ADDISON-WESLEY WORLD STUDENT SERIES

ALGEBRA

SERGE LANG

ALGEBRA

SERGE LANG
Columbia University, New York, New York

ADDISON-WESLEY WORLD STUDENT SERIES

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts
Amsterdam • London • Manila • Singapore • Sydney • Tokyo

THIS BOOK IS AN ADDISON-WESLEY
WORLD STUDENT SERIES EDITION

NINTH PRINTING 1980

A complete and unabridged reprint of the original American textbook, this World Student Series edition may be sold only in those countries to which it is consigned by Addison-Wesley or its authorized trade distributors. It may not be re-exported from the country to which it has been consigned, and it may not be sold in the United States of America or its possessions.

Library of Congress Catalog Card No. 65-23677

ALGEBRA

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.

One can also treat first the linear algebra, after covering the basic definitions, and postpone the field theory. 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.

I have followed Artin in the treatment of Galois theory, except for minor modifications. The reader can profitably consult Artin's short book on the subject to see the differences. Furthermore, the reader would also profit from seeing an exposition based on the Jacobson-Bourbaki theorem, which is useful in the inseparable case. However, the standard case is sufficiently important in most applications to warrant the classical treatment which I have chosen here.

Since Artin taught me algebra, my indebtedness to him is all-pervasive. It is perhaps least in the section on linear algebra and representations, where the influence of Bourbaki is more decisive (in content, not expository style). However, in choice of subject matter, I am more selective than Bourbaki, with the resulting advantages and disadvantages of being less encyclopaedic.

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. For instance, I have deliberately avoided getting too involved in commutative algebra. I could not write a basic course in algebra as an exclusive training ground for future algebraic geometers. However, anyone teaching the course will want to impress his 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.

The order of the book is still remarkably like that given by Artin-Noether-Van der Waerden some thirty years ago. I agree wholeheartedly with Van der Waerden's inclusion of the representation theory of finite groups in a basic text. In view of progress made by Brauer during the past thirty years, it has been possible to give a much more complete treatment than Van der Waerden could at that time.

There is some reason to include more on linear groups and their representations than I could do and still have a reasonably sized book. This can be done especially with students who have a proper background in linear algebra from their undergraduate days. Fortunately, several texts dealing with Lie algebras and Lie groups are now becoming available, so that I did not feel too guilty in omitting these topics. (Cf. in particular Serre's notes, *Lie Algebras and Lie Groups*.)

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

New York, 1965 SERGE LANG

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 $\mapsto$.

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 $f|A'$.

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*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & {\scriptstyle h}\searrow \quad \swarrow{\scriptstyle g} & \\ & C & \end{array}$$

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

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle g} \\ C & \xrightarrow[\psi]{} & D \end{array}$$

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 **Z** and **Q**. For many of our examples, we also assume that the reader knows the real and complex numbers, denoted by **R** and **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.

Bibliography

[1] E. ARTIN, *Galois Theory*, Notre Dame Mathematical Lectures, No. 2, 1946.

[2] ——, *Geometric Algebra*, Interscience, New York, 1957.

[3] N. BOURBAKI, *Algèbre commutative*, Hermann, Paris, 1962.

[4] ——, *Formes sesquilinéaires et formes quadratiques*, Hermann, Paris, 1959.

[5] ——, *Algèbre*, Hermann, Paris.

[6] R. GODEMENT, *Cours d'algèbre*, Hermann, Paris, 1963.

[7] N. JACOBSON, *Lectures in abstract algebra*, Van Nostrand, Princeton, N. J., Vol. 1 (1951), Vol. 2 (1953), Vol. 3 (1964).

[8] S. LANG, *Algebraic numbers*, Addison-Wesley, Reading, Mass., 1964.

[9] ——, *Diophantine geometry*, Interscience, New York, 1960.

[10] VAN DER WAERDEN, *Moderne Algebra*, Springer Verlag, Berlin, 1931.

[11] H. WEBER, *Lehrbuch der Algebra*, 1898 (reprinted by Chelsea, 1963).

[12] O. ZARISKI and P. SAMUEL, *Commutative algebra*, Van Nostrand, Princeton, N. J., Vol. 1 (1958), Vol. 2 (1960).

The above is a very brief list of texts and treatises in algebra. Bourbaki is always the most complete, and is excellent as a reference. Jacobson treats the Galois theory from the point of view of the Jacobson-Bourbaki theorem, which is useful among other things when dealing with purely inseparable extensions. The reader should browse through all the above books to be aware of points of view different from those given in the present book.

Contents

Part One
Groups, Rings, and Modules

CHAPTER I

Groups

1. Monoids . . . 5
2. Groups . . . 9
3. Cyclic groups . . . 13
4. Normal subgroups . . . 14
5. Operation of a group on a set . . . 19
6. Sylow subgroups . . . 23
7. Categories and functors . . . 25
8. Free groups . . . 33
9. Direct sums and free abelian groups . . . 40
10. Finitely generated abelian groups . . . 45
11. The dual group . . . 50

CHAPTER II

Rings

1. Rings and homomorphisms . . . 56
2. Commutative rings . . . 62
3. Localization . . . 66
4. Principal rings . . . 70

CHAPTER III

Modules

1. Basic definitions . . . 74
2. The group of homomorphisms . . . 76
3. Direct products and sums of modules . . . 79
4. Free modules . . . 84
5. Vector spaces . . . 85
6. The dual space . . . 88

CHAPTER IV

Homology

1. Complexes . . . 94
2. Homology sequence . . . 95
3. Euler characteristic . . . 98
4. The Jordan-Hölder theorem . . . 102

CHAPTER V

Polynomials

1. Free algebras . . . 106
2. Definition of polynomials . . . 110
3. Elementary properties of polynomials . . . 115
4. The Euclidean algorithm . . . 120
5. Partial fractions . . . 123
6. Unique factorization in several variables . . . 126
7. Criteria for irreducibility . . . 128
8. The derivative and multiple roots . . . 130
9. Symmetric polynomials . . . 132
10. The resultant . . . 135

CHAPTER VI

Noetherian Rings and Modules

1. Basic criteria . . . 142
2. Hilbert's theorem . . . 144
3. Power series . . . 146
4. Associated primes . . . 148
5. Primary decomposition . . . 152

Part Two
Field Theory

CHAPTER VII

Algebraic Extensions

1. Finite and algebraic extensions . . . 161
2. Algebraic closure . . . 166
3. Splitting fields and normal extensions . . . 173
4. Separable extensions . . . 176
5. Finite fields . . . 182
6. Primitive elements . . . 185
7. Purely inseparable extensions . . . 186

Chapter VIII

Galois Theory

1. Galois extensions 192
2. Examples and applications 199
3. Roots of unity 203
4. Linear independence of characters 208
5. The norm and trace 210
6. Cyclic extensions 213
7. Solvable and radical extensions 216
8. Kummer theory 218
9. The equation $X^n - a = 0$ 221
10. Galois cohomology 224
11. Algebraic independence of homomorphisms 225
12. The normal basis theorem 229

Chapter IX

Extensions of Rings

1. Integral ring extensions 237
2. Integral Galois extensions 244
3. Extension of homomorphisms 249

Chapter X

Transcendental Extensions

1. Transcendence bases 253
2. Hilbert's Nullstellensatz 255
3. Algebraic sets 257
4. Noether normalization theorem 260
5. Linearly disjoint extensions 261
6. Separable extensions 264
7. Derivations 266

Chapter XI

Real Fields

1. Ordered fields 271
2. Real fields 273
3. Real zeros and homomorphisms 278

Chapter XII

Absolute Values

1. Definition, dependence, and independence 283
2. Completions 286

3. Finite extensions 292
4. Valuations 296
5. Completions and valuations 304
6. Discrete valuations 305
7. Zeros of polynomials over complete fields 308

Part Three
Linear Algebra and Representations

Chapter XIII

Matrices and Linear Maps

1. Matrices 321
2. The rank of a matrix 323
3. Matrices and linear maps 324
4. Determinants 328
5. Duality 337
6. Matrices and bilinear forms 342
7. Sesquilinear duality 346

Chapter XIV

Structure of Bilinear Forms

1. Preliminaries, orthogonal sums 354
2. Quadratic maps 357
3. Symmetric forms, orthogonal bases 358
4. Hyperbolic spaces 359
5. Witt's theorem 360
6. The Witt group 363
7. Symmetric forms over ordered fields 365
8. The Clifford algebra 367
9. Alternating forms 370
10. The Pfaffian 372
11. Hermitian forms 374
12. The spectral theorem (hermitian case) 376
13. The spectral theorem (symmetric case) 378

Chapter XV

Representation of One Endomorphism

1. Representations 384
2. Modules over principal rings 386
3. Decomposition over one endomorphism 395
4. The characteristic polynomial 399

Chapter XVI

Multilinear Products

1. Tensor product 408
2. Basic properties 412
3. Extension of the base 418
4. Tensor product of algebras 420
5. The tensor algebra of a module 421
6. Alternating products 424
7. Symmetric products 427
8. The Euler-Grothendieck ring 429
9. Some functorial isomorphisms 431

Chapter XVII

Semisimplicity

1. Matrices and linear maps over non-commutative rings 438
2. Conditions defining semisimplicity 441
3. The density theorem 443
4. Semisimple rings 446
5. Simple rings 448

Chapter XVIII

Representations of Finite Groups

1. Semisimplicity of the group algebra 453
2. Characters 455
3. One-dimensional representations 459
4. The space of class functions 461
5. Orthogonality relations 465
6. Induced characters 468
7. Induced representations 471
8. Positive decomposition of the regular character 475
9. Supersolvable groups 478
10. Brauer's theorem 480
11. Field of definition of a representation 485

Appendixes

1. The transcendence of e and π 493
2. Some set theory 501

Index 521

PART ONE

GROUPS, RINGS
and
MODULES