Graduate Texts in Mathematics

Stanley Burris
H.P. Sankappanavar

A Course in Universal Algebra

Springer-Verlag
New York Heidelberg Berlin
World Publishing Corporation Beijing China

Stanley Burris
H. P. Sankappanavar

A Course in Universal Algebra

With 36 Illustrations

Springer-Verlag
New York Heidelberg Berlin
World Publishing Corporation, Beijing, China

Stanley Burris
Department of Pure Mathematics
Faculty of Mathematics
University of Waterloo
Waterloo, Ontario N2L 3G1
CANADA

H. P. Sankappanavar
Instituto de Matemática
Universidade Federal da Bahia
Salvador, Bahia 40000
BRAZIL

AMS Subject Classification (1980): 08-01, 08AXX, 03C05

Library of Congress Cataloging in Publication Data
Burris, S.
A course in universal algebra.
(Graduate texts in mathematics; 78)
Bibliography: p.
Includes index.
1. Algebra, Universal. I. Sankappanavar, H. P.
II. Title. III. Series.
QA251.B87 512 81-1619
AACR2

Reprinted in China by World Publishing Corporation
For distribution and sale in the People's Republic of China only
只限在中华人民共和国发行

ISBN 0-387-90578-2 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90578-2 Springer-Verlag Berlin Heidelberg New York
7-5062-0108-9 World Publishing Corporation China

This book is dedicated to our children

Kurosh Phillip Burris
Veena and Geeta Sankappanavar

Acknowledgments

First we would like to express gratitude to our colleagues who have added so much vitality to the subject of Universal Algebra during the past twenty years. One of the original reasons for writing this book was to make readily available the beautiful work on sheaves and discriminator varieties which we had learned from, and later developed with H. Werner. Recent work of, and with, R. McKenzie on structure and decidability theory has added to our excitement, and conviction, concerning the directions emphasized in this book.

In the late stages of polishing the manuscript we received valuable suggestions from M. Valeriote, W. Taylor, and the reviewer for Springer-Verlag. For help in proof-reading we also thank A. Adamson, M. Albert, D. Higgs, H. Kommel, G. Krishnan, and H. Riedel. A great deal of credit for the existence of the final product goes to Sandy Tamowski whose enthusiastic typing has been a constant inspiration. The Natural Sciences and Engineering Research Council of Canada has generously funded both the research which has provided much of the impetus for writing this book as well as the preparation of the manuscript through NSERC Grant No. A7256. Also thanks go to the Pure Mathematics Department of the University of Waterloo for their kind hospitality during the several visits of the second author, and to the Institute of Mathematics, Federal University of Bahia, for their generous cooperation in this venture.

The second author would most of all like to express his affectionate gratitude and appreciation to his wife—Nalinaxi—who, over the past four years has patiently endured the many trips between South and North America which were necessary for this project. For her understanding and encouragement he will always be indebted.

And finally we are delighted that Springer-Verlag agreed to our request to have this book appear in their GTM series.

Preface

Universal algebra has enjoyed a particularly explosive growth in the last twenty years, and a student entering the subject now will find a bewildering amount of material to digest.

This text is not intended to be encyclopedic; rather, a few themes central to universal algebra have been developed sufficiently to bring the reader to the brink of current research. The choice of topics most certainly reflects the authors' interests.

Chapter I contains a brief but substantial introduction to lattices, and to the close connection between complete lattices and closure operators. In particular, everything necessary for the subsequent study of congruence lattices is included.

Chapter II develops the most general and fundamental notions of universal algebra—these include the results that apply to all types of algebras, such as the homomorphism and isomorphism theorems. Free algebras are discussed in great detail—we use them to derive the existence of simple algebras, the rules of equational logic, and the important Mal'cev conditions. We introduce the notion of classifying a variety by properties of (the lattices of) congruences on members of the variety. Also, the center of an algebra is defined and used to characterize modules (up to polynomial equivalence).

In Chapter III we show how neatly two famous results—the refutation of Euler's conjecture on orthogonal Latin squares and Kleene's characterization of languages accepted by finite automata—can be presented using universal algebra. We predict that such "applied universal algebra" will become much more prominent.

Chapter IV starts with a careful development of Boolean algebras, including Stone duality, which is subsequently used in our study of Boolean sheaf representations; however, the cumbersome formulation of general sheaf theory has been replaced by the considerably simpler definition of a Boolean product. First we look at Boolean powers, a beautiful tool for transferring results about Boolean algebras to other varieties as well as for providing a structure theory for certain varieties. The highlight of the chapter is the study of discriminator varieties. These varieties have played a remarkable role in the study of spectra, model companions, decidability, and Boolean product representations. Probably no other class of varieties is so well-behaved yet so fascinating.

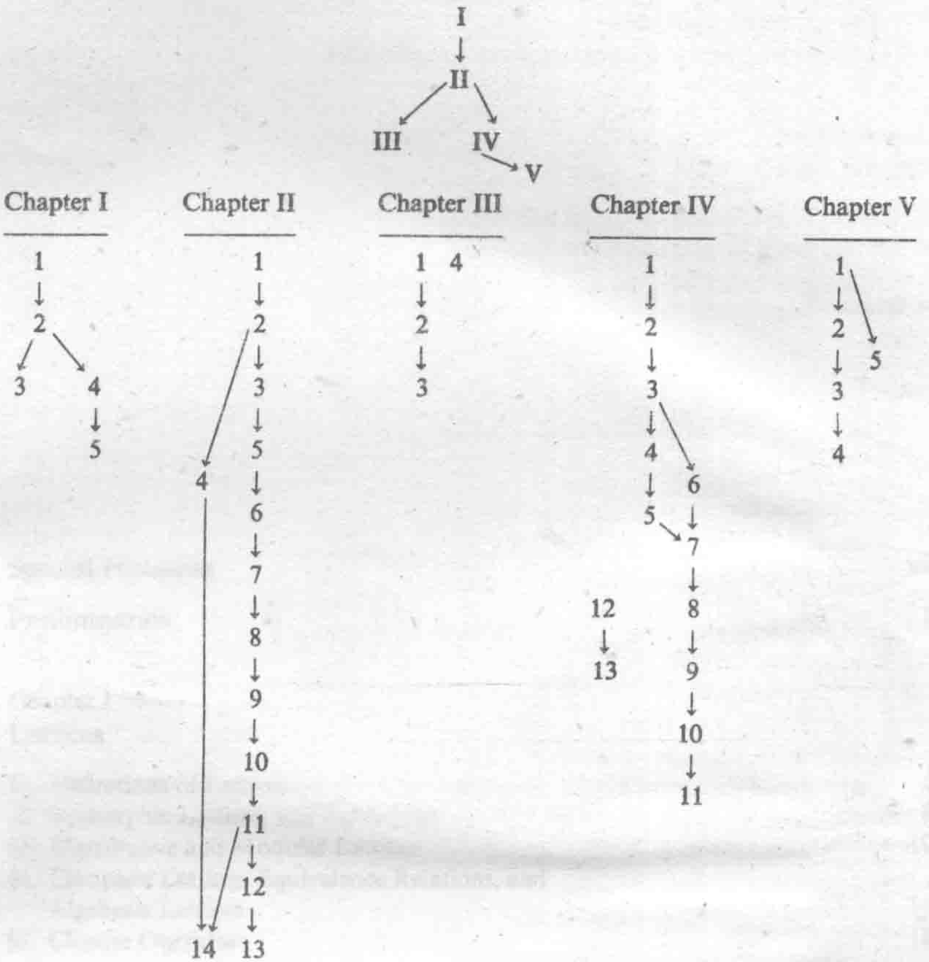
The final chapter gives the reader a leisurely introduction to some basic concepts, tools, and results of model theory. In particular, we use the ultraproduct construction to derive the compactness theorem and to prove fundamental preservation theorems. Principal congruence formulas are a favorite model-theoretic tool of universal algebraists, and we use them in the study of the sizes of subdirectly irreducible algebras. Next we prove three general results on the existence of a finite basis for an equational theory. The last topic is semantic embeddings, a popular technique for proving undecidability results. This technique is essentially algebraic in nature, requiring no familiarity whatsoever with the theory of algorithms. (The study of decidability has given surprisingly deep insight into the limitations of Boolean product representations.)

At the end of several sections the reader will find selected references to source material plus state of the art texts or papers relevant to that section, and at the end of the book one finds a brief survey of recent developments and several outstanding problems.

The material in this book divides naturally into two parts. One part can be described as "what every mathematician (or at least every algebraist) should know about universal algebra." It would form a short introductory course to universal algebra, and would consist of Chapter I; Chapter II except for §4, §12,§13, and the last parts of §11, §14; Chapter IV §1–4; and Chapter V §1 and the part of §2 leading to the compactness theorem. The remaining material is more specialized and more intimately connected with current research in universal algebra.

Chapters are numbered by Roman numerals I through V, the sections in a chapter are given by Arabic numerals, §1, §2, etc. Thus II§6.18 refers to item 18, which happens to be a theorem, in Section 6 of Chapter II. A citation within Chapter II would simply refer to this item as 6.18. For the exercises we use numbering such as II§5 Ex. 4, meaning the fourth exercise in §5 of Chapter II. The bibliography is divided into two parts, the first containing books and survey articles, and the second research papers. The books and survey articles are referred to by number, e.g., G. Birkhoff [3], and the research papers by year, e.g., R. McKenzie [1978].

Diagram of Prerequisites



Special Notation

Contents

Preliminaries

We have attempted to keep our notation and conventions in agreement with those of the closely related subject of model theory, especially as presented in Chang and Keisler's *Model Theory* [8]. The reader needs only a modest exposure to classical algebra; for example he should know what groups and rings are.

We will assume a familiarity with the most basic notions of *set theory*. Actually, we use *classes* as well as *sets*. A class of sets is frequently called a *family* of sets. The notations A_i, $i \in I$, and $(A_i)_{i \in I}$ refer to a *family of sets indexed by a set I*. A naive theory of sets and classes is sufficient for our purposes. We assume the reader is familiar with *membership* ($\in$), *set-builder notation* ($\{—:—\}$), *subset* ($\subseteq$), *union* ($\cup$), *intersection* ($\cap$), *difference* ($-$), *ordered n-tuples* ($\langle x_1, \ldots, x_n \rangle$), *(direct) products* of sets ($A \times B$, $\prod_{i \in I} A_i$), and *(direct) powers* of sets (A^I). Also, it is most useful to know that

(a) concerning relations:
- (i) an *n-ary relation* on a set A is a subset of A^n;
- (ii) if $n = 2$ it is called a *binary* relation on A;
- (iii) the *inverse* $r^{\smile}$ of a binary relation r on A is specified by $\langle a,b \rangle \in r^{\smile}$ iff $\langle b,a \rangle \in r$;
- (iv) the *relational product* $r \circ s$ of two binary relations r, s on A is given by: $\langle a,b \rangle \in r \circ s$ iff for some c, $\langle a,c \rangle \in r$, $\langle c,b \rangle \in s$;

(b) concerning functions:
- (i) a *function* f from a set A to a set B, written $f: A \to B$, is a subset of $A \times B$ such that for each $a \in A$ there is exactly one $b \in B$ with $\langle a,b \rangle \in f$; in this case we write $f(a) = b$ or $f: a \mapsto b$;
- (ii) the set of all functions from A to B is denoted by B^A;
- (iii) the function $f \in B^A$ is *injective* (or *one-to-one*) if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$;
- (iv) the function $f \in B^A$ is *surjective* (or *onto*) if for every $b \in B$ there is an $a \in A$ with $f(a) = b$;

(v) the function $f \in B^A$ is *bijective* if it is both injective and surjective;
(vi) for $f \in B^A$ and $X \subseteq A$, $f(X) = \{b \in B : f(a) = b \text{ for some } a \in X\}$;
(vii) for $f \in B^A$ and $Y \subseteq B$, $f^{-1}(Y) = \{a \in A : f(a) \in Y\}$;
(viii) for $f: A \to B$ and $g: B \to C$, let $g \circ f: A \to C$ be the function defined by $(g \circ f)(a) = g(f(a))$. [This does not agree with the relational product defined above—but the ambiguity causes no problem in practice.];

(c) given a family F of sets, the *union* of F, $\bigcup F$, is defined by $a \in \bigcup F$ iff $a \in A$ for some $A \in F$ (define the *intersection* of F, $\bigcap F$, dually);
(d) a *chain* of sets C is a family of sets such that for each $A,B \in C$ either $A \subseteq B$ or $B \subseteq A$;
(e) *Zorn's lemma* says that if F is a nonempty family of sets such that for each chain C of members of F there is a member of F containing $\bigcup C$ (i.e., C has an *upper bound* in F) then F has a *maximal* member M (i.e., $M \in F$ and $M \subseteq A \in F$ implies $M = A$);
(f) concerning ordinals:
(i) the *ordinals* are generated from the empty set $\varnothing$ using the operations of *successor* ($x^+ = x \cup \{x\}$) and *union*;
(ii) $0 = \varnothing$, $1 = 0^+$, $2 = 1^+$, etc.; the *finite ordinals* are $0,1,\ldots$; and $n = \{0,1,\ldots,n-1\}$; the *natural numbers* are $1,2,3,\ldots$, the nonzero finite ordinals;
(iii) the first *infinite ordinal* is $\omega = \{0,1,2,\ldots\}$;
(iv) the ordinals are *well-ordered* by the relation $\in$, also called $<$;
(g) concerning cardinality:
(i) two sets A and B have the *same cardinality* if there is a bijection from A to B;
(ii) the *cardinals* are those ordinals κ such that no earlier ordinal has the same cardinality as κ. The *finite cardinals* are $0,1,2,\ldots$; and ω is the smallest *infinite cardinal*;
(iii) the *cardinality* of a set A, written $|A|$, is that (unique) cardinal κ such that A and κ have the same cardinality;
(iv) $|A| \cdot |B| = |A \times B|$ [$= \max(|A|,|B|)$ if either is infinite and $A,B \neq \varnothing$]. $A \cap B = \varnothing \Rightarrow |A| + |B| = |A \cup B|$ [$= \max(|A|,|B|)$ if either is infinite];
(h) one usually recognizes that a *class* is not a set by noting that it is *too big* to be put in one-to-one-correspondence with a cardinal (for example, the class of all groups).

In Chapter IV the reader needs to know the basic definitions from point set topology, namely what a *topological space*, a *closed* (*open*) *set*, a *subbasis* (*basis*) for a topological space, a closed (open) *neighborhood* of a point, a *Hausdorff* space, a *continuous* function, etc., are.

The symbol "$=$" is used to express the fact that both sides name the same object, whereas "$\approx$" is used to build equations which may or may not be true of particular elements. (A careful study of $\approx$ is given in Chapter II.)

CHAPTER I
Lattices

In the study of the properties common to all algebraic structures (such as groups, rings, etc.) and even some of the properties that distinguish one class of algebras from another, lattices enter in an essential and natural way. In particular, congruence lattices play an important role. Furthermore, lattices, like groups or rings, are an important class of algebras in their own right, and in fact one of the most beautiful theorems in universal algebra, Baker's finite basis theorem, was inspired by McKenzie's finite basis theorem for lattices. In view of this dual role of lattices in relation to universal algebra, it is appropriate that we start with a brief study of them. In this chapter the reader is acquainted with those concepts and results from lattice theory which are important in later chapters. Our notation in this chapter is less formal than that used in subsequent chapters. We would like the reader to have a casual introduction to the subject of lattice theory.

The origin of the lattice concept can be traced back to Boole's analysis of thought and Dedekind's study of divisibility. Schroeder and Peirce were also pioneers at the end of the last century. The subject started to gain momentum in the 1930's, and was greatly promoted by Birkhoff's book *Lattice Theory* in the 1940's.

§1. Definitions of Lattices

There are two standard ways of defining lattices—one puts them on the same (algebraic) footing as groups or rings, and the other, based on the notion of order, offers geometric insight.

Definition 1.1. A nonempty set L together with two binary operations $\vee$ and $\wedge$ (read "*join*" and "*meet*" respectively) on L is called a *lattice* if it satisfies the following identities:

L1: (a) $x \vee y \approx y \vee x$
(b) $x \wedge y \approx y \wedge x$ (commutative laws)
L2: (a) $x \vee (y \vee z) \approx (x \vee y) \vee z$
(b) $x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$ (associative laws)
L3: (a) $x \vee x \approx x$
(b) $x \wedge x \approx x$ (idempotent laws)
L4: (a) $x \approx x \vee (x \wedge y)$
(b) $x \approx x \wedge (x \vee y)$ (absorption laws).

EXAMPLE. Let L be the set of propositions, let $\vee$ denote the connective "or" and $\wedge$ denote the connective "and". Then L1 to L4 are well-known properties from propositional logic.

EXAMPLE. Let L be the set of natural numbers, let $\vee$ denote the least common multiple and $\wedge$ denote the greatest common divisor. Then properties L1 to L4 are easily verifiable.

Before introducing the second definition of a lattice we need the notion of a partial order on a set.

Definition 1.2. A binary relation $\leq$ defined on a set A is a *partial order* on the set A if the following conditions hold identically in A:

(i) $a \leq a$ (reflexivity)
(ii) $a \leq b$ and $b \leq a$ imply $a = b$ (antisymmetry)
(iii) $a \leq b$ and $b \leq c$ imply $a \leq c$ (transitivity).

If, in addition, for every a,b in A

(iv) $a \leq b$ or $b \leq a$

then we say $\leq$ is a *total order* on A. A nonempty set with a partial order on it is called a *partially ordered set*, or more briefly a *poset*, and if the relation is a total order then we speak of a *totally ordered set*, or a *linearly ordered set*, or simply a *chain*. In a poset A we use the expression $a < b$ to mean $a \leq b$ but $a \neq b$.

EXAMPLES. (1) Let Su(A) denote the *power set* of A, i.e., the set of all subsets of A. Then $\subseteq$ is a partial order on Su(A).

(2) Let A be the set of natural numbers and let $\leq$ be the relation "divides." Then $\leq$ is a partial order on A.

(3) Let A be the set of real numbers and let $\leq$ be the usual ordering. Then $\leq$ is a total order on A.

Most of the concepts developed for the real numbers which involve only the notion of order can be easily generalized to partially ordered sets.

Definition 1.3. Let A be a subset of a poset P. An element p in P is an *upper bound* for A if $a \leq p$ for every a in A. An element p in P is the *least upper bound* of A (l.u.b. of A), or *supremum* of A (sup A) if p is an upper bound of A, and $a \leq b$ for every a in A implies $p \leq b$ (i.e., p is the smallest among the upper bounds of A). Similarly we can define what it means for p to be a *lower bound* of A, and for p to be the *greatest lower bound* of A (g.l.b. of A), also called the *infimum* of A (inf A). For a,b in P we say *b covers a*, or *a is covered by b*, if $a < b$, and whenever $a \leq c \leq b$ it follows that $a = c$ or $c = b$. We use the notation $a \prec b$ to denote a is covered by b. The *closed interval* $[a,b]$ is defined to be the set of c in P such that $a \leq c \leq b$, and the *open interval* (a,b) is the set of c in P such that $a < c < b$.

Posets have the delightful characteristic that we can draw pictures of them. Let us describe in detail the method of associating a diagram, the so-called *Hasse diagram*, with a finite poset P. Let us represent each element of P by a small circle "$\circ$". If $a \prec b$ then we draw the circle for b above the circle for a, joining the two circles with a line segment. From this diagram we can recapture the relation $\leq$ by noting that $a < b$ holds iff for some finite sequence of elements $c_1, \ldots, c_n$ from P we have $a = c_1 \prec c_2 \cdots c_{n-1} \prec c_n = b$. We have drawn some examples in Figure 1. It is not so clear how one would draw

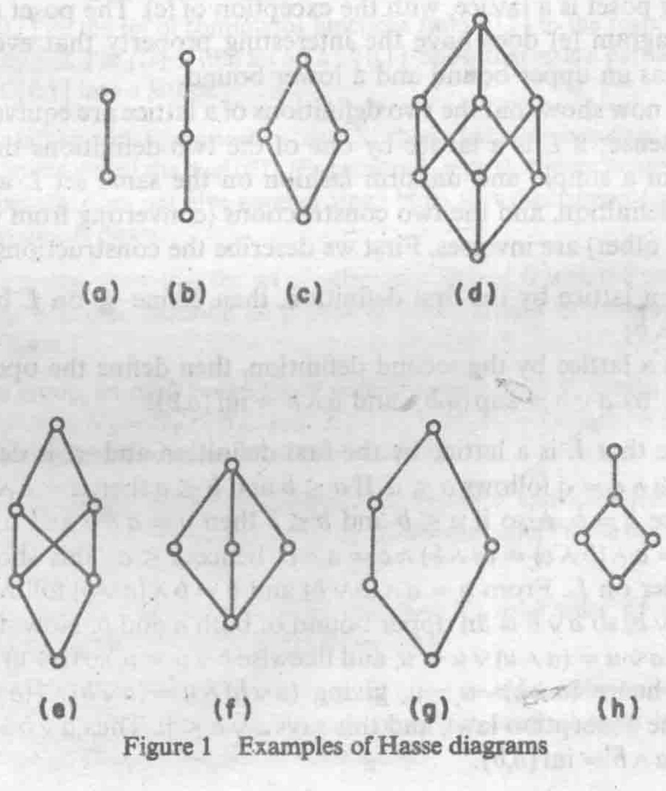


Figure 1 Examples of Hasse diagrams