

ALGEBRA

Second Edition

Serge Lang

ALGEBRA

Second Edition

Serge Lang

Yale University, New Haven, Connecticut



1984

Addison-Wesley Publishing Company, Inc.
Advanced Book Program
Menlo Park, California

Reading, Massachusetts · London · Amsterdam · Don Mills, Ontario · Sydney · Tokyo

Library of Congress Cataloging in Publication Data

Lang, Serge, 1927-
Algebra.

Includes index.

1. Algebra. I. Title.

QA154.2.L36 1984 512 84-6711
ISBN 0-201-05487-6

Copyright © 1984 by Addison-Wesley Publishing Company, Inc.
Published simultaneously in Canada.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher, Addison-Wesley Publishing Company, Inc., Advanced Book Program, Menlo Park, California 94025, U.S.A.

Manufactured in the United States of America

ABCDEFGHIJ-HA-8987654

FOREWORD

*Je préfère la nommer ainsi [algèbre abstraite]
plutôt qu'algèbre moderne, parce qu'elle
vivra sans doute longtemps et finira donc
par devenir l'algèbre ancienne.*

F. SEVERI
Liège, 1949

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

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.

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.

I have added a section on non-abelian Kummer theory, because several times during the last ten years I have seen the need for this kind of material in several contexts of number theory, and there was no satisfactory reference for it.

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.

Instead of going into field theory, one can also first treat the theory of rings, modules, and commutative Noetherian rings, taking the direction of commutative algebra; or one can also treat the linear algebra, after covering the basic definitions. The chapters have been so written as to allow maximal flexibility in this respect, and I have frequently committed the crime of lèse-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. The chapters on real fields and absolute

values, for instance, can be omitted safely, or can be read by students independently of the class. The chapter on group representations also. The Witt theorem on quadratic forms can also be omitted. However, any book with the aims of the present one must include a choice of these topics, pushing ahead in deeper waters, while stopping short of full involvement, and keeping the number of pages within reasonable bounds. 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.

In this second edition, I have added several topics, having mostly to do with commutative algebra and homological algebra, for instance: projective and injective modules, leading to an extended treatment of homological algebra, with derived functors, the Hilbert syzygy theorem, and a more thorough discussion of K -groups and Euler characteristics; the Quillen–Suslin theorem (previously Serre’s conjecture) that finite projective modules over a polynomial ring are free; the Weierstrass preparation theorem; the Hilbert polynomial in connection with filtered and graded modules; more material on tensor products, like flat modules and derivations; etc. In light of the pervasive use of all this material in algebraic geometry, topology, representation theory (finite and infinite dimensional), differential geometry, several complex variables and whatnot (e.g. Griffiths–Harris), it seemed important to expand the treatment of these topics. Today, one has a better perspective than twenty years ago as to what constitutes fundamentally important results which can be covered in a few pages, maximizing the results and minimizing the cost in space. For a more complete treatment of commutative algebra, I recommend Matsumura’s book on the subject.

As in the first edition, there is some reason to include more on linear groups and their representations, and on Lie algebras, than I could do and still have a reasonably sized book, say holding in one volume. However, I have added a proof of the simplicity of SL_n modulo its center. But again, several excellent texts on Lie algebras and Lie groups have become available, so I do not feel too guilty in omitting these topics. See in particular Serre’s notes, *Lie Algebras and Lie Groups*, and for a more complete treatment, Bourbaki’s and Jacobson’s books on the same subject.

I have added a number of new exercises, especially in the chapters which are most likely to be of fundamental use, like the chapter on group theory, Noetherian rings, Galois theory, and tensor products.

As prerequisites, I assume only that the reader is acquainted with the basic language of mathematics (i.e. essentially sets and mappings), and the integers and rational numbers. A more specific description of what is assumed is summarized on the following pages. On a few occasions, I use determinants

before treating these formally in the text. Most readers will already be acquainted with determinants, and I feel it is better for the organization of the whole book to allow such minor deviations from a total ordering of the logic involved.

SERGE LANG
New Haven, 1984

PREREQUISITES

We assume that the reader is familiar with sets, and 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.

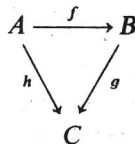
A subset A' of a set B is said to be **proper** if $A' \neq B$.

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 $f|_{A'}$.

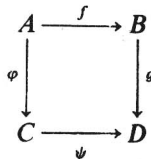
If $f: A \rightarrow B$ and $g: B \rightarrow C$ are maps, then we have a composite map $g \circ f$ such that $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

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 PREREQUISITES

is said to be **commutative** if $g \circ f = \psi \circ \varphi$. 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

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_n} A_n$$

and

$$A_1 \xrightarrow{g_1} B_2 \xrightarrow{g_2} \dots \xrightarrow{g_m} B_m = A_n,$$

then

$$f_n \circ f_{n-1} \circ \dots \circ f_1 = g_m \circ g_{m-1} \circ \dots \circ g_1,$$

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 $A_1 \times \dots \times A_n$, and products of families of sets.

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

CONTENTS

Part One Groups, Rings, and Modules

Chapter I	Groups	3
1.	Monoids	3
2.	Groups	7
3.	Cyclic groups	11
4.	Normal subgroups	12
5.	Operations of a group on a set	20
6.	Sylow subgroups	24
7.	Categories and functors	26
8.	Free groups	34
9.	Direct sums and free abelian groups	41
10.	Finitely generated abelian groups	47
11.	The dual group	51
Chapter II	Rings	60
1.	Rings and homomorphisms	60
2.	Commutative rings	66
3.	Localization	71
4.	Principal rings	74
5.	Spec of a ring	77
Chapter III	Modules	81
1.	Basic definitions	81
2.	The group of homomorphisms	84
3.	Direct products and sums of modules	86
4.	Free modules	92
5.	Vector spaces	93
6.	The dual space	96
7.	The snake lemma	100

xii CONTENTS

- 8. Projective and injective modules 101
- 9. Direct and inverse limits 106

Chapter IV Homology 116

- 1. Complexes 117
- 2. Homology sequence 121
- 3. Euler characteristic 123
- 4. Special complexes 133
- 5. Homotopies of morphisms of complexes 137
- 6. Derived functors 141
- 7. Delta-functors 148
- 8. Bifunctors 155
- 9. Spectral sequences 163

Chapter V Polynomials 176

- 1. Free algebras 176
- 2. Definition of polynomials 180
- 3. Elementary properties of polynomials 185
- 4. The Euclidean algorithm 190
- 5. Partial fractions 194
- 6. Unique factorization in several variables 197
- 7. Criteria for irreducibility 200
- 8. The derivative and multiple roots 202
- 9. Symmetric polynomials 204
- 10. The resultant 206
- 11. Power series 211

Chapter VI Noetherian Rings and Modules 222

- 1. Basic criteria 222
- 2. Hilbert's theorem 226
- 3. Power series are Noetherian 227
- 4. Associated primes 228
- 5. Primary decomposition 233
- 6. Nakayama's lemma 236
- 7. Filtered and graded modules 238
- 8. The Hilbert polynomial 243
- 9. Indecomposable modules 246
- 10. Finite free resolutions 250

Part Two Field Theory**Chapter VII Algebraic Extensions****265**

1. Finite and algebraic extensions 265
2. Algebraic closure 271
3. Splitting fields and normal extensions 278
4. Separable extensions 281
5. Finite fields 287
6. Primitive elements 290
7. Purely inseparable extensions 291

Chapter VIII Galois Theory**300**

1. Galois extensions 300
2. Examples and applications 308
3. Roots of unity 313
4. Linear independence of characters 318
5. The norm and trace 320
6. Cyclic extensions 323
7. Solvable and radical extensions 326
8. Abelian Kummer theory 328
9. The equation $X^n - a = 0$ 331
10. Galois cohomology 334
11. Non-abelian Kummer extensions 336
12. Algebraic independence of homomorphisms 340
13. The normal basis theorem 344

Chapter IX Extensions of Rings**355**

1. Integral ring extensions 355
2. Integral Galois extensions 362
3. Extension of homomorphisms 368

Chapter X Transcendental Extensions**372**

1. Transcendence bases 372
2. Hilbert's Nullstellensatz 374
3. Algebraic sets 376
4. Noether normalization theorem 378
5. Linearly disjoint extensions 379
6. Separable extensions 382
7. Derivations 385

Chapter XI Real Fields 390

- 1. Ordered fields 390
- 2. Real fields 392
- 3. Real zeros and homomorphisms 398

Chapter XII Absolute Values 404

- 1. Definitions, dependence, and independence 404
- 2. Completions 407
- 3. Finite extensions 414
- 4. Valuations 417
- 5. Completions and valuations 425
- 6. Discrete valuations 426
- 7. Zeros of polynomials in complete fields 430

Part Three Linear Algebra and Representations

Chapter XIII Matrices and Linear Maps 441

- 1. Matrices 441
- 2. The rank of a matrix 444
- 3. Matrices and linear maps 445
- 4. Determinants 449
- 5. Duality 458
- 6. Matrices and bilinear forms 463
- 7. Sesquilinear duality 467
- 8. The simplicity of $SL_2(F)/\pm 1$ 472
- 9. The group $SL_n(F)$, $n \geq 3$ 476
- 10. Fitting ideals 480
- 11. Unimodular polynomial vectors

Chapter XIV Structure of Bilinear Forms 498

- 1. Preliminaries, orthogonal sums 498
- 2. Quadratic maps 501
- 3. Symmetric forms, orthogonal bases 502
- 4. Hyperbolic spaces 503
- 5. Witt's theorem 505
- 6. The Witt group 508
- 7. Symmetric forms over ordered fields 509
- 8. The Clifford algebra 511
- 9. Alternating forms 515
- 10. The Pfaffian 517
- 11. Hermitian forms 519
- 12. The spectral theorem (hermitian case) 521
- 13. The spectral theorem (symmetric case) 524

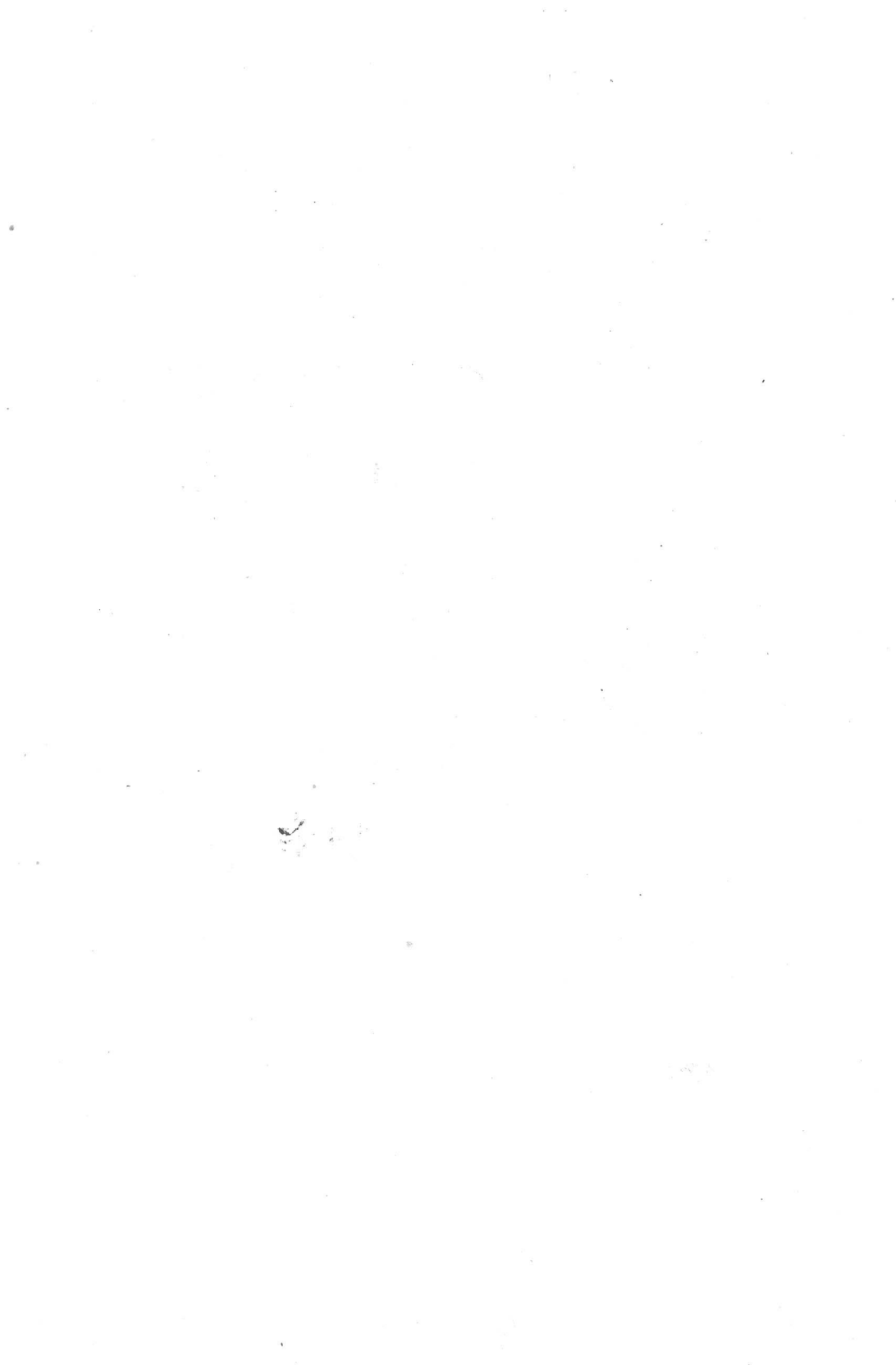
Chapter XV	Representation of One Endomorphism	529
1.	Representations	529
2.	Modules over principal rings	532
3.	Decomposition over one endomorphism	541
4.	The characteristic polynomial	545
Chapter XVI	Multilinear Products	554
1.	Tensor product	554
2.	Basic properties	560
3.	Flat modules	565
4.	Extension of the base	575
5.	Some functorial isomorphisms	
6.	Tensor product of algebras	581
7.	The tensor algebra of a module	583
8.	Symmetric products	586
9.	Alternating products	588
10.	The Koszul complex	593
11.	The Grothendieck ring	605
12.	Universal derivations	610
Chapter XVII	Semisimplicity	621
1.	Matrices and linear maps over non-commutative rings	621
2.	Conditions defining semisimplicity	625
3.	The density theorem	626
4.	Semisimple rings	629
5.	Simple rings	632
6.	Balanced modules	636
Chapter XVIII	Representations of Finite Groups	639
1.	Semisimplicity of the group algebra	639
2.	Characters	641
3.	1-dimensional representations	645
4.	The space of class functions	647
5.	Orthogonality relations	651
6.	Induced characters	659
7.	Induced representations	661
8.	Positive decomposition of the regular character	666
9.	Supersolvable groups	668
10.	Brauer's theorem	671
11.	Field of definition of a representation	674
Appendix 1	The Transcendence of e and π	681
Appendix 2	Some Set Theory	688
Index		707

Part One

GROUPS, RINGS and MODULES

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.



CHAPTER I

Groups

§1. MONOIDS

Let S be a set. A mapping

$$S \times S \rightarrow S$$

is sometimes called a **law of composition** (of S into itself). If x, y are elements of S , the image of the pair (x, y) under this mapping is also called their **product** under the law of composition, and will be denoted by xy . (Sometimes, we also write $x \cdot y$, and in many cases it is also convenient to use an additive notation, and thus to write $x + y$. In that case, we call this element the **sum** of x and y . It is customary to use the notation $x + y$ only when the relation $x + y = y + x$ holds.)

Let S be a set with a law of composition. If x, y, z are elements of S , then we may form their product in two ways: $(xy)z$ and $x(yz)$. If $(xy)z = x(yz)$ for all x, y, z in S then we say that the law of composition is **associative**.

An element e of S such that $ex = x = xe$ for all $x \in S$ is called a **unit element**. (When the law of composition is written additively, the unit element is denoted by 0 , and is called a **zero element**.) A unit element is unique, for if e' is another unit element, we have

$$e = ee' = e'$$

by assumption. In most cases, the unit element is written simply 1 (instead of e). For most of this chapter, however, we shall write e so as to avoid confusion in proving the most basic properties.

A **monoid** is a set G , with a law of composition which is associative, and having a unit element (so that in particular, G is not empty).

Let G be a monoid, and x_1, \dots, x_n elements of G (where n is an integer > 1). We define their product inductively:

$$\prod_{v=1}^n x_v = x_1 \cdots x_n = (x_1 \cdots x_{n-1})x_n.$$

We then have the following rule:

$$\prod_{\mu=1}^m x_\mu \cdot \prod_{v=1}^n x_{m+v} = \prod_{v=1}^{m+n} x_v,$$

which essentially asserts that we can insert parentheses in any manner in our product without changing its value. The proof is easy by induction, and we shall leave it as an exercise.

One also writes

$$\prod_{m+1}^{m+n} x_v \quad \text{instead of} \quad \prod_{v=1}^n x_{m+v}$$

and we define

$$\prod_{v=1}^0 x_v = e.$$

As a matter of convention, we agree also that the empty product is equal to the unit element.

It would be possible to define more general laws of composition, i.e. maps $S_1 \times S_2 \rightarrow S_3$ using arbitrary sets. One can then express associativity and commutativity in any setting for which they make sense. For instance, for commutativity we need a law of composition

$$f: S \times S \rightarrow T$$

where the two sets of departure are the same. **Commutativity** then means $f(x, y) = f(y, x)$, or $xy = yx$ if we omit the mapping f from the notation. For associativity, we leave it to the reader to formulate the most general combination of sets under which it will work. We shall meet special cases later, for instance arising from maps

$$S \times S \rightarrow S \quad \text{and} \quad S \times T \rightarrow T.$$

Then a product $(xy)z$ makes sense with $x \in S$, $y \in S$, and $z \in T$. The product $x(yz)$ also makes sense for such elements x, y, z and thus it makes sense to say that our law of composition is associative, namely to say that for all x, y, z as above we have $(xy)z = x(yz)$.

If the law of composition of G is commutative, we also say that G is **commutative (or abelian)**.