B P

SAM PERLIS
Purdue University, Lafayette, Indiana

Introduction to Algebra

BLAISDELL PUBLISHING COMPANY
A Division of Ginn and Company
WALTHAM, MASSACHUSETTS · TORONTO · LONDON

Library of Congress Catalog Card Number: 66-14622
Printed in the United States of America.

INTRODUCTION TO ALGEBRA

A BLAISDELL BOOK IN
PURE AND APPLIED MATHEMATICS

CONSULTING EDITOR

George Springer
Indiana University

To *DONALD* and *ROBERT*

PREFACE

THIS IS AN UNDERGRADUATE TEXT intended for a one-year introductory course in modern algebra. Although it can be used for separate courses of one semester each in linear algebra and in abstract algebra, it is offered in the belief that a one-year course in algebra will soon become as well established in the curriculum as calculus has been for many decades.

At the present time, only a few years since algebra has achieved widespread recognition in the undergraduate curriculum, it is desirable to have a lively dialogue on the aims of this newcomer to the curriculum. I would suggest the following: (1) The student must be made aware of algebra not as a mass of manipulations but as an activity carried on within specified algebraic systems. (2) He must be made to feel at home with the concepts and elementary facts of five of these systems: groups, rings, integral domains, fields, and vector spaces. (3) He should be able to give specific examples of these systems illustrating or disproving any of a wide variety of propositions. (4) The course should be used to wipe out pockets of ignorance concerning such low-level topics as induction, roots of unity, multiple roots of polynomials, and irreducibility; and this should be done within a context of modern algebra so that, for example, roots of unity are associated with cyclic groups and their generators. (5) The student must master the basic facts of matrix algebra, rank, and nonsingularity, and the related theory of linear systems, as well as the theory of finite-dimensional vector spaces, their bases and dimensions, and elementary facts about linear transformations. (6) Connections with elementary mathematics must be apparent to the student at almost every point, not only because of the implied understanding but also because of the motivation which is essential at this stage. (7) Although some minimal list of indispensable subject matter could be compiled [and I hope it is a subset of this book's table of contents!] there are indications that it may be more important to set upper bounds against an excess of difficult abstractions and deep theorems. I am convinced that restraint in this matter will result in a far better product, including better graduate students. Certainly, few teachers expect the student to master the concepts of limit and continuity in his first year of calculus, and in the course of four years of college mathematics these topics are presented several times. Yet the abstractions of modern algebra are more troublesome for the beginner.

There is no need to summarize the table of contents here to show how I went about writing a book that is intended to assist in accomplishing the aims just outlined, but it is appropriate to point to certain features which I believe to be distinctive or at least worthy of comment.

First, I have used matrix theory as a transitional device from the concrete to the abstract, from the elementary to the advanced, and from the familiar to the new. By starting with systems of linear equations one is led naturally and with strong motivation to matrices, row equivalence, echelon form, nonsingular matrices, and inverses. In a relatively short time the student finds himself in a fascinating new world, solidly tied to his past experiences and to practical applications, yet flowing with new ideas. The subject is sufficiently easy and concrete so that its fundamentals can be mastered by all, yet it is of sufficient depth to offer challenges to the most capable. Because the vista includes noncommutativity and divisors of zero, matrix theory offers a perfect example with which to begin the study of rings. In fact it provides a prime source of examples, throughout the book, for groups, rings, fields, and vector spaces, as well as for nontrivial examples of isomorphisms. It would be difficult to imagine a more suitable means of transition to the abstract systems of modern algebra.

A major barrier impeding the progress of students into post-calculus mathematics is language. One could assemble a small book of everyday mathematical terminology or jargon which causes much puzzlement to serious students, a simple example being the term "well defined." I have tried throughout to smooth the road by giving full consideration to such difficulties and all other difficulties which I could recognize.

Students entering this course directly from calculus find it so different that they often ask what they are expected to know. I have, therefore, at the end of each chapter excepting the first, included a brief review of the conceptual content of the chapter. Each review requires the student to do the work, and merely gives an indication of some of the major ideas with which he should be familiar.

With each type of algebraic system I have devoted a little more attention than is common to the matter of generating subsystems. This not only is useful directly in various proofs and in providing a fund of examples, but also is a powerful unifying agent. After discussing the subgroup generated by a subset S, for example, one may define a cyclic group as a group having a generating set containing only one element. This is far prettier than making the definition by using a flurry of exponents.

I have included many proofs that need not occupy much class time, if any. This is true of distributivity and associativity proofs for constructed systems, particularly in the first half of the book. The generalized associative law is universally used in mathematics, but virtually no recognition is given to its existence. A full treatment of it is recorded here and in my classes this is assigned as private reading.

In the matter of polynomials one may skip the development given here and save time by the traditional treatment in which x is merely a "mark." I consider an arbitrary ring R with unity, and inquire as to the existence of a ring R' containing R as a subring and generated by R and an element x, the latter being required to have two properties: It commutes with every element of R and has the further property described by the word "indeterminate." For many students this is the first experience in constructing an algebraic system tailored to specified purposes. I have known students to receive a tremendous stimulus from this particular episode.

I am grateful to many for their helpful comments on reading parts of the manuscript, particularly to Professors John Dyer-Bennet, Ladnor Geissinger, and George Springer; and to two students, L. Q. Eifler and Donald Perlis. For their assistance in preparing the manuscript I am deeply indebted to Esther and Robert Perlis. My sincere thanks are

extended to the Blaisdell Publishing Company for unfailing courtesy and competence and generous offers of assistance at every difficult turn.

My introduction to modern algebra came in the invigorating lectures of A. A. Albert when I was a first-year graduate student. The existence of the subject took me totally by surprise and its beauty made a grip which has never weakened its hold on me. It is my hope that this book will be helpful in enabling many undergraduates to obtain a similar feeling of appreciation and exhilaration.

Organization and Usage of this Book

This book can serve as a text for three courses:

A. a course of one semester in abstract algebra;

B. a course of one semester in linear algebra;

C. a one-year course integrating abstract and linear algebra.

Purpose A is served by Chapters I through VIII and X. Chapter X, on algebraic extensions of a field, includes much to interest students, and faster classes may be able to cover it. The dimension theory of the preceding chapter is required, but instructors will probably find that a single lecture suffices to provide a summary of this theory adequate for the purposes of Chapter X.

Chapters VII, VIII, and X are, apart from trivialities, independent of one another and of all that follows them. Any of these three chapters may be skipped, or partially skipped, to provide time for covering other sections.

Purpose B is served by Chapters I, II, IX, and XI through XIV, together with certain parts of III. The latter are Sections 3.1, 3.5, and 3.6, all of which should be read before Chapter IX. Beyond Chapter II the word "field" should be interpreted, as it is in Chapter II, as a "complex field," that is, any subfield of the field of all complex numbers. An occasional problem will refer to groups or rings and will have to be omitted, but this will cause no difficulty.

Purpose C is obviously served by Chapters I through XIV. As mentioned earlier, any of Chapters VII, VIII, and X can be omitted without repercussion, and this is true of many individual sections throughout the book.

Finally, some comments must be made about Chapters I and II. Some instructors will prefer to take all of Chapter I at the outset; others will take only two sections, then refer back to various parts of Chapter I as the need arises. As an aid to the latter, the second chapter contains numerous references to the first as well as brief repetitions of some of the definitions.

It is to be noticed that Chapter II, on linear equations and matrices, is recommended for the one-semester course in abstract algebra as well as for the other purposes. It would be a sad mistake to omit this chapter. Its function in providing the student with a smooth transition from the concrete to the abstract and, in many cases, from the loose to the rigorous, is vital.

SAM PERLIS

INDEX OF COMMON SYMBOLS

(Note: "ex." refers to the exercises.)

Section	*Symbol*	*Brief Definition*
1.1	$\supseteq$	contains
1.1	$\supset$	contains properly
1.1	$\subseteq$	is contained in
1.1	$\subset$	is properly contained in
1.1	$\in$	is a member of
1.7	$\notin$	is not a member of
1.2	$\cup$	union
1.2	$\cap$	intersection
1.2	$\varnothing$	empty set
1.5	$\square$	end of proof
1.1	$\{\ldots;\ldots\}$	set
1.1	$\{a_1, \ldots, a_n\}$	set whose elements are $a_1, \ldots, a_n$
1.8	$a\,R\,b$	a is in the relation R to b
1.8	$a \not{R}\, b$	a is not in the relation R to b
1.8	$a \equiv b \pmod{n}$	a is congruent to b modulo n
2.1, 5.11	$\mathscr{I}$	ring of integers
4.3	$\mathscr{I}/(n)$	ring of integers modulo n
2.3	$\mathscr{Q}$	rational number system
2.3	$\mathscr{R}$	real number system
2.3	$\mathscr{C}$	complex number system
4.11	R/S	residue class ring R modulo S
4.11	$[a]$	— member of R/S
1.9		— member of $\mathscr{I}/(n)$
1.9		— equivalence class with respect to an equivalence relation
4.15	$R_1\,[+]\,R_2$	constructed direct sum of rings R_1 and R_2
4.15	$S_1 \oplus S_2$	direct sum of subrings S_1 and S_2
4.2	u	unity element of a ring

Section	*Symbol*	*Brief Definition*
3.1	e	identity element of a group
3.7	G_4	Klein's four-group
3.3	S_n	symmetric group of degree n
4.1	$(R, +)$	additive group of the ring R
4.2	R^*, F^*	multiplicative group of the ring R with unity, or of the field F
6.3, 6.4	R^q	quotient field of the integral domain R
5.6	R_p	set of positive elements in the ordered integral domain R
10.13	I_F	domain of algebraic integers in the algebraic number field F
10.14	$N(a)$, $T(a)$	norm and trace of the algebraic number a
7.1	$a \mid b$	a divides b
7.1	$a \nmid b$	a does not divide b
7.3	$\gcd \{a_1, \ldots, a_n\}$	greatest common divisor of the integers or polynomials $a_1, \ldots, a_n$
7.5	$\operatorname{lcm} \{a_1, \ldots, a_n\}$	least common multiple of $a_1, \ldots, a_n$
6.3	$D(x)$, $F(x)$	field of rational expressions in x with coefficients in D or F
4.9	$R[x]$, $F[x]$	polynomial domain over the ring R with unity, or over the field F
9.2	$F^n[x]$	subset of $F[x]$ containing 0 and the polynomials of degree $\leqq n$
10.2	$F[S]$	subdomain [of an extension field of F] generated by F and the subset S
10.2	$F(S)$	subfield generated by F and S
10.2	$F(s_1, \ldots, s_n)$	subfield generated by F and $s_1, \ldots, s_n$
10.5	$[K:F]$	degree of the field K over the subfield F
9.1	$F_{s,n}$	set of all $s \times n$ matrices over F
4.1	F_n	set of all $n \times n$ matrices over F
4.6 ex.	$F_n^{(d)}$	set of $n \times n$ diagonal matrices over F
4.6 ex.	$F_n^{(s)}$	set of $n \times n$ scalar matrices over F
4.6 ex.	$F_n^{(t)}$	set of $n \times n$ triangular matrices over F
4.6 ex.	$F_n^{(st)}$	set of $n \times n$ strictly triangular matrices over F
2.5	$V_n(F)$	vector space of ordered n-tuples of elements of F
9.2	$V_\infty(F)$	vector space of sequences of elements of F
9.2	$V^*_\infty(F)$	subspace of $V_\infty(F)$ each of whose vectors has only a finite number of nonzero components
2.5	$\epsilon_1, \ldots, \epsilon_n$	unit vectors in $V_n(F)$
9.2	$\langle {}^v S \rangle$	vector subspace generated by S
3.7	$\langle {}^g S \rangle$	subgroup generated by S
4.6	$\langle {}^r S \rangle$	subring generated by S
5.2	$\langle {}^d S \rangle$	subdomain generated by S
6.6	$\langle {}^f S \rangle$	subfield generated by S
4.11 ex.	$\langle {}^i S \rangle$	ideal generated by S
1.4	I	identity mapping
2.14	I	identity matrix

Section	*Symbol*	*Brief Definition*
2.14	I_n	$n \times n$ identity matrix
2.14	diag $[a_1, \ldots, a_n]$	diagonal matrix
2.9	$s \times n$	describes a matrix having s rows and n columns
2.9, 9.10	A_e	echelon matrix row equivalent to A
2.11	A_i	row i of matrix A
2.11	$A^{(j)}$	column j of matrix A
2.9	R_{ij}	types of row operations
2.9	$R_i(k)$	
2.9	$R_{ij}(k)$	
2.16	C_{ij}	types of column operations
2.16	$C_i(k)$	
2.16	$C_{ij}(k)$	
2.9	RA	result of performing row operation R,
2.16	CA	or column operation C, on matrix A
2.14	E_{ij}	types of elementary matrices
2.14	$E_i(k)$	
2.14	$E_{ij}(k)$	
9.9	$RS(A)$	row space of matrix A
9.9	$CS(A)$	column space of matrix A
9.11	rank A	rank of matrix A
12.1	$L(V, W)$	set of linear transformations on V to W
12.1	$L(V)$	set of linear transformations on V (to V)
12.1	λ	linear transformation
12.1	λ_k	multiplication by the scalar k
12.3	$V\lambda$	image space of V under the linear transformation λ
12.4	$K(\lambda)$	kernel of the linear transformation λ
4.14	$K(\rho)$	kernel of the homomorphism ρ
12.3	rank λ	rank of linear transformation λ
12.9	Λ	matrix representing λ
12.9	Λ_B	matrix representing λ relative to basis B
9.7	α_B	coordinate n-tuple of the vector α relative to basis B
14.4	$\mathcal{O}(T)$	orthogonal complement of the subset T
14.6	$\alpha_T, \alpha_{\mathcal{O}(T)}$	perpendicular projections of α on the subspaces T and $\mathcal{O}(T)$, respectively
9.1	$\Phi(a, b)$	set of all real-valued functions defined on the interval (a, b)
9.2	$C(a, b)$	set of all continuous real-valued functions defined on (a, b)
9.2	$D_n(a, b)$	set of all real-valued functions that are differentiable n times on (a, b)
9.2	$D_\infty(a, b)$	set of all real-valued functions having derivatives of all orders on (a, b)

GREEK ALPHABET

Letters		*Names*	*Letters*		*Names*
Α	α	Alpha	Ν	ν	Nu
Β	β	Beta	Ξ	ξ	Xi
Γ	γ	Gamma	Ο	ο	Omicron
Δ	δ	Delta	Π	π	Pi
Ε	ϵ	Epsilon	Ρ	ρ	Rho
Ζ	ζ	Zeta	Σ	σ	Sigma
Η	η	Eta	Τ	τ	Tau
Θ	θ	Theta	ϒ	υ	Upsilon
Ι	ι	Iota	Φ	ϕ	Phi
Κ	κ	Kappa	Χ	χ	Chi
Λ	λ	Lambda	Ψ	ψ	Psi
Μ	μ	Mu	Ω	ω	Omega

CONTENTS

Chapter V. INTEGRAL DOMAINS

Chapter VI. FIELDS

Chapter VII. DIVISIBILITY

Chapter VIII. CLASSICAL ALGEBRA

Chapter IX. VECTOR SPACES

Chapter X. EXTENSION FIELDS