12-2016

AN INTRODUCTION TO BOOLEAN ALGEBRAS

Amy Schardijn
California State University - San Bernardino, schardia@coyote.csusb.edu

An Introduction to Boolean Algebras

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Amy Michiel Schardijn

December 2016

An Introduction to Boolean Algebras

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Amy Michiel Schardijn

December 2016

Approved by:

Dr. Giovanna Llosent, Committee Chair	Date
Dr. Jeremy Aikin, Committee Member	
Dr. Corey Dunn, Committee Member	
Dr. Charles Stanton, Chair, Department of Mathematics	Dr. Corey Dunn Graduate Coordinator, Department of Mathematics

Abstract

This thesis discusses the topic of Boolean algebras. In order to build intuitive understanding of the topic, research began with the investigation of Boolean algebras in the area of Abstract Algebra. The content of this initial research used a particular notation. The ideas of partially ordered sets, lattices, least upper bounds, and greatest lower bounds were used to define the structure of a Boolean algebra. From this fundamental understanding, we were able to study atoms, Boolean algebra isomorphisms, and Stone's Representation Theorem for finite Boolean algebras. We also verified and proved many properties involving Boolean algebras and related structures.

We then expanded our study to more thoroughly developed theory. This comprehensive theory was more abstract and required the use of a different, more universal, notation. We continued examining least upper and greatest lower bounds but extended our knowledge to subalgebras and families of subsets. The notions of cardinality, cellularity, and pairwise disjoint families were investigated, defined, and then used to understand the Erdös-Tarski Theorem.

Lastly, this study concluded with the investigation of denseness and incomparability as well as normal forms and the completion of Boolean algebras.

Acknowledgements

I would like to thank my advisor, Dr. Giovanna Llosent. You have unwaveringly supported me through this journey. You have given me much needed advice and guidance and always remained patient with me. I would not have completed this achievement without you. Though I can say "thank you," I will never be able to truly express how appreciative I am for your impact on my life. Thank you for everything.

I would like to thank my committee members, Dr. Jeremy Aikin and Dr. Corey Dunn. Dr. Aikin, thank you for agreeing to be on my committee and for devoting your time to help me on top of all of the other students you so generously support. Dr. Dunn, thank you for your support and advice over these past years. You have helped me immensely with making the best decisions for my academic career.

I also wish thank Joyce Ahlgren. Without ever hesitating, you always help me in any and every way that you possibly can. I am very thankful for you.

To my family, you always believe in me, never doubting that I can accomplish anything I set out to achieve. Tunji, you believe in me more than I believe in myself most of the time. Whenever I am struggling, I turn to you and to God and find renewed strength. You encourage me, you help me grow, and you inspire me to think harder and dream bigger each day. Thank you for taking this journey with me.

To my high school counselor, Mr. Rodney Hoopai, without whom I would not be who or where I am today. You asked if I planned to go to college. My response was, "I guess...." Then you sat with me in your office and we filled out the application together.

Thank you.

Table of Contents

List of Figures

Chapter 1

Introduction

The topic of Boolean algebra is a branch of algebra first introduced by George Boole that involves mathematical logic. Computations with Boolean algebras involve the operations of greatest lower bound, least upper bound, and complementation. The structure of a Boolean algebra develops from a partially ordered set and, subsequently, from a lattice.

The literature on this subject uses two different types of notation. Because of this fact, this thesis contains multiple notations to denote a single concept. For example, $\wedge$ and $\cdot$ both denote *least upper bound*. The varied notation will allow us to understand all of the necessary definitions and it will also allow the reader to be familiar with the different notation when reading various articles on the subject.

The motivation to study Boolean algebras comes from an interest in set theory and mathematical logic, as well as a desire understand some of the mathematics that apply to the computer design process.

1.1 Notation

$\mathbb{N}$	$\{0, 1, 2, 3, \dots\}$ — The set of natural numbers
$\mathbb{Z}$	$\{0 \pm 1, \pm 2, \pm 3, \dots\}$ — The set of integers
$\mathbb{Z}^*$	$\mathbb{Z} \setminus \{0\}$
$\mathbb{Q}$	$\left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}^*\right\}$ — The set of rational numbers
$\mathbb{Q}^*$	$\mathbb{Q} \setminus \{0\}$
$\mathbb{R}$	The set of real numbers
$\mathbb{R}^*$	$\mathbb{R} \setminus \{0\}$
$\mathbb{C}$	$\left\{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\right\}$ —The set of complex numbers
$\mathbb{C}^*$	$\mathbb{C} \setminus \{0\}$
$\in$	"is an element of"
$\cup$	The union of sets — $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
$\cap$	The intersection of sets — $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
$\varnothing$ or $\{\ \}$	The empty set
$\subseteq$	Subset
$\subset$	Proper subset
$gcd(a, d)$	The greatest common divisor of a and b $(a, b \in \mathbb{Z})$
$lcm(a, b)$	The least common multiple of a and b $(a, b \in \mathbb{Z})$
$min(a, b)$	The minimum or least value of a and b
$max(a, b)$	The maximum or greatest value a and b
$a < b$	$a \leq b$ and $a \neq b$
ω	The set of all finite ordinals

1.2 Preliminaries

The following will help provide the necessary background for the content discussed in this thesis.

Definition 1.1. A *set* S is a collection of elements. A *subset* A of a set S is a set in which all of the elements of A are elements of S. For $s \in S$, the *complement of* s is all of S except s, denoted $S \setminus s$. A set is considered to be *open* if its complement is closed and *closed* if its complement is open.

Definition 1.2. A number a is *congruent modulo* n, or mod n, to b if and only if n divides $(b - a)$. We write $a \equiv b \pmod{n}$.

Definition 1.3. For a set S, a *partition* is a collection of nonempty disjoint subsets of S whose union is the set S.

Definition 1.4. A *binary operation* on a set G is a function that, for each pair of elements in G, assigns a single element in G.

Definition 1.5. When a binary operation, denoted $*$ is applied to a nonempty set G, then G is a *group* under $*$ if the following properties are true:

(i) For any three elements $a, b, c \in G$, then $(a * b) * c = a * (b * c)$. This is called the *associative property.*

(ii) There exists an element $e \in G$ such that, for all $a \in G$, $a*e = a$ and $e*a = a$. The element e is called the *identity.*

(iii) For each $a \in G$, there exists an *inverse* of a, denoted a^{-1}, in G such that $a * a^{-1} = e$ and $a^{-1} * a = e$.

Definition 1.6. The number of elements of a group G is called the *order* of G and is denoted $\mid G \mid$.

Definition 1.7. An *ordinal number*, or *ordinal*, is the ordering type of a well ordered set. The *cardinal number*, or *cardinality* of a set X, is the least ordinal with which X has a one-to-one correspondence. The cardinality of X is denoted $\mid X \mid$.

Definition 1.8. A set X is *finite* if it contains a finite number of elements. A subset A of X is *cofinite in* X if $X \setminus A$ is finite. A group G is *finite* if the order of G, $\mid G \mid$, is finite.

Definition 1.9. If G is a group and $a \in G$, then the *order of* a, denoted $\mid a \mid$, is the smallest number n (where $n \in \mathbb{Z}^*$), such that $a^n = e$ (where e is the identity element of G). Note: if the operation on G is addition, then $\mid a \mid = n$ such that $na = e = 0$.

Definition 1.10. If A and B are sets, then a *map* (or function) ϕ from A to B, denoted $\phi : A \longrightarrow B$, assigns to each element of A exactly one element from B. We use the notation $\phi : a \mapsto b$ for $a \in A, b \in B$ such that $\phi(a) = b$. If $\phi : A \longrightarrow B$, then the *image* of an element $a \in A$ is $\phi(a) \in B$, where $\phi : a \mapsto \phi(a)$. Then we call a the *preimage* of $\phi(a)$.

Definition 1.11. A map $\phi : A \longrightarrow B$ is *well defined* if it unambiguously assigns one and only one element of B to each element of A; that is, if $x = y$, for $x, y \in A$, then $\phi(x) = \phi(y)$.

Definition 1.12. A map $\phi : A \longrightarrow B$ is *one to one* (or an injection) if whenever $a_1 \neq a_2$, then $\phi(a_1) \neq \phi(a_2)$. Also, $\phi : A \longrightarrow B$ is *onto* (or a surjection) if for every $b \in B$, there is an element $a \in A$ such that $\phi(a) = b$. If $\phi : A \longrightarrow B$ is one to one and onto, then we say it is a *bijection*.

Definition 1.13. If G is a group with operation $*$ and H is a group with operation $\dagger$, then the map $\phi : G \longrightarrow H$ is a *group homomorphism* if $\phi(a * b) = \phi(a) \dagger \phi(b)$ for all $a, b \in G$.

Definition 1.14. If $\phi : G \longrightarrow H$ is a homomorphism and e is the identity element in H, then the *kernel* of ϕ, denoted $Ker\phi$ is the set $\{g \in G \mid \phi(g) = e\}$.

Definition 1.15. A homomorphism $\phi : G \longrightarrow H$ is an *group isomorphism* if ϕ is a bijection and we say that G and H are *isomorphic*, denoted $G \cong H$.

Definition 1.16. If $\phi : A \longrightarrow B$ and there exists a map $\phi^{-1} : B \longrightarrow A$ such that $\phi^{-1} \circ \phi$ is the *identity map* on A (that is, $\phi^{-1} \circ \phi : A \longrightarrow A$ maps a to $\phi^{-1} \circ \phi(a)$ for all $a \in A$), and $\phi \circ \phi^{-1}$ is the identity map on B, then $\phi : A \longrightarrow B$ is said to be *invertible*. In this case, ϕ^{-1} is the *inverse* of ϕ.

Definition 1.17. A *topological space* is a nonempty set X with a family of subsets, that are all open sets, such that $\emptyset$ and X are open sets, the union of an any number of open sets is open, and the intersection of a finite amount of open sets is open.

Definition 1.18. For a topological space X, a *cover* C of X is a collection of sets M_i, where $i \in I$, such that $X = \bigcup_{i \in I} M_i$. If M_i are open sets, then C is an *open cover*. A *subcover* of C is a subset of C that is also a cover of X.

Definition 1.19. A topological space X is *compact* if every open cover of X has a finite subcover.

Definition 1.20. A topological space X is a *Hausdorff space* if, for any $x, y \in X$ with $x \neq y$, there exist open sets M and N, with $x \in M$ and $y \in N$, such that $M \cap N = \{\ \}$.

Axiom 1.1. Every nonempty set can be well ordered.

Chapter 2

Partially Ordered Sets and Lattices

In order to study Boolean algebras, we begin by developing an understanding of partially ordered sets, followed by lattices. A lattice, equipped with additional characteristics, is the underlying structure of a Boolean algebra.

Definition 2.1. If S is a set and $\leq$ is a relation on S, then S is a *partially ordered set*, denoted $\langle S, \leq \rangle$, if the following axioms are true for any $a, b, c \in S$:

(i) $a \leq a$ (reflexivity).

(ii) If $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry).

(iii) If $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

Definition 2.2. An element $b \in \langle S, \leq \rangle$ is said to *cover* an element $a \in S$ if $a < b$ and there is no $c \in S$ such that $a < c < b$.

Definition 2.3. A partially ordered set $\langle S, \leq \rangle$ that also satisfies $a \leq b$ or $b \leq a$ for any $a, b \in S$ (comparability) is called a *linearly ordered set* or a *total order set*.

A totally ordered set is *well ordred* if and only if all of its nonempty subsets contain a least element.

Example 2.1. The set of integers, $\mathbb{Z}$, is a partially ordered set, where $a \leq b$ is defined as a less than or equal to b.

Exercise 2.1. Determine whether the indicated set or relation is an example of a partially ordered set: the set of integers $\mathbb{Z}$ with $a \leq b$ to mean $a \mid b$ (a divides b).

Solution. $a \mid b \implies a * m = b$ for $m \in \mathbb{Z}$. Then $a \leq a$ (reflexivity) since $a * m = a$, where $m = 1 \in \mathbb{Z}$. Let $a \leq b$ and $b \leq a$ for $a, b \in \mathbb{Z}$. Then $a * m = b$ and $b * n = a$ for $m, n \in \mathbb{Z}$. So $a * m = b \implies b * n * m = b$ (since $a = b * n$) $\implies b * (n * m) = b$. Similarly, $b * n = a \implies a * m * n = a$ (since $b = a * m$) $\implies a * (m * n) = a$. So $b * (m * n) = b \implies m * n = \frac{b}{b} = 1$ and $a * (m * n) = a \implies m * n = \frac{a}{a} = 1$. But $m, n \in \mathbb{Z}$, so $m = \pm 1$ and $n = \pm 1$ since $m * n = 1$. Then $a * m = b \implies a * (\pm 1) = b \implies a = \pm b$. Then $a \neq b$ (when $a = -b$) and antisymmetry does not hold. Therefore, this is not an example of a partially ordered set.

Exercise 2.2. Determine whether the indicated set or relation is an example of a partially ordered set: the set of natural numbers $\mathbb{N}$ with $a \leq b$ to mean $a \mid b$ (a divides b).

Solution. $a \mid b \implies a * m = b$ for $m \in \mathbb{N}$. Then $a \leq a$ (reflexivity) since $a * m = a$, where $m = 1 \in \mathbb{N}$. Let $a \leq b$ and $b \leq a$ for $a, b \in \mathbb{N}$. Then $a * m = b$ and $b * n = a$ for $m, n \in \mathbb{N}$. So $a * m * n = a$ since $b = a * m$ and $b * n * m = b$ since $a = b * n$. Then $a * (m * n) = a \implies (m * n) = 1$ and $b * (n * m) = b \implies n * m = 1$. Then $m = 1$ and $n = 1$ since $m * n = 1$ for $m, n \in \mathbb{N}$. So $a * m = b * n$ (since $a * m = b$ and $b * n = a$) and $a * 1 = b * 1$. Then $a = b$ (antisymmetry).

Now, let $c \in \mathbb{N}$ and $a \leq b$ and $b \leq c$. Then $a * m = b$ and $b * n = c$. So $a * m * n = c$, but $(m * n) \in \mathbb{N}$ since the set of natural numbers is closed under multiplication. Then $a * (m * n) = c \implies a \leq c$ (transitivity). Therefore, the set of natural numbers $\mathbb{N}$ with $a \leq b$ to mean a divides b is an example of a partially ordered set.

Definition 2.4. For a set A, a subset B of A is *cofinal* if for every $a \in A$ there exists $b \in B$ such that $a \leq b$. If A is a partially ordered set, then the smallest of the cardinalities of the cofinal subsets of A is called the *cofinality of* A, denoted $cf(A)$.

Definition 2.5. A cardinal number k is *regular* if and only if k is infinite and the cofinality of k is k. If k is an infinite cardinal that is not regular, then k is *singular*.

Definition 2.6. A nonempty set H of a group G is a *subgroup* of G if H is a subset of G and it is a group under the same operation as G. It is denoted by $H \leq G$.

Definition 2.7. A subgroup H of a group G is *maximal* if there does not exist a subgroup J of G such that $H < J < G$.

Definition 2.8. If G is a group and $a \in G$, then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is the *cyclic subgroup generated by a*. Note: if the operation on G is addition, then $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$.

Definition 2.9. If H is a subgroup of G and $a \in G$, then the set $aH = \{ah \mid h \in H\}$ is a *left coset* of H in G and the set $Ha = \{ha \mid h \in H\}$ is a *right coset* of H in G.

Definition 2.10. A subgroup H of G is a *normal subgroup* of G if for all $a \in G$, then $aH = Ha$; or equivalently, if for all $a \in G$, then $aHa^{-1} = H$. We denote H as a normal subgroup of G by $H \trianglelefteq G$.

Definition 2.11. If H is a normal subgroup of G, then the set of cosets of H in G, denoted $G/H = \{aH \mid a \in G\}$ and read "G modulo H", is a group under the operation $(aH)(bH) = (ab)H$ and is called the *quotient group* (or factor group) of G by H.

Exercise 2.3. Determine whether the indicated set or relation is an example of a partially ordered set: the set of all subgroups of a group G with $H \leq K$ to mean that H is a normal subgroup of K, denoted $H \trianglelefteq K$.

Solution. $H \leq H$ (reflexivity) since for all $h \in H$, then $hH = Hh$. That is, $\{hh \mid h \in H\} = \{hh \mid h \in H\}$.

Now consider $H \leq K$ and $K \leq H$. If $H \leq K$, then $H \subseteq K$. Similarly, if $K \leq H$, then $K \subseteq H$. Thererfore $H = K$ (antisymmetry).

For transitivity, we would show that for $H \leq K$ and $K \leq L$, then $H \leq L$. Consider the following sets: $L = A_4$, $K = \{e, (12)(34), (13)(24), (14)(23)\}$, and $H = \{e, (12)(34)\}$. Then $H \leq K$ and $K \leq L$. But for $h = (12)(34)$ and $l = (123)$, then $H \not\leq L$ since $(14)(23) \notin H$.

Therefore, the set of all subgroups of a group G with $H \leq K$ to mean that H is a normal subgroup of K is not an example of a partially ordered set.

Definition 2.12. A group G with operation $*$ is *Abelian* if, for all $a, b \in G$, $a * b = b * a$. This property is called *commutativity*.

Definition 2.13. A *ring* is a set R equipped with two operations $(*, +)$ such that, for all $a, b, c \in R$, then:

(i) R is an Abelian group under $+$

(ii) $a * b \in R$ (closure)

(iii) $a * (b * c) = (a * b) * c$ (associativity)

(iv) $a * (b + c) = a * b + a * c$ and $(b + c) * a = b * a + c * a$ (distributivity)

Definition 2.14. A ring R is a *commutative ring* if, for all $a, b \in R$, then $a * b = b * a$. It is a *commutative ring with unity* if there exits $1 \in R$ such that $a * 1 = a = 1 * a$ for all $a \in R$.

Definition 2.15. A *subring* S of a ring R is a subset S of R such that S is a ring under the operations of R.

Definition 2.16. An *ideal* of a ring R is a subring S such that for every $r \in R$ and every $s \in S$, then $rs \in S$ and $sr \in S$.

Exercise 2.4. Determine whether the indicated set or relation is an example of a partially ordered set: the set of all ideals in a ring R with $I \leq J$ to mean that I is an ideal in J.

Solution. Since I is an ideal in J, then for all $b \in J$ and for all $a \in I$, $ba \in I$ and $ab \in I$. Also, I is a subring. J is an ideal in R, which implies that for all $r \in R$ and for all $b \in J$, then $rb \in J$ and $br \in J$. Also, J is a subring.

Now $I \leq I$ (reflexivity) since for all $a \in I$, then $aa \in I$ (since I is a subring). Let $I \leq J$ and $J \leq I$. Then I is a subring of J and J is a subring of I. Therefore $I = J$ (antisymmetry).

Consider $I \leq J$ and $J \leq K$. We want to show that $I \leq K$. Consider the following: let R be the ring of polynomials of x over $\mathbb{Q}$. Then $K = a_n x^n + \ldots + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x$, $J = a_n x^n + \ldots + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2$, and $I = a_n x^n + \ldots + a_5 x^5 + a_4 x^4 + a_2 x^2$ are ideals in R such that $I \leq J$ and $J \leq K$. But I is not an ideal in K since $x^2 \in I$ and $x \in K$ but $x \cdot x^2 = x^3 \notin I$. Therefore transitivity fails.

So the set of all ideals in a ring R with $I \leq J$ to mean that I is an ideal in J is not an example of a partially ordered set.

Definition 2.17. A nonzero element a in a commutative ring R is a *zero-divisor* if there is a nonzero element $b \in R$ such that $a * b = 0$.

Definition 2.18. A commutative ring with unity and no zero-divisors is an *integral domain.*

Definition 2.19. In a commutative ring with unity R, an element a in R is a *unit* if there exists an inverse element of a in R, denoted a^{-1}, such that $a * a^{-1} = 1 = a^{-1} * a$.

Definition 2.20. A *field* F is a commutative ring with unity such that every nonzero element in F is a unit.

Definition 2.21. For a commutative ring R with identity I_R, a ring A with identity I_A, and a ring homomorphism $f : R \longrightarrow A$ such that $f(I_R) = I_A$, an *R-algebra* is the ring A together with f such that $f(R)$, is contained in the center of A (where the center of A is the set of all elements $a \in A$ such that a commutes with every element in A).

Definition 2.22. If S is a set, then the *power set* of S, denoted $P(S)$, is the set of all subsets of S, where addition and multiplication on $P(S)$ are defined as $A + B = \{c \mid c \in A \cup B, c \notin A \cap B\}$ and $A \times B = \{c \mid c \in A \cap B\}$.

Definition 2.23. A *Hasse diagram* displays the elements of a partially ordered set $\langle S, \leq \rangle$ such that a line is drawn upward from an element a to another element b if b covers a.

Definition 2.24. If A is a subset of S, where $\langle S, \leq \rangle$ is a partially ordered set, then $u \in S$ is an *upper bound* for A if for all $a \in A$, then $a \leq u$. If $v \in S$ and $v \leq a$ for all $a \in A$, then v is a *lower bound* for A. The element $w \in S$ is a *least upper bound (lub)* of A if it is an upper bound of A and $w \leq u$ for each upper bound u of A. The element $w \in S$ is a *greatest lower bound (glb)* of A if it is a lower bound of A and $v \leq w$ for each lower bound v of A.

The *lub* of a set is also called the *supremum*, denoted *sup*, and the *glb* is also called the *infimum*, denoted inf.

Proposition 2.1. *If $\langle S, \leq \rangle$ is a partially ordered set and A is a subset of S, then*

(i) the lub of A is unique, if it exists, and

(ii) the glb of A is unique, if it exists.

Proof. (i) Suppose w_1 and w_2 are each a *lub* of A. Then w_1 and w_2 are each an upper bound of A. Now, since w_1 is a least upper bound of A, then $w_1 \leq u$, for all upper bounds u of A. So $w_1 \leq w_2$. Similarly, since w_2 is a least upper bound of A, then $w_2 \leq u$, and so, $w_2 \leq w_1$. Then, by antisymmetry of partially ordered sets, $w_1 = w_2$ and therefore, any *lub* of A is unique.

(ii) Suppose w_1 and w_2 are each a *glb* of A. Then w_1 and w_2 are each a lower bound of A. Since w_1 is a greatest lower bound of A, then $w_2 \leq w_1$. Similarly, since w_2 is a greatest lower bound of A, then $w_1 \leq w_2$. Then, by antisymmetry, $w_1 = w_2$, and therefore any *glb* of A is unique. □

Example 2.2. Let $S = \{a, b, c\}$.

Then the power set of S is $P(S) = \{\{\ \}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. The Hasse diagram of S is

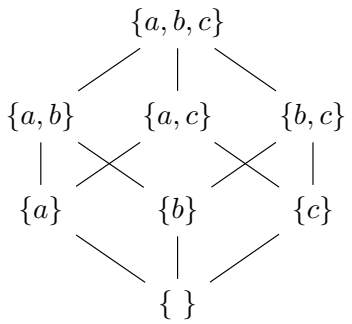

Figure 2.1: Hasse Diagram of S

Let $X \subseteq S$ such that $X = \{\{a\}, \{a, b\}\}$. Then $\underline{lub}\{X\} = \{a, b\}$ and $\underline{glb}\{X\} = \{a\}$.

Definition 2.25. A *lattice* is a partially ordered set $\langle L, \leq \rangle$ such that for any pair of elements $a, b \in L$:

(i) The lub of $\{a, b\}$, denoted $a \vee b$, exists. $a \vee b$ is read as "a join b" or "a or b".

(ii) The glb of $\{a, b\}$, denoted $a \wedge b$, exists. $a \wedge b$ is read as "a meet b" or "a and b".

Alternatively, $lub\{x, y\} = x + y$ and $glb\{x, y\} = x \cdot y$.

A lattice is *complete* if each subset of $\langle L, \leq \rangle$ has a lub and a glb.

Definition 2.26. A *subgroup lattice* is a lattice whose elements are the subgroups of a group and whose relation is set inclusion.

Definition 2.27. If $\langle L, \leq \rangle$ is a lattice, then

(i) An element $0 \in L$ is called a *zero* if $0 \leq a$ for all $a \in L$.

(ii) An element $1 \in L$ is called a *unity* if $a \leq 1$ for all $a \in L$.

(iii) An element $a' \in L$ is called the *complement* of a if for any $a \in L$, then $a \vee a' = 1$ and $a \wedge a' = 0$. Alternatively, if $-x$ is the *complement* of x, then $x + (-x) = 1$ and $x \cdot (-x) = 0$.

Example 2.3. Let $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$ be the set of positive divisors of 30. Then S is a lattice with unity = 30 and zero = 1.

Exercise 2.5. Determine whether the indicated set or relation is an example of a lattice: the set of all positive divisors of 70 with $a \leq b$ to mean a divides b.

Solution. Let $S = \{1, 2, 5, 7, 10, 14, 35, 70\}$. If $a \leq b$, then $b = a * n$ for $n \in \mathbb{Z}$. First, $a \leq a$ since $a = a * 1$ (reflexivity). Now suppose $a \leq b$ and $b \leq a$. Then $b = a * n$ and $a = b * m$ for $m, n \in \mathbb{Z}$. So $b = a * n = (b * m) * n = b * (m * n) \implies m * n = 1 \implies m = 1, n = 1$ (since $a > 0, b > 0$). Then $a = b$ (antisymmetry).

Suppose $a \leq b$ and $b \leq c$. Then $b = a * n$ and $c = b * m$ for $m, n \in \mathbb{Z}$. So $c = b * m = (a * n) * m = a * (n * m)$ (since $\mathbb{Z}$ is closed under multiplication). Therefore $c = a * k$ for some $k = n * m \in \mathbb{Z}$ and so $a \leq c$ (transitivity).

For any $a, b \in S$, $lcm(a, b) \in S$ and $gcd(a, b) \in S$. So $a \vee b = lcm(a, b)$ (lub exists) and $a \wedge b = gcd(a, b)$ (glb exists). Therefore S is an example of a lattice.

Exercise 2.6. Determine whether the indicated set or relation is an example of a lattice: the set of all positive divisors of 60 with $a \leq b$ to mean a divides b.

Solution. Let $S = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Then $a \leq a$ since $a = a * 1$ (reflexivity). From Exercise 1.5, we can see that for $a \leq b$ and $b \leq a$, then $a = b$ and for $a \leq b$ and $b \leq c$, then $a \leq c$ (antisymmetry and transitivity). For any $a, b \in S$, then $lcm(a, b) \in S$ and $gcd(a, b) \in S$. So $a \vee b = lcm(a, b)$ and $a \wedge b = gcd(a, b)$ (lub and glb exist). Therefore S is an example of a lattice.

Definition 2.28. If A and B are sets, then the *Cartesian product* of A and B is the collection of ordered pairs of elements of A and B and is denoted $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Definition 2.29. If S is a set and R is a subset of $S \times S$, then R is a *relation* on S. For $a, b \in S$, then $(a, b) \in R$, or equivalently aRb.

Exercise 2.7. Determine whether the indicated set or relation is an example of a lattice: the set $L \times M = \{(a, b) \mid a \in L, b \in M\}$ where L and M are lattices, with $(a, b) \leq (c, d)$ to mean that $a \leq c \in L$ and $b \leq d \in M$.

Solution. Since L and M are lattices, then $a \leq a \in L$ and $b \leq b \in M$. So $(a, b) \leq (a, b)$ (reflexivity). Suppose $(a, b) \leq (c, d)$ and $(c, d) \leq (a, b)$. Then $a \leq c \in L$, $b \leq d \in M$ and $c \leq a \in L$, $d \leq b \in M$. Since L and M are lattices, $a \leq c \in L$ and $c \leq a \in L \implies a = c$. Also, $b \leq d \in M$ and $d \leq b \in M \implies b = d$. Therefore $(a, b) = (c, d)$ (antisymmetry).

Now consider $(a, b) \leq (c, d)$ and $(c, d) \leq (e, f)$. Then $a \leq c$ and $c \leq e \in L$. Also, $b \leq d$ and $d \leq f \in M$. Since L and M are lattices, $a \leq c, c \leq e \in L \implies a \leq e$ and $b \leq d, d \leq f \in M \implies b \leq f$. Therefore $(a, b) \leq (e, f)$ (transitivity).

For any $a, c \in L$, $a \vee c \in L$ and $a \wedge c \in L$ since L is a lattice. Similarly, for any $b, d \in M$, $b \vee d \in M$ and $b \wedge d \in M$ since M is a lattice. Then $(a, b) \vee (c, d) = (a \vee c, b \vee d) \in L \times M$ and $(a, b) \wedge (c, d) = (a \wedge c, b \wedge d) \in L \times M$ (lub and glb exist). Therefore, $L \times M$ is an example of a lattice.

Definition 2.30. If R is a relation on a set S and $a, b, c \in S$ then R is an *equivalence relation* on S if the following properties are true:

(i) For all $a \in S$, $(a, a) \in R$. This is called *reflexivity.*

(ii) If $(a, b) \in R$, then $(b, a) \in R$. This is called *symmetry.*

(iii) If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. This is called *transitivity.*

Definition 2.31. If R is an equivalence relation on a set S and $a \in S$, then the set $[a] = \{b \in S \mid (a, b) \in R\}$ is the *equivalence class* of S containing a.

Theorem 2.1. *If $\langle L, \leq \rangle$ is a lattice and $a, b, c \in \langle L, \leq \rangle$, then*

(i) $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$ (Commutativity)

(ii) $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (Associativity)

(iii) $a \vee a = a$ and $a \wedge a = a$ (Idempotence)

(iv) $(a \vee b) \wedge a = a$ and $(a \wedge b) \vee a = a$ (Absorption)

Proof. (i) $a \vee b = lub\{a, b\}$ and $b \vee a = lub\{b, a\}$. Since $\{a, b\} = \{b, a\}$ as sets, then $a \vee b = b \vee a$. Similarly, $a \wedge b = glb\{a, b\}$ and $b \wedge a = glb\{b, a\}$. Since $\{a, b\} = \{b, a\}$ as sets, then $a \wedge b = b \wedge a$.

(ii) $a \vee (b \vee c) = lub\{a, lub\{b, c\}\}$ and $(a \vee b) \vee c = lub\{lub\{a, b\}, c\}$. Suppose $lub\{a, b, c\} = d$. Then $a \vee (b \vee c) = lub\{a, lub\{b, c\}\} = lub\{a, d\} = d = lub\{d, c\} = lub\{lub\{a, b\}, c\} = (a \vee b) \vee c$. Therefore, $a \vee (b \vee c) = (a \vee b) \vee c$). Similarly, $a \wedge (b \wedge c) = glb\{a, glb\{b, c\}\}$ and $(a \wedge b) \wedge c = glb\{glb\{a, b\}, c\}$ and therefore, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

(iii) $a \vee a = lub\{a, a\} = a$, and therefore $a \vee a = a$. Also, $a \wedge a = glb\{a, a\} = a$, and therefore $a \wedge a = a$.

(iv) We know that $a \leq a \vee b$ and $a \leq a$ by definition of *lub* and by reflexivity. Then $a \wedge a \leq (a \vee b) \wedge a$. Then since $a \wedge a = a$ (idempotence), we have $a \leq (a \vee b) \wedge a$. But $(a \vee b) \wedge a \leq a$ by definition of *glb*. Therefore, by antisymmetry, $(a \vee b) \wedge a = a$.

Similarly, we know that $a \wedge b \leq a$ and $a \leq a$ (*glb* and reflexivity). So $(a \wedge b) \vee a \leq a \vee a = a$ (idempotence). But $a \leq (a \wedge b) \vee a$ (*lub*). Therefore, $(a \wedge b) \vee a = a$ by antisymmetry. □

Proposition 2.2. *Any statement that is true for every lattice continues to be true if*

(i) $\leq$ *and* $\geq$ *are interchanged throughout the statement and*

(ii) $\vee$ *and* $\wedge$ *are interchanged throughout the statement.*

The new statement that is obtained from interchanging $\leq$ *and* $\geq$ *and also* $\vee$ *and* $\wedge$ *is called the* ***dual*** *of the original statement.*

A dual statement for a Boolean Algebra is obtained by interchanging $+$ *and* $\cdot$ *and interchanging* 0 *and* 1. *If a statement is true for every Boolean algebra, then so is its dual statement.*

Proof. Let ϕ represent a statement that holds in every Boolean algebra. Consider a Boolean algebra B and let B' be the dual algebra of B, that is, the Boolean algebra resulting from interchanging $+$, $\cdot$, 0, and 1 in B for $\cdot$, $+$, 1, and 0, respectively, in B'. Let ϕ' be the dual of ϕ. If ϕ holds in any Boolean algebra, say B', then by interchanging $+$ and $\cdot$, also 0 and 1, we have that ϕ' holds in B. □

Theorem 2.2. *If* L *is a set with operations* $\vee$ *and* $\wedge$ *such that the axioms of commutativity, associativity, idempotence, and absorption are satisfied, and* $\leq$ *on* L *is defined by* $a \leq b$ *if and only if* $a \vee b = b$ *or* $a \wedge b = a$ *(for* $a, b \in L$*), then* $\langle L, \leq \rangle$ *is a lattice.*

Proof. We begin by showing that $a \vee b = b$ and $a \wedge b = a$ are equivalent. Consider $a \vee b = b$. Then $a \wedge b = a \wedge (a \vee b) = (a \vee b) \wedge a = a$ (by commutativity and absorption). So $a \vee b = b$ implies $a \wedge b = a$. Conversely, if $a \wedge b = a$, then $a \vee b = (a \wedge b) \vee b = (b \wedge a) \vee b = b$. And

so $a \wedge b = a$ implies $a \vee b = b$. Now we want to show that L is a partially ordered set under $\leq$.

(i) (Reflexivity) If $a \in L$, then $a \wedge a = a$ (idempotence). Then $a \leq a$ (since $a \leq b$ if and only if $a \wedge b = a$).

(ii) (Antisymmetry) If $a \leq b$ then $a \wedge b = a$. If $b \leq a$, then $b \wedge a = b$. Since commutativity is satisfied under $\wedge$, then $a \wedge b = b \wedge a$ and therefore $a = b$.

(iii) (Transitivity) If $a \leq b$, then $a \wedge b = a$. If $b \leq c$, then $b \wedge c = b$. Since associativity is satisfied under $\wedge$, $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a$. Therefore $a \wedge c = a$, and so $a \leq c$.

Lastly, we want to show that $a \vee b$ is the $lub\{a, b\}$ and $a \wedge b$ is the $glb\{a, b\}$. Let us evaluate $a \vee b$. Consider $a \wedge (a \vee b) = (a \vee b) \wedge a = a$. Then $a \leq a \vee b$. Also, $b \wedge (a \vee b) = (a \vee b) \wedge b = (b \vee a) \wedge b = b$. Then $b \leq a \vee b$. Therefore, $a \vee b$ is an upper bound for a and b. Now, let $c \in L$ such that $a \leq c$ and $b \leq c$. Then $a \vee c = c$ and $b \vee c = c$.

So $(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$. Therefore $a \vee b \leq c$, so $a \vee b$ is the $lub\{a, b\}$. By duality (interchanging $\leq$ and $\geq$ and also $\vee$ and $\wedge$), then $glb\{a, b\} = a \wedge b$. □

Exercise 2.8. Show that the lattice L is distributive if and only if for all $a, b, c \in L$, then $a \wedge b = a \wedge c$ and $a \vee b = a \vee c \implies b = c$.

Solution.
($\implies$) Let L be a distributive lattice. We want to show that for all $a, b, c \in L$, if $a \wedge b = a \wedge c$ and $a \vee b = a \vee c$, then $b = c$.

Since L is distributive, then we have the following:

$$
\begin{aligned}
b &= (a \vee b) \wedge b && \text{(absorption)} \\
&= (a \vee c) \wedge b && \text{(since } a \vee b = a \vee c\text{)} \\
&= b \wedge (a \vee c) && \text{(commutativity)} \\
&= (b \wedge a) \vee (b \wedge c) && \text{(distribution)} \\
&= (a \wedge b) \vee (c \wedge b) && \text{(commutativity)} \\
&= (a \wedge c) \vee (c \wedge b) && \text{(since } a \wedge b = a \wedge c\text{)} \\
&= (c \wedge a) \vee (c \wedge b) && \text{(commutativity)} \\
&= c \wedge (a \vee b) && \text{(distribution)} \\
&= c \wedge (a \vee c) && \text{(since } a \vee b = a \vee c\text{)} \\
&= c.
\end{aligned}
$$

Therefore, $b = c$.

($\Longleftarrow$) Now assume that for a, b, c in a lattice L, if $a \wedge b = a \wedge c$ and $a \vee b = a \vee c \implies b = c$. We want to show that L is distributive.

Consider $(a \vee b) \wedge (a \vee c)$.

$$\begin{aligned}(a \vee b) \wedge (a \vee c) &= (a \vee c) \wedge (a \vee c) && \text{(since } a \vee b = a \vee c\text{)} \\ &= a \vee c && \text{(idempotence)} \\ &= a \vee (c \wedge c) && \text{(idempotence)} \\ &= a \vee (b \wedge b) && \text{(since } b = c\text{).}\end{aligned}$$

Similarly, $(a \wedge b) \vee (a \wedge c) = (a \wedge c) \vee (a \wedge c) = a \wedge c = a \wedge (c \vee c) = a \wedge (b \vee c)$.

Therefore, L is distributive.

Exercise 2.9. Construct the Hasse diagram for the lattice of subgroups of S_3.

Solution.

The elements of S_3 are $e, (12), (13), (23), (123)$, and (132).

The subgroups of S_3 are $\{\ e, (12)\}, \{e, (13)\}, \{e, (23)\}, \{e, (123), (132)\}$.

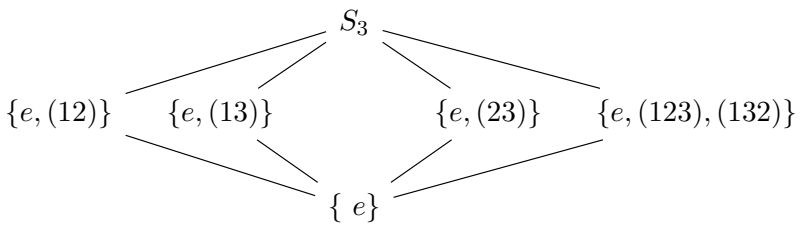

Figure 2.2: Hasse Diagram of the Lattice of Subgroups of S_3

Exercise 2.10. Construct the Hasse diagram for the lattice of subgroups of D_4.

Solution. $D_4 = \{\rho_0, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$. The subgroups of D_4 are generated by the elements in the Hasse diagram:

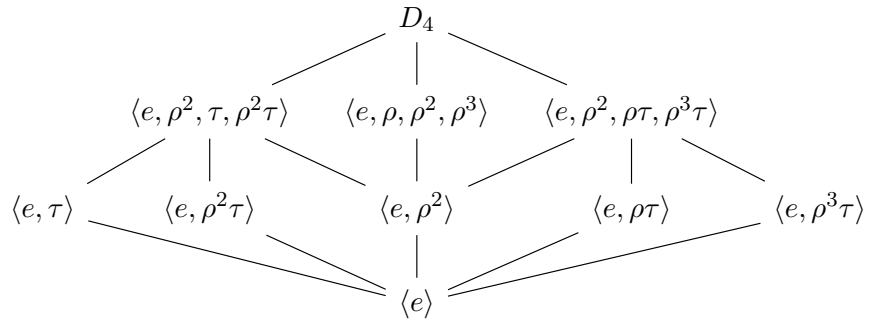

Figure 2.3: Hasse Diagram of the Lattice of Subgroups of D_4

Chapter 3

Introduction to Boolean Algebras

Now that we've established the notion of lattices, we can begin exploring Boolean algebras and some of their characteristics.

Definition 3.1. If B is a lattice with zero and unity, then B is a *Boolean algebra* if

(i) For all $a, b, c \in B$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ (Distributivity)

(ii) For each $a \in B$, there exists an $a' \in B$ such that $a \vee a' = 1$ and $a \wedge a' = 0$ (Complements).

Alternatively, a *Boolean Algebra* is a structure $(A, +, \cdot, -, 0, 1)$ with binary operations $+$ and $\cdot$, unary operation $-$, zero element 0, and unity element 1, such that for all $x, y, z \in A$

(i) $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativity)

(ii) $x + y = y + x$ and $x \cdot y = y \cdot x$ (commutativity)

(iii) $x + (x \cdot y) = x$ and $x \cdot (x + y) = x$ (absorption)

(iv) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $x + (y \cdot z) = (x + y) \cdot (x + z)$ (distributivity)

(v) $x + (-x) = 1$ and $x \cdot (-x) = 0$ (complementation).

Note: The following operations are equivalent: $\wedge$ and $\cdot$, $\vee$ and $+$, $'$ and $-$.

Example 3.1. $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$ is a Boolean algebra such that, for $a, b \in S$, then $a \leq b$ means a divides b. Then $a \vee b = lcm\{a, b\}$ and $a \wedge b = gcf\{a, b\}$.

Definition 3.2. If B is a Boolean algebra with operations $+_B, \cdot_B, -_B$ and zero and unity,

0_B and 1_B, then A is a *subalgebra* of B if $A \subseteq B$ and $0_A = 0_B$, $1_A = 1_B$, and $+_A, \cdot_A, -_A$ are equivalent to the restrictions of $+_B, \cdot_B, -_B$ to A.

Definition 3.3. If A is a set and $P(A)$ is its power set, then $P(A)$ is the *power set algebra* of A equipped with zero, unity A, and the operations $\cup$, $\cap$, and $-$, where $-a = A \setminus a$ (the complement of a).

Definition 3.4. For a set $X = \{x\}$, the power set algebra $P(X)$ is $\{0, 1\}$, where $0 = \{\ \}$ and $1 = X$, is called the *two-element algebra* and is denoted 2.

Definition 3.5. For a set A, a collection of subsets M of A is an *algebra of sets* if $\emptyset \in M$, for $M_1, M_2 \in M$ then $M_1 \cup M_2 \in M$ and $M_1 \cap M_2 \in M$, and $A \setminus M_1 \in M$ for $M_1 \in M$. Equivalently, if M is a subalgebra of the power set algebra $P(A)$, then M is an *algebra of sets over* A. If a Boolean algebra B is an algebra of sets over A, then B is an *algebra of sets*.

Definition 3.6. A *finite-cofinite algebra* A on X is the algebra of sets over X such that A is the set of all $a \subseteq X$, where a is either finite or cofinite.

Definition 3.7. For a subset X of a Boolean algebra B, the *subalgebra generated by* X in B is $\langle X \rangle = \bigcap\{A \subseteq B \mid X \subseteq A \text{ and } A \text{ is a subalgebra of } B\}$. If $X \subseteq B$ and $\langle X \rangle = B$, then X is a *set of generators* for a Boolean algebra B.

Exercise 3.1. Draw the Hasse diagrams of all nonisomorphic Boolean algebras of orders $| B | = 2, 4,$ or 8.

Solution.

$$| B | = 2 \implies B = \{0, 1\}$$

Figure 3.1: Hasse Diagram of the 2-element Boolean Algebra

$| B |= 4 \implies B = \{0, a, b, 1\}$

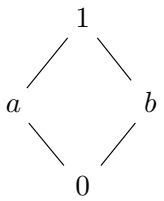

Figure 3.2: Hasse Diagram of a 4-element Boolean Algebra

$| B |= 8 \implies B = \{0, a, b, c, d, e, f, 1\} \cong P(S)$, where $S = \{x, y, z\}$

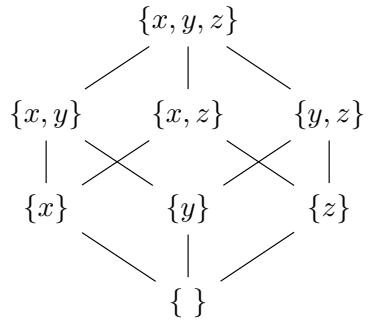

Figure 3.3: Hasse Diagram of an 8-element Boolean Algebra

Exercise 3.2. Let $n \in \mathbb{N}$ and let $B(n)$ be the set of all positive divisors of n. Show that $B(n)$ with $\wedge = gcd$ and $\vee = lcm$ is a Boolean algebra if and only if in the prime factorization of n no prime appears with an exponent ≥ 2.

Solution.

($\implies$) Assume $B(n)$ is a Boolean algebra. Suppose x and y are factors of n and $y = x'$. Then $x \wedge y = 1$ and $x \vee y = n$. But if n has repeated prime factors, then it could be that $x \vee y = x$. Therefore, in the prime factorization of n no prime appears with an exponent ≥ 2.

($\Longleftarrow$) Assume that in the prime factorization of n, no prime appears with an exponent ≥ 2. For $x, y \in B(n)$, $x \vee y = lcm(x, y)$ and $x \wedge y = gcd(x, y)$. We will show that $B(n)$ is a Boolean algebra.

Distribution: We know $x \wedge (y \vee z) = gcd(x, lcm(y, z))$. Consider the exponents on the prime factors of x, y, and z. Let x be the product of prime factors with exponents i, y with j, and z with k, where i, j, k can be 0 or 1. Then the exponent of a prime factor in $gcd(x, lcm(y, z))$ is $min(i, max(j, k))$, which equals $max(min, (i, j), min(i, k))$, the exponent of a prime factor in $lcm(gcd(x, y), gcd(x, z)) = (x \wedge y) \vee (x \wedge z)$. Similarly, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Complementation: $x \wedge x' = gcd(x, x') = gcd(x, \frac{n}{x}) = 1$ and $x \vee x' = lcm(x, x') = lcm(x, \frac{n}{x}) = n$.

Commutativity: $x \wedge y = gcd(x, y) = gcd(y, x) = y \wedge x$ and $x \vee y = lcm(x, y) = lcm(y, x) = y \vee x$.

Associativity: $x \vee (y \vee z) = lcm(x, lcm(y, z)) = lcm(lcm(x, y), z) = (x \vee y) \vee z$ and $x \wedge (y \wedge z) = gcd(x, gcd(y, z)) = gcd(gcd(x, y), z) = (x \wedge y) \wedge z$.

Absorption: $x \wedge (x \vee y) = gcd(x, lcm(x, y)) = x$ and $x \vee (x \wedge y) = lcm(x, gcd(x, y)) = x$.

Proposition 3.1. *If B is a Boolean algebra, then for any $a \in B$, $a \wedge 1 = a$ and $a \vee 0 = a$.*

Proof. By definition of unity in a lattice, $a \leq 1$ for all $a \in L$. Then $a \wedge 1 = a$. By definition of zero in a lattice, $0 \leq a$ for all $a \in L$. Then $a \vee 0 = a$. Therefore, 1 is an identity element under $\wedge$ and 0 is an identity element under $\vee$. □

Proposition 3.2. *If B is a Boolean algebra, then*

(i) the 1 and 0 elements in B are unique,

(ii) the complement, a', of a in B is unique.

Proof. (i) Let e_1 and e_2 be identity elements in B under $\wedge$ and $\vee$. Then $e_1 = e_1 \wedge e_2 = e_2 \wedge e_1 = e_2$. Similarly, $e_1 = e_1 \vee e_2 = e_2 \vee e_1 = e_2$. Then, by Proposition 3.1, the 1 and 0 elements in B are unique.

(ii) Let a in B have complements b and c in B . Then

$$\begin{aligned}
b &= b \vee 0 && \text{(identity)}\\
&= b \vee (a \wedge c) && \text{(definition of complement)}\\
&= (b \vee a) \wedge (b \vee c) && \text{(distribution)}\\
&= (a \vee b) \wedge (b \vee c) && \text{(commutativity)}\\
&= 1 \wedge (b \vee c) && \text{(definition of complement)}\\
&= b \vee c && \text{(identity)}
\end{aligned}$$

Therefore $b = b \vee c$ and similarly, $c = c \vee b$. Then $b = b \vee c = c \vee b = c$ by commutativity. And so, the complement of a is unique. □

Proposition 3.3. *If B is a Boolean algebra, then for any $a, b \in B$*

(i) $a \wedge 0 = 0$ *and* $a \vee 1 = 1$

(ii) $(a \wedge b)' = a' \vee b'$ *and* $(a \vee b)' = a' \wedge b'$ *(de Morgan's Law)*

(iii) $(a')' = a$ *(Involution)*

(iv) $0' = 1$ *and* $1' = 0$.

Proof. (i) $a \wedge 0 = a \wedge (a \wedge a') = (a \wedge a) \wedge a' = a \wedge a' = 0$ (by complement, associativity, and idempotence). By duality, $a \vee 1 = 1$.

(ii) We first show that $(a \wedge b) \wedge (a' \vee b') = 0$. From (i), we have

$$\begin{aligned}
&(a \wedge b) \wedge (a' \vee b')\\
&= [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b'] && \text{(distributivity)}\\
&= [(a \wedge a') \wedge b] \vee [a \wedge (b \wedge b')] && \text{(associativity and commutativity)}\\
&= (0 \wedge b) \vee (a \wedge 0) && \text{(complement)}\\
&= 0 \vee 0 = 0
\end{aligned}$$

Also,

$$\begin{aligned}
&(a \wedge b) \vee (a' \vee b')\\
&= [a \vee (a' \vee b')] \wedge [(b \vee (a' \vee b')] && \text{(distributivity)}\\
&= [(a \vee a') \vee b'] \wedge [a' \vee (b \vee b')] && \text{(associativity and commutativity)}\\
&= (1 \vee b') \wedge (a' \vee 1) && \text{(complement)}\\
&= 1 \vee 1 = 1
\end{aligned}$$

Therefore, $a' \vee b'$ is the complement of $a \wedge b$ and by duality, $a' \wedge b'$ is the complement of $a \vee b$.

(iii) Since $a \wedge a' = a' \wedge a = 0$ and also $a' \vee a = 1$, then a is the complement of a'. Now, since complements are unique, then $(a')' = a$.

(iv) By definition of complement, $0 \vee 0' = 1$. Then by commutativity, $0' \vee 0 = 1$ and so, by Proposition 3.1, $0' = 1$. Similarly, $1 \wedge 1' = 0$ by definition. Then $1' \wedge 1 = 0$ and by Proposition 3.1, then $1' = 0$. □

Lemma 3.1. *For b, c in a boolean algebra B , the following are equivalent:*

(i) $b \leq c$

(ii) $b \wedge c' = 0$

(iii) $b' \vee c = 1$

Proof. We will show that (i) $\implies$ (ii), (ii) $\implies$ (iii), and (iii) $\implies$ (i), therefore showing that (i), (ii), and (iii) are equivalent.

If $b \leq c$, then $b \vee c = c$ (Theorem 2.2). Then we have

$$\begin{aligned} b \wedge c' &= b \wedge (b \vee c)' && (b \vee c = c) \\ &= b \wedge (b' \wedge c') && \text{(de Morgan's)} \\ &= (b \wedge b') \wedge c' && \text{(associativity)} \\ &= 0 \wedge c' && \text{(definition of complement)} \\ &= 0 \end{aligned}$$

Therefore, (i) $\implies$ (ii).

If $b \wedge c' = 0$, then

$$\begin{aligned} b' \vee c &= b' \vee (c')' && \text{(involution)} \\ &= (b \wedge c')' && \text{(de Morgan's)} \\ &= 0' && (b \wedge c' = 0) \\ &= 1 && \text{(Proposition 3.3)} \end{aligned}$$

Therefore, (ii) $\implies$ (iii).

If $b' \vee c = 1$, then

$$\begin{aligned} b &= b \wedge 1 && \text{(Proposition 3.1)} \\ &= b \wedge (b' \vee c) && (b' \vee c = 1) \\ &= (b \wedge b') \vee (b \wedge c) && \text{(distribution)} \\ &= 0 \vee (b \wedge c) && \text{(definition of complement)} \\ &= b \wedge c && \text{(Proposition 3.1)} \end{aligned}$$

Since $b = b \wedge c$, then by definition of *glb*, $b \leq c$. So (iii) $\implies$ (i), and therefore (i), (ii), and (iii) are equivalent. □

Exercise 3.3. Let B be a Boolean algebra and $a, b \in B$. Show that

(i) $a \leq b$ if and only if $b' \leq a'$

(ii) $a \leq b'$ if and only if $a \wedge b = 0$

(iii) $a \leq b$ if and only if $a' \vee b = 1$.

Solution.

(i) ($\Longrightarrow$) Suppose $a \leq b$. Then

$$\begin{array}{ll} a \wedge b' = 0 & \text{(Lemma 3.1)} \\ \Longrightarrow\ b' \wedge a = 0 & \text{(commutativity)} \\ \Longrightarrow\ b' \wedge (a')' = 0 & \text{(complement)} \\ \Longrightarrow\ b' \leq a' & \text{(Lemma 3.1)} \end{array}$$

($\Longleftarrow$) Now suppose $b' \leq a'$. Then

$$\begin{array}{ll} b' \wedge (a')' = 0 & \text{(Lemma 3.1)} \\ \Longrightarrow\ b' \wedge a = 0 & \text{(complement)} \\ \Longrightarrow\ a \wedge b' = 0 & \text{(commutativity)} \\ \Longrightarrow\ a \leq b & \text{(Lemma 3.1)} \end{array}$$

(ii) ($\Longrightarrow$) Suppose $a \leq b'$. Then $a \wedge (b')' = 0 \implies a \wedge b = 0$ (Lemma 3.1).

($\Longleftarrow$) Suppose $a \wedge b = 0$. Then $a \wedge (b')' = 0 \implies a \leq b'$ (complement and Lemma 3.1).

(iii) ($\Longrightarrow$) Suppose $a \leq b$. Then $a' \vee b = 1$ (Lemma 3.1).

($\Longleftarrow$) Suppose $a' \vee b = 1$. Then $a \leq b$ (Lemma 3.1).

Definition 3.8. If A and B are algebras and R is a field (or ring), then $\phi : A \longrightarrow B$ is an *algebra homomorphism* if, for all $r \in R$ and $a, b \in A$, then

(i) $\phi(ra) = r\phi(a)$

(ii) $\phi(a + b) = \phi(a) + \phi(b)$

(iii) $\phi(ab) = \phi(a)\phi(b)$.

If A and B are Boolean algebras and $x, y \in A$, then ϕ is a *Boolean algebra homomorphism* if

(i) $\phi(0) = 0$ and $\phi(1) = 1$

(ii) $\phi(x + y) = \phi(x) + \phi(y)$

(iii) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

(iv) $\phi(-x) = -\phi(x)$

If ϕ is one-to-one, it is a *monomorphism* or *embedding* of A into B and if ϕ is onto, it is an *endomorphism*.

Definition 3.9. If A and B are Boolean algebras, then $\phi : A \longrightarrow B$ is an *Boolean algebra isomorphism* if

(i) ϕ is bijective (one-to-one and onto)

(ii) For all $a, b \in A$, then $a \leq b \in A$ if and only if $\phi(a) \leq \phi(b) \in B$ (for this, we say ϕ is *order preserving*).

Alternately, if ϕ is a bijective homomorphism, then ϕ is an *isomorphism* and A is *isomorphic* to B, $A \cong B$.

Definition 3.10. For a subset p of a Boolean algebra A, the homomorphism from A into the two-element Boolean algebra is called the *characteristic homomorphism* and is denoted $\chi_p : A \longrightarrow 2$.

Exercise 3.4. Show that if $\phi : B \longrightarrow C$ is a Boolean algebra isomorphism, then for all $a, b \in B$

(i) $\phi(a \vee b) = \phi(a) \vee \phi(b)$

(ii) $\phi(a \wedge b) = \phi(a) \wedge \phi(b)$

Solution. (i) Since ϕ is a Boolean algebra isomorphism, then ϕ is one-to-one, onto, and $a \leq b$ if and only if $\phi(a) \leq \phi(b)$.

Consider $\phi(a) \leq \phi(b)$. Then $\phi(a) \vee \phi(b) = \phi(b)$. Now consider $a \leq b$. Then $a \vee b = b$, which implies $\phi(a \vee b) = \phi(b)$. Therefore, $\phi(a \vee b) = \phi(b) = \phi(a) \vee \phi(b)$.

(ii) Similar to (i), $\phi(a) \leq \phi(b) \implies \phi(a) \wedge \phi(b) = \phi(a)$ and $a \leq b \implies a \wedge b = a \implies \phi(a \wedge b) = \phi(a)$. Therefore, $\phi(a \wedge b) = \phi(a) = \phi(a) \wedge \phi(b)$.

Exercise 3.5. Show that if $\phi : B \longrightarrow C$ is a Boolean algebra isomorphism, then

(i) $\phi(1_B) = 1_C$

(ii) $\phi(0_B) = 0_C$

(iii) $\phi(a') = (\phi(a))'$ for all $a \in B$.

Solution.

(i) For all $b \in B$, $b \leq 1_B$. For all $\phi(b) \in C$, $\phi(b) \leq 1_C$. Then $b \vee 1_B = 1_B$. Since ϕ is an isomorphism, then $\phi(b \vee 1_B) = \phi(1_B)$ and by Exercise 3.4, $\phi(b) \vee \phi(1_B) = \phi(1_B)$.

Now, by definition of unity, $\phi(b) \vee 1_C = 1_C$ in C. Since ϕ is onto, there exists $1_{C_1} \in B$ such that $\phi(1_{C_1}) = 1_C$. If $1_B = 1_{C_1}$, then $\phi(1_B) = 1_C$. Suppose $1_B \neq 1_{C_1}$. Then $1_{C_1} \vee 1_B = 1_B$ (definition of unity) and so, $\phi(1_{C_1} \vee 1_B) = \phi(1_{C_1}) \vee \phi(1_B) = \phi(1_B)$. But $\phi(1_{C_1}) = 1_C$ and so $\phi(1_{C_1}) \vee \phi(1_B) = 1_C \vee \phi(1_B) = 1_C$. Therefore, $\phi(1_B) = 1_C$.

(ii) For all $b \in B$, $0_B \leq b$. For all $\phi(b) \in C$, $0_c \leq \phi(b)$. So $0_B \wedge b = 0_B$ and $\phi(0_B \wedge b) = \phi(0_B) \wedge \phi(b) = \phi(0_B)$.

In C, $0_C \wedge \phi(b) = 0_C$. Since ϕ is onto, $\exists\ 0_{C_1} \in B$ such that $\phi(0_{C_1}) = 0_C$. If $0_B = 0_{C_1}$, then $\phi(0_B) = 0_C$. Suppose $0_B \neq 0_{C_1}$. Then $0_{C_1} \wedge 0_B = 0_B$ (definition of zero) and so, $\phi(0_{C_1} \wedge 0_B) = \phi(0_{C_1}) \wedge \phi(0_B) = \phi(0_B)$. But $\phi(0_{C_1}) = 0_C$ and so $\phi(0_{C_1}) \wedge \phi(0_B) = 0_C \wedge \phi(0_B) = 0_C$. Therefore, $\phi(0_B) = 0_C$.

(iii) By (i) and complementation, $1_C = \phi(1_B) = \phi(a \vee a') = \phi(a) \vee \phi(a')$. But $1_C = \phi(a) \vee (\phi(a))'$. So $\phi(a) \vee \phi(a') = \phi(a) \vee (\phi(a))'$. Similary, by (ii) and complementation, $0_C = \phi(0_B) = \phi(a \wedge a') = \phi(a) \wedge \phi(a')$ and $0_C = \phi(a) \wedge (\phi(a))'$. Then $\phi(a) \wedge \phi(a') = \phi(a) \wedge (\phi(a))'$. Therefore, by Exercise 2.8, $\phi(a') = (\phi(a))'$.

Definition 3.11. A ring R with unity is a *Boolean ring* if $a \cdot a = a$ and $a + a = 0$ for all $a \in R$. A Boolean ring is commutative.

Exercise 3.6. Let R be a Boolean ring with unity 1 and for $a, b \in R$ define $a \vee b = a + b - a \cdot b$ and $a \wedge b = a \cdot b$. Show that R with $\vee$ and $\wedge$ is a Boolean algebra with unity 1, zero element 0, and $a' = 1 - a$.

Solution. We know that all of the ring axioms hold for R under $+$, $\cdot$, and $'$, and for all $a \in R$, then $a \cdot a = a$ and $a + a = 0$. Also, R is commutative.
Complementation: We will show $a \vee a' = 1$ and $a \wedge a' = 0$.

$$\begin{aligned}
a \vee a' &= a + a' + (-a) \cdot a' \\
&= a + (1 + (-a)) + (-a) \cdot (1 + (-a)) && (a' = 1 + (-a)) \\
&= a + [(1 + (-a)) \cdot (1 + (-a))] && \text{(distribution)} \\
&= a + (1 + (-a)) && \text{(idempotence)} \\
&= a + a' && (a' = 1 + (-a)) \\
&= 1 && (\ + \text{ complementation})
\end{aligned}$$

Since $a \cdot a' = 0$, then $a \wedge a' = a \cdot a' = 0$.

Commutativity: We will show $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$.

$$\begin{aligned}
a \vee b &= a + b + (-a) \cdot b \\
&= b + a + (-a) \cdot b && (+ \text{ commutativity}) \\
&= b \cdot b + a + (-a) \cdot b && (\text{idempotence}) \\
&= b \cdot (b + (-a)) + a && (\text{distribution and } + \text{ commutativity}) \\
&= b + a && (\text{absorption}) \\
&= a + b && (+ \text{ commutativity}) \\
&= a \cdot (a + (-b)) + b && (\text{absorption}) \\
&= a \cdot a + b + (-b) \cdot a && (\text{distribution and commutativity}) \\
&= a + b + (-b) \cdot a && (\text{idempotence}) \\
&= b + a + (-b) \cdot a && (+ \text{ commutativity}) \\
&= b \vee a.
\end{aligned}$$

Since R is commutative, then $a \wedge b = a \cdot b = b \cdot a = b \wedge a$.

Absorption: We will show $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$.

$$\begin{aligned}
a \vee (a \wedge b) &= a + (a \cdot b) + (-a) \cdot (a \cdot b) \\
&= a + (a \cdot b) + (-a \cdot a) \cdot b && (\cdot \text{ associativity}) \\
&= a + (a \cdot b) + 0 \cdot b && (\text{complementation}) \\
&= a + (a \cdot b) + 0 && (glb) \\
&= a + (a \cdot b) && (\text{identity}) \\
&= a && (\text{absorption})
\end{aligned}$$

$$\begin{aligned}
a \wedge (a \vee b) &= a \cdot (a + b + (-a) \cdot b) \\
&= a \cdot a + a \cdot b + a \cdot (-a) \cdot b && (\text{distribution}) \\
&= a \cdot (a + b) + 0 \cdot b && (\text{distribution and compl.}) \\
&= a \cdot (a + b) + 0 && (glb) \\
&= a \cdot (a + b) && (\text{identity}) \\
&= a && (\text{absorption})
\end{aligned}$$

Distribution: We will show $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

$$\begin{aligned}
a \wedge (b \vee c) &= a \cdot (b + c + (-b) \cdot c) \\
&= a \cdot (b + c) + a \cdot ((-b) \cdot c) && (\text{distribution}) \\
&= a \cdot (b + c) + (-b) \cdot (a \cdot c) && (\text{comm. and assoc.}) \\
&= a \cdot (b + c) + 0 + (-b) \cdot (a \cdot c) && (\text{identity}) \\
&= a \cdot (b + c) + 0 \cdot c + (-b) \cdot (a \cdot c) && (glb) \\
&= a \cdot (b + c) + (-a \cdot a) \cdot c + (-b) \cdot (a \cdot c) && (\text{complementation}) \\
&= a \cdot (b + c) + (-a) \cdot (a \cdot c) + (-b) \cdot (a \cdot c) && (\text{associativity}) \\
&= (a \cdot b) + (a \cdot c) + (-a + b) \cdot (a \cdot c) && (\text{distribution}) \\
&= (a \cdot b) + (a \cdot c) + (-(a \cdot b)) \cdot (a \cdot c) && (\text{de Morgan's}) \\
&= (a \wedge b) \vee (a \wedge c)
\end{aligned}$$

$$\begin{aligned}
a \vee (b \wedge c) &= a + (b \cdot c) + (-a) \cdot (b \cdot c) \\
&= a + (b \cdot c) \cdot 1 + (b \cdot c) \cdot (-a) && \text{(identity and comm.)} \\
&= a + [(b \cdot c) \cdot (1 + (-a))] && \text{(distribution)} \\
&= a + [(b \cdot c) \cdot (1 + (-a)) \cdot (1 + (-a))] && \text{(idempotence)} \\
&= a + [(b \cdot (1 + (-a)) \cdot (c \cdot (1 + (-a))] && \text{(comm. and associativity)} \\
&= a + [(b + b \cdot (-a)) \cdot (c + c \cdot (-a))] && \text{(distribution)} \\
&= a + (b + b \cdot (-a)) \cdot a + (c + c \cdot (-a)) && \text{(distribution)} \\
&= (a + b + (-a) \cdot b) \cdot (a + c + (-a) \cdot c) && \text{(associativity and comm.)} \\
&= (a \vee b) \wedge (a \vee c)
\end{aligned}$$

Associativity: We will show $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

First, we will establish that $a + a' \cdot b = a + b$. By distribution, $a + a' \cdot b = (a + a') \cdot (a + b)$. Then, $(a + a') \cdot (a + b) = 1 \cdot (a + b) = a + b$ by complementation and identity. Therefore, $a + a' \cdot b = a + b$, which we will refer to as $\star$.

$$\begin{aligned}
a \vee (b \vee c) &= a + (b + c + (-b) \cdot c) + (-a) \cdot (b + c + (-b) \cdot c) \\
&= a + (b + c) + (-a) \cdot (b + c) && \text{(absorption)} \\
&= a + (b + c) \cdot (1 + (-a)) && \text{(distribution)} \\
&= a + (b + c) \cdot a' && (a' = 1 + (-a)) \\
&= (a + b) + c && (\star \text{ and } + \text{ associativity}) \\
&= (a + b) + c \cdot (a + b)' && (\star) \\
&= (a + b) + c \cdot (1 + -(a + b)) && (a' = 1 + (-a)) \\
&= (a + b) + c + -(a + b) \cdot c && \text{(distribution)} \\
&= (a + b + (-a) \cdot b) + c + -(a + b + (-a) \cdot b) \cdot c && \text{(absorption)} \\
&= (a \vee b) \vee c.
\end{aligned}$$

Since $\cdot$ is associative, $a \wedge (b \wedge c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \wedge b) \wedge c$.

Therefore, R is a Boolean algebra.

Exercise 3.7. Define, in a Boolean algebra A, the binary operations $\mid$ and $\uparrow$ by $x \mid y = -x \cdot -y$ and $x \uparrow y = -x + -y$. Prove that $0, 1$ and the Boolean operations are definable, in terms of equations, both by $\mid$ and $\uparrow$.

Solution.

We will show that $x + y$ and $x \cdot y$ are definable in terms of $\uparrow$ and $\mid$.

$-x \uparrow -y = -(-x) + -(-y) = x + y$ and $-x \mid -y = -(-x) \cdot -(-y) = x \cdot y$.

Now, we will show $x \mid -x = 0$ and $x \uparrow -x = 1$.

By $+, \cdot$ complementation and $-(-x) = x$, then $x \mid -x = -x \cdot -(-x) = -x \cdot x = 0$ and $x \uparrow -x = -x + -(-x) = -x + x = 1$.

Definition 3.12. For a Boolean algebra B with $x, y \in B$, the *symmetric difference* of x and y is $x\Delta y = x \cdot (-y) + y \cdot (-x)$.
Alternately, the symmetric difference of a and b is $a + b = (a \wedge b') \vee (a' \wedge b)$.

Exercise 3.8. Using the following notation, check that bR is a Boolean algebra and that $brB = B$ and $rbR = R$:

$R = (R, \oplus, \cdot, 0, 1)$ is a Boolean ring,
$B = (B, +, \cdot, -, 0, 1)$ is a Boolean algebra,
$rB = (B, \triangle, \cdot, 0, 1)$ where $x \triangle y = x \cdot -y + y \cdot -x$,
$bR = (R, +, \cdot, -, 0, 1)$ where $x + y = x \oplus y \oplus (x \cdot y)$ and $x \oplus 1 = -x$.

Solution. We want to show that bR is a Boolean algebra. First, we will show that R is commutative.

Consider $x \oplus y$. By idempotence and distribution, $x \oplus y = (x \oplus y) \cdot (x \oplus y) = x \cdot x \oplus x \cdot y \oplus y \cdot x \oplus y \cdot y = x \oplus x \cdot y \oplus y \cdot x \oplus y = x \oplus 0 \oplus y$. Then $x \cdot y \oplus y \cdot x = 0$.

If $x = y$, then $x \cdot x \oplus x \cdot x = x \oplus x = 0$. So $x \cdot y = y \cdot x$ and R is commutative.
Commutativity: Since R is commutative under $\cdot$ and $\oplus$, then $x + y = x \oplus y \oplus (x \cdot y) = y \oplus x \oplus (y \cdot x) = y + x$.
Absorption: We will show $x + (x \cdot y) = x$ and $x \cdot (x + y) = x$.

$$\begin{aligned} x + (x \cdot y) &= x \oplus (x \cdot y) \oplus (x \cdot (x \cdot y)) \\ &= x \oplus (x \cdot y) \oplus ((x \cdot x) \cdot y) && (\cdot \text{ associativity}) \\ &= x \oplus (x \cdot y) \oplus (x \cdot y) && (\text{idempotence}) \\ &= x \oplus 0 && (x \oplus x = 0) \\ &= x && (x \oplus 0 = x). \end{aligned}$$

$$\begin{aligned} x \cdot (x + y) &= x \cdot (x \oplus y \oplus (x \cdot y)) \\ &= x \cdot (y \oplus (x \cdot y) \oplus x) && (\oplus \text{ commutativity}) \\ &= x \cdot y \oplus x \cdot (x \cdot y) \oplus x \cdot x && (\text{distribution}) \\ &= 0 \oplus x && (\text{idempotence } \& \ x \oplus x = 0) \\ &= x && (x \oplus 0 = x). \end{aligned}$$

Distribution: We will show $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $x + (y \cdot z) = (x + y) \cdot (x + z)$.

$$\begin{aligned} x \cdot (y + z) &= x \cdot (y \oplus z \oplus (y \cdot z)) \\ &= (x \cdot y) \oplus (x \cdot z) \oplus (x \cdot (y \cdot z)) && (\text{distribution}) \\ &= (x \cdot y) \oplus (x \cdot z) \oplus ((x \cdot y) \cdot (x \cdot z)) && (\text{assoc., comm., idemp.}) \\ &= (x \cdot y) + (x \cdot z) \end{aligned}$$

$$
\begin{aligned}
x + (y \cdot z) &= x \oplus (y \cdot z) \oplus (x \cdot (y \cdot z)) \\
&= (x \oplus (y \cdot z) \oplus x) \cdot (x \oplus (y \cdot z) \oplus (y \cdot z)) && \text{(distribution)} \\
&= (0 \oplus (y \cdot z)) \cdot (x \oplus 0) && \text{(comm. \& } x \oplus x = 0) \\
&= (y \cdot z) \cdot x && (x \oplus x = 0) \\
&= (y \cdot x) \cdot (z \cdot x) && \text{(idemp., comm., assoc.)} \\
&= ((x \oplus y \oplus x) \cdot (x \oplus y \oplus y)) \cdot ((x \oplus z \oplus x) \cdot (x \oplus z \oplus z)) && (x \oplus x = 0, \text{ id, comm.}) \\
&= (x \oplus y \oplus (x \cdot y)) \cdot (x \oplus z \oplus (x \cdot z)) && \text{(distribution)} \\
&= (x + y) \cdot (x + z).
\end{aligned}
$$

Complementation: Since complementation holds in R for $\cdot$ and $\oplus$ and $x \oplus 0 = x$, then $x + -x = x \oplus -x \oplus (x \cdot -x) = x \oplus -x \oplus 0 = x \oplus -x = 1$.

Associativity: Since R is associative for $\cdot$ and $\oplus$, we will show $x + (y + z) = (x + y) + z$.

$$
\begin{aligned}
x + (y + z) &= x \oplus (y \oplus z \oplus (y \cdot z)) \oplus (x \cdot (y \oplus z \oplus (y \cdot z)) \\
&= (x \oplus y \oplus z \oplus (y \cdot z) \oplus x) \cdot (x \oplus y \oplus z \oplus (y \cdot z) \oplus y \oplus z \oplus (y \cdot z)) && \text{(distribution)} \\
&= (x \oplus x \oplus y \oplus z \oplus (y \cdot z)) \cdot (x \oplus y \oplus y \oplus z \oplus z \oplus (y \cdot z) \oplus (y \cdot z)) && \text{(commutativity)} \\
&= (0 \oplus y \oplus z \oplus (y \cdot z)) \cdot (x \oplus 0 \oplus 0 \oplus 0) && (x \oplus x = 0) \\
&= (y \oplus z \oplus (y \cdot z)) \cdot x && (x \oplus 0 = x) \\
&= (y \oplus z \oplus y) \cdot (y \oplus z \oplus z) \cdot x && \text{(distribution)} \\
&= (0 \oplus z) \cdot (y \oplus 0) \cdot (x) && (x \oplus x = 0, \text{ comm.}) \\
&= (z) \cdot (0 \oplus y) \cdot (x \oplus 0) && (x \oplus 0 = x, \text{ comm.}) \\
&= z \cdot (x \oplus x \oplus y) \cdot (x \oplus y \oplus y) && (x \oplus x = 0) \\
&= z \cdot (x \oplus y \oplus (x \cdot y)) && \text{(comm. \& dist.)} \\
&= (0 \oplus 0 \oplus 0 \oplus z) \cdot (x \oplus y \oplus (x \cdot y) \oplus 0) && (x \oplus 0 = x) \\
&= (x \oplus x \oplus y \oplus y \oplus (x \cdot y) \oplus (x \cdot y) \oplus z) \cdot (x \oplus y \oplus (x \cdot y) \oplus z \oplus z) && (x \oplus x = 0) \\
&= (x \oplus y \oplus (x \cdot y) \oplus z \oplus x \oplus y \oplus (x \cdot y)) \cdot (x \oplus y \oplus (x \cdot y) \oplus z \oplus z) && \text{(commutativity)} \\
&= (x \oplus y \oplus (x \cdot y)) \oplus z \oplus ((x \oplus y \oplus (x \cdot y) \cdot z) && \text{(distribution)} \\
&= (x + y) + z.
\end{aligned}
$$

Therefore, bR is a Boolean algebra. Now we want to show $brB = B$ and $rbR = R$.

For rbR, we want to show $x \oplus 1 = -x$ and $x \oplus y \oplus (x \cdot y) = x + y$ and for brB, we want to show $-x = x \triangle 1$ and $x + y = x \triangle y \triangle (x \cdot y)$.

By complementation and the zero and unity properties, $x \oplus 1 = (x \cdot -1) \oplus (1 \cdot -x) \oplus ((x \cdot -1) \cdot (1 \cdot -x)) = (x \cdot 0) \oplus (-x) \oplus ((x \cdot 0) \cdot (-x)) = -x$. Similarly, $x \triangle 1 = (x \cdot -1) + (1 \cdot -x) = (x \cdot 0) + (-x) = 0 + -x = -x$. Now, we will show $x \oplus y \oplus (x \cdot y) = x + y$:

$$
\begin{aligned}
& x \oplus y \oplus (x \cdot y) \\
&= ((x \cdot -y + y \cdot -x) \cdot -(x \cdot y)) + ((x \cdot y) \cdot -(x \cdot -y + y \cdot -x)) \\
&= ((x \cdot -y + y \cdot -x) \cdot (-x + -y)) + ((x \cdot y) \cdot (-x + y \cdot -y + x)) && \text{(de Morgan's)} \\
&= ((x \cdot -y) \cdot (-x + -y)) + ((y \cdot -x) \cdot (-x + -y)) \\
&+ ((x \cdot y) \cdot (((-x + y) \cdot -y) + ((-x + y) \cdot x))) && \text{(distribution)} \\
&= (x \cdot -y \cdot -x) + (x \cdot -y \cdot -y) + (y \cdot -x \cdot -x) + (y \cdot -x \cdot -y) \\
&+ ((x \cdot y) \cdot ((-x \cdot -y) + (y \cdot -y) + (-x \cdot x) + (y \cdot x))) && \text{(distribution)} \\
&= (x \cdot -y) + (y \cdot -x) + (x \cdot y \cdot -x \cdot -y) + (x \cdot y \cdot y \cdot x) && \text{(comp., zero, dist.)} \\
&= (x \cdot -y) + (y \cdot -x) + (x \cdot y) && \text{(comp., zero)} \\
&= x \cdot (-y + y) + y \cdot -x && \text{(comm., dist.)} \\
&= x + (y \cdot -x) && \text{(comp., unity)} \\
&= x + y \cdot x + -x && \text{(comp., unity)} \\
&= x + y.
\end{aligned}
$$

Similarly, $x \triangle y \triangle (x \cdot y) =$ $((x \cdot -y + y \cdot -x) \cdot -(x \cdot y)) + ((x \cdot y) \cdot -(x \cdot -y + y \cdot -x)) = x + y$. Therefore, $rbR = R$ and $brB = B$.

Chapter 4

Atoms and Ultrafilters

We have developed an understanding for Boolean algebras and some of their properties thus far. We can now examine atoms and ultrafilters, which are foundational elements of Boolean algebras.

Definition 4.1. If B is a Boolean algebra and $a < b$, then $a \in B$ is an *atom* if $0 < a$ and there does not exist $x \in B$ such that $0 < x < a$. The set of atoms of B is denoted $At\ B$. We say B is *atomless* if it contains no atoms, and *atomic* if there exists an atom $a \leq x$ for each positive $x \in B$.

Example 4.1. For the Boolean algebra $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$, the elements $2, 3$, and 5 are all atoms in S.

Example 4.2. The power set algebra $P(X)$ of a set X and the finite-cofinite algebra on X are both atomic sets.

The interval algebra of the real number line and the regular open algebra of the real numbers are both atomless sets.

Lemma 4.1. *If B is a finite Boolean algebra and b is any nonzero element in B, then there exists an atom a in B such that $a \leq b$.*

Proof. If b is an atom in B, then $b = a$.

Suppose b is not an atom in B. Then there exists $a_1 \in B$ such that $0 < a_1 < b$. If a_1 is an atom, then $a_1 = a$. If a_1 is not an atom, then there exists $a_2 \in B$ such that

$0 < a_2 < a_1$. If a_2 is an atom, then $a_2 = a$. If a_2 is not an atom, then we continue in this manner and eventually obtain $0 < a_n < \ldots < a_2 < a_1 < b$ since B is finite. Then $a_n = a$. □

Definition 4.2. A subset p of a Boolean algebra A is a *filter* if (i) $1 \in p$, (ii) if $x, y \in p$, then $x \cdot y \in p$, and (iii) if $x \in p$, $y \in A$, and $x \leq y$, then $y \in p$. For $a \in A$, p is a *principal filter* if $p = \{x \in X \mid a \leq x\}$. We say p is the *principal filter generated by* a. If $p = \{1\}$, then p is the *trivial filter* and if $0 \notin p$, then p is a *proper filter*.

Definition 4.3. If $M \subseteq A$ for a Boolean algebra A, then M is said to have the *finite intersection property* if $\bigcap\{m_1, m_2, \ldots, m_n\} \neq \emptyset$ for $m_i \in M$ $(i = 1, 2, \ldots, n)$.

Definition 4.4. An *ultrafilter* is a filter p of a Boolean algebra A where $x \in p$ or $-x \in p$, but not both, for each $x \in A$. If p is proper and $x + y \in p \implies x \in p$ or $y \in p$ for $x, y \in A$, then p is a *prime filter*. If p is proper and $\nexists$ proper filter q of A with $p \subset q$, then p is a *maximal filter*.

The *set of ultrafilters of* A is $Ult\ A = \{p \subseteq A \mid p\ is\ an\ ultrafilter\ of\ A\}$.

Example 4.3. The set $\{a \in A \mid x \in a\}$, where A is an algebra of sets over X and x is any point in X, is an ultrafilter.

Definition 4.5. The *Stone map* of a Boolean algebra A is the map $s : A \longrightarrow P(Ult\ A)$, where $s(x) = \{p \in Ult\ A \mid x \in p\}$.

Definition 4.6. If $\phi : A \longrightarrow B$ is a Boolean algebra homomorphism and $\Sigma^A M$ exists for $M \subseteq A$, then ϕ *preserves* $\Sigma^A M$ if $\Sigma^B \phi[M]$ exists and $\phi\left(\Sigma^A M\right) = \Sigma^B \phi[M]$. Similarly, ϕ preserves $\Pi^A M$ if $\phi\left(\Pi^A M\right) = \Pi^B \phi[M]$. For an ultrafilter p of A, p preserves ΣM if, for some $m \in M$, $\Sigma M \in p \implies m \in p$ and preserves ΠM if $M \subseteq p \implies \Pi M \in p$.

Exercise 4.1. In a Boolean algebra A, let $M \subseteq A$ such that ΣM exists. The Stone homomorphism $s : A \longrightarrow P(Ult\ A)$ preserves ΣM if and only if $\Sigma M = \Sigma M_0$ for some finite subset M_0 of M.

Similarly, let M and N be subsets of A such that $\bigcap s[M] \subseteq \bigcup s[N]$. Then there are finite subsets M_0 of M and N_0 of N such that $\bigcap s[M_0] \subseteq \bigcup s[N_0]$.

Solution.

($\Longrightarrow$) We know $M \subseteq A$ and ΣM exists. Suppose $s : A \longrightarrow P(Ult\ A)$ preserves ΣM; that is, $s[\Sigma M] = \Sigma s[M]$. We want to show $\Sigma M = \Sigma M_0$ for finite $M_0 \subseteq M$.

Suppose $\Sigma M \neq \Sigma M_0$. Then $\Sigma M_0 < \Sigma M$ or $\Sigma M < \Sigma M_0$. Consider $\Sigma M_0 < \Sigma M$. Since $M_0 \subseteq M$, then $\forall\ y \in M_0$, $y \in M$. Now, since ΣM exists and $\Sigma M \leq x$ for all $x \in M$, then $\Sigma M \leq y \in M_0$. So $\Sigma M_0 \not< \Sigma M \implies \Sigma M_0 \leq \Sigma M$. Now consider $\Sigma M < \Sigma M_0$. Suppose $\exists\ x \in M$ such that $x < y\ \forall\ y \in M_0$. Then $x \notin M_0$ since ΣM_0 exists because M_0 is finite. But $M_0 \subseteq M$ and $\forall\ x \in M_0 \implies x \in M$. So $\Sigma M \not< \Sigma M_0 \implies \Sigma M \leq \Sigma M_0$. Therefore $\Sigma M = \Sigma M_0$.

($\Longleftarrow$) We know that $\Sigma M = \Sigma M_0$ for some finite $M_0 \subseteq M$. Also, $\Sigma s[M] \in P(Ult\ A)$. We want to show that $s[\Sigma M] = \Sigma s[M]$. Since s is a homomorphism, $s[\Sigma M \cap x] = s[\Sigma M] \cap s[x]$ for $x \in M$. But $\Sigma M \cap x = \Sigma M$ for all $x \in M$. So $s[\Sigma M \cap x] = s[\Sigma M] \cap s[x] = s[\Sigma M]$ for all $s[x] \in P(Ult\ A)$. Therefore, $s[\Sigma M] = \Sigma s[M]$.

Now, let $M, N \subseteq A$ such that $\bigcap s[M] \subseteq \bigcup s[N]$. We want to show that for $M_0 \subseteq M$ and $N_0 \subseteq N$, where M_0 and N_0 are finite, then $\bigcap s[M_0] \subseteq \bigcup s[N_0]$. Since s preserves ΣM, then $\Sigma M = \Sigma M_0$.

Lemma 4.2. *If a_1 and a_2 are atoms in B and $a_1 \wedge a_2 \neq 0$, then $a_1 = a_2$.*

Proof. By the definition of *glb*, $a_1 \wedge a_2 \leq a_1$. Since a_1 is an atom, either $a_1 \wedge a_2 = 0$ or $a_1 \wedge a_2 = a_1$. But $a_1 \wedge a_2 \neq 0$. Then $a_1 \wedge a_2 = a_1$.

Similarly, $a_1 \wedge a_2 \leq a_2$. Since a_2 is an atom and $a_1 \wedge a_2 \neq 0$, then $a_1 \wedge a_2 = a_2$. Therefore $a_1 = a_1 \wedge a_2 = a_2$. □

Lemma 4.3. *If $b, c \in B$ and $b \not\leq c$, then there exists an atom $a \in B$ such that $a \leq b$ and $a \not\leq c$.*

Proof. Since $b \not\leq c$, then $b > c$ and $b \wedge c' \neq 0$ (Lemma 3.1). Then by Lemma 4.1, there exists an atom $a \in B$ such that $a \leq b \wedge c'$. By definition of *glb*, $a \leq b$ and $a \leq c'$. Now, if $a \leq c'$ and $a \leq c$, then $a \leq c \wedge c'$. But $c \wedge c' = 0$ and so $a \leq 0$. This contradictions the fact that a is an atom in B. Therefore $a \not\leq c$. □

Lemma 4.4. *If $b \in B$ and $a_1, a_2, \ldots, a_n$ are all of the atoms that satisfy $a_i \leq b$ (where $i = 1, 2, \ldots, n$) in B, then $b = a_1 \vee a_2 \vee \cdots \vee a_n$.*

Proof. We will let $a_1 \vee a_2 \vee \cdots \vee a_n = c$. Since each $a_i \leq b$, then $c \leq b$. Now suppose $b \not\leq c$. Then by Lemma 4.3, there exists an atom in B such that $a \leq b$ and $a \not\leq c$. But since $a \leq b$ and a is an atom in B, then $a = a_i$, for some $i = 1, 2, \ldots, n$. Therefore $a \leq c$, contradicting $a \not\leq c$, so $b \leq c$. Then $c \leq b$ and $b \leq c$, implying $b = c$. Therefore $b = a_1 \vee a_2 \vee \cdots \vee a_n$. □

Lemma 4.5. *Suppose $b \in B$ and $a_1, a_2, \ldots, a_n$ are all of the atoms in B such that $b = a_1 \vee a_2 \vee \cdots \vee a_n$. If a is an atom in B and $a \leq b$, then $a = a_i$ for some $i = 1, 2, \ldots, n$.*

Proof. Since $a \leq b$, then $a \wedge b = a$ (Theorem 2.2).
So $a = a \wedge b = a \wedge (a_1 \vee a_2 \vee \cdots \vee a_n) = (a \wedge a_1) \vee (a \wedge a_2) \vee \cdots \vee (a \wedge a_n)$ (by distribution). Now since a is an atom in B, then $a \neq 0$. So for some $i = 1, 2, \ldots, n$, $a \wedge a_i \neq 0$ (Proposition 3.2). Therefore, by Lemma 4.2, $a = a_i$. □

Proposition 4.1. *For a Boolean algebra A and a power set algebra $P(At\ A)$, $\phi : A \longrightarrow P(At\ A)$, where $\phi(b) = \{a \in At\ A \mid a \leq b\}$, is a homomorphism. If A is atomic, ϕ is an embedding and if A is complete, ϕ is an epimorphism.*

Proof. Since $\phi(b) = \{a \in At\ A \mid a \leq b\}$, we know that $\phi(0) = \{\ \}$ and $\phi(1) = At\ A$. Now, $\phi(-b) = \{a \in At\ A \mid a \leq -b\}$, which equals $At\ A \setminus \{a \in At\ A \mid a \leq b\}$. Then $At\ A \setminus \{a \in At\ A \mid a \leq b\} = At\ A \setminus \phi(b)$ and so $\phi(-b) = -\phi(b)$. Then, we know that for every $a \in A$, then $a \leq b \cdot c \iff a \leq b$ and $a \leq c$ by definition of *lub* and atom and so, $\phi(b \cdot c) = \phi(b) \cap \phi(c)$. In a similar manner, $\phi(b + c) = \phi(b) \cup \phi(c)$. Therefore, ϕ is a homomorphism.

Now let A be atomic and consider $b \neq c$. Then $b \not\leq c$ or $c \not\leq b$. Without loss of generality, say $b \not\leq c$. Then, by Lemma 3.1, $b \cdot -c \neq 0$ and so, there exists an atom $a \in A$ such that $a \leq b \cdot -c$. So $a \leq b$ and $a \leq -c$. Since $a \leq -c$, then $a \not\leq c$ and so $a \in \phi(b)$ and $a \notin \phi(c)$. Therefore $\phi(b) \neq \phi(c)$ and so ϕ is an embedding.

Lastly, we will let A be complete and $M \subseteq At\ A$ and show ϕ is an epimorphism if $M = \phi(b)$, where $b = \Sigma M$. If $a \in M$, then $a \in \phi(b)$ since $a \leq b = \Sigma M$. Suppose A is not in M. Then $a \in At\ A \setminus M$ and so a is distinct from m for every $m \in M$ and $a \not\leq m$. Then, $a \leq -m$ and so $a \cdot m = 0$ by Lemma 3.1. Therefore $a \notin \phi(b)$. □

Chapter 5

More on Boolean Algebras

For the end of this study, we used the knowledge and understanding developed throughout the previous chapters in order to research the more complex aspects of Boolean algebras.

Theorem 5.1. *If B is a finite Boolean algebra, then B is isomorphic to the power set $P(S)$ of some nonempty finite set S. This is* ***Stone's representation theorem for finite Boolean algebras****.*

Proof. Let B be a finite Boolean algebra and let S be the set of all atoms in B. We want to show that B is isomorphic to the power set of S ($B \cong P(S)$); that is, we want to show there exists a map $\phi : B \longrightarrow P(S)$ such that ϕ is a bijection and ϕ is order preserving.

Since $B \neq \{\ \}$, there exists some $b \in B$. We will define $\phi : B \longrightarrow P(S)$ such that for $b \in B$, then $\phi(b) = A$, where $A = \{a \mid a \in S \text{ and } a \leq b\}$. Note that if $b = 0$, then $\phi(b) = \{\ \}$, since there does not exist $a \in S$ such that $a \leq 0$ (by the definition of atom). Also, if $b = 1$, then $\phi(b) = S$, since for all $a \in S$, $a \leq 1$ (definition of unity). We will assume $b \neq 0, b \neq 1$.

First, we will consider $\{a \in S \mid a \leq b, \text{ for some } b \in B\} = \{a_1, a_2, \ldots, a_k\} \subseteq S$. Then $b = a_1 \vee a_2 \vee \cdots \vee a_k$ by Lemma 4.4. Now, by Lemma 4.5, for any atom $a \leq b$ in B, then $a = a_i$ for some $i = 1, 2, \ldots k$. Therefore, $\phi(b) = \phi(a_1 \vee a_2 \vee \cdots \vee a_k) = \{a_1, a_2, \ldots, a_k\}$ and so ϕ is onto.

Now, ϕ is order preserving if for $b, c \in B$, $b \leq c$ in B if and only if $\phi(b) \subseteq \phi(c)$ in $P(S)$. If $b \leq c$, then every atom a, such that $a \leq b$, is an atom such that $a \leq c$. Therefore

$\phi(b) \subseteq \phi(c)$. Now assume that $b \not\leq c$. Then there exists an atom a such that $a \leq b$ and $a \not\leq c$ (Lemma 4.3). Then $a \in \phi(b)$ and $a \notin \phi(c)$. This implies $\phi(b) \not\subseteq \phi(c)$.

Lastly, if $\phi(b) = \phi(c)$, then $\phi(b) \subseteq \phi(c)$ and $\phi(c) \subseteq \phi(b)$. Since ϕ is order preserving, $\phi(b) \leq \phi(c)$ implies $b \leq c$ and similarly, $\phi(c) \leq \phi(b)$ implies $c \leq b$. Then, by antisymmetry, $b = c$ and therefore ϕ is one-to-one. □

Corollary 5.1. *If B is a finite Boolean algebra, then $\mid B \mid = 2^n$ for some positive integer n.*

Proof. Since B is a finite Boolean algebra, then by Theorem 5.1, there exists a map $\phi : B \longrightarrow P(S)$ for a finite set S, where ϕ is one-to-one and onto. So $\mid B \mid = \mid P(S) \mid$. Then, since S is finite, $\mid S \mid = n$, for some $n > 0$. By induction on n, S has 2^n subsets. Therefore, $\mid P(S) \mid = 2^n$ and so $\mid B \mid = 2^n$. □

Definition 5.1. Let A be a Boolean algebra and let $a \in A$. Then the subset $\{x \in A \mid x \leq a\}$ of A, denoted $A \restriction a$, is a Boolean algebra with the partial order inherited from A and is called the *relative algebra* or *factor algebra* of A with respect to a.

Lemma 5.1. *For each a in A, $A \cong (A \restriction a) \times (A \restriction -a)$*

Proof. Let f be a function such that $f : A \longrightarrow (A \restriction a) \times (A \restriction -a)$, where $f(x) = (x \cdot a, x \cdot -a)$. Let g be a function such that $g : (A \restriction a) \times (A \restriction -a) \longrightarrow A$, where $g(y, z) = y + z$.

Now, let $x \cdot a = y$ and $x \cdot -a = z$. Then $x = y + z$ (since $y + z = (x \cdot a) + (x \cdot -a) = x \cdot (a + -a) = x \cdot 1 = x$). So $f(x) = (x \cdot a, x \cdot -a) = (y, z)$ and $g(y, z) = y + z = x$. Therefore, f and g are inverses.

Now, f is a homomorphism:

(i) $f(x) = f(y + z) = (x \cdot a, x \cdot -a) = (x \cdot a, 0) + (0, x \cdot -a) = (x \cdot a \cdot a, x \cdot a \cdot -a) + (x \cdot -a \cdot a, x \cdot -a \cdot -a) = f(x \cdot a) + f(x \cdot -a) = f(y) + f(z)$.

(ii) $f(y \cdot z) = f(x \cdot a \cdot x \cdot -a) = f(0) = 0 = (0, 0) = (x \cdot a \cdot 0, 0 \cdot x \cdot -a) = (x \cdot a, 0) \cdot (0, x \cdot -a) = f(x \cdot a) \cdot f(x \cdot -a) = f(y) \cdot f(z)$.

(iii) $f(-x) = (-x \cdot a, -x \cdot -a) = (-x \cdot -a, -x \cdot a) = -(x \cdot a, x \cdot -a) = -f(x)$.

Then f is a bijective homomorphism and therefore $A \cong (A \restriction a) \times (A \restriction -a)$.

□

Definition 5.2. Let x and y be in A, a Boolean algebra, and let $X \subseteq A$. If $x \cdot y = 0$, then x and y are *disjoint*. If $0 < x$ for $x \in X$ and any two distinct elements in X are disjoint, then X is said to be a *pairwise disjoint family*.

Definition 5.3. For a Boolean algebra A, a subset $X \subseteq A$ is a *partition of unity* if it is a maximal pairwise disjoint family.

Proposition 5.1. *Let A be an infinite Boolean algebra. Then*

(i) X, an infinite pairwise disjoint family, is in A,

(ii) $(a_n)_{n\in\omega}$, a strictly decreasing infinite sequence, is in A, and

(iii) $(-a_n)_{n\in\omega}$, a strictly increasing infinite sequence, is in A.

Proof. Let $A \restriction a_n$ be infinite for every $n \in \omega$ and consider $(a_n)_{n\in\omega}$, a strictly decreasing sequence in A. Now, let $a_0 = 1$. Consider $a \in A \restriction a_n$ such that $0 < a < a_n$. If $A \restriction a$ is infinite, then let $a = a_{n+1}$. If $A \restriction a$ is finite, then $A \restriction (a_n \cdot -a)$ is infinite (Lemma 1.9) and so we let $a_{n+1} = a_n \cdot -a$.

Since $(a_n)_{n\in\omega}$ is strictly decreasing, then $(-a_n)_{n\in\omega}$ is strictly increasing. Now, $a_n \leq a_{m+1}$ for $m < n$ and $(a_m \cdot -a_{m+1}) \cdot (a_n \cdot -a_{n+1}) \leq a_n \cdot -a_{m+1} = 0$, so $\{a_n \cdot -a_{n+1} \mid n \in \omega\}$ is an infinite pairwise disjoint family. □

Definition 5.4. Let A be a Boolean algebra and $M \subseteq A$. Then ΣM is the *least upper bound (lub)* of M and ΠM is the *greatest lower bound (glb)* of M in $(A, \leq)$. Σ is referred to as *sum* and Π as *product*. If ΣM and ΠM exist for every $M \subseteq A$, then A is said to be a *complete* Boolean algebra.

If M is a family of subsets of A, then the *lub* and *glb* of M in $(P(A), \subseteq)$ are $\bigcup M$ and $\bigcap M$, respectively.

If A is a subalgebra of a Boolean algebra B and $M \subseteq A$, then the *least upper bound of M in A* is $\Sigma^A M$ and the *lub* of M in B is $\Sigma^B M$. Similarly, the *greatest lower bound of M in A* is $\Pi^A M$ and the *glb* of A in B is $\Pi^B M$.

Definition 5.5. If B is a Boolean algebra, then a subalgebra A of B is a *regular subalgebra* if for each $M \subseteq A$ such that $\Sigma^A M$ exists, then $\Sigma^B M$ also exists and $\Sigma^A M = \Sigma^B M$. Similarly, if for each $M \subseteq A$ such that $\Pi^A M$ exists, then $\Pi^B M$ also exists and $\Pi^A M = \Pi^B M$. A is a *complete subalgebra* if for each $M \subseteq A$ such that $\Sigma^B M$ exists, then $\Sigma^A M$ also exists and $\Sigma^B M = \Sigma^A M$.

Definition 5.6. A subalgebra A of a Boolean algebra B is a *k-complete subalgebra* of B if for each subset M of A, where $\mid M \mid < k$ (some cardinal) and $\Sigma^B M$ exists, then $\Sigma^A M$ exists and $\Sigma^A M = \Sigma^B M$. A is a *σ-complete subalgebra* of B if for each countable subset M of A where $\Sigma^B M$ exists, the $\Sigma^A M$ exists and $\Sigma^A M = \Sigma^B M$.

Definition 5.7. If M is an algebra of sets and $\bigcup M_i \in M$ and $\bigcap M_i \in M$ for each $M_i \subseteq M$, then M is a *complete algebra of sets.* If $\bigcup M_i \in M$ and $\bigcap M_i \in M$ for each $M_i \subseteq M$ of size less than k, then M is a *k-algebra of sets.* M is a *σ-algebra of sets* if $\bigcup M_i \in M$ and $\bigcap M_i \in M$ for each countable $M_i \subseteq M$.

Definition 5.8. Let B be a Boolean algebra and $[0,1]$ be the real unit interval. The map $\mu : B \longrightarrow [0,1]$ is called a finitely *additive measure* if $\mu(1) = 1$ and $\mu\left(\Sigma_{i\in I} a_i\right) = \Sigma_{i\in I}\mu(a_i)$ for every finite set $\{a_i \mid i \in I\}$, where $\{a_i \mid i \in I\}$ consists of pairwise disjoint elements. Additionally, if $\mu\left(\Sigma_{i\in I} a_i\right) = \Sigma_{i\in I}\mu(a_i)$ for every countable set, where $\{a_i \mid i \in I\}$ consists of pairwise disjoint elements and $\Sigma_{i\in I} a_i$ exists, then μ is said to be a *σ-additive measure.* If $a > 0 \implies \mu(a) > 0$, then μ is *strictly positive.*

Corollary 5.2. *An infinite σ-complete Boolean algebra has cardinality of at least 2^ω.*

Proof. Let A be an infinite σ-complete Boolean algebra. Then there exists a pairwise disjoint family $\{d_m \mid m \in \omega\}$ in A. Now, let $f : P(\omega) \longrightarrow A$ be a function such that $f(M) = \Sigma_{m\in M} d_m$ and let M and N be distinct subsets of ω. Then, without loss of generality, there exists m in $M \setminus N$ and so $d_m \leq f(M)$. Therefore $d_m \cdot f(M) = d_m > 0$. But $d_m \cdot f(N) = \Sigma_{n\in N}(d_m \cdot d_n) = 0$. Therefore, $f : P(\omega) \longrightarrow A$ is one-to-one. □

Lemma 5.2. *A pairwise disjoint family X is maximal if and only if $\Sigma X = 1$.*

Proof. ($\Longrightarrow$) Let X be a maximal pairwise disjoint family. Then $\Sigma X = 1$.
($\Longleftarrow$) Assume that $\Sigma X < 1$. Then there exist $a \in X$ such that $\Sigma X = a$ and $a < 1$. But then X is not maximal since X is a pairwise disjoint family and $\Sigma\ X \cup \{-a\} = 1$. □

Definition 5.9. For a Boolean algebra A and a cardinal k, the *cellularity* of A is $cA = sup\{\ |\ X\ |\ |\ X$ is a pairwise disjoint family in $A\}$. If $cA =|\ X\ |$ for some pairwise disjoint family X in A, then cA is said to be *attained.* The *saturation* of A is $sat\ A = min\{\mu \mid \mu$ is a cardinal,$|\ X\ | < \mu$ for each pairwise disjoint family X in $A\}$. The *cellularity of $A \restriction a$* is denoted ca.

Theorem 5.2. *For every Boolean algebra A, cA is attained if singular.* ***This is the Erdös-Tarski Theorem.***

Proof. Let us first consider the following fact: let $a \in A$ and μ be some cardinal. If $\mu < ca$, then there exists a pairwise disjoint family Y in $A \restriction a$ such that $\mu \leq |\ Y\ |$. Then there also exists a pairwise disjoint family $X \subseteq Y$ in $A \restriction a$ such that $|\ X\ | = \mu$.

Now, let $cA = \lambda$ such that $\lambda = sup_{\alpha<k}\lambda_\alpha$ for a strictly increasing sequence of cardinals, where k is the cofinality of A. We will consider three cases.

Case 1: There exists $b \in A$ such that, for every $x \in A$ such that $0 < x \leq b$, $cx = \lambda$. Since cA is singular, then $cb = \lambda > k$. Let $\{b_\alpha \mid \alpha < k\}$ be a pairwise disjoint family in $A \restriction b$. Then $cb_\alpha = \lambda > \lambda_\alpha$. Let Z_α be a pairwise disjoint family in $A \restriction b_\alpha$ such that $\mid Z_\alpha \mid = \lambda_\alpha$. Then $Z = \bigcup_{\alpha<k} Z_\alpha$ and Z is a pairwise disjoint family such that $\mid Z \mid = \lambda$.

Now, if Case 1 does not hold, then let $S = \{a \in A^+ \mid ca < \lambda\}$ and let X be a maximal pairwise disjoint family in S. Then there exists $s \in S$ such that $s \leq b$ for each $b \in A^+$. Therefore X is a partition of unity.

Case 2: Suppose $sup_{x\in X}cx = \lambda$. Let $(x_\alpha)_{\alpha<k}$ be a recursively constructed sequence of pairwise distinct elements x_α of X such that $\lambda_\alpha < cx_\alpha$. This is possible because $cx < \lambda$ for $x \in X$. Then, for each $\alpha < k$, choose a pairwise disjoint family Z_α of size λ_α in $A \restriction x_\alpha$. Let $Z = \bigcup_{\alpha<k} Z_\alpha$. Therefore Z is a pairwise disjoint family such that $\mid Z \mid = \lambda$.

Case 3: Suppose $sup_{x\in X}cx = \mu < \lambda$. We want to show that $\mid X \mid = \lambda$. Suppose not. Let $\mid X \mid < \lambda$ and let $\mu' = max\,(\mid X \mid, \mu)^+$. Then $\mu' < \lambda = cA$. Now, let Y be a pairwise disjoint family in A such that $\mid Y \mid = \mu'$ and let $Y_x = \{y \in Y \mid x \cdot y > 0\}$ for $x \in X$. Since X is maximal, then $\Sigma X = 1$ by Lemma 8. So $\bigcup_{x\in X} Y_x = Y$. Now, $\{x \cdot y \mid y \in Y_x\}$ is a pairwise disjoint family in $A \restriction x$. Then $\mid Y_x \mid \leq cx \leq \mu$. And so $\mid Y \mid \leq \mu \cdot \mid X \mid < \mu'$. But we chose Y such that $\mid Y \mid = \mu'$, and so there is a contradiction. Therefore $\mid X \mid = \lambda$.

Thus, if cA is singular then $cA = \lambda$, where λ is the cardinality of a pairwise disjoint family in A. □

Definition 5.10. For a Boolean algebra B, let $\epsilon x \in B$ be $(+1)x = x$ or $(-1)x = -x$, where $x \in B$ and $\epsilon = +1$ or -1. Then for $X \subseteq B$, an *elementary product over* X is a finite product with factors of the form ϵx. An element of B is said to be in *normal form over* X if it is represented as a finite sum of pairwise disjoint elementary products over X.

Definition 5.11. If A is a subalgebra of B and $x_1, x_2, \ldots, x_n \in B$, then the *finite extension* of A by $x_1, x_2, \ldots, x_n$ is $\langle A \cup \{x_1, x_2, \ldots, x_n\}\rangle$ and is denoted $A(x_1, x_2, \ldots, x_n)$. The *simple extension* of A by x is $\langle A \cup \{x\}\rangle$ and is denoted $A(x)$.

Theorem 5.3. *The subalgebra generated by $X \subseteq B$ contains exactly the elements of B representable in normal form over X.*

Proof. First we will prove that an element b in a Boolean algebra B is generated by X if and only if b is generated by a finite subset Y of X.

Suppose b is generated by X and consider $A = \cup\{Y\}$. Then $A \subseteq \langle X \rangle$ since $Y \subseteq X \implies \langle Y \rangle \subseteq \langle X \rangle$ (order-preserving). Also, A is a subalgebra of B since the subalgebras generated by Y make up a directed family.

Now suppose b is generated by Y. Then for every $x \in X$, $x \in \langle x \rangle \subseteq \cup\{Y\} = A$. So $X \subseteq A$ and $\langle X \rangle \subseteq A$.

Now we want to show that for $b \in B$ generated by a finite subset X of B, b is representable in normal form over X.

Let $X = \{x_1, x_2, \ldots, x_n\}$ and let $R = \{\rho\}$, where $\rho : \{1, 2, \ldots, n\} \mapsto \{+1, -1\}$. Then for $\rho \in R$, let $h_\rho = \rho(1)x_1 \cdot \rho(2)x_2 \cdot \cdots \cdot \rho(n)x_n$, an elementary product over X. Consider $\rho \neq \rho'$.

Without loss of generality, let $\rho(3) = +1$ and $\rho'(3) = -1$. So $h_\rho \cdot h_{\rho'} = \rho(1)x_1 \cdot \rho(2)x_2 \cdot (+1)x_3 \cdot \rho'(1)x_1 \cdot \rho'(2)x_2 \cdot (-1)x_3 = \rho(1)x_1 \cdot \rho(2)x_2 \cdot x_3 \cdot \rho'(1)x_1 \cdot \rho'(2)x_2 \cdot -x_3 = \rho(1)x_1 \cdot \rho(2)x_2 \cdot \rho'(1)x_1 \cdot \rho'(2)x_2 \cdot x_3 \cdot -x_3 = \rho(1)x_1 \cdot \rho(2)x_2 \cdot \rho'(1)x_1 \cdot \rho'(2)x_2 \cdot 0 = 0$. Then, $h_\rho \cdot h_{\rho'} = 0$ for $\rho \neq \rho'$.

Now consider $\Sigma_{\rho \in R} h_\rho$. By distribution, $h_{\rho_1} + h_{\rho_2} + \cdots + h_{\rho_n} = (x_1 + -x_1) \cdot (x_2 + -x_2) \cdot \cdots \cdot (x_n + -x_n) = 1$. Therefore, $\Sigma_{\rho \in R} h_\rho = 1$. So $\Sigma_{\rho \in M} h_\rho$, for $M \subseteq R$, is in normal form over X and we will let $A = \cup\{Y\} = \{\Sigma_{\rho \in M} h_\rho \mid M \subseteq R\}$. We will show that $\langle X \rangle \subseteq A$.

Since $h_\rho \cdot h_{\rho'} = 0$ and $\Sigma_{\rho \in R} h_\rho = 1$, then $\Sigma_{\rho \in M} h_\rho + \Sigma_{\rho \in M'} h_\rho = \Sigma_{\rho \in M \cup M'} h_\rho$ and $-\Sigma_{\rho \in M} h_\rho = \Sigma_{\rho \in R \setminus M} h_\rho$. Therefore, A is non-empty and closed under the operations $+$ and $-$, and so A is a subalgebra of B.

Lastly, consider $x_i \in B$. Then $x_i = x_i \cdot \Pi_{j \neq i}(x_j + -x_j)$ and, by distribution, $x_i = \Sigma_{\rho \in M} h_\rho$ for $M = \{\rho \in R \mid \rho(i) = +1\}$. Then every x_i is in A and therefore $\langle X \rangle \subseteq A$. □

Corollary 5.3. *If A is a subalgebra of B, then for $x \in B$, $A(x) = \{a \cdot x + a' \cdot -x \mid a, a' \in A\} = \{a_1 \cdot x + a_2 \cdot -x + a_3 \mid a_1, a_2, a_3 \in A$ are pairwise disjoint$\}$.*

Proof. We know that $A(x) = \langle A \cup \{x\} \rangle$ and so, by Theorem 5.3, $A(x) = \{a \cdot x + a' \cdot -x\}$, where $a, a' \in A$. Now, to show $A(x) = \{a_1 \cdot x + a_2 \cdot -x + a_3\}$, where $a_1, a_2, a_3 \in A$ are

pairwise disjoint, consider $a \cdot x + a' \cdot -x$.

$$a \cdot x + a' \cdot -x = a \cdot (-a' + a') \cdot x + a' \cdot (-a + a) \cdot -x = (a \cdot -a' + a \cdot a') \cdot x + (a' \cdot -a + a \cdot a') \cdot -x$$

$$= (a \cdot -a') \cdot x + (a' \cdot -a) \cdot -x + a \cdot a'.$$

Since $(a \cdot -a')$, $(a' \cdot -a)$, and $(a \cdot a')$ are disjoint, let $a_1 = a \cdot -a'$, $a_2 = a' \cdot -a$, and $a_3 = a \cdot a'$. □

Definition 5.12. For a Boolean algebra B, a subset X of B^* is *dense* in B if for every $b \in B^*$, there exists $x \in X$ such that $0 < x \leq b$. For a subalgebra A of B, if A^* is dense in B, then A is a *dense subalgebra*. The *density* of a Boolean algebra B is denoted πB and is the minimum of $\{| X |\}$, where X is a dense subset in B.

Definition 5.13. For a Boolean algebra A, a subset X of A is called a *chain* in A if X is a linear order under the partial order inherited from A. The set X is a *well-ordered chain* in A if it is a well-ordering under the partial order of A.

Definition 5.14. If $| X | < k$ for each pairwise disjoint family X in a Boolean algebra A, that is if $sat\ A \leq k$, then A satisfies the *k-chain condition*. If each pairwise disjoint family in A is at most countable, then A satisfies the *countable chain condition*.

Lemma 5.3. *For $X \subseteq B^*$, the following are equivalent:*
(i) X is dense in B.
(ii) For every $b \in B$, there is a pairwise disjoint family $M \subseteq X$ such that $\Sigma M = b$.
(iii) For every $b \in B$, there exists $M \subseteq X$ such that $\Sigma M = b$.
(iv) For every $b \in B$, $b = \Sigma\{x \in X \mid x \leq b\}$.

Proof. We will first show (i) $\implies$ (ii): Let $b \in B$ and let M be a pairwise disjoint family such that $M \subseteq X \cap (B \restriction b)$ and M is maximal (well ordering principle). If $\Sigma M \neq b$, then there exists an upper bound c of M such that $c < b$. Now, since X is dense in B, let $0 < x \leq b \cdot -c$. Then $M \cup \{x\}$ is maximal. But this contradicts that M is maximal. Therefore $\Sigma M = b$. Next, (ii) immediately implies (iii). For (iii) $\implies$ (iv), let $M = \{x \in X \mid x \leq b\}$. Lastly, by the definition of dense, (iv) $\implies$ (i). □

Definition 5.15. For a subset A of a topological space X, the *interior* of A, denoted *int* A, is the union of all open sets contained in A. The *closure* of A is denoted *cl* A and is the intersection of all closed sets containing A. The *regularization* of A is the interior of the closure of A and is denoted $rA = int\ cl\ A$.

Definition 5.16. A subset A of a topological space X is said to be *regular open* if $rA = A$ and *regular closed* if $A = cl\ int\ A$. The *regular open algebra* of X is $RO(X) = \{A \subseteq X \mid A\ is\ regular\ open\}$.

Definition 5.17. For a topological space X, $a \subseteq X$ is said to be *nowhere dense* if $int\ cl\ a = \emptyset$. If a is the union of a countable number of nowhere dense sets then it is said to be *meager*.

Definition 5.18. Two elements p and q of a partial order P are *compatible* if there exists $r \in P$ such that $r \leq p$ and $r \leq q$. If there does not exist such an r in P, then p and q are *incompatible*. The *partial order topology* is a topology of P where $\{u_p \mid p \in P\}$ is the base, with $u_p = \{q \in P \mid q \leq p\}$.

Definition 5.19. For a partial order P, a complete Boolean algebra B, and a mapping λ from P into B^*, the pair (λ, B) is a *completion* of P if

(i) λ is order-preserving

(ii) λ preserves compatability

(iii) $\lambda[P]$, the image of P under λ, is dense in B.

Theorem 5.4. *Every partial order P has $RO(P)$ as a completion.*

Proof. Let $\{u_p \mid p \in P\}$ be the partial order topology of P. The regular open algebra of P, $RO(P)$, is $\{p \subseteq P \mid p = int\ cl\ p\}$. Let h be a mapping from P into $RO(P)$ such that $h(p) = int\ cl\ u_p$.

Since $h(p) \subseteq cl\ u_p$ and $cl\ h(p) \subseteq cl\ u_p$, then $h(h(p)) \subseteq h(p)$, where $h(h(p)) = int\ cl\ h(p)$. But $h(p) \subseteq h(h(p))$, and therefore $h(h(p)) = h(p)$. So, for every $p \in P$, $h(p)$ is regular open. Now, $u_p \subseteq P$ is non-empty and so $u_p \subseteq h(p)$, since $u_p \subseteq cl\ u_p$ and $u_p = int\ u_p \subseteq int\ cl\ h(p)$. Therefore $h(p) \in RO(P)^*$.

We will show that $(h, RO(P))$ is a completion of P. First, we will show that the image of P under h, $h[P]$, is dense in $RO(P)$. If $r \subseteq P$ is non-empty and regular open, then there exists p such that $u_p \subseteq r$, since $\{u_p \mid p \in P\}$ is the partial order topology. Then $h(p)$ is the least regular open subset of P such that $u_p \subseteq h(p)$ since $u_p \subseteq h(p) \in RO(P)$ and $u_p \subseteq u_r \in RO(P) \implies h(p) \subseteq h(r) = u_r$. Therefore $h(p) \subseteq r$ and so $h[P]$ is dense in $RO(P)$. Now, since $q \leq p \implies u_q \subseteq u_p$, then $h(q) \subseteq h(p)$ and order is preserved. Lastly, if p and q are incompatible then u_p and u_q are disjoint. Then $u_p \subseteq P \setminus u_q$ and so

$cl\ u_p \subseteq cl\ P \setminus u_q$, where $cl\ P \setminus u_q = P \setminus u_q$. Then $cl\ u_q$ and u_p are disjoint. Similarly, u_q and $cl\ u_p$ are disjoint. Therefore $h(p)$ and $h(q)$ are disjoint and so $(h, RO(P))$ is a completion of P. □

Definition 5.20. If for all p and q in a partial order P such that $q \not\leq p$ there exists $r \leq q$, where r is incompatible with p, then P is said to be *separative*.

Definition 5.21. For a Boolean algebra A and a complete Boolean algebra B, B is a *completion* of A, denoted $B = \bar{A}$, if A is a dense subalgebra of B.

Theorem 5.5. *Every Boolean algebra has a unique completion, up to isomorphism.*

Proof. First, we will prove that for a Boolean algebra A, there exists a complete Boolean algebra B such that $B = \bar{A}$. Consider $A^* \subseteq A$. If $q \not\leq p$ in A^*, then $q \cdot -p \neq 0$ in A. Since A^* is dense in A, there exists $r \in A^*$ such that $0 < r \leq q \cdot -p$. Then $r \leq q$ and $r \cdot p = 0$, so r and p are incompatible in A^*. Therefore A^* is a separative partial order. We will pick B to equal $RO(A^*)$ and let $h(p) = int\ cl\ u_p$. Then (h, B) is the completion of A^*.

Now, we will extend $h : A^* \longrightarrow B$ to f such that $f : A \longrightarrow B$ with $f(0) = 0$. If we can show that f is a Boolean homomorphism, then $f[A]$ is a dense subalgebra of B and B is the completion of $f[A]$.

Since A^* is separative, h is one-to-one. Then, since $f(0) = 0$ and $f[A] \subseteq B^*$, f is also one-to-one. We know $f(0_A) = 0_B$ and $f(1_A) = 1_B$. Consider $p, q \in A$. If $p \cdot q > 0$, then $f(p \cdot q) = u_{p \cdot q} = u_p \cap u_q$. But $f(p) \cdot f(q) = u_p \cap u_q$. So $f(p \cdot q) = f(p) \cdot f(q)$. If $p \cdot q = 0$, then $f(p \cdot q) = f(0) = 0$ and $f(p) \cdot f(q) = f(p) \cap f(q) = \emptyset$. Therefore $f(p) \cdot f(-p) = 0$.

Now if $p = 0$, then $f(p) + f(-p) = 0 + 1 = 1$ and if $-p = 0$, then $f(p) + f(-p) = 1 + 0 = 1$. So consider $p \neq 0$ and $-p \neq 0$. Since $h[A^*]$ is dense in B, then there exists $q \in A^*$ such that $h(q) \cdot h(p) = 0$ and $h(q) \cdot h(-p) = 0$. But $h(q) \cdot h(p) = 0 \implies h(q \cdot p) = 0 \implies q \cdot p = 0$. Similarly, $h(q) \cdot h(-p) = 0 \implies q \cdot -p = 0$. And since $p, -p \neq 0$, then $q = 0$. But this is a contradiction since $q \in A^*$. Therefore $f(p) + f(-p) = 1$. Then f preserves $\cdot$ and $-$ and so, $f : A \longrightarrow B$ is a homomorphism. Then $f[A]$ is a dense subalgebra of B since $h[A^*]$ is dense in B.

Now, to show uniqueness, let B and C be complete Boolean algebras and let A be a dense subalgebra of B and of C. Then A^* is a dense subset of B and C. Then $h : B \longrightarrow C$ is an isomorphism such that $h \restriction A = id_A$. □

Chapter 6

Conclusion

The structure of a Boolean algebra developed from partially ordered sets and lattices and the operations of least upper bound, greatest lower bound, and complementation were used to establish its characteristics. Atoms and ultrafilters are underlying elements of some Boolean algebras that lead to useful properties. By Stone's representation theorem for finite Boolean algebras, we concluded that every finite Boolean algebra is isomorphic to the power set of a finite set. We showed that the cellularity of a Boolean algebra is attained if it is singular by the Erdös-Tarski theorem. Lastly, we proved that, up to isomorphism, every Boolean algebra has a unique completion.

Bibliography

[Bel85] J. L. Bell. *Boolean-valued models and independence proofs in set theory*, volume 12 of *Oxford Logic Guides*. The Clarendon Press, Oxford University Press, New York, second edition, 1985. With a foreword by Dana Scott.

[DF99] David S. Dummit and Richard M. Foote. *Abstract algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, second edition, 1999.

[Dur00] John R. Durbin. *Modern algebra*. John Wiley & Sons, Inc., New York, fourth edition, 2000. An introduction.

[Gal13] Joseph A. Gallian. *Contemporary abstract algebra*. Brooks/Cole, Pacific Grove, CA, eighth edition, 2013.

[JW97] Winfried Just and Martin Weese. *Discovering modern set theory. II*, volume 18 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997. Set-theoretic tools for every mathematician.

[Kop89] Sabine Koppelberg. *Handbook of Boolean algebras. Vol. 1*. North-Holland Publishing Co., Amsterdam, 1989. Edited by J. Donald Monk and Robert Bonnet.

[Pap02] A. Papantonopoulou. *Algebra: Pure & Applied*. Prentice Hall, Inc., Upper Saddle River, NJ, 2002.

[Rud74] Sergiu Rudeanu. *Boolean functions and equations*. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1974. With a preface by Gr. C. Moisil.