Ministry of Higher Education and
Scientific Research
University of Basrah
College of Education for Pure
Sciences
Department of Mathematics

Boolean Algebra

Submitted to the Department of Mathematics, College of Education for Pure Sciences, and is part of the requirements for obtaining the Bachelors degree in Mathematics

By
Sajad Ahmed Jasim

Supervisor
Jasim Mohammed Jwad

2023 - 2024

Thanks

I extend my heartfelt gratitude to my parents and friends, whose unwavering support and encouragement have been my pillars of strength throughout this journey. Their belief in me has been a constant source of inspiration, driving me to strive for excellence. I am especially indebted to my supervisor, Jasim Mohammed Jwad, whose guidance, wisdom, and mentorship have been invaluable. His dedication to my project, insightful feedback, and unwavering belief in my capabilities have played a pivotal role in shaping my academic and personal growth. I am profoundly grateful for his patience, encouragement, and expertise, which have empowered me to overcome challenges and achieve milestones.

Contents

Introduction

In mathematics and mathematical logic, Boolean algebra is a branch of algebra distinguished by the values of its variables, typically represented as true and false, denoted as 1 and 0, respectively. Unlike elementary algebra, which operates with numerical values, Boolean algebra employs logical operators such as conjunction ($\wedge$), disjunction ($\vee$), and negation ($\sim$), whereas elementary algebra employs arithmetic operators like addition, multiplication, subtraction, and division. Boolean algebra provides a formal framework for describing logical operations, similar to how elementary algebra deals with numerical operations.

George Boole introduced Boolean algebra in his first book, "The Mathematical Analysis of Logic" (1847), further expounded in "An Investigation of the Laws of Thought" (1854). Henry M. Sheffer first proposed the term "Boolean algebra" in 1913, though Charles Sanders Peirce had earlier referred to it as "A Boolian Algebra with One Constant" in the first chapter of his work "The Simplest Mathematics" (1880). Boolean algebra has played a pivotal role in the advancement of digital electronics and is incorporated into all modern programming languages. It also finds applications in set theory and statistics.

Chapter 1

Basic Concepts

1.1 Relations

Definition 1.1.1 [1]. A ***relation*** between sets A and B is a subset R of $A \times B$. We read $(a, b) \in$ R as "a is related to b" and write a R b.

We will refer to any relation between a set S and itself, as in the next example, as a relation on S.

Example 1.1.2 . Consider the set of all integers $\mathbb{Z}$. Define a relation $\sim$ on $\mathbb{Z}$ (i.e. $\sim \subseteq \mathbb{Z} \times \mathbb{Z}$) such that for all $a, b \in \mathbb{Z}$ we have $a \sim b$ if and only if $a + b$ even, we see that $3 \sim 1$ and $2 \sim 4$ because $3 + 1$ and $2 + 4$ are both even.

Definition 1.1.3 [1]. A ***function*** ϕ mapping X into Y is a relation between X and Y with the property that each $x \in X$ appears as the first member of exactly one ordered pair $(x, y) \in \phi$. Such a function is also called map or mapping of X into Y. We write $\phi : X \longrightarrow Y$ and express $(x, y) \in \phi$ by $\phi(x) = y$. The domain of ϕ is the set X and the set Y is the codomain of ϕ. The range of ϕ is $\phi(X) = \{\phi(x) \mid x \in X\}$.

Example 1.1.4 . We can view the addition of real numbers as a function $+ : (\mathbb{R} \times \mathbb{R}) \longrightarrow \mathbb{R}$, that is, as a mapping of $\mathbb{R} \times \mathbb{R}$ into $\mathbb{R}$. For instant, the action of $+$ on $(2, 3) \in \mathbb{R} \times \mathbb{R}$ is given in function notation by $+\big((2, 3)\big) = 5$. In set notation we write $\big((2, 3), 5\big) \in +$. Of course our familiar notation is $2 + 3 = 5$.

1.2 Binary Operations

Definition 1.2.1 [1]. A ***binary operation*** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*\big((a, b)\big)$ of S by $a * b$.

Example 1.2.2 . The usual addition $+$ and the usual multiplication $\cdot$ are both binary operations on the set $\mathbb{R}$.

Definition 1.2.3 [1]. Let $*$ be a binary operation S and let H be a subset of S. The subset H is closed under $*$ if for all $a, b \in H$ we also have $a * b \in H$.

By our very definition of a binary operation $*$ on S, the set S is closed under $*$, but a subset may not be, as the following example shows.

Example 1.2.4 . Our usual addition $+$ on the set $\mathbb{R}$ does not induce a binary operation on the set $\mathbb{R}^*$ of nonzero real numbers because $2 \in \mathbb{R}^*$ and $-2 \in \mathbb{R}^*$, but $2 + (-2) = 0$ and $0 \notin \mathbb{R}^*$. Thus $\mathbb{R}^*$ is not closed under $+$.

Definition 1.2.5 [1]. A binary operation $*$ on a set S is *commutative* if (and only if) $a * b = b * a$, for all $a, b \in S$.

Definition 1.2.6 [1]. A binary operation $*$ on a set S is *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Example 1.2.7 . The usual addition $+$ and the usual multiplication $\cdot$ are both commutative and associative binary operations on the set $\mathbb{R}$.

1.3 Groups

Definition 1.3.1 [1]. A ***Group*** $(G, *)$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied

1. For all $a, b, c \in G$, we have

$$(a * b) * c = a * (b * c), \quad \textbf{associativity of } *$$

2. There is an element $e \in G$ such that for all $x \in G$,

$$e * x = x * e, \quad \textbf{identity elemente of } *$$

3. Corresponding to each element $a \in G$, there is an element $a' \in G$ such that,

$$a * a' = a' * a = e, \quad \textbf{inverse } a' \text{ of } a$$

Definition 1.3.2 [1]. A Group $(G, *)$ is ***abelian*** if its binary operation $*$ is commutative.

Example 1.3.3 . $(\mathbb{Z}, +)$, the group of integers with the regular addition $+$ and the identity 0 and for each $n \in \mathbb{Z}$ we know $n + (-n) = 0$ so the inverse of n is $-n$. Since the addition is commutative then $(\mathbb{Z}, +)$ is abelian group.

1.4 Rings

Definition 1.4.1 [6]. Let R be a nonempty set and let $+$ and $\cdot$ denote two binary operations on R, which we refer to as "addition" and "multiplication," respectively. Then $(R, +, \cdot)$ is called a ***ring*** if the following conditions hold

1. $(R, +)$ is a commutative (abelian) group.

2. $\cdot$ is associative. That is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

3. $\cdot$ is distributive over $+$. That is,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \qquad \text{for all } a, b, c \in R.$$

Notation

1. When no ambiguity exists we shall refer to the ring $(R, +, \cdot)$ simply as R.

2. The identity of $(R, +)$ is denoted by 0 and if there exists element $e \in R$ such that for all $x \in R$, $e \cdot x = x \cdot e = x$. We usually write 1 instead of e.

3. For all $x \in R$, the additive inverse of x is denoted by $-x$.

4. For all $x \in R$, the multiplicative inverse (if exist) is denoted by x^{-1}.

5. For all $x \in R$ the repeated addition n times is denoted by nx. That is

$$nx = \underbrace{x + x + \cdots + x}_{n-\text{times}}$$

and we use the power to denote the repeated multiplication n times ,

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n-\text{times}}$$

Example 1.4.2 . $(\mathbb{Z}, +, \cdot)$, the ring of integers with usual operations $+$ and $\cdot$, where the additive identity is 0 and the multiplicative identity is 1.

Example 1.4.3 . Let $\mathbb{Z}_n$ be the set of all residue classes modulo n positive integer. That is for each integer m,

$$[m] = \{k \in \mathbb{Z} \mid k = m + r \cdot n \text{ for some integer } r\}$$

then $\mathbb{Z}_n = \{[1], [2], \ldots, [n-1]\}$. For any $[a], [b] \in \mathbb{Z}_n$ define the two operations $+_n$ and $\cdot_n$ as follows :

$$[a] +_n [b] = [a + b],$$
$$[a] \cdot_n [b] = [a \cdot b].$$

Then $(\mathbb{Z}_n, +_n, \cdot_n)$ is a ring with the additive identity $[0] \in \mathbb{Z}_n$ and the multiplicative identity $[1] \in \mathbb{Z}_n$. For a simpler notation we will drop the brackets from the elements in $\mathbb{Z}_n$. Hence we have $\mathbb{Z}_n = \{1, 2, \ldots, n-1\}$.

Example 1.4.4 . Let X he a set and let $\mathcal{P}(X)$ be the collection of all subsets of X.

For any $A, B \in \mathcal{P}(X)$ we define $+$ and $\cdot$ as follows :

$$A + B = A \,\Delta\, B = (A - B) \cup (B - A),$$

$$A \cdot B = A \cap B.$$

Then $(\mathcal{P}(X), \Delta, \cap)$ is a ring with the set $\varnothing$ serving as the identity of $(\mathcal{P}(X), \Delta)$. The set X is the multiplication of the ring $\mathcal{P}(X)$.

1.5 Some Special Types of Rings

Definition 1.5.1 [6]. Let $(R, +, \cdot)$ be a ring. R is called a ***commutative ring*** if $x \cdot y = y \cdot x$ for all $x, y \in R$. Otherwise R is called noncommutative ring.

Definition 1.5.2 [6]. Let $(R, +, \cdot)$ be a ring. R is called a ***ring with identity*** if there exists an element $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$.

Examples 1.4.2, 1.4.3 and 1.4.4 are commutative rings with identity.

Definition 1.5.3 [6]. Let $(R, +, \cdot)$ be a ring and let $R^* = R - \{0\}$. Then R is called a ***Division ring*** if $(R^*, \cdot)$ is a group. If in addition, R is commutative, that is, $(R^*, \cdot)$ is an abelian group, then R is called a *field*.

In other words, a ring $(R, +, \cdot)$ be a field if every nonzero element in R has multiplicative inverse. In this case

Example 1.5.4 . The real number system, the rational number system and the complex number system are examples of fields.

Example 1.5.5 . Let p be a prime. Then $(\mathbb{Z}_p, +_p, \cdot_p)$ is a field.

1.6 Homomorphisms, Kernels, and Ideals

Definition 1.6.1 [6]. Let $(R, +, \cdot)$ be a ring. Let S be a nonempty subset of R. Then S is a ***subring*** of R if $(S, +, \cdot)$ is also a ring.

Example 1.6.2 . Since $\mathbb{Z} \subseteq \mathbb{R}$ and $(\mathbb{Z}, +, \cdot)$ is ring. Then $\mathbb{Z}$ is a subring of $\mathbb{R}$.

Definition 1.6.3 [6]. Let $(R, +, \cdot)$ be a ring. A nonempty subset I of R is an ***ideal*** of R if

1. I is a subring of R,

2. Whenever $i \in I$ and $r \in R$, then $i \cdot r \in I$ and $r \cdot i \in I$.

Example 1.6.4 . Let R be a ring. then the set $\{0\}$ is an ideal in R. Also R is an ideal in R.

Example 1.6.5 . Not every subring of a ring is an ideal. For example, let R be the ring of rational numbers. $\mathbb{Z}$ is a subring of R, but not an ideal in R, since $\frac{1}{2} \in R, 1 \in \mathbb{Z}$ but $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

Definition 1.6.6 [6]. Let $(R, +, \cdot)$ and $(T, \oplus, \odot)$ be rings. Let $f : R \longrightarrow T$ satisfy

a) $f(x + y) = f(x) \oplus f(y)$ b) $f(x \cdot y) = f(x) \odot f(y)$

for all $x, y \in R$. Then f is called a (ring) ***homomorphism*** from R to T.

Note : If the function f in the definition above is one-to-one and onto, then it is called ***isomorphism*** and we say R is isomorphic to T and we write $R \simeq T$

Definition 1.6.7 [6]. Let $f : R \to T$ be a homomorphism from the ring R to the ring T. We call the set $K = \{x \in R \mid f(x) = 0\}$ the kernel of f, denoted by $\ker f$

Theorem 1.6.8 [6]. *Let $f : R \to T$ be a homomorphism from the ring R to the ring T. Let $K = \ker f$. Then $(K, +, \cdot)$ is an ideal of $(R, +, \cdot)$*

Proof. Let $a, b \in K$ arbitrary elements. Then

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0$$

so $a-b \in K$. Hence K is an subring of R. Now let $r \in R$ and $k \in K$ be arbitrary elements. Then

$$f(r \cdot k) = f(r) \cdot f(k) = f(r) \cdot 0 = 0$$

Similarly we can show $f(k \cdot r) = 0$. Thus $r \cdot k \in K$, therefore K is an ideal in R. □

Definition 1.6.9 [6]. Let $(R, +, \cdot)$ be a ring and $(I, +, \cdot)$ be an ideal of the ring R, for each $a \in R$ define the left coset $a + I = \{a + i \mid i \in I\}$. Let R/I be the set of all cosets. Define the two operations on R/I as follows

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (a \cdot b) + I$$

Then $(R/I, +, \cdot)$ is called the quotient ring of R modulo the ideal I.

Theorem 1.6.10 [6]. *Let R and T be two ring. Let $f : R \to T$ be ring homomorphism. Then $R/\ker f \simeq f(R)$, where $f(R) = \{f(r) \mid r \in R\}$.*

Theorem 1.6.11 [6]. *Let R be a ring, I an ideal in R. Then there exists an onto homomorphism $f : R \to R/I$ defined by $f(r) = r + I$ such that $\ker f = I$. We call f the **natural homomorphism** from R to R/I. and denoted by nat_I.*

Proof. For all $a, b \in R$, we have

$$\text{nat}_I(a + b) = (a + b) + I = (a + I) + (b + I) = \text{nat}_I(a) + \text{nat}_I(b)$$

similarly

$$\text{nat}_I(a \cdot b) = (a \cdot b) + I = (a + I) \cdot (b + I) = \text{nat}_I(a) \cdot \text{nat}_I(b)$$

and clearly nat_I is onto mapping. Hence $\text{nat}_I : R \to R/I$ is a onto homomorphism.

Theorem 1.6.12 [6]. *Let R_1 and R_2 be two rings and let f be a homomorphism from R_1 onto R_2. Then f is an isomorphism if and only if $\ker f = \{0\}$.*

Proof. Let f be is isomorphism, then f is one to one mapping. Now let $a \in \ker f$ such that $a \neq 0$. We have

$$f(a) = 0 = f(0)$$

we conclude that $a = 0$ and this is a contradiction. Thus $\ker f = \{0\}$.
Now let $\ker f = \{0\}$ we prove f is one to one. Let $f(a) = f(b)$, we have

$$f(a) - f(b) = 0 \Longrightarrow f(a-b) = 0$$

Thus $a - b \in \ker f$, so $a - b = 0$, then, $a = b$, and therefore f is one to one. Hence it is isomorphism. □

Definition 1.6.13 [5]. An ideal in R generated by one element of R is capped the ***principle ideal***. The ideal generated by the element a is denoted by (a) and given by

$$(a) = \{r \cdot a \mid r \in R\}$$

Definition 1.6.14 [2]. A ***field*** is a commutative ring which contains for each element $a \neq 0$ an "inverse" element a^{-1} satisfying the equation $a \cdot a^{-1} = 1$.

Definition 1.6.15 [5]. An ideal I in a ring R is called a ***maximal ideal*** if $I \neq R$ and there exists no ideal J in R such that $I \subset J \subset R$.

Definition 1.6.16 [1]. An ideal $I \neq R$ in a commutative ring R is a ***prime ideal*** if $a \cdot b \in I$ implies either $a \in I$ or $b \in I$ for $a, b \in R$.

Theorem 1.6.17 [1]. *If R is a ring with identity, and I is an ideal of R containing the identity. Then $I = R$.*

Proof. Let $a \in R$ be arbitrary element, note that

$$a = \underbrace{a}_{\in R} \cdot \underbrace{1}_{\in I}$$

since I an ideal in R we conclude $a \in I$, then $I \subseteq R$. Consequently $I = R$. □

Theorem 1.6.18 [1]. *Every maximal ideal in a commutative ring R with identity is a prime ideal.*

Theorem 1.6.19 (Krull-Zorn) [4]. *In a commutative ring with identity, each proper ideal is contained in a maximal ideal.*

Theorem 1.6.20 [1]. *Let R be a commutative ring with identity. Then M is a maximal ideal of R if and only if R/M is a field.*

Chapter 2

Boolean Rings and Boolean Algebra

2.1 Boolean Rings

Definition 2.1.1 [4]. A Boolean ring $(R, +, \cdot)$ is a ring with identity in which every element is idempotent, that is, $a^2 = a$ for every $a \in R$.

Example 2.1.2 . The ring of the integers modulo 2, $(\mathbb{Z}_2, +_2, \cdot_2)$ forms a Boolean ring, since, $0^2 = 0 \cdot_2 0 = 0$ and $1^2 = 1 \cdot 1 = 1$.

Example 2.1.3 . The ring $(\mathcal{P}(X), \Delta, \cap)$ of subsets of a nonempty set X is easily verified to be a Boolean ring, since $A^2 = A \cap A = A$ for every $A \subseteq X$.

Theorem 2.1.4 [4]. *Every Boolean ring $(R, +, \cdot)$ is a commutative ring of characteristic 2.*

Proof. For every $a, b \in R$ we have

$$a + b = (a + b)^2 = a^2 + a \cdot b + b \cdot a + b^2 = a + a \cdot b + b \cdot a + b$$

then $a \cdot b + b \cdot a = 0$. In particular setting $a = b$ we get $2a = a + a = a^2 + a^2 = 0$, this shows that $\text{char}(R) = 2$. Now for every $a, b \in R$

$$\begin{aligned} a \cdot b &= a \cdot b + (a \cdot b + b \cdot a) \\ &= (a \cdot b + a \cdot b) + b \cdot a \\ &= 2(a \cdot b) + b \cdot a \\ &= b \cdot a \end{aligned}$$

Hence R is commutative. □

Theorem 2.1.5 [4]. *Let $(R,+,\cdot)$ be a Boolean ring , A proper ideal $(I,+,\cdot)$ of $(R,+,\cdot)$ is prime ideal if and only if it's maximal ideal.*

Proof. Assume I is maximal ideal then by Theorem 1.6.18 I is prime ideal. Conversely, let I be prime ideal and J ideal of R such that $I \subset J \subseteq R$, we want to prove $J = R$
Now, consider any $x \in J - I$. Since $x = x^2$, it implies $x(1-x) = 0 \in I$. Using the fact I is a prime ideal with $x \notin I$, we conclude

$$1 - x \in I \subset J$$

As both elements x and $1-x$ lie in J , it follows that,

$$1 = x + (1-x) \in J$$

The ideal J thus contains the identity , and consequently $J = R$. □

Theorem 2.1.6 [4]. *A Boolean ring $(R,+,\cdot)$ is a field if and only if $(R,+,\cdot) \simeq (\mathbb{Z}_2,+_2,\cdot_2)$*

Proof. ($\Leftarrow$) Let $(R,+,\cdot) \simeq (\mathbb{Z}_2,+_2,\cdot_2)$, then $(R,+,\cdot)$ is a field since $(\mathbb{Z}_2,+_2,\cdot_2)$ is itself a field.
($\Rightarrow$) Let $(R,+,\cdot)$ be a Boolean field, then for every nonzero element $x \in R$ we have :

$$x = x \cdot 1 = x \cdot (x \cdot x^{-1}) = x^2 \cdot x^{-1} = x \cdot x^{-1} = 1$$

Then the only nonzero element in R is $1 \Longrightarrow R = \{0,1\} \simeq \mathbb{Z}_2$ by the homomorphism $\phi : R \longrightarrow \mathbb{Z}_2$ where $\phi(0) = 0$ and $\phi(1) = 1$. □

Corollary 2.1.7 [4]. *A proper ideal $(I,+,\cdot)$ of the Boolean ring $(R,+,\cdot)$ is a maximal ideal if and only if $(R/I,+,\cdot) \simeq (\mathbb{Z}_2,+_2,\cdot_2)$*

Proof. First we notice that R/I is itself Boolean ring since,

$$(x+I)^2 = x^2 + I = x + I \ , \forall \ x \in R$$

By Theorem 1.6.20 we know I is a maximal ideal if and only if R/I is a field and using Theorem 2.1.6 we conclude that I is a maximal ideal if and only if $R/I \simeq \mathbb{Z}_2$. □

Lemma 2.1.8 [4]. *Let $(R, +, \cdot)$ be a Boolean ring. For each nonzero element $x \in R$ there exists a homomorphism ϕ from $(R, +, \cdot)$ onto the field $(\mathbb{Z}_2, +_2, \cdot_2)$ such that $\phi(x) = 1$*

Proof. Let I be the principle ideal generated by $1 + x$ that is

$$I = (1+x) = \{r \cdot (1+x) : r \in R\}$$

I is proper ideal , since $1 \notin I$ because if so , then for some $r \in R$ we have

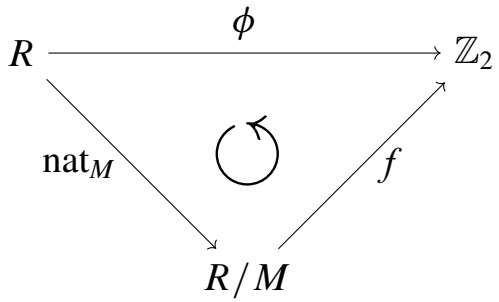
$$1 = r \cdot (1+x) = r \cdot (1+x)^2 = [r \cdot (1+x)] \cdot (1+x) = 1 \cdot (1+x)$$

$$\Longrightarrow 1 = 1 + x \Longrightarrow x = 0$$

which is contradiction (since $x \neq 0$)

Now since I is proper ideal of R by Theorem 1.6.19 there is a maximal ideal M of R such that $I \subseteq M$, so by the corollary 2.1.7 we have $R/M \simeq \mathbb{Z}_2$ by some homomorphism $f : R/M \to \mathbb{Z}_2$

Now define the function $\phi : R \to \mathbb{Z}_2$ by taking $\phi = f \circ \text{nat}_M$ where nat_M is the natural homomorphism from R onto R/M.



We now show ϕ is onto homomorphism , so for every $a, b \in R$:

with respect to addition :

$$\phi(a+b) = f(\text{nat}_M(a+b)) = f(\text{nat}_M(a)+\text{nat}_M(b)) = f(\text{nat}_M(a))+_2 f(\text{nat}_M(b))$$
$$\Longrightarrow \phi(a+b) = \phi(a) +_2 \phi(b)$$

with respect to multiplication :

$$\phi(a \cdot b) = f(\text{nat}_M(a \cdot b)) = f(\text{nat}_M(a) \cdot \text{nat}_M(b)) = f(\text{nat}_M(a)) \cdot_2 f(\text{nat}_M(b))$$
$$\Longrightarrow \phi(a \cdot b) = \phi(a) \cdot_2 \phi(b)$$

Now let $k \in \mathbb{Z}_2$ be arbitrary , since f is onto , then there exists $x \in R$ such that $f(x+M) = k$ so we have :

$$\forall\, k \in \mathbb{Z}_2, \exists\, a \in R : \phi(a) = f(\text{nat}_M(a)) = f(a+M) = k.$$

So we showed that ϕ is onto homomorphism. Now since $1 + x \in I \subseteq M \Longrightarrow$ the coset $(1+x)+M = M$ so that

$$1 +_2 \phi(x) = \phi(1+x) = f(\text{nat}_M(1+x)) = f((1+x)+M) = f(M) = 0$$
$$\Longrightarrow \phi(x) = 1$$

□

Theorem 2.1.9 (Stone Representation Theorem)[4]. *Every Boolean ring* $(R, +, \cdot)$ *is isomorphic to a ring of subsets of some fixed set.*

Proof. Let

$$H = \{f : R \longrightarrow \mathbb{Z}_2 \mid f \text{ is homomorphism }\}$$

Now, define the function h from the ring $(R, +, \cdot)$ into the ring $(\mathcal{P}(H), \Delta, \cap)$ such that

$$h(x) = \{f \in H \mid f(x) = 1\} \text{ for every } x \in R$$

Now for every $x, y \in R$ if we assume $f : R \longrightarrow \mathbb{Z}_2$ is homomorphism then,

$$\begin{aligned} f \in h(x \cdot y) &\iff f(x \cdot y) = 1 \\ &\iff f(x) \cdot_2 f(y) = 1 \\ &\iff f(x) = 1 \text{ and } f(y) = 1 \\ &\iff f \in h(x) \text{ and } f \in h(y) \\ &\iff f \in h(x) \cap h(y) \end{aligned}$$

Therefore,

$$h(x \cdot y) = h(x) \cap h(y)$$

Similarly for the addition , but first we observe that

$$f \notin h(x) \iff f(x) \neq 1 \iff f(x) = 0$$

So we have,

$$\begin{aligned} f \in h(x + y) &\iff f(x + y) = 1 \\ &\iff f(x) +_2 f(y) = 1 \\ &\iff (f(x) = 1 \text{ and } f(y) = 0) \text{ or } (f(x) = 0 \text{ and } f(y) = 1) \\ &\iff (f \in h(x) \text{ and } f \notin h(y)) \text{ or } (f \notin h(x) \text{ and } f \in h(y)) \\ &\iff f \in h(x) \ \Delta \ h(y) \end{aligned}$$

Therefore,

$$h(x + y) = h(x) \ \Delta \ h(y)$$

Hence h is homomorphism. Now to prove h is one-to-one we find the kernel

$$\ker(h) = \{x \in R \mid h(x) = \varnothing\}$$

but $h(x) = \varnothing$ if and only if $x = 0$ by Lemma 2.1.8 $\implies \ker(h) = \{0\}$ Hence R is isomorphic to a subring of $(\mathcal{P}(H), \Delta, \cap)$ namely the image of R under the mapping h

$$(R, +, \cdot) \simeq (h(R), \Delta, \cap)$$

□

2.2 Boolean Algebra

Definition 2.2.1 [4]. A Boolean Algebra is mathematical system $(B, \vee, \wedge)$ consisting of a nonempty set B and two binary operations $\vee$ and $\wedge$ defined on B such that:

(P_1) Each of the operations $\vee$ and $\wedge$ is commutative; that is,

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a \quad \text{for all } a, b \in B.$$

(P_2) Each operation is distributive over the other; that is,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad \text{for all } a, b, c \in B$$

(P_3) There exist distinct identity elements 0 and 1 relative to the operations $\vee$ and $\wedge$, respectively; that is,

$$a \vee 0 = a, \quad a \wedge 1 = a \quad \text{for all } a \in B.$$

(P_4) For each element $a \in B$, there exists an element $a' \in B$, called the complement of a, such that

$$a \vee a' = 1, \quad a \wedge a' = 0$$

.

Example 2.2.2 . Let X be a nonempty set and consider the system $(\mathcal{P}(X), \cup, \cap)$

(P_1) $A \cup B = B \cup A, \quad A \cap B = B \cap A \quad$ for all $A, B \subseteq X$

(P_2) For all $A, B, C \subseteq X$

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

(P_3) For all $A \subseteq X$ we have,

$$A \cap X = A, \quad A \cup \varnothing = A$$

(P_4) For each $A \subseteq X$ we can take $A' = X - A$ since

$$A \cup (X - A) = X, \quad A \cap (X - A) = \varnothing$$

2.3 The Relation $\leq$

Definition 2.3.1 [2]. In a Boolean algebra $(B, \vee, \wedge)$. Let $\leq$ be a relation defined on B such that for each $a, b \in B$

$$a \leq b \longleftrightarrow a \wedge b = a$$

Note 1: It is clear to see that $a \wedge b \leq a$, since

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

Note 2: This definition inspired from set theory as we will see in the next example.

Example 2.3.2 . In the Boolean algebra $(\mathcal{P}(X), \cup, \cap)$ we define the relation $\leq$ to be the inclusion since, for each $A, B \subseteq X$ we have

$$A \subseteq B \longleftrightarrow A \cap B = A$$

2.4 Some Theorems and Results

Theorem 2.4.1 [4]. *In any Boolean algebra $(B, \vee, \wedge)$, the following properties hold*

1. *The elements* 0 *and* 1 *are unique*
2. *For each $a \in B$: $a \vee a = a, \quad a \wedge a = a$*
3. *For each element $a \in B$: $a \vee 1 = 1, \quad a \wedge 0 = 0$*
4. *For each $a, b \in B$:*

$$a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$$

Proof.

1. Suppose there are other identity elements for the operations $\vee$ and $\wedge$ say $\bar{0}$ and $\bar{1}$ respectively, that is,

$$a \wedge \bar{1} = a, \quad a \vee \bar{0} = a \quad \forall a \in B$$

So we have

$$0 = 0 \vee \bar{0} = \bar{0} \vee 0 = \bar{0}$$

and

$$1 = 1 \wedge \bar{1} = \bar{1} \wedge 1 = \bar{1}$$

2.

$$\begin{aligned} a &= a \vee 0 && (\text{by } P_3) \\ &= a \vee (a \wedge a') && (\text{by } P_4) \\ &= (a \vee a) \wedge (a \vee a') && (\text{by } P_2) \\ &= (a \vee a) \wedge 1 && (\text{by } P_4) \\ &= a \vee a && (\text{by } P_3) \end{aligned}$$

Similarly

$$\begin{aligned} a &= a \wedge 1 && (\text{by } P_3) \\ &= a \wedge (a \vee a') && (\text{by } P_4) \\ &= (a \wedge a) \vee (a \wedge a') && (\text{by } P_2) \\ &= (a \wedge a) \wedge 0 && (\text{by } P_4) \\ &= a \wedge a && (\text{by } P_3) \end{aligned}$$

3.

$$\begin{aligned} 1 &= a \vee a' && (\text{by } P_4)\\ &= a \vee (a' \wedge 1) && (\text{by } P_3)\\ &= (a \vee a') \wedge (a \vee 1) && (\text{by } P_2)\\ &= 1 \wedge (a \vee 1) && (\text{by } P_4)\\ &= a \vee 1 && (\text{by } P_3) \end{aligned}$$

Similarly

$$\begin{aligned} 0 &= a \wedge a' && (\text{by } P_4)\\ &= a \wedge (a' \vee 1) && (\text{by } P_3)\\ &= (a \wedge a') \vee (a \vee 1) && (\text{by } P_2)\\ &= 1 \vee (a \wedge 1) && (\text{by } P_4)\\ &= a \wedge 1 && (\text{by } P_3) \end{aligned}$$

4.

$$\begin{aligned} a &= a \wedge 1 && (\text{by } P_3)\\ &= a \wedge (b \vee 1) && (\text{by 3})\\ &= (a \wedge b) \vee (a \wedge 1) && (\text{by } P_2)\\ &= (a \wedge b) \vee a && (\text{by } P_3)\\ &= a \vee (a \wedge b) && (\text{by } P_1) \end{aligned}$$

Similarly

$$\begin{aligned} a &= a \vee 0 && (\text{by } P_3)\\ &= a \vee (b \wedge 0) && (\text{by 3})\\ &= (a \vee b) \wedge (a \vee 0) && (\text{by } P_2)\\ &= (a \vee b) \wedge a && (\text{by } P_3)\\ &= a \wedge (a \vee b) && (\text{by } P_1) \end{aligned}$$

□

Theorem 2.4.2 [4]. *In any Boolean algebra* $(B, \vee, \wedge)$ *each of the operations* $\vee$ *and* $\wedge$ *is associative, that is*

$$a \vee (b \vee c) = (a \vee b) \vee c,$$
$$a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad \textit{for all } a, b, c \in B$$

Proof. First set $x = a \vee (b \vee c)$ and $y = (a \vee b) \vee c$, we want to prove $x = y$. Note that

$$\begin{aligned} a \wedge x &= (a \wedge a) \vee [a \wedge (b \vee c)] && (\text{by } P_2) \\ &= a \vee [a \wedge (b \vee c)] && [\text{by Theorem 2.4.1(2)}] \\ &= a && [\text{by Theorem 2.4.1(4)}] \end{aligned}$$

and also

$$\begin{aligned} a \wedge y &= [a \wedge (a \vee b)] \vee (a \wedge c) && (\text{by } P_2) \\ &= a \vee (a \wedge c) && [\text{by Theorem 2.4.1(4)}] \\ &= a && [\text{by Theorem 2.4.1(4)}] \end{aligned}$$

Therefore $a \wedge x = a \wedge y$. Now,

$$\begin{aligned} a' \wedge x &= (a' \wedge a) \vee [a' \wedge (b \vee c)] && (\text{by P})_2 \\ &= 0 \vee [a' \wedge (b \vee c)] && (\text{by } P_1, P_4) \\ &= a' \wedge (b \vee c) && (\text{by } P_3) \end{aligned}$$

and also

$$\begin{aligned} a' \wedge y &= [a' \wedge (a \vee b)] \vee (a' \wedge c) && (\text{by } P_2) \\ &= [(a' \wedge a) \vee (a' \wedge b)] \vee (a' \wedge c) && (\text{by } P_2) \\ &= [0 \vee (a' \wedge b)] \vee (a' \wedge c) && (\text{by } P_1, P_4) \\ &= (a' \wedge b) \vee (a' \wedge c) && (\text{by } P_3) \\ &= a' \wedge (b \vee c) && (\text{by } P_2) \end{aligned}$$

Therefore $a' \wedge x = a' \wedge y$, we conclude that

$$\begin{aligned}
(a \wedge x) \vee (a' \wedge x) &= (a \wedge y) \vee (a' \wedge y) \\
(a \wedge a') \vee x &= (a \vee a') \vee y && (\text{by } P_1, P_2) \\
1 \vee x &= 1 \vee y && (\text{by } P_4) \\
x &= y && (\text{by } P_3)
\end{aligned}$$

The same steps can be applied on the operation $\wedge$. □

Theorem 2.4.3 [4]. *In any Boolean algebra $(B, \vee, \wedge)$ the following hold*

1. *Each element $a \in B$ has unique complement.*
2. *For each element $a \in B$, $a'' = a$; where $a'' = (a')'$.*
3. *$0' = 1$ and $1' = 0$.*
4. *For all $a, b \in B$,*

$$(a \vee b)' = a' \wedge b', \quad (a \wedge b)' = a' \vee b'$$

Proof.

1. Assume there are two elements x and y such that,

$$a \vee x = 1, \quad a \wedge x = 0$$
$$a \vee y = 1, \quad a \wedge y = 0$$

Then we have

$$\begin{aligned}
x &= x \wedge 1 && (\text{by } P_3) \\
&= x \wedge (a \vee y) && (\text{by hypothesis}) \\
&= (x \wedge a) \vee (x \wedge y) && (\text{by } P_2) \\
&= (a \wedge x) \vee (x \wedge y) && (\text{by } P_1) \\
&= 0 \vee (x \wedge y) && (\text{by hypothesis}) \\
&= x \wedge y && (\text{by } P_3)
\end{aligned}$$

Similarly we can show that $y = y \wedge x = x \wedge y$. Hence $x = y$

2. From the definition of the complement of a, $a \vee a' = 1$ and $a \wedge a' = 0$. Hence by P_1,

$$a' \vee a = 1 \quad \text{and} \quad a' \wedge a = 0$$

From this, we conclude,

$$a'' = (a')' = a$$

3. By P_3 we have,

$$0 \vee 1 = 1, \quad 0 \wedge 1 = 0$$

Hence

$$0' = 1, \quad \text{and then } 0 = 0'' = 1'$$

4. Since the complement is unique, it is enough to show,

$$(a \vee b) \vee (a' \wedge b') = 1, \quad (a \vee b) \wedge (a' \wedge b') = 0$$

Now,

$$\begin{aligned}(a \vee b) \vee (a' \wedge b') &= [(a \vee b) \vee a'] \wedge [(a \vee b) \vee b'] \\ &= [(a \vee a') \vee b] \wedge [a \vee (b \vee b')] \\ &= (1 \wedge b) \wedge (a \vee 1) \\ &= 1 \wedge 1 \\ &= 1\end{aligned}$$

Further

$$\begin{aligned}(a \vee b) \wedge (a' \wedge b') &= (a' \wedge b') \wedge (a \vee b) \\ &= [(a' \wedge b') \wedge a] \wedge [(a' \wedge b') \wedge b] \\ &= [(a' \wedge a) \wedge b'] \wedge [a' \wedge (b' \wedge b)] \\ &= (0 \wedge b') \wedge (a' \vee 0) \\ &= 0 \wedge 0 \\ &= 0\end{aligned}$$

Hence $(a \vee b)' = a' \wedge b'$. Note that

$$(a' \vee b')' = a'' \wedge b'' = a \wedge b$$

so we get

$$(a \wedge b)' = (a' \vee b')'' = a' \vee b'$$

□

Corollary 2.4.4 [3]. *In any Boolean algebra* $(B, \vee, \wedge)$ *we have for all* $x, y \in B$

$$x \leq y \longleftrightarrow y' \leq x'$$

Proof. Let $x \leq y$, then, $x \wedge y = x$. Now

$$\begin{aligned}x' \wedge y' &= (x \wedge y)' \wedge y' \\ &= (x' \vee y') \wedge y' \\ &= y'\end{aligned}$$

so, $y' \leq x'$. Now let $y' \leq x'$, then from first direction we have $x'' \leq y''$. Hence $x \leq y$ □

Theorem 2.4.5 [3]. *In any Boolean algebra* $(B, \vee, \wedge)$ *we have for all* $x, y \in B$

$$x \leq y \longleftrightarrow x \wedge y' = 0$$

Proof. Let $x \leq y$, then, $x \wedge y = x$. Now

$$\begin{aligned} x \wedge y' &= (x \wedge y) \wedge y' \\ &= x \wedge (y \wedge y') \\ &= x \wedge 0 \\ &= 0 \end{aligned}$$

Now let $x \wedge y' = 0$, then we have

$$\begin{aligned} x \wedge y &= (x \wedge y) \vee 0 \\ &= (x \wedge y) \vee (x \wedge x') \\ &= x \wedge (y \vee x') \\ &= x \wedge (x \wedge y')' \\ &= x \wedge 0' \\ &= x \wedge 1 \\ &= x \end{aligned}$$

Hence $x \leq y$ □

2.5 Boolean Homomorphism

Definition 2.5.1 [3]. Let $(B_1, \vee_1, \wedge_1)$ and $(B_2, \vee_2, \wedge_2)$ be Boolean algebras then the function $f : B_1 \longrightarrow B_2$ is called *Boolean homomorphism* if the following hold

1. $f(x \vee_1 y) = f(x) \vee_2 f(y)$, for all $x, y \in B_1$
2. $f(x \wedge_1 y) = f(x) \wedge_2 f(y)$, for all $x, y \in B_1$
3. $f(x') = [f(x)]'$, for all $x \in B_1$

Notes

1. If the function in the definition above is bijective (one to one and onto), then, it is called *Boolean isomorphism* and we write $B_1 \simeq_b B_2$

2. For a simpler notation, we will note the identities of B_1 and B_2 by 0 and 1 for the operations $\vee_1, \vee_2$ and $\wedge_1, \wedge_2$ respectively.

Theorem 2.5.2 [3]. *Let $f : B_1 \longrightarrow B_2$ be a Boolean homomorphism, then,*

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

2. *for all $x, y \in B_1$, if $x \leq y$ then $f(x) \leq f(y)$*

Proof.

1. Note that

$$\begin{aligned} f(0) &= f(0 \wedge_1 0') \\ &= f(0) \wedge_2 f(0') \\ &= f(0) \wedge_2 [f(0)]' \\ &= 0 \end{aligned}$$

   Similarly

$$\begin{aligned} f(1) &= f(1 \vee_1 1') \\ &= f(1) \vee_2 f(1') \\ &= f(1) \vee_2 [f(1)]' \\ &= 0 \end{aligned}$$

2. Let $x \leq y$, then it follows that

$$\begin{aligned} &\Longrightarrow x \wedge y = x \\ &\Longrightarrow f(x \wedge_1 y) = f(x) \\ &\Longrightarrow f(x) \wedge_2 f(y) = f(x) \\ &\Longrightarrow f(x) \leq f(y) \end{aligned}$$

□

2.6 Finite Boolean Algebra

In this section we will classify all the finite Boolean algebras up to isomorphism

Definition 2.6.1 [7]. A Boolean algebra $(B, \vee, \wedge)$ is a finite Boolean algebra if B contains a finite number of elements.

Definition 2.6.2 [7]. In a Boolean algebra $(B, \vee, \wedge)$. An element $a \in B$ called an *atom* if $a \neq 0$ and there is no nonzero element $b \in B$ distinct from a such that $b \leq a$.

Note : If a is atom and since $a \wedge b \leq a$ then it follows that $a \wedge b = 0$ or $a \wedge b = a$, so the definition of the atom is equivalent to say $a \leq b$ or $a \wedge b = 0$.

Lemma 2.6.3 [7]. *In a Boolean algebra $(B, \vee, \wedge)$. If $a \in B$ is an atom, then for all $b, c \in B$*

1. *If $a \leq b \wedge c \Longrightarrow a \leq b$ and $a \leq c$*
2. *If $a \leq b \vee c \Longrightarrow a \leq b$ or $a \leq c$*

Proof.

1. Let $a \leq b \wedge c$, then, $a \wedge (b \wedge c) = a$, so

$$\begin{aligned} a \wedge b &= [a \wedge (b \wedge c)] \wedge b \\ &= a \wedge [(b \wedge c) \wedge b] \\ &= a \wedge (b \wedge c) \\ &= a \end{aligned}$$

   Hence $a \leq b$, similarly we can show that $a \leq c$.

2. Let $a \leq b \vee c$, then, $a \wedge (b \vee c) = a$. Suppose that $a \not\leq b$ and $a \not\leq c$, and since a is atom we get $a \wedge b = 0$ and $a \wedge c = 0$

$$(a \wedge b) \vee (a \wedge c) = 0$$

$$a \wedge (b \vee c) = 0$$

Which is contradiction. Hence $a \leq b$ or $a \leq c$ □

Lemma 2.6.4 [7]. *Let $(B, \vee, \wedge)$ be a Boolean algebra and $a_1, a_2 \in B$ be atoms. Then either $a_1 = a_2$ or $a_1 \wedge a_2 = 0$.*

Proof. Since a_1 is an atom in B. Then either $a_1 \leq a_2$ or $a_1 \wedge a_2 = 0$, therefore either $a_1 \wedge a_2 = a_1$ or $a_1 \wedge a_2$ similarly for a_2, that is, $a_2 \wedge a_1 = a_2$ or $a_1 \wedge a_2 = 0$. In conclusion using P_1 we have either $a_1 = a_2$ or $a_1 \wedge a_2 = 0$. □

Lemma 2.6.5 [7]. *Let $(B, \vee, \wedge)$ be a finite Boolean algebra. If b is a nonzero element of B, then there is an atom a in B such that $a \leq b$.*

Proof. If b is an atom, let $a = b$. Otherwise, choose an element b_1, not equal to 0 or b, such that $b_1 \leq b$. We are guaranteed that this is possible since b is not an atom. If b_1 is an atom, then we are done. If not, choose b_2 , not equal to 0 or b_1 , such that $b_2 \leq b_1$. Again, if b_2 is an atom, let $a = b_2$. Continuing this process, we can obtain a chain

$$0 \leq \cdots \leq b_3 \leq b_2 \leq b_1 \leq b$$

Since B is a finite Boolean algebra, this chain must be finite. That is, for some k, b_k is an atom. Let $a = b_k$ □

Lemma 2.6.6 [7]. *Let $(B, \vee, \wedge)$ be a Boolean algebra and $b, c \in B$ such that $b \not\leq c$. Then there exists an atom $a \in B$ such that $a \leq b$ and $a \not\leq b$.*

Proof. By Theorem 2.4.5 we have $b \wedge c' \neq 0$. Hence by Lemma 2.6.5 there exists an atom a such that $a \leq b \wedge b'$, therefore by Lemma 2.6.3, $a \leq b$ and $a \leq c'$. Hence $a \wedge c = 0$. Then $a \not\leq c$. □

Lemma 2.6.7 [7]. *Let $(B, \vee, \wedge)$ be a finite Boolean algebra and let $b \in B$ not equal to 0. Let $a_1, a_2, \ldots, a_n$ be the atoms of B such that $a_i \leq b$. Then $b = a_1 \vee a_2 \vee \cdots \vee a_n$.*

Proof. Let $b_1 = a_1 \vee a_2 \vee \cdots \vee a_n$. Since $a_i \leq b$ for each i, then, $a_i \wedge b = a_i$. So

$$\begin{aligned} b_1 \wedge b &= (a_1 \vee \cdots \vee a_n) \wedge b \\ &= (a_1 \wedge b) \vee \cdots \vee (a_n \wedge b) \\ &= a_1 \vee \cdots \vee a_n \\ &= b_1 \end{aligned}$$

Hence $b_1 \leq b$. Assume $b \not\leq b_1$. Then there exists an atom $a \in B$ such that $a \leq b$ and $a \not\leq b_1$. Since a is an atom and $a \leq b$, it follows that, $a = a_k$ for some k. So

$$\begin{aligned} a \wedge b_1 &= a_k \wedge (a_1 \vee \cdots \vee a_k \vee \cdots \vee a_n) \\ &= (a_k \wedge a_1) \vee \cdots \vee (a_k \vee a_k) \vee \cdots \vee (a_k \wedge a_n) \\ &= 0 \vee 0 \vee \cdots \vee a_k \vee \cdots \vee 0 \\ &= a_k \\ &= a \end{aligned}$$

Therefore $a \leq b_1$. This is a contradiction. Hence $b \leq b_1$, we conclude

$$b = b \wedge b_1 = b_1 \wedge b = b_1$$

□

Theorem 2.6.8 (Representation Theorem)[3]. *Let $(B, \vee, \wedge)$ be a finite Boolean algebra and let A denote the set of all atoms in B. Then B is isomorphic to $\mathcal{P}(A)$.*

Proof. Let $v \in B$ be an arbitrary element and let $A(v) := \{a \in A \mid a \leq v\}$. Now define the function

$$h : B \longrightarrow \mathcal{P}(A)\,; \quad h(v) = A(v)$$

We show h is Boolean homomorphism. For an atom $a \in B$ and for $v, w \in B$ we

have

$$\begin{aligned} a \in A(v \wedge w) &\iff a \leq v \wedge w \\ &\iff a \leq v \quad \text{and} \quad a \leq w \\ &\iff a \in A(v) \quad \text{and} \quad a \in A(w) \\ &\iff a \in A(v) \cap A(w) \end{aligned}$$

This shows $h(v \wedge w) = h(v) \cap h(w)$. Similarly

$$\begin{aligned} a \in A(v \vee w) &\iff a \leq v \vee w \\ &\iff a \leq v \quad \text{or} \quad a \leq w \\ &\iff a \in A(v) \quad \text{or} \quad a \in A(w) \\ &\iff a \in A(v) \cup A(w) \end{aligned}$$

This shows $h(v \vee w) = h(v) \cup h(w)$. Finally

$$\begin{aligned} a \in A(v') \iff a \leq v' &\iff a \wedge v = 0 \\ &\iff a \not\leq v \\ &\iff a \in A - A(v) \end{aligned}$$

Hence $h(v') = A(v') = A - A(v) = A - h(v) = [h(v)]'$. Since B is finite we know $A(v)$ will be also finite say $A(v) = \{a_1, a_2, \ldots, a_n\}$. Now by Lemma 2.6.7 we can write v as $v = a_1 \vee a_2 \vee \cdots \vee a_n$, Let $A(v) = A(w)$, then $a_i \leq w$ for each i, so

$$\begin{aligned} v \wedge w &= (a_1 \vee \cdots \vee a_n) \wedge w \\ &= (a_1 \wedge w) \vee \cdots \vee (a_n \wedge w) \\ &= a_1 \vee \cdots \vee a_n \\ &= v \end{aligned}$$

Similarly we can show $w \wedge v = w$. Hence $v = w$. Therefore h is one to one map. To show h is onto let $C \subseteq A$ say $C = \{c_1, c_2, \ldots, c_k\}$. Let $x = c_1 \vee \cdots \vee c_k$, we

need to show $A(x) = C$. If $a \in B$ an atom, then,

$$\begin{aligned} a \in A(x) &\iff a \leq x \\ &\iff a \wedge x = a \\ &\iff a \wedge (c_1 \vee \cdots \vee c_k) = a \\ &\iff (a \wedge c_1) \vee \cdots \vee (a \wedge c_k) = a \\ &\iff a = c_j, \quad \text{for some } j \\ &\iff a \in C \end{aligned}$$

So $A(x) = C$. Hence h is onto so it is isomorphism, i.e $B \simeq_b P(A)$. □

Conclusion

In conclusion of our research, we have acquainted ourselves with two important algebraic structures in mathematics: the Boolean ring and the Boolean algebra. Additionally, we have demonstrated key results related to them. We have observed how every Boolean ring is isomorphic to the ring of power sets, but not entirely so for Boolean algebras, where we have seen that only finite Boolean algebras possess this property.

References

[1] John B.Fraleigh. *A First Course in Abstract Algebra*. Addison-Wasley, 2003.

[2] Garrett Birkhoff and Saunders Mac Lane. *A Survey of Modern Algebra*. A K Paters CRC Press, 2010.

[3] Rudolf Lidl and Günter Pilz. *Applied Abstract Algebra*. Springer, 1998.

[4] David M.Burton. *Introduction to Modern Algebra*. Addison-Wasley, 1967.

[5] N. McCoy. *The Theory of Rings*. New York:Mocmillan, 1964.

[6] Hiram Paley. *A First Course in Abstract Algebra*. International Thomson Publishing, 1966.

[7] Thomas W.Judson. *Abstract Algebra Theory and Applications*. PWS Pub co, 1993.