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

Published simultaneously in Canada.

Manufactured in the United States of America

ABCDEFGHIJ-HA-8987654

FOREWORD

Je préfère la nommer ainsi [algèbre abstraite] plutôt qu'algèbre moderne, parcequ'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 $f: A \to B$ 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 $\to$ and $\mapsto$. We denote by $f(A)$ the set of all elements $f(x)$, with $x \in A$.

Let $f: A \to B$ 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.

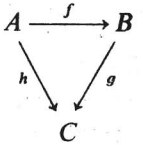
A subset A of a set B is said to be **proper** if $A \neq B$.

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

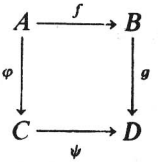
If $f: A \to B$ and $g: B \to C$ are maps, then we have a composite map $g \circ f$ such that $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

Let $f: A \to B$ 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**



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

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

and

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

then

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

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 $f: I \to A$. 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.

CONTENTS

Part Two Field Theory

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

$$S \times S \to S$$

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 $x_1, \ldots, x_n$ elements of G (where n is an integer > 1). We define their product inductively:

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

We then have the following rule:

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

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

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

and we define

$$\prod_{\nu=1}^{0} x_\nu = e.$$

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 $S_1 \times S_2 \to S_3$ 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

$$f : S \times S \to T$$

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

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

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)**.