Basic Algebra I

NATHAN JACOBSON

Basic Algebra I

NATHAN JACOBSON
YALE UNIVERSITY

W. H. FREEMAN AND COMPANY
San Francisco

Library of Congress Cataloging in Publication Data

Jacobson, Nathan, 1910-
Basic algebra.

Includes bibliographical references.
1. Algebra. I. Title.
QA154.2.J32 512.9 73-22316
ISBN 0-7167-0453-6 (v. 1.)

Printed in the United States of America

1 2 3 4 5 6 7 8 9

Preface

It is more than twenty years since the author began the project of writing the three volumes of *Lectures in Abstract Algebra*. The first and second of these books appeared in 1951 and 1953 respectively, the third in 1964. In the period which has intervened since this work was conceived—around 1950—substantial progress in algebra has occurred even at the level of these texts. This has taken the form first of all of the introduction of some basic new ideas. Notable examples are the development of category theory, which provides a useful framework for a large part of mathematics, homological algebra, and applications of model theory to algebra. Perhaps even more striking than the advent of these ideas has been the acceptance of the axiomatic conceptual method of abstract algebra and its pervading influence throughout mathematics. It is now taken for granted that the methodology of algebra is an essential tool in mathematics. On the other hand, in recent research one can observe a return to the challenge presented by fairly concrete problems, many of which require for their solution tools of considerable technical complexity.

Another striking change that has taken place during the past twenty years—especially since the Soviet Union startled the world by orbiting its "sputniks"

—has been the upgrading of training in mathematics in elementary and secondary schools. (Although there has recently been some regression in this process, it is to be hoped that this will turn out to be only a temporary aberration.) The upgrading of school mathematics has had as a corollary a corresponding upgrading of college mathematics. A notable instance of this is the early study of linear algebra, with a view of providing the proper background for the study of multivariable calculus as well as for applications to other fields. Moreover, courses in linear algebra are quite often followed immediately by courses in "abstract" algebra, and so the type of material which twenty years ago was taught at the graduate level is now presented to students with comparatively little experience in mathematics.

The present book, *Basic Algebra* I, and the forthcoming *Basic Algebra* II were originally envisioned as new editions of our *Lectures*. However, as we began to think about the task at hand, particularly that of taking into account the changed curricula in our undergraduate and graduate schools, we decided to organize the material in a manner quite different from that of our earlier books: a separation into two levels of abstraction, the first—treated in this volume—to encompass those parts of algebra which can be most readily appreciated by the beginning student. Much of the material which we present here has a classical flavor. It is hoped that this will foster an appreciation of the great contributions of the past and especially of the mathematics of the nineteenth century. In our treatment we have tried to make use of the most efficient modern tools. This has necessitated the development of a substantial body of foundational material of the sort that has become standard in text books on abstract algebra. However, we have tried throughout to bring to the fore well-defined objectives which we believe will prove appealing even to a student with little background in algebra. On the other hand, the topics considered are probed to a depth that often goes considerably beyond what is customary, and this will at times be quite demanding of talent and concentration on the part of the student. In our second volume we plan to follow a more traditional course in presenting material of a more abstract and sophisticated nature. It is hoped that after the study of the first volume a student will have achieved a level of maturity that will enable him to take in stride the level of abstraction of the second volume.

We shall now give a brief indication of the contents and organization of *Basic Algebra* I. The Introduction, on set theory and the number system of the integers, includes material that will be familiar to most readers: the algebra of sets, definition of maps, and mathematical induction. Less familiar, and of paramount importance for subsequent developments, are the concepts of an equivalence relation and quotient sets defined by such relations.

We introduce also commutative diagrams and the factorization of a map through an equivalence relation. The fundamental theorem of arithmetic is proved, and a proof of the Recursion theorem (or defintion by induction) is included.

Chapter 1 deals with monoids and groups. Our starting point is the concept of a monoid of transformations and of a group of transformations. In this respect we follow the historical development of the subject. The concept of homomorphism appears fairly late in our discussion, after the reader has had a chance to absorb some of the simpler and more intuitive ideas. However, once the concept of homomorphism has been introduced, its most important ramifications (the fundamental isomorphism theorems and the correspondence between subgroups of a homomorphic image and subgroups containing the kernel) are developed in considerable detail. The concept of a group acting on a set, which now plays such an important role in geometry, is introduced and illustrated with many examples. This leads to a method of enumeration for finite groups, a special case of which is contained in the class equation. These results are applied to derive the Sylow theorems, which constitute the last topic of Chapter 1.

The first part of Chapter 2 repeats in the context of rings many of the ideas that have been developed in the first chapter. Following this, various constructions of new rings from given ones are considered: rings of matrices, fields of fractions of commutative domains, polynomial rings. The last part of the chapter is devoted to the elementary factorization theory of commutative monoids with cancellation property and of commutative domains.

The main objective in Chapter 3 is the structure theory of finitely generated modules over a principal ideal domain and its applications to abelian groups and canonical forms of matrices. Of course, before this can be achieved it is necessary to introduce the standard definitions and concepts on modules. The analogy with the concept of a group acting on a set is stressed, as is the idea that the concept of a module is a natural generalization of the familiar notion of a vector space. The chapter concludes with theorems on the ring of endomorphisms of a finitely generated module over a principal ideal domain, which generalize classical results of Frobenius on the ring of matrices commuting with a given matrix.

Chapter 4 deals almost exclusively with the ramifications of two classical problems: solvability of equations by radicals and constructions with straight-edge and compass. The former is by far the more difficult of the two. The tool which was forged by Galois for handling this, the correspondence between subfields of the splitting field of a separable polynomial and subgroups of the group of automorphisms, has attained central importance in algebra and number theory. However, we believe that at this stage it is more effective to concentrate on the problems which gave the original impetus to Galois' theory and to treat these in a thoroughgoing manner. The theory of finite groups which was initiated in Chapter 1 is amplified here by the inclusion of the results needed to establish Galois' criterion for solvability of an equation by radicals. We have included also a proof of the transcendence of π since this is needed to prove the impossibility of "squaring the circle" by straight-edge and compass. (In fact, since it requires very little additional effort, the more general theorem of Lindemann and Weierstrass on algebraic independence of exponentials has been proved.) At the end of the chapter we have undertaken to round out the Galois theory by applying it to derive the main results on finite fields and to prove the theorems on primitive elements and normal bases as well as the fundamental theorems on norms and traces.

Chapter 5 continues the study of polynomial equations. We now operate in a real closed field—an algebraic generalization of the field of real numbers. We prove a generalization of the "fundamental theorem of algebra": the algebraic closure of $R(\sqrt{-1})$ for R any real closed field. We then derive Sturm's theorem, which gives a constructive method of determining the number of roots in R of a polynomial equation in one unknown with coefficients in R. The last part of the chapter is devoted to the study of systems of polynomial equations and inequations in several unknowns. We first treat the purely algebraic problem of elimination of unknowns in such a system and then establish a far-reaching generalization of Sturm's theorem that is due to Tarski. Throughout this chapter the emphasis is on constructive methods.

The first part of Chapter 6 covers the basic theory of quadratic forms and alternate forms over an arbitrary field. This includes Sylvester's theorem on the inertial index and its generalization that derives from Witt's cancellation theorem. The important theorem of Cartan-Dieudonné on the generation of the orthogonal group by symmetries is proved. The second part of the chapter is concerned with the structure theory of the so-called classical groups: the full linear group, the orthogonal group, and the symplectic group. In this analysis we have employed a uniform method applicable to all three types of groups. This method was originated by Iwasawa for the full linear group and was extended to orthogonal groups by Tamagawa. The results provide some important classes of simple groups whose orders for finite fields are easy to compute.

Chapter 7 gives an introduction to the theory of algebras, both associative and non-associative. An important topic in the associative theory we consider is the exterior algebra of a vector space. This algebra plays an important role in geometry, and is applied here to derive the main theorems on determinants.

We define also the regular representation, trace, and norm of an associative algebra, and prove a general theorem on transitivity of these functions. For non-associative algebras we give definitions and examples of the most important classes of non-associative algebras. We follow this with a completely elementary proof of the beautiful theorem on composition of quadratic forms which is due to Hurwitz, and we conclude the chapter with proofs of Frobenius' theorem on division algebras over the field of real numbers and Wedderburn's theorem on finite division algebras.

Chapter 8 provides a brief introduction to lattices and Boolean algebras. The main topics treated are the Jordan-Hölder theorem on semi-modular lattices; the so-called "fundamental theorem of projective geometry"; Stone's theorem on the equivalence of the concepts of Boolean algebras and Boolean rings, that is, rings all of whose elements are idempotent; and finally the Möbius function of a partially ordered set.

Basic Algebra I is intended to serve as a text for a first course in algebra beyond linear algebra. It contains considerably more material than can be covered in a year's course. Based on our own recent experience with earlier versions of the text, we offer the following suggestions on what might be covered in a year's course divided into either two semesters or three quarters. We have found it possible to cover the Introduction (treated lightly) and nearly all the material of Chapters 1–3 in one semester. We found it necessary to omit the proof of the Recursion theorem in the Introduction, the section on free groups in Chapter 1, the last section (on "rngs") in Chapter 2, and the last section of Chapter 3. Chapter 4, Galois theory, is an excellent starting point for a second semester's course. In view of the richness of this material not much time will remain in a semester's course for other topics. If one makes some omissions in Chapter 4, for example, the proof of the theorem of Lindemann-Weierstrass, one is likely to have several weeks left after the completion of this material. A number of alternatives for completing the semester may be considered. One possibility would be to pass from the study of equations in one unknown to systems of polynomial equations in several unknowns. One aspect of this is presented in Chapter 5. A part of this chapter would certainly fit in well with Chapter 4. On the other hand, there is something to be said for making an abrupt change in theme. One possbility would be to take up the chapter on algebras. Another would be to study a part of the chapter on quadratic forms and the classical groups. Still another would be to study the last chapter, on lattices and Boolean algebras.

A program for a course for three quarters might run as follows: Introduction and Chapters 1 and 2 for a first quarter; Chapter 3 and a substantial part of Chapter 6 for a second quarter. This will require a bit of filling in of the field theory from Chapter 4 which is needed for Chapter 6. One could conclude with a third quarter's course on Chapter 4, the Galois theory.

It is hoped that a student will round out formal courses based on the text by independent reading of the omitted material. Also we feel that quite a few topics lend themselves to programs of supervised independent study.

We are greatly indebted to a number of friends and colleagues for reading portions of the penultimate version of the text and offering valuable suggestions which were taken into account in preparing the final version. Walter Feit and Richard Lyons suggested a number of exercises in group theory: Abraham Robinson, Tsuneo Tamagawa, and Neil White have read parts of the book on which they are experts (Chapters 5, 6, and 8 respectively) and detected some flaws which we had not noticed. George Seligman has read the entire manuscript and suggested some substantial improvements. S. Robert Gordon, James Hurley, Florence Jacobson, and David Rush have used parts of the earlier text in courses of a term or more, and have called our attention to numerous places where improvements in the exposition could be made.

A number of people have played an important role in the production of the book, among them we mention especially Florence Jacobson and Jerome Katz, who have been of great assistance in the tedious task of proofreading. Finally, we must add a special word for Mary Scheller, who cheerfully typed the entire manuscript as well as the preliminary version of about the same length.

We are deeply indebted to the individuals we have mentioned—and to others—and we take this opportunity to offer our sincere appreciation and thanks.

Hamden, Connecticut *Nathan Jacobson*
November 21, 1973

Contents

INTRODUCTION

Concepts from Set Theory. The Integers

The main purpose of this volume is to provide an introduction to the basic structures of algebra: groups, rings, fields, modules, algebras, and lattices—concepts that give a natural setting for a large body of algebra, including classical algebra. It is noteworthy that many of these concepts have arisen either to solve concrete problems in geometry, number theory, or the theory of algebraic equations, or to afford a better insight into existing solutions of such problems. A good example of the interplay between abstract theory and concrete problems can be seen in the Galois theory, which was created by Galois to answer a concrete question: "What polynomial equations in one unknown have solutions expressible in terms of the given coefficients by rational operations and extraction of roots?" To solve this we must first have a precise formulation of the problem, and this requires the concepts of field, extension field, and splitting field of a polynomial. To understand Galois' solution of the problem of algebraic equations we require the notion of a group and properties of solvable groups. In Galois' theory the results were stated in terms of groups of permutations of the roots. Subsequently, a much deeper understanding of what was involved emerged in passing from permutations of the roots to the more abstract notion of the group of automorphisms of an extension field. All of this will be discussed fully in Chapter 4.

Of course, once the machinery has been developed for treating one set of problems, it is likely to be useful in other circumstances, and, moreover, it generates new problems that appear interesting in their own right.

Throughout this presentation we shall seek to emphasize the relevance of the general theory in solving interesting problems, in particular, problems of classical origin. This will necessitate developing the theory beyond the foundational level to get at some of the interesting theorems. Occasionally, we shall find it convenient to develop some of the applications in exercises. For this reason, as well as others, the working of a substantial number of the exercises is essential for a thorough understanding of the material.

The basic ingredients of the structures we shall study are sets and mappings (or, as we shall call them in this book, **maps**). It is probable that the reader already has an adequate knowledge of the set theoretic background that is required. Nevertheless, for the purpose of fixing the notations and terminology, and to highlight the special aspects of set theory that will be fundamental for us, it seems desirable to indicate briefly some of the elements of set theory.[1] From the point of view of what follows the ideas that need to be stressed concern equivalence relations and the factorization of a mapping through an equivalence relation. These will reappear in a multitude of forms throughout our study. In the second part of this introduction we shall deal briefly with the number system $\mathbb{Z}$ of the integers and the more primitive system $\mathbb{N}$ of natural numbers or counting numbers: $0, 1, 2, \ldots$, which serve as the starting point for the constructive development of algebra. In view of the current emphasis on the development of number systems in primary and secondary schools, it seems superfluous to deal with $\mathbb{N}$ and $\mathbb{Z}$ in a detailed fashion. We shall therefore be content to review in outline the main steps in one of the ways of introducing $\mathbb{N}$ and $\mathbb{Z}$ and to give careful proofs of two results that will be needed in the discussion of groups in Chapter 1. These are the existence of greatest common divisors (g.c.d.'s) of integers and "the fundamental theorem of arithmetic," which establishes the unique factorization of any natural number $\neq 0, 1$ as a product of prime factors. Later (in Chapter 2), we shall derive these results again as special cases of the arithmetic of principal ideal domains.

0.1 THE POWER SET OF A SET

We begin our discussion with a brief survey of some set theoretic notions which will play an essential role in this book.

[1] For a general reference book on set theory adequate for our purposes we refer the reader to the very attractive little book, *Naive Set Theory*, by Paul R. Halmos, Van Nostrand Reinhold, 1960.

Let S be an arbitrary set (or collection) of elements which we denote as a, b, c, etc. The nature of these elements is immaterial. The fact that an element a belongs to the set S is indicated by writing $a \in S$ (occasionally $S \ni a$) and the negation of $a \in S$ is written as $a \notin S$. If S is a finite set with elements a_i, $1 \leq i \leq n$, then we write $S = \{a_1, a_2, \ldots, a_n\}$. Any set S gives rise to another set $\mathscr{P}(S)$, the set of subsets of S. Among these are included the set S itself and the vacuous subset or null set, which we denote as $\varnothing$. For example, if S is a finite set of n elements, say, $S = \{a_1, a_2, \ldots, a_n\}$, then $\mathscr{P}(S)$ consists of $\varnothing$, the n sets $\{a_i\}$ containing single elements, $n(n-1)/2$ sets $\{a_i, a_j\}$, $i \neq j$, containing two elements, $\binom{n}{i} = n!/i!\,(n-i)! = n(n-1)\cdots(n-i+1)/1\cdot 2\cdots i$ subsets containing i elements, and so on. Hence the cardinality of S, that is, the number of elements in $\mathscr{P}(S)$ is

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1+1)^n = 2^n.$$

We shall call $\mathscr{P}(S)$, the *power set* of the set S.[2] Often we shall specify a subset of S by a property or set of properties. The standard way of doing this is to write

$$A = \{x \in S \mid \cdots\}$$

(or, if S is clear, $A = \{x \mid \cdots\}$) where $\cdots$ lists the properties characterizing A. For example, if $\mathbb{Z}$ denotes the set of integers, then $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$ defines the subset of non-negative integers, or natural numbers.

If A and $B \in \mathscr{P}(S)$ (that is, A and B are subsets of S) we say that A is *contained in* B or is a *subset of* B (or B *contains* A) and denote this as $A \subset B$ (or $B \supset A$) if every element a in A is also in B. Symbolically, we can write this as $a \in A \Rightarrow a \in B$ where the $\Rightarrow$ is read as "implies." The statement $A = B$ is equivalent to the two statements $A \supset B$ and $B \supset A$ (symbolically, $A = B \Leftrightarrow A \supset B$ and $B \supset A$ where $\Leftrightarrow$ reads "if and only if"). If $A \subset B$ and $A \neq B$ we write $A \subsetneq B$ and say that A is a *proper subset* of B. Alternatively, we can write $B \supsetneq A$.

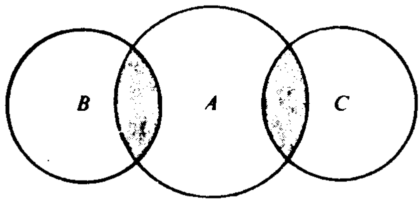
If A and B are subsets of S, the subset of S of elements c such that $c \in A$ *and* $c \in B$ is called the *intersection* of A and B. We denote this subset as $A \cap B$. If there are no elements of S contained in both A and B, that is, $A \cap B = \varnothing$, then A and B are said to be *disjoint* (or *non-overlapping*). The *union* (or *logical sum*) $A \cup B$ of A and B is the subset of elements d such that either $d \in A$ *or* $d \in B$. An important property connecting $\cap$ and $\cup$ is the distributive law:

(1) $$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

---

[2] This is frequently called the *Boolean of S*, $\mathscr{B}(S)$, after George Boole who initiated its systematic study. The justification of the terminology "power set" is indicated in the footnote on p. 5.

This can be indicated pictorially by



where the shaded region represents (1). To prove (1), let $x \in A \cap (B \cup C)$. Since $x \in (B \cup C)$ either $x \in B$ or $x \in C$, and since $x \in A$ either $x \in (A \cap B)$ or $x \in (A \cap C)$. This shows that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Now let $y \in (A \cap B) \cup (A \cap C)$ so either $y \in A \cap B$ or $y \in A \cap C$. In any case $y \in A$ and $y \in B$ or $y \in C$. Hence $y \in A \cap (B \cup C)$. Thus $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Hence we have both $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$ and $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$ and consequently we have (1).

We also have another distributive law which dualizes (1) in the sense that it is obtained from (1) by interchanging $\cup$ and $\cap$:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{2}$$

It is left to the reader to draw a diagram for this law and carry out the proof. Better still, the reader can show that (2) is a consequence of (1)—and that, by symmetry, (1) is a consequence of (2). These two properties are sometimes called *De Morgan's laws* after the mathematician who first called attention to them.

Intersections and unions can be defined for an arbitrary set of subsets of a set S. Let Γ be such a set of subsets (= subset of $\mathscr{P}(S)$). Then we define $\bigcap_{A \in \Gamma} A = \{x \mid x \in A \text{ for every } A \text{ in } \Gamma\}$ and $\bigcup_{A \in \Gamma} A = \{x \mid x \in A \text{ for some } A \text{ in } \Gamma\}$. If Γ is finite, say, $\Gamma = \{A_1, A_2, \ldots, A_n\}$ then we write also $\bigcap_{i=1}^{n} A_i$ or $A_1 \cap A_2 \cap \cdots \cap A_n$ for the intersection and we use a similar designation for the union. It is easy to see that De Morgan's laws carry over to arbitrary intersections and unions.

0.2 THE CARTESIAN PRODUCT SET. MAPS

The reader is undoubtedly aware of the central role of the concept of function in mathematics and its applications. The case of interest in beginning calculus is that of a real-valued function of a real variable. Here we have a subset of the real line $\mathbb{R}$; usually, an open or closed interval or the whole of $\mathbb{R}$; and a rule which associates with every element x of this subset a unique real number $f(x)$. Associated with a function as thus "defined" we have the graph in the two-dimensional number space $\mathbb{R}^{(2)}$ consisting of the points $(x, f(x))$. We soon realize that f is determined by its graph and that the characteristic property of the graph is that