Steven Givant
Paul Halmos

UNDERGRADUATE TEXTS IN MATHEMATICS

Introduction to Boolean Algebras

Springer

Undergraduate Texts in Mathematics

Undergraduate Texts in Mathematics

For other titles published in this series, go to
http://www.springer.com/series/666

Steven Givant • Paul Halmos

Introduction to Boolean Algebras

Springer

Steven Givant
Mills College
Department of Mathematics
and Computer Science
5000 MacArthur Blvd
Oakland CA 94613-1301
USA
givant@mills.edu

Paul Halmos
(Deceased)

ISSN: 0172-6056
ISBN: 978-0-387-40293-2 e-ISBN: 978-0-387-68436-9
DOI: 10.1007/978-0-387-68436-9

Library of Congress Control Number: 2008939810

Mathematics Subject Classification (2000): 06Exx

Printed on acid-free paper

springer.com

Contents

Preface

The theory of Boolean algebras was created in 1847 by the English mathematician George Boole. He conceived it as a calculus (or arithmetic) suitable for a mathematical analysis of logic. The form of his calculus was rather different from the modern version, which came into being during the period 1864–1895 through the contributions of William Stanley Jevons, Augustus De Morgan, Charles Sanders Peirce, and Ernst Schröder. A foundation of the calculus as an abstract algebraic discipline, axiomatized by a set of equations, and admitting many different interpretations, was carried out by Edward Huntington in 1904.

Only with the work of Marshall Stone and Alfred Tarski in the 1930s, however, did Boolean algebra free itself completely from the bonds of logic and become a modern mathematical discipline, with deep theorems and important connections to several other branches of mathematics, including algebra, analysis, logic, measure theory, probability and statistics, set theory, and topology. For instance, in logic, beyond its close connection to propositional logic, Boolean algebra has found applications in such diverse areas as the proof of the completeness theorem for first-order logic, the proof of the Łoś conjecture for countable first-order theories categorical in power, and proofs of the independence of the axiom of choice and the continuum hypothesis in set theory. In analysis, Stone's discoveries of the Stone–Čech compactification and the Stone–Weierstrass approximation theorem were intimately connected to his study of Boolean algebras. Countably complete Boolean algebras (also called σ-algebras) and countably complete fields of sets (also called σ-fields) play a key role in the foundations of measure theory. Outside the realm of mathematics, Boolean algebra has found applications in such diverse areas as anthropology, biology, chemistry, ecology, economics, sociology, and especially computer science and philosophy. For example, in computer science, Boolean algebra is used in electronic circuit design (gating networks), programming languages, databases, and complexity theory.

Most books on Boolean algebra fall into one of two categories. There are elementary texts that emphasize the arithmetic aspects of the subject (in particular, the laws that can be expressed and proved in the theory), and that often explore applications to propositional logic, philosophy, and electronic circuit design. There are also advanced treatises that present the deeper mathematical aspects of the theory at a level appropriate for graduate students and professional mathematicians (in terms of the mathematical background and level of sophistication required for understanding the presentation).

This book, a substantially revised version of the second author's *Lectures on Boolean Algebras*, tries to steer a middle course. It is aimed at undergraduates who have studied, say, two years of college-level mathematics, and have gained enough mathematical maturity to be able to read and write proofs. It does not assume the usual background in algebra, set theory, and topology that is required by more advanced texts. It does attempt to guide readers to some of the deeper aspects of the subject, and in particular to some of the important interconnections with topology. Those parts of algebra and topology that are needed to understand the presentation are developed within the text itself. There is a separate appendix that covers the basic notions, notations, and theorems from set theory that are occasionally needed.

The first part of the book, through Chapter 28, emphasizes the arithmetical and algebraic aspects of Boolean algebra. It requires no topology, and little set theory beyond what is learned in the first two years of college-level mathematics, with two important exceptions. First, two of the proofs use a form of mathematical induction that extends beyond the natural numbers to what are sometimes called "transfinite ordinal numbers". Transfinite ordinals and transfinite induction are discussed in Appendix A, but the key ideas of the two proofs can already be grasped in the context of the natural numbers and standard mathematical induction. Second, Chapter 10 presents an important example of a Boolean algebra that is based on topological notions. These notions are discussed in Chapter 9. The example itself, and the requisite topology, are not needed to understand the remaining chapters of the first part of the book. (Some of the more advanced exercises in the chapters do require an understanding of this material, but these exercises may be ignored by readers who wish to skip Chapters 9 and 10.) The second part of the book, in particular Chapters 29, 34–41, and 43, emphasizes the interconnections between Boolean algebra and topology, and consequently does make extensive use of topological ideas and results. The necessary topological background is provided in Chapters 9, 29, 32, and 33.

Some of the important results discussed in the first part of the book are the normal form theorem (which gives a description of the Boolean subalgebra generated by a set of elements, Chapter 11), and its analogue for Boolean ideals (Chapter 18); the homomorphism extension theorem (Chapter 13) and its application to the proofs of the isomorphism theorem for countable, atomless Boolean algebras (Chapter 16) and the existence theorem for free algebras (Chapter 28); the representation theorem for atomic Boolean algebras (every atomic Boolean algebra can be mapped isomorphically to a field of sets in a way that preserves all existing suprema as unions, Chapter 14); the maximal ideal theorem (every proper ideal can be extended to a maximal ideal, Chapter 20), and its application to the celebrated representation theorem (every Boolean algebra is isomorphic to a field of sets, Chapter 22); the existence and uniqueness theorems for completions (every Boolean algebra has a minimal complete extension that is unique up to isomorphisms, Chapter 25); the isomorphism of factors theorem (two countably complete Boolean algebras that are factors of one another must be isomorphic) and the counterexamples demonstrating that the theorem cannot be extended to all Boolean algebras, or even to all countable Boolean algebras (Chapters 27 and 45).

Many of the highlights of the second part of the book center on the fundamental duality theorems for Boolean algebras and Boolean spaces: to every Boolean algebra there corresponds a Boolean space that is uniquely determined up to homeomorphism, and, conversely, to every Boolean space there corresponds a Boolean algebra that is uniquely determined up to isomorphism (Chapter 34). These theorems imply that every notion or theorem concerning Boolean algebras has a “dual” topological counterpart concerning Boolean spaces, and conversely. For instance, ideals correspond to open sets (Chapter 35), homomorphisms to continuous functions (Chapter 36), quotient algebras to closed subspaces and subalgebras to Boolean quotient spaces (Chapter 37), direct products of Boolean algebras to Stone–Čech compactifications of unions of Boolean spaces (Chapter 43), and complete Boolean algebras to extremally disconnected spaces (Chapter 38). A related result, discussed in Chapter 40, is the representation theorem for σ-algebras (every σ-algebra is isomorphic to a σ-field of sets modulo a σ-ideal).

It is not necessary to read all the chapters in the order in which they appear, since there is a fair degree of independence among them. The diagram at the end of the preface shows the main chapter dependencies. Three examples may serve to demonstrate how the diagram is to be understood. First, Chapter 28 depends on Chapters 1–8 and 11–13. Second, Chapter 24 depends on Chapters 1–8, 11–12, and 17–19. Finally, Chapter 31 depends on Chapters 1–12, 17–18, and 29–30. These remarks do not apply to the exercises, some of which depend on earlier chapters for which no dependency is indicated in the diagram. Also, minor references to earlier chapters are not indicated in the diagram. For instance, an application in Chapter 36 of the principal result of that chapter depends on the definition of a free algebra (given in Chapter 28), but not on any of the results about free algebras. Similarly, a corollary at the end of Chapter 21 depends on the notion of a maximal ideal and the easily comprehended statement of the maximal ideal theorem (given in Chapter 20).

A large number of exercises of varying levels of difficulty have been included in the text. There are routine problems that help readers understand the basic definitions and theorems; intermediate problems that extend or enrich material developed in the text; and difficult problems that often present important results not covered in the text. The harder exercises are labeled as such, and hints for their solutions are given in Appendix B. Some of the exercises are formulated, not as assertions, but as questions that readers are invited to ponder.

There is an instructor's manual that contains complete solutions to the exercises. It may serve as a guide to instructors, and in particular it may help them select problems at an appropriate level of difficulty for their students. Instructors may also wish to assign the solutions of some of the more difficult problems to individual students or groups of students for independent study or as class projects.

Historical remarks are sprinkled throughout the text. We are indebted to Don Monk for his help in tracking down the authorship of some of the main results. Regrettably, it has not been feasible to determine the origin of every theorem.

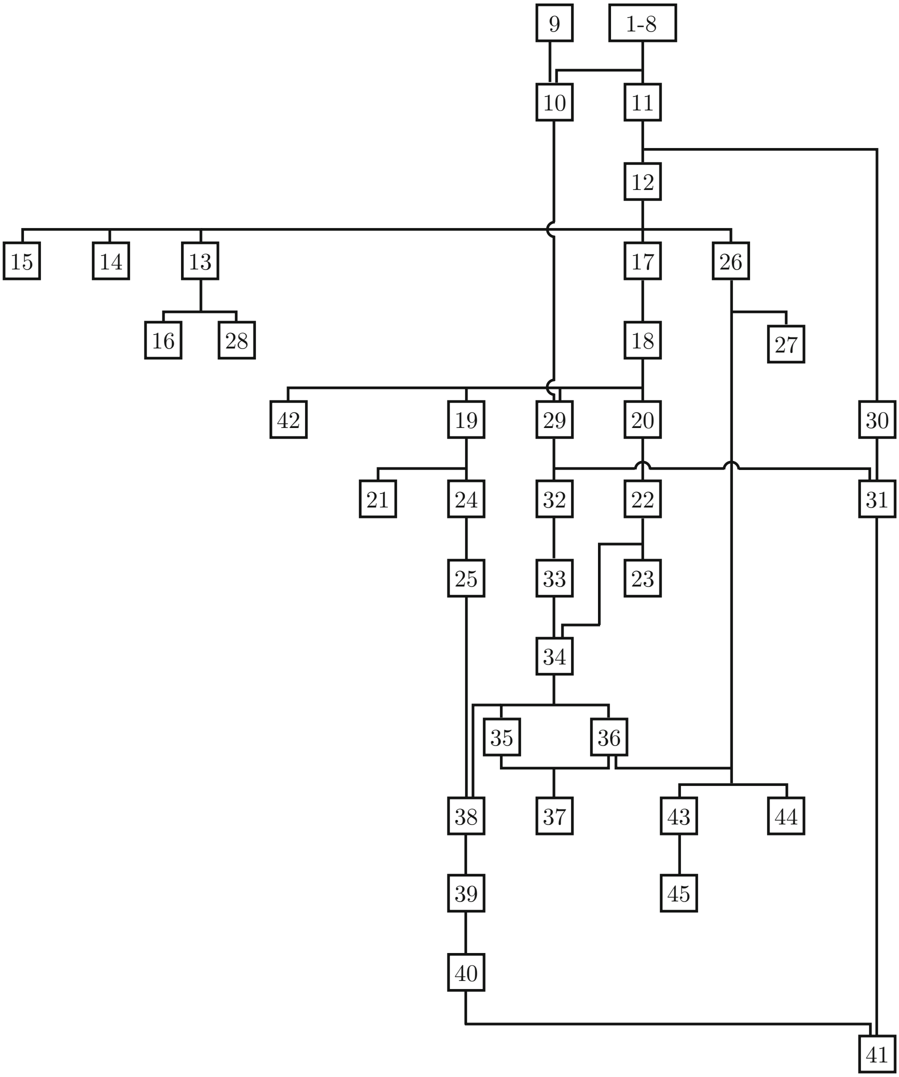
The book can serve as a basis for a variety of courses. A one-semester course that focuses on the algebraic material might cover some subset of Chapters 1–28, for instance Chapters 1–8, 11–14, and 17–27. A one-semester course that includes some of the interconnections with topology might cover Chapters 1–8, 11–12, 14, 17–22, parts of 9 and 29, and 32–36. Most of the text could be covered in a one-year course.

A quick word about terminology. In this book, the phrase "just in case" is used as a variant of the phrase "in this case, and only in this case". In other words, it is a synonym for "if and only if".

This revision of Halmos's book was planned and initially executed by both authors. Due to declining health, however, Halmos was not able to review the later versions of the manuscript. He died on October 2, 2006. Whatever imperfections remain in the text are my sole responsibility.

Steven Givant
San Francisco, California
August, 2007

Chapter dependence diagram



Chapter 1

Boolean Rings

A ring is an abstract version of arithmetic, the kind of thing you studied in school. The prototype is the ring of integers. It consists of a universe — the set of integers — and three operations on the universe: the binary operations of addition and multiplication, and the unary operation of negation (forming negatives). There are also two distinguished integers, zero and one. The ring of integers satisfies a number of basic laws that are familiar from school mathematics: the associative laws for addition and multiplication,

$$p + (q + r) = (p + q) + r, \tag{1}$$

$$p \cdot (q \cdot r) = (p \cdot q) \cdot r, \tag{2}$$

the commutative laws for addition and multiplication,

$$p + q = q + p, \tag{3}$$

$$p \cdot q = q \cdot p, \tag{4}$$

the identity laws for addition and multiplication,

$$p + 0 = p, \tag{5}$$

$$p \cdot 1 = p, \tag{6}$$

the inverse law for addition,

$$p + (-p) = 0, \tag{7}$$

and the distributive laws for multiplication over addition,

$$p \cdot (q + r) = p \cdot q + p \cdot r, \tag{8}$$

S. Givant, P. Halmos, *Introduction to Boolean Algebras*,
Undergraduate Texts in Mathematics, DOI: 10.1007/978-0-387-68436-9_1,

$$(q+r)\cdot p = q\cdot p + r\cdot p. \tag{9}$$

The difference between the ring of integers and an arbitrary ring is that, in the latter, the universe may be an arbitrary non-empty set of elements, not just a set of numbers, and the operations take their arguments and values from this set. The associative, commutative, identity, and inverse laws for addition, the associative law for multiplication, and the distributive laws are required to hold: they are the ring axioms. The commutative law for multiplication is not required to hold in an arbitrary ring; if it does, the ring is said to be *commutative.* Also, a ring is not always required to have a unit, an element 1 satisfying (6); if it does, it is called a ring *with unit.*

There are other natural examples of rings besides the integers. The most trivial is the ring with just one element in its universe: zero. It is called the *degenerate* ring. The simplest non-degenerate ring with unit has just two elements, zero and one. The operations of addition and multiplication are described by the arithmetic tables

$+$	0	1
0	0	1
1	1	0

and

$\cdot$	0	1
0	0	0
1	0	1

.

An examination of the tables shows that the two-element ring has several special properties. First of all, every element is its own additive inverse:

$$p+p=0. \tag{10}$$

Therefore, the operation of negation is superfluous: every element is its own negative. Rings satisfying condition (10) are said to have *characteristic* 2. Second, every element is its own square:

$$p\cdot p = p. \tag{11}$$

Elements with this property are called *idempotent.* When every element is idempotent, the ring itself is said to be idempotent.

A *Boolean ring* is an idempotent ring with unit. (Warning: some authors define a Boolean ring to be just an idempotent ring, which may or may not have a unit. They call the concept we have defined a “Boolean ring with unit”.) The two-element ring is the simplest non-degenerate example of a Boolean ring. It will be denoted throughout by the same symbol as the ordinary integer 2. The notation is not commonly used, but it is very convenient. It is in accordance with von Neumann’s definition of the ordinal numbers (under which the ordinal number 2 coincides with the set $\{0,1\}$), with sound general principles of notational economy, and (in logical expressions such as "two-valued") with idiomatic linguistic usage.

The condition of idempotence in the definition of a Boolean ring has quite a strong influence on the structure of such rings. Two of its most surprising consequences are that (a) a Boolean ring always has characteristic 2 and (b) a Boolean ring is always commutative. For the proof, compute $(p+q)^2$, and use idempotence to conclude that

$$0 = q \cdot p + p \cdot q. \tag{12}$$

In more detail,

$$p + q = (p+q)^2 = p^2 + q \cdot p + p \cdot q + q^2 = p + q \cdot p + p \cdot q + q,$$

by the distributive and idempotent laws. Add the inverse of p to the left sides of the first and last terms, add the inverse of q to the right sides, and use the laws governing addition, in particular the inverse and identity laws, to arrive at (12).

This result implies the two assertions, one after another, as follows. Put $p = q$ in (12) and use idempotence to get (a):

$$0 = p^2 + p^2 = p + p.$$

Assertion (a) implies that every element is equal to its own negative, so

$$p \cdot q = -(p \cdot q). \tag{13}$$

Add the left and right sides of (13) to the left and right sides of (12) respectively, and apply the inverse and identity laws for addition to obtain (b):

$$p \cdot q = q \cdot p + p \cdot q + -(p \cdot q) = q \cdot p + 0 = q \cdot p.$$

Since, as we now know, negation in Boolean rings is the identity operation, it is never necessary to use the minus sign for additive inverses, and we shall never again do so. (A little later we shall meet another natural use for it.) Only a slight modification in the set of axioms is needed: the identity (7) should be replaced by (10). From now on, the official axioms for a Boolean ring are (1)–(3), (5), (6), and (8)–(11).

Boolean rings are the only rings that will be considered in this book, so it is worth looking at another example. The universe of this example consists of ordered pairs (p, q) of elements from 2. In other words, it consists of the four ordered pairs

$$(0,0), \quad (0,1), \quad (1,0), \quad (1,1).$$

This set will be denoted by 2^2, in agreement with the notation $\mathbb{R}^2$ that is used to denote the set of ordered pairs of real numbers. To add or multiply two pairs in 2^2, just add or multiply the corresponding coordinates in 2:

$$(p_0, p_1) + (q_0, q_1) = (p_0 + q_0, p_1 + q_1)$$

and

$$(p_0, p_1) \cdot (q_0, q_1) = (p_0 \cdot q_0, p_1 \cdot q_1).$$

These equations make sense: their right sides refer to the elements and operations of 2. The zero and unit of the ring are the pairs $(0, 0)$ and $(1, 1)$.

It is a simple matter to check that the axioms for Boolean rings are true in 2^2. In each case, the verification of an axiom reduces to its validity in 2. For example, here is the verification of the commutative law for addition:

$$\begin{aligned}(p_0, p_1) + (q_0, q_1) &= (p_0 + q_0, p_1 + q_1)\\ &= (q_0 + p_0, q_1 + p_1) = (q_0, q_1) + (p_0, p_1).\end{aligned}$$

The first and last equalities use the definition of addition of ordered pairs, and the middle equality uses the commutative law for addition in 2.

The preceding example can easily be generalized to each positive integer n. The universe of the ring is the set 2^n of n-termed sequences

$$(p_0, \dots, p_{n-1})$$

of elements from 2. The sum and product of two such n-tuples are defined coordinatewise, just as in the case of ordered pairs:

$$(p_0, \dots, p_{n-1}) + (q_0, \dots, q_{n-1}) = (p_0 + q_0, \dots, p_{n-1} + q_{n-1})$$

and

$$(p_0, \dots, p_{n-1}) \cdot (q_0, \dots, q_{n-1}) = (p_0 \cdot q_0, \dots, p_{n-1} \cdot q_{n-1}).$$

The zero and unit are the n-tuples $(0, \dots, 0)$ and $(1, \dots, 1)$. Verifying the axioms for Boolean rings is no more difficult in this example than it is in the example 2^2.

To generalize the example still further, it is helpful to look at the set 2^n another way, namely, as the set of functions with domain $\{0, \dots, n-1\}$ and with values in 2, that is, with possible values 0 and 1. Let X be an arbitrary set, and 2^X the set of all functions from X into 2. The elements of 2^X will be called 2-*valued functions* on X. The distinguished elements and the operations of 2^X are defined pointwise. This means that 0 and 1 in 2^X are the constant functions defined, for each x in X, by

$$0(x) = 0 \qquad \text{and} \qquad 1(x) = 1,$$

and if p and q are 2-valued functions on X, then the functions $p + q$ and $p \cdot q$ are defined by

$$(p+q)(x) = p(x) + q(x) \qquad \text{and} \qquad (p \cdot q)(x) = p(x) \cdot q(x).$$

Again, these equations make sense; their right sides refer to elements and operations of 2.

Verifying that 2^X is a Boolean ring is conceptually the same as verifying that 2^2 is a Boolean ring, but notationally it looks a bit different. Consider, as an example, the verification of the distributive law (8). In the context of 2^X, the left and right sides of (8) denote functions from X into 2. It must be shown that these two functions are equal. They obviously have the same domain X, so it suffices to check that the values of the two functions at each element x in the domain agree, that is,

$$\big(p \cdot (q + r)\big)(x) = \big(p \cdot q + p \cdot r\big)(x). \tag{14}$$

The left and right sides of (14) evaluate to

$$p(x) \cdot (q(x) + r(x)) \qquad \text{and} \qquad p(x) \cdot q(x) + p(x) \cdot r(x) \tag{15}$$

respectively, by the definitions of addition and multiplication in 2^X. Each of these terms denotes an element of 2. Since the distributive law holds in 2, the two terms in (15) are equal. Therefore, equation (14) is true. The other Boolean ring axioms are verified for 2^X in a similar fashion.

For another example of a Boolean ring let A be the set of all idempotent elements in a commutative (!) ring R with unit, with addition redefined so that the new sum of p and q in A is $p + q - 2pq$. The distinguished elements of A are the same as those of R, and multiplication in A is just the restriction of multiplication in R. The verification that A becomes a Boolean ring in this way is an amusing exercise in ring axiomatics. Commutativity is used repeatedly; it is needed, for instance, to prove that A is closed under multiplication.

Exercises

1. Verify that 2 satisfies ring axioms (1)–(9).

2. Verify that 2^3 satisfies ring axioms (1)–(9).

3. Verify that 2^X satisfies ring axioms (1)–(9) for any set X. What ring do you get when X is the empty set?

4. Essentially, what ring is 2^X when X is a set consisting of just one element? Can you make this statement precise?

5. A *group* is a non-empty set, together with a binary operation $+$ (on the set), a unary operation $-$, and a distinguished element 0, such that the associative law (1), the identity laws

$$p + 0 = p \qquad \text{and} \qquad 0 + p = p,$$

and the inverse laws

$$p + -p = 0 \qquad \text{and} \qquad -p + p = 0$$

are all valid. Show that in a group the cancellation laws hold: if

$$p + q = p + r \qquad \text{or} \qquad q + p = r + p,$$

then $q = r$. Conclude that in a group, the inverse element is unique: if $p + q = 0$, then $q = -p$.

6. Prove that in an arbitrary ring,

$$p \cdot 0 = 0 \cdot p = 0 \qquad \text{and} \qquad p \cdot (-q) = (-p) \cdot q = -(p \cdot q)$$

for all elements p and q.

7. Let A be the set of all idempotent elements in a commutative ring R with unit. Define the sum $p \oplus q$ of two elements p and q in A by

$$p \oplus q = p + q - 2pq,$$

where the right-hand term is computed in R (and pq means $p \cdot q$). The distinguished elements of A are the same as those of R, and multiplication in A is the restriction of multiplication in R. Show that A is a Boolean ring.

8. A *Boolean group* is a group in which every element has order two (in other words, the law (10) is valid). Show that every Boolean group is commutative (that is, the commutative law (3) is valid).

9. A *zero-divisor* in a ring is a non-zero element p such that $p \cdot q = 0$ for some non-zero element q. Prove that a Boolean ring (with or without a unit) with more than two elements has zero-divisors. (This observation is due to Stone [66].)

10. (Harder.) Prove that every Boolean ring without a unit can be extended to a Boolean ring with a unit. To what extent is this extension procedure unique? (This result is due to Stone [66].)

11. (Harder.) Does every finite Boolean ring have a unit? (The answer to this question is due to Stone [66].)

12. Give an example of a Boolean ring that has no unit. Exercise 10 implies that your example can be extended to a Boolean ring with unit; describe the elements of that extension.

13. (Harder.) Can every non-degenerate Boolean ring with unit be obtained by adjoining a unit to a Boolean ring without a unit?

14. (Harder.) Is every Boolean group the additive group of some Boolean ring?

Chapter 2

Boolean Algebras

Let X be an arbitrary set and let $\mathcal{P}(X)$ be the class of all subsets of X (the *power set* of X). Three natural set-theoretic operations on $\mathcal{P}(X)$ are the binary operations of union and intersection, and the unary operation of complementation. The union $P \cup Q$ of two subsets P and Q is, by definition, the set of elements that are either in P or in Q, the intersection $P \cap Q$ is the set of elements that are in both P and Q, and the complement P' is the set of elements (of X) that are not in P. There are also two distinguished subsets: the empty set $\varnothing$, which has no elements, and the universal set X. The class $\mathcal{P}(X)$, together with the operations of union, intersection, and complementation, and the distinguished subsets $\varnothing$ and X, is called the *Boolean algebra* (or *field*) *of all subsets* of X, or the *power set algebra* on X.

The arithmetic of this algebra bears a striking resemblance to the arithmetic of Boolean rings. Some of the most familiar and useful identities include the laws for forming the complements of the empty and the universal sets,

$$(1) \qquad \varnothing' = X, \qquad X' = \varnothing,$$

the laws for forming an intersection with the empty set and a union with the universal set,

$$(2) \qquad P \cap \varnothing = \varnothing, \qquad P \cup X = X,$$

the identity laws,

$$(3) \qquad P \cap X = P, \qquad P \cup \varnothing = P,$$

the complement laws,

$$(4) \qquad P \cap P' = \varnothing, \qquad P \cup P' = X,$$

S. Givant, P. Halmos, *Introduction to Boolean Algebras*,
Undergraduate Texts in Mathematics, DOI: 10.1007/978-0-387-68436-9_2,

the double complement law,

$$(P')' = P, \tag{5}$$

the idempotent law,

$$P \cap P = P, \qquad P \cup P = P, \tag{6}$$

the De Morgan laws,

$$(P \cap Q)' = P' \cup Q', \qquad (P \cup Q)' = P' \cap Q', \tag{7}$$

the commutative laws,

$$P \cap Q = Q \cap P, \qquad P \cup Q = Q \cup P, \tag{8}$$

the associative laws,

$$P \cap (Q \cap R) = (P \cap Q) \cap R, \qquad P \cup (Q \cup R) = (P \cup Q) \cup R, \tag{9}$$

and the distributive laws,

$$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R), \qquad P \cup (Q \cap R) = (P \cup Q) \cap (P \cup R). \tag{10}$$

Each of these identities can be verified by an easy set-theoretic argument based on the definitions of the operations involved. Consider, for example, the verification of the first De Morgan law. It must be shown that each element x of X belongs to $(P \cap Q)'$ just in case it belongs to $P' \cup Q'$. The argument goes as follows:

$$\begin{aligned} x \in (P \cap Q)' \quad & \text{if and only if} \quad x \notin P \cap Q, \\ & \text{if and only if} \quad x \notin P \text{ or } x \notin Q, \\ & \text{if and only if} \quad x \in P' \text{ or } x \in Q', \\ & \text{if and only if} \quad x \in P' \cup Q'. \end{aligned}$$

The first and third equivalences use the definition of complementation, the second uses the definition of intersection, and the last uses the definition of union.

While (1)–(10) bear a close resemblance to laws that are true in Boolean rings, there are important differences. Negation in Boolean rings is the identity operation, whereas complementation is not. Addition in Boolean rings is not an idempotent operation, whereas union is. The distributive law for addition over multiplication fails in Boolean rings, whereas the distributive law for union over intersections holds.

Boolean rings are an abstraction of the ring 2. The corresponding abstraction of $\mathcal{P}(X)$ is called a Boolean algebra. Specifically, a *Boolean algebra* is a non-empty set A, together with two binary operations $\wedge$ and $\vee$ (on A), a unary operation $'$, and two distinguished elements 0 and 1, satisfying the following axioms, the analogues of identities (1)–(10):

$$0' = 1, \qquad 1' = 0, \tag{11}$$

$$p \wedge 0 = 0, \qquad p \vee 1 = 1, \tag{12}$$

$$p \wedge 1 = p, \qquad p \vee 0 = p, \tag{13}$$

$$p \wedge p' = 0, \qquad p \vee p' = 1, \tag{14}$$

$$(p')' = p, \tag{15}$$

$$p \wedge p = p, \qquad p \vee p = p, \tag{16}$$

$$(p \wedge q)' = p' \vee q', \qquad (p \vee q)' = p' \wedge q', \tag{17}$$

$$p \wedge q = q \wedge p, \qquad p \vee q = q \vee p, \tag{18}$$

$$p \wedge (q \wedge r) = (p \wedge q) \wedge r, \qquad p \vee (q \vee r) = (p \vee q) \vee r, \tag{19}$$

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r), \qquad p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r). \tag{20}$$

This set of axioms is wastefully large, more than strong enough for the purpose. The problem of selecting small subsets of this set of conditions that are strong enough to imply them all is one of dull axiomatics. For the sake of the record: one solution of the problem, essentially due to Huntington [28], is given by the *identity laws* (13), the *complement laws* (14), the *commutative laws* (18), and the *distributive laws* (20). To prove that these four pairs imply all the other conditions, and, in particular, to prove that they imply the *De Morgan laws* (17) and the *associative laws* (19), involves some non-trivial trickery.

There are several possible widely adopted names for the operations $\wedge$, $\vee$, and $'$. We shall call them *meet*, *join*, and *complement* (or *complementation*), respectively. The distinguished elements 0 and 1 are called *zero* and *one*. One is also known as the *unit*.

Equations (1)–(10) imply that the class of all subsets of an arbitrary set X is an example of a Boolean algebra. When the underlying set X is empty, the resulting algebra is *degenerate* in the sense that it has just one element. In this case, the operations of join, meet, and complementation are all constant, and $0 = 1$. The simplest non-degenerate Boolean algebra is the class of all subsets of a one-element set. It has just two elements, 0 (the empty set) and 1 (the one-element set). The operations of join and meet are described by the arithmetic tables

$\vee$	0	1
0	0	1
1	1	1

and

$\wedge$	0	1
0	0	0
1	0	1

,

and complementation is the unary operation that maps 0 to 1, and conversely. We shall see in a moment that this algebra and the two-element Boolean ring are interdefinable. For that reason, the same symbol 2 is used to denote both structures.

Here is a comment on notation, inspired by the associative laws (19). It is an elementary consequence of those laws that if $p_1, \ldots, p_n$ are elements of a Boolean algebra, then $p_1 \vee \cdots \vee p_n$, makes sense. The point is, of course, that since such joins are independent of how they are bracketed, it is not necessary to indicate any bracketing at all. The element $p_1 \vee \cdots \vee p_n$ may alternatively be denoted by $\bigvee_{i=1}^n p_i$, or, in case no confusion is possible, simply by $\bigvee_i p_i$.

If we make simultaneous use of both the commutative and the associative laws, we can derive a slight but useful generalization of the preceding comment. If E is a non-empty finite subset of a Boolean algebra, then the set E has a uniquely determined join, independent of any order or bracketing that may be used in writing it down. (In case E is a singleton, it is natural to identify that join with the unique element in E.) We shall denote the join of E by $\bigvee E$.

Both the preceding comments apply to meets as well as to joins. The corresponding symbols are, of course,

$$\bigwedge_{i=1}^{n} p_i, \quad \text{or} \quad \bigwedge_i p_i, \quad \text{and} \quad \bigwedge E.$$

The conventions regarding the order of performing different operations in the absence of any brackets are the following: complements take priority over meets and joins, while meets take priority over joins. Example: the expression $p' \vee q \wedge p$ should be read as $(p')\vee(q \wedge p)$. It is convenient to write successive applications of complement without any bracketing, for instance p'' instead of $(p')'$.

Exercises

1. Verify that the identities (1)–(10) are true in every Boolean algebra of all subsets of a set.

2. (Harder.) Show that the identities in (13), (14), (18), and (20) together form a set of axioms for the theory of Boolean algebras. In other words, show that they imply the identities in (11), (12), (15), (16), (17), and (19). (This result is essentially due to Huntington [30].)

3. Prove directly that the two-element structure 2 defined in the chapter is a Boolean algebra, by showing that axioms (13), (14), (18), and (20) are all valid in 2.

4. In analogy with the construction, for each set X, of the Boolean ring 2^X in Chapter 1, define operations of join, meet, and complementation on 2^X, and distinguished constants zero and one, and prove that the resulting structure is a Boolean algebra.

5. (Harder.) A member of a set of axioms is said to be *independent* of the remaining axioms if it is not derivable from them. One technique for demonstrating the independence of a given axiom is to construct a model in which that axiom fails while the remaining axioms hold. The given axiom cannot then be derivable from the remaining ones, since if it were, it would have to hold in the model as well. The four pairs of identities (13), (14), (18), and (20) constitute a set of eight axioms for Boolean algebras.

   (a) Show that the distributive law for join over meet in (20) is independent of the remaining seven axioms.

   (b) Show that the distributive law for meet over join in (20) is independent of the remaining seven axioms.

   (c) Show that each of the complement laws in (14) is independent of the remaining seven axioms.

   (These proofs of independence are due to Huntington [28].)

6. (Harder.) A set of axioms is said to be *independent* if no one of the axioms can be derived from the remaining ones. Do the four pairs of identities (13), (14), (18), and (20) constitute an independent set of axioms for Boolean algebras?

7. (Harder.) The operation of meet and the distinguished elements zero and one can be defined in terms of join and complement by the equations

$$p \wedge q = (p' \vee q')', \qquad 0 = (p \vee p')', \qquad 1 = p \vee p'.$$

A Boolean algebra may therefore be thought of as a non-empty set together with two operations: join and complement. Prove that the following identities constitute a set of axioms for this conception of Boolean algebras: the commutative and associative laws for join, and

$$\text{(H)} \qquad (p' \vee q')' \vee (p' \vee q)' = p.$$

(This axiomatization, and the proof of its equivalence to the set of axioms (13), (14), (18), and (20), is due to Huntington [30]. In fact, (H) is often called *Huntington's axiom.*)

8. (Harder) Prove that the three axioms in Exercise 7 are independent. (The proof of independence is due to Huntington [30].)

9. (Harder.) Prove that the following identities constitute a set of axioms for Boolean algebras:

$$p'' = p, \quad p \vee (q \vee q')' = p, \quad p \vee (q \vee r)' = ((q' \vee p)' \vee (r' \vee p)')'.$$

(This axiomatization, and the proof of its equivalence with the axiom set in Exercise 7, is due to Huntington [30].)

10. (Harder.) Prove that the three axioms in Exercise 9 are independent. (The proof of independence is due to Huntington [30].)

11. (Harder.) Prove that the commutative and associative laws for join, and the equivalence

$$p \vee q' = r \vee r' \qquad \text{if and only if} \qquad p \vee q = p,$$

together constitute a set of axioms for Boolean algebras. (This axiomatization, and the proof of its equivalence with the axiom set in Exercise 7, is due to Byrne [11].)

Chapter 3

Boolean Algebras Versus Rings

The theories of Boolean algebras and Boolean rings are very closely related; in fact, they are just different ways of looking at the same subject. More precisely, every Boolean algebra can be turned into a Boolean ring by defining appropriate operations of addition and multiplication, and, conversely, every Boolean ring can be turned into a Boolean algebra by defining appropriate operations of join, meet, and complement. The precise way of accomplishing this can be elucidated by comparing the Boolean algebra $\mathcal{P}(X)$ of all subsets of X and the Boolean ring 2^X of all 2-valued functions on X. Each subset P of X is naturally associated with a function p from X into 2, namely the *characteristic function* of P, defined for each x in X by

$$p(x) = \begin{cases} 1 & \text{if } x \in P, \\ 0 & \text{if } x \notin P. \end{cases}$$

The correspondence that maps each subset to its characteristic function is a *bijection* (a one-to-one, onto function) from $\mathcal{P}(X)$ to 2^X. The inverse correspondence maps each function q in 2^X to its *support*, the set of elements x in X for which $q(x) = 1$.

How should the operations of addition and multiplication, and the distinguished elements zero and the unit, be defined in $\mathcal{P}(X)$ so that it becomes a Boolean ring? To answer this question, it is helpful to analyze more closely the definitions of the ring operations in 2^X, and to translate these definitions (via the bijective correspondence) into the language of $\mathcal{P}(X)$. Suppose P and Q are subsets of X, and let p and q be their characteristic functions.

S. Givant, P. Halmos, *Introduction to Boolean Algebras*,
Undergraduate Texts in Mathematics, DOI: 10.1007/978-0-387-68436-9_3,

The sum $p + q$ and the product $p \cdot q$ are defined pointwise: for any x in X,

$$(p+q)(x) = p(x) + q(x) = \begin{cases} 1 & \text{if} \quad p(x) \neq q(x), \\ 0 & \text{if} \quad p(x) = q(x), \end{cases}$$

and

$$(p \cdot q)(x) = p(x) \cdot q(x) = \begin{cases} 1 & \text{if} \quad p(x) = q(x) = 1, \\ 0 & \text{otherwise}, \end{cases}$$

as is clear from the arithmetic tables for the ring 2. The values $p(x)$ and $q(x)$ are different just in case one of them is 1 and the other is 0, that is to say, just in case x is in P but not in Q, or vice versa. The values $p(x)$ and $q(x)$ are both 1 just in case x is in both P and Q. These observations suggest the following definitions of ring addition and multiplication in $\mathcal{P}(X)$:

$$(1) \qquad P + Q = (P \cap Q') \cup (P' \cap Q) \qquad \text{and} \qquad P \cdot Q = P \cap Q.$$

(The Boolean sum $P + Q$ is usually called the *symmetric difference* of P and Q.) A similar analysis suggests the definitions

$$(2) \qquad 0 = \varnothing \qquad \text{and} \qquad 1 = X$$

for the distinguished ring elements zero and one in $\mathcal{P}(X)$.

With these operations and distinguished elements, the set $\mathcal{P}(X)$ becomes a Boolean ring: it satisfies axioms (1.1)–(1.3), (1.5), (1.6), and (1.8)–(1.11). In fact, the correspondence h that takes each function in 2^X to its support is what is usually called an *isomorphism* between the two rings: it maps 2^X one-to-one onto $\mathcal{P}(X)$, and it *preserves* the ring operations and distinguished elements in the sense that

$$h(p+q) = h(p) + h(q), \quad h(p \cdot q) = h(p) \cdot h(q), \quad h(0) = 0, \quad h(1) = 1.$$

The operations and distinguished elements on the left sides of the equations are those of the ring 2^X, while the ones on the right are those of the ring $\mathcal{P}(X)$. These equations just express, in a slightly different form, the definitions in (1) and (2) of the ring operations and distinguished elements for $\mathcal{P}(X)$. The whole state of affairs can be summarized by saying that the Boolean rings 2^X and $\mathcal{P}(X)$ are *isomorphic* via the correspondence that takes each function in 2^X to its support. The two rings are structurally the same (which is what really matters); they differ only in the "shape" of their elements.

It is also possible to turn the ring 2^X into a Boolean algebra. To understand how the Boolean operations and distinguished elements should be defined in 2^X, it is helpful to analyze the definitions of these operations