline.com*

---

## FOREWORD

---

The present book is meant as a basic text for a one-year course in algebra, at the graduate level.

### A perspective on algebra

As I see it, the graduate course in algebra must primarily prepare students to handle the algebra which they will meet in all of mathematics: topology, partial differential equations, differential geometry, algebraic geometry, analysis, and representation theory, not to speak of algebra itself and algebraic number theory with all its ramifications. Hence I have inserted throughout references to papers and books which have appeared during the last decades, to indicate some of the directions in which the algebraic foundations provided by this book are used; I have accompanied these references with some motivating comments, to explain how the topics of the present book fit into the mathematics that is to come subsequently in various fields; and I have also mentioned some unsolved problems of mathematics in algebra and number theory. The *abc* conjecture is perhaps the most spectacular of these.

Often when such comments and examples occur out of the logical order, especially with examples from other branches of mathematics, of necessity some terms may not be defined, or may be defined only later in the book. I have tried to help the reader not only by making cross-references within the book, but also by referring to other books or papers which I mention explicitly.

I have also added a number of exercises. On the whole, I have tried to make the exercises complement the examples, and to give them aesthetic appeal. I have tried to use the exercises also to drive readers toward variations and applications of the main text, as well as toward working out special cases, and as openings toward applications beyond this book.

### Organization

Unfortunately, a book must be projected in a totally ordered way on the page axis, but that's not the way mathematics "is", so readers have to make choices how to reset certain topics in parallel for themselves, rather than in succession.

I have inserted cross-references to help them do this, but different people will make different choices at different times depending on different circumstances.

The book splits naturally into several parts. The first part introduces the basic notions of algebra. After these basic notions, the book splits in two major directions: the direction of algebraic equations including the Galois theory in Part II; and the direction of linear and multilinear algebra in Parts III and IV. There is some sporadic feedback between them, but their unification takes place at the next level of mathematics, which is suggested, for instance, in §15 of Chapter VI. Indeed, the study of algebraic extensions of the rationals can be carried out from two points of view which are complementary and interrelated: representing the Galois group of the algebraic closure in groups of matrices (the linear approach), and giving an explicit determination of the irrationalities generating algebraic extensions (the equations approach). At the moment, representations in  $GL_2$  are at the center of attention from various quarters, and readers will see  $GL_2$  appear several times throughout the book. For instance, I have found it appropriate to add a section describing all irreducible characters of  $GL_2(F)$  when  $F$  is a finite field. Ultimately,  $GL_2$  will appear as the simplest but typical case of groups of Lie types, occurring both in a differential context and over finite fields or more general arithmetic rings for arithmetic applications.

After almost a decade since the second edition, I find that the basic topics of algebra have become stable, with one exception. I have added two sections on elimination theory, complementing the existing section on the resultant. Algebraic geometry having progressed in many ways, it is now sometimes returning to older and harder problems, such as searching for the effective construction of polynomials vanishing on certain algebraic sets, and the older elimination procedures of last century serve as an introduction to those problems.

Except for this addition, the main topics of the book are unchanged from the second edition, but I have tried to improve the book in several ways.

First, some topics have been reordered. I was informed by readers and reviewers of the tension existing between having a textbook usable for relatively inexperienced students, and a reference book where results could easily be found in a systematic arrangement. I have tried to reduce this tension by moving all the homological algebra to a fourth part, and by integrating the commutative algebra with the chapter on algebraic sets and elimination theory, thus giving an introduction to different points of view leading toward algebraic geometry.

### **The book as a text and a reference**

In teaching the course, one might wish to push into the study of algebraic equations through Part II, or one may choose to go first into the linear algebra of Parts III and IV. One semester could be devoted to each, for instance. The chapters have been so written as to allow maximal flexibility in this respect, and I have frequently committed the crime of *l'èse-Bourbaki* by repeating short arguments or definitions to make certain sections or chapters logically independent of each other.

Granting the material which under no circumstances can be omitted from a basic course, there exist several options for leading the course in various directions. It is impossible to treat all of them with the same degree of thoroughness. The precise point at which one is willing to stop in any given direction will depend on time, place, and mood. However, any book with the aims of the present one must include a choice of topics, pushing ahead in deeper waters, while stopping short of full involvement.

There can be no universal agreement on these matters, not even between the author and himself. Thus the concrete decisions as to what to include and what not to include are finally taken on grounds of general coherence and aesthetic balance. Anyone teaching the course will want to impress their own personality on the material, and may push certain topics with more vigor than I have, at the expense of others. Nothing in the present book is meant to inhibit this.

Unfortunately, the goal to present a fairly comprehensive perspective on algebra required a substantial increase in size from the first to the second edition, and a moderate increase in this third edition. These increases require some decisions as to what to omit in a given course.

Many shortcuts can be taken in the presentation of the topics, which admits many variations. For instance, one can proceed into field theory and Galois theory immediately after giving the basic definitions for groups, rings, fields, polynomials in one variable, and vector spaces. Since the Galois theory gives very quickly an impression of depth, this is very satisfactory in many respects.

It is appropriate here to recall my original indebtedness to Artin, who first taught me algebra. The treatment of the basics of Galois theory is much influenced by the presentation in his own monograph.

### Audience and background

As I already stated in the forewords of previous editions, the present book is meant for the graduate level, and I expect most of those coming to it to have had suitable exposure to some algebra in an undergraduate course, or to have appropriate mathematical maturity. I expect students taking a graduate course to have had some exposure to vector spaces, linear maps, matrices, and they will no doubt have seen polynomials at the very least in calculus courses.

My books *Undergraduate Algebra* and *Linear Algebra* provide more than enough background for a graduate course. Such elementary texts bring out in parallel the two basic aspects of algebra, and are organized differently from the present book, where both aspects are deepened. Of course, some aspects of the linear algebra in Part III of the present book are more "elementary" than some aspects of Part II, which deals with Galois theory and the theory of polynomial equations in several variables. Because Part II has gone deeper into the study of algebraic equations, of necessity the parallel linear algebra occurs only later in the total ordering of the book. Readers should view both parts as running simultaneously.

Unfortunately, the amount of algebra which one should ideally absorb during this first year in order to have a proper background (irrespective of the subject in which one eventually specializes) exceeds the amount which can be covered physically by a lecturer during a one-year course. Hence more material must be included than can actually be handled in class. I find it essential to bring this material to the attention of graduate students.

I hope that the various additions and changes make the book easier to use as a text. By these additions, I have tried to expand the general mathematical perspective of the reader, insofar as algebra relates to other parts of mathematics.

### Acknowledgements

I am indebted to many people who have contributed comments and criticisms for the previous editions, but especially to Daniel Bump, Steven Krantz, and Diane Meuser, who provided extensive comments as editorial reviewers for Addison-Wesley. I found their comments very stimulating and valuable in preparing this third edition. I am much indebted to Barbara Holland for obtaining these reviews when she was editor. I am also indebted to Karl Matsumoto who supervised production under very trying circumstances. Finally I thank the many people who have made suggestions and corrections, especially George Bergman, Chee-Whye Chin, Ki-Bong Nam, David Wasserman, and Randy Scott, who provided me with a list of errata. I also thank Thomas Shipley and Paul Vojta for their lists of errata to the third edition. These have been corrected in the subsequent printings.

Serge Lang  
New Haven

### For the 2002 and beyond Springer printings

From now on, *Algebra* appears with Springer-Verlag, like the rest of my books. With this change, I considered the possibility of a new edition, but decided against it. I view the book as very stable. The only addition which I would make, if starting from scratch, would be some of the algebraic properties of  $SL_n$  and  $GL_n$  (over  $\mathbf{R}$  or  $\mathbf{C}$ ), beyond the proof of simplicity in Chapter XIII. As things stood, I just inserted some exercises concerning some aspects which everybody should know. Readers can see these worked out in Jorgenson/Lang, *Spherical Inversion on  $SL_n(\mathbf{R})$* , Springer Verlag 2001, as well as other basic algebraic properties on which analysis is superimposed so that algebra in this context appears as a supporting tool.

I thank specifically Tom von Foerster, Ina Lindeman and Mark Spencer for their editorial support at Springer, as well as Terry Kornak and Brian Howe who have taken care of production.

Serge Lang  
New Haven 2002



# Logical Prerequisites

We assume that the reader is familiar with sets, and with the symbols  $\cap$ ,  $\cup$ ,  $\supset$ ,  $\subset$ ,  $\in$ . If  $A$ ,  $B$  are sets, we use the symbol  $A \subset B$  to mean that  $A$  is contained in  $B$  but may be equal to  $B$ . Similarly for  $A \supset B$ .

If  $f: A \rightarrow B$  is a mapping of one set into another, we write

$$x \mapsto f(x)$$

to denote the effect of  $f$  on an element  $x$  of  $A$ . We distinguish between the arrows  $\rightarrow$  and  $\mapsto$ . We denote by  $f(A)$  the set of all elements  $f(x)$ , with  $x \in A$ .

Let  $f: A \rightarrow B$  be a mapping (also called a map). We say that  $f$  is **injective** if  $x \neq y$  implies  $f(x) \neq f(y)$ . We say  $f$  is **surjective** if given  $b \in B$  there exists  $a \in A$  such that  $f(a) = b$ . We say that  $f$  is **bijective** if it is both surjective and injective.

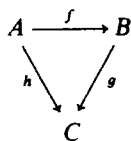
A subset  $A$  of a set  $B$  is said to be **proper** if  $A \neq B$ .

Let  $f: A \rightarrow B$  be a map, and  $A'$  a subset of  $A$ . The restriction of  $f$  to  $A'$  is a map of  $A'$  into  $B$  denoted by  $f|A'$ .

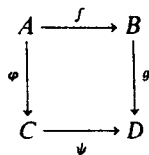
If  $f: A \rightarrow B$  and  $g: B \rightarrow C$  are maps, then we have a composite map  $g \circ f$  such that  $(g \circ f)(x) = g(f(x))$  for all  $x \in A$ .

Let  $f: A \rightarrow B$  be a map, and  $B'$  a subset of  $B$ . By  $f^{-1}(B')$  we mean the subset of  $A$  consisting of all  $x \in A$  such that  $f(x) \in B'$ . We call it the **inverse image** of  $B'$ . We call  $f(A)$  the **image** of  $f$ .

A **diagram**



is said to be **commutative** if  $g \circ f = h$ . Similarly, a **diagram**



## X LOGICAL PREREQUISITES

is said to be **commutative** if  $g \circ f = \psi \circ \phi$ . We deal sometimes with more complicated diagrams, consisting of arrows between various objects. Such diagrams are called commutative if, whenever it is possible to go from one object to another by means of two sequences of arrows, say

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} A_n$$

and

$$A_1 \xrightarrow{g_1} B_2 \xrightarrow{g_2} \cdots \xrightarrow{g_{m-1}} B_m = A_n,$$

then

$$f_{n-1} \circ \cdots \circ f_1 = g_{m-1} \circ \cdots \circ g_1,$$

in other words, the composite maps are equal. Most of our diagrams are composed of triangles or squares as above, and to verify that a diagram consisting of triangles or squares is commutative, it suffices to verify that each triangle and square in it is commutative.

We assume that the reader is acquainted with the integers and rational numbers, denoted respectively by  $\mathbf{Z}$  and  $\mathbf{Q}$ . For many of our examples, we also assume that the reader knows the real and complex numbers, denoted by  $\mathbf{R}$  and  $\mathbf{C}$ .

Let  $A$  and  $I$  be two sets. By a family of elements of  $A$ , indexed by  $I$ , one means a map  $f: I \rightarrow A$ . Thus for each  $i \in I$  we are given an element  $f(i) \in A$ . Although a family does not differ from a map, we think of it as determining a collection of objects from  $A$ , and write it often as

$$\{f(i)\}_{i \in I}$$

or

$$\{a_i\}_{i \in I},$$

writing  $a_i$  instead of  $f(i)$ . We call  $I$  the indexing set.

We assume that the reader knows what an equivalence relation is. Let  $A$  be a set with an equivalence relation, let  $E$  be an equivalence class of elements of  $A$ . We sometimes try to define a map of the equivalence classes into some set  $B$ . To define such a map  $f$  on the class  $E$ , we sometimes first give its value on an element  $x \in E$  (called a representative of  $E$ ), and then show that it is independent of the choice of representative  $x \in E$ . In that case we say that  $f$  is **well defined**.

We have products of sets, say finite products  $A \times B$ , or  $A_1 \times \cdots \times A_n$ , and products of families of sets.

We shall use Zorn's lemma, which we describe in Appendix 2.

We let  $\#(S)$  denote the number of elements of a set  $S$ , also called the **cardinality** of  $S$ . The notation is usually employed when  $S$  is finite. We also write  $\#(S) = \text{card}(S)$ .

---

# CONTENTS

---

## Part One      The Basic Objects of Algebra

|  |                |            |
|--|----------------|------------|
| <b>Chapter I</b>                       | <b>Groups</b>  | <b>3</b>   |
| 1. Monoids                             | 3              |            |
| 2. Groups                              | 7              |            |
| 3. Normal subgroups                    | 13             |            |
| 4. Cyclic groups                       | 23             |            |
| 5. Operations of a group on a set      | 25             |            |
| 6. Sylow subgroups                     | 33             |            |
| 7. Direct sums and free abelian groups | 36             |            |
| 8. Finitely generated abelian groups   | 42             |            |
| 9. The dual group                      | 46             |            |
| 10. Inverse limit and completion       | 49             |            |
| 11. Categories and functors            | 53             |            |
| 12. Free groups                        | 66             |            |
| <br>                                   |                |            |
| <b>Chapter II</b>                      | <b>Rings</b>   | <b>83</b>  |
| 1. Rings and homomorphisms             | 83             |            |
| 2. Commutative rings                   | 92             |            |
| 3. Polynomials and group rings         | 97             |            |
| 4. Localization                        | 107            |            |
| 5. Principal and factorial rings       | 111            |            |
| <br>                                   |                |            |
| <b>Chapter III</b>                     | <b>Modules</b> | <b>117</b> |
| 1. Basic definitions                   | 117            |            |
| 2. The group of homomorphisms          | 122            |            |
| 3. Direct products and sums of modules | 127            |            |
| 4. Free modules                        | 135            |            |
| 5. Vector spaces                       | 139            |            |
| 6. The dual space and dual module      | 142            |            |
| 7. Modules over principal rings        | 146            |            |
| 8. Euler-Poincaré maps                 | 155            |            |
| 9. The snake lemma                     | 157            |            |
| 10. Direct and inverse limits          | 159            |            |

**Chapter IV      Polynomials** **173**

1. Basic properties for polynomials in one variable      173
2. Polynomials over a factorial ring      180
3. Criteria for irreducibility      183
4. Hilbert's theorem      186
5. Partial fractions      187
6. Symmetric polynomials      190
7. Mason-Stothers theorem and the *abc* conjecture      194
8. The resultant      199
9. Power series      205

**Part Two      Algebraic Equations**

**Chapter V      Algebraic Extensions** **223**

1. Finite and algebraic extensions      225
2. Algebraic closure      229
3. Splitting fields and normal extensions      236
4. Separable extensions      239
5. Finite fields      244
6. Inseparable extensions      247

**Chapter VI      Galois Theory** **261**

1. Galois extensions      261
2. Examples and applications      269
3. Roots of unity      276
4. Linear independence of characters      282
5. The norm and trace      284
6. Cyclic extensions      288
7. Solvable and radical extensions      291
8. Abelian Kummer theory      293
9. The equation  $X^n - a = 0$       297
10. Galois cohomology      302
11. Non-abelian Kummer extensions      304
12. Algebraic independence of homomorphisms      308
13. The normal basis theorem      312
14. Infinite Galois extensions      313
15. The modular connection      315

**Chapter VII      Extensions of Rings** **333**

1. Integral ring extensions      333
2. Integral Galois extensions      340
3. Extension of homomorphisms      346

**Chapter VIII Transcendental Extensions 355**

1. Transcendence bases 355
2. Noether normalization theorem 357
3. Linearly disjoint extensions 360
4. Separable and regular extensions 363
5. Derivations 368

**Chapter IX Algebraic Spaces 377**

1. Hilbert's Nullstellensatz 377
2. Algebraic sets, spaces and varieties 381
3. Projections and elimination 388
4. Resultant systems 401
5. Spec of a ring 405

**Chapter X Noetherian Rings and Modules 413**

1. Basic criteria 413
2. Associated primes 416
3. Primary decomposition 421
4. Nakayama's lemma 424
5. Filtered and graded modules 426
6. The Hilbert polynomial 431
7. Indecomposable modules 439

**Chapter XI Real Fields 449**

1. Ordered fields 449
2. Real fields 451
3. Real zeros and homomorphisms 457

**Chapter XII Absolute Values 465**

1. Definitions, dependence, and independence 465
2. Completions 468
3. Finite extensions 476
4. Valuations 480
5. Completions and valuations 486
6. Discrete valuations 487
7. Zeros of polynomials in complete fields 491

**Part Three Linear Algebra and Representations****Chapter XIII Matrices and Linear Maps 503**

1. Matrices 503
2. The rank of a matrix 506

## **xiv** CONTENTS

- 3. Matrices and linear maps 507
- 4. Determinants 511
- 5. Duality 522
- 6. Matrices and bilinear forms 527
- 7. Sesquilinear duality 531
- 8. The simplicity of  $SL_2(F)/\pm 1$  536
- 9. The group  $SL_n(F)$ ,  $n \geq 3$  540

### **Chapter XIV Representation of One Endomorphism 553**

- 1. Representations 553
- 2. Decomposition over one endomorphism 556
- 3. The characteristic polynomial 561

### **Chapter XV Structure of Bilinear Forms 571**

- 1. Preliminaries, orthogonal sums 571
- 2. Quadratic maps 574
- 3. Symmetric forms, orthogonal bases 575
- 4. Symmetric forms over ordered fields 577
- 5. Hermitian forms 579
- 6. The spectral theorem (hermitian case) 581
- 7. The spectral theorem (symmetric case) 584
- 8. Alternating forms 586
- 9. The Pfaffian 588
- 10. Witt's theorem 589
- 11. The Witt group 594

### **Chapter XVI The Tensor Product 601**

- 1. Tensor product 601
- 2. Basic properties 607
- 3. Flat modules 612
- 4. Extension of the base 623
- 5. Some functorial isomorphisms 625
- 6. Tensor product of algebras 629
- 7. The tensor algebra of a module 632
- 8. Symmetric products 635

### **Chapter XVII Semisimplicity 641**

- 1. Matrices and linear maps over non-commutative rings 641
- 2. Conditions defining semisimplicity 645
- 3. The density theorem 646
- 4. Semisimple rings 651
- 5. Simple rings 654
- 6. The Jacobson radical, base change, and tensor products 657
- 7. Balanced modules 660

|  |   |            |
|--|---|------------|
| <b>Chapter XVIII</b>                               | <b>Representations of Finite Groups</b>                         | <b>663</b> |
| 1. Representations and semisimplicity              | 663   |            |
| 2. Characters                                      | 667   |            |
| 3. 1-dimensional representations                   | 671   |            |
| 4. The space of class functions                    | 673   |            |
| 5. Orthogonality relations                         | 677   |            |
| 6. Induced characters                              | 686   |            |
| 7. Induced representations                         | 688   |            |
| 8. Positive decomposition of the regular character | 699   |            |
| 9. Supersolvable groups                            | 702   |            |
| 10. Brauer's theorem                               | 704   |            |
| 11. Field of definition of a representation        | 710   |            |
| 12. Example: $GL_2$ over a finite field            | 712   |            |
| <b>Chapter XIX</b>                                 | <b>The Alternating Product</b>                                  | <b>731</b> |
| 1. Definition and basic properties                 | 731   |            |
| 2. Fitting ideals                                  | 738   |            |
| 3. Universal derivations and the de Rham complex   | 746   |            |
| 4. The Clifford algebra                            | 749   |            |
| <b>Part Four</b>                                   | <b>Homological Algebra</b>                                      |            |
| <b>Chapter XX</b>                                  | <b>General Homology Theory</b>                                  | <b>761</b> |
| 1. Complexes                                       | 761   |            |
| 2. Homology sequence                               | 767   |            |
| 3. Euler characteristic and the Grothendieck group | 769   |            |
| 4. Injective modules                               | 782   |            |
| 5. Homotopies of morphisms of complexes            | 787   |            |
| 6. Derived functors                                | 790   |            |
| 7. Delta-functors                                  | 799   |            |
| 8. Bifunctors                                      | 806   |            |
| 9. Spectral sequences                              | 814   |            |
| <b>Chapter XXI</b>                                 | <b>Finite Free Resolutions</b>                                  | <b>835</b> |
| 1. Special complexes                               | 835   |            |
| 2. Finite free resolutions                         | 839   |            |
| 3. Unimodular polynomial vectors                   | 846   |            |
| 4. The Koszul complex                              | 850   |            |
| <b>Appendix 1</b>                                  | <b>The Transcendence of <math>e</math> and <math>\pi</math></b> | <b>867</b> |
| <b>Appendix 2</b>                                  | <b>Some Set Theory</b>  | <b>875</b> |
| <b>Bibliography</b>                                |   | <b>895</b> |
| <b>Index</b>                                       |   | <b>903</b> |

---

# **Part One**

---

## **THE BASIC OBJECTS OF ALGEBRA**

---

This part introduces the basic notions of algebra, and the main difficulty for the beginner is to absorb a reasonable vocabulary in a short time. None of the concepts is difficult, but there is an accumulation of new concepts which may sometimes seem heavy.

To understand the next parts of the book, the reader needs to know essentially only the basic definitions of this first part. Of course, a theorem may be used later for some specific and isolated applications, but on the whole, we have avoided making long logical chains of interdependence.



