A CONNECTION BETWEEN ALGEBRAIC STRUCTURES AND PROPOSITIONAL LOGIC

By

Wanda Ortiz Hernández

A project submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS

December, 2006

Approved by:

Dr. Luis F. Cáceres, Ph.D President, Graduate Committee	Date
Dr. Gabriele Castellini, Ph.D Member, Graduate Committee	Date
Dr. Balchandra Oltikar, Ph.D Member, Graduate Committee	Date
Dr. Raúl Macchiavelli, Ph.D Representative of Graduate Studies	Date
Dr. Luis F. Cáceres, Ph.D Chairperson of the Department	Date

Abstract of Project Presented to the Graduate School
of the University of Puerto Rico in Partial Fulfillment of the
Requirements for the Degree of Master of Science

A CONNECTION BETWEEN ALGEBRAIC STRUCTURES AND PROPOSITIONAL LOGIC

By

Wanda Ortiz Hernández

December 2006

Chair: Dr. Luis F. Cáceres
Major Department: Mathematics

In this project, the relationship between propositional logic using theories and models, and algebraic structures, such as groups, rings, lattices, R-modules and algebras, including Boolean Algebras, has been studied.

From Caceres [1], we have that given a ring R, a one to one correspondence exists between the ideals of R and the models associated with the sentential theory $T(R)$. A similar approach was followed to show that given a group G, and the associated sentential theory $T(G)$, a one to one correspondence exists between the subgroup of G and the models associated with the theory $T(G)$. Several results were presented for lattice structures, L, and Boolean Algebras, B. Their associated sentential theories, $T(L)$ and $T(B)$, were also established. Concrete examples to support these results were presented and explained. For some structures, the cardinality of its corresponding propositional theory was studied and a formula for its calculation was established.

Resumen de Proyecto Presentado a Escuela Graduada
de la Universidad de Puerto Rico como requisito parcial de los
Requerimientos para el grado de Maestría en Ciencias

UNA CONEXIÓN ENTRE ESTRUCTURAS ALGEBRAICAS Y LA LÓGICA PROPOSICIONAL

Por

Wanda Ortiz Hernández

Diciembre 2006

Consejero: Dr. Luis F. Cáceres
Departamento: Matemáticas

En este proyecto se estudió la relación entre la lógica proposicional utilizando teorías y modelos, y estructuras algebraicas como: grupos, anillos, retículos, R-módulos y álgebras , incluyendo álgebras de Boole.

De Cáceres [1] tenemos que dado un anillo R, existe una correspondencia uno a uno entre los ideales de R y los modelos asociados a la teoría sentencial T(R). Utilizando un procedimiento similar se demostró que dado un grupo G y la teoría sentencial asociada, T(G), existe una correspondencia uno a uno entre los subgrupos de G y los modelos asociados con la teoría, T(G). Para los retículos, L, y las álgebras de Boole, B, se presentaron varios resultados y propiedades. Además, se establecieron sus teorías sentenciales, T(L) y T(B), respectivamente. Varios ejemplos y contraejemplos concretos se presentaron para reforzar los resultados establecidos. Para algunas estructuras se estudió la cardinalidad de sus teorías proposicionales correspondientes y se estableció una fórmula para su computación.

To my family.

ACKNOWLEDGMENTS

I want to acknowledge the support given by my chairman, Dr. Luis F. Cáceres during my Graduate Studies in the Mathematics Department at the University of Puerto Rico in Mayagüez, especially during this investigation process. Also, I want to acknowledge the support given by Dr. Pedro Vasquez, all the staff of the Mathematics Department, and the support given by the Mathematics Graduate Students, particulary to Moisés Delgado, Humberto Pérez, Jhonny Navarro, Lissette Gaona, Leonid Sepúlveda, Carmen Saldaña and William Sarmiento.

Finally, but not less important, I want to thank my parents, Jesús Ortiz and María del C. Hernández, for always being there to support and encourage me to continue with this goal.

TABLE OF CONTENTS

page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION AND HISTORICAL BACKGROUND

1.1 Introduction

In this project, the relationship between propositional logic and algebraic structures will be studied. In Chapter 2, basic definitions of algebraic structures such as: groups, rings, lattices, algebras and R-modules will be presented. Special attention will be given to the study of lattice theory and algebras, where important results and properties will be presented and proved.

In Chapter 3, basic concepts of propositional logic will be presented. Then, we will establish the relationship between propositional logic and algebraic structures taking into consideration the results presented by Dr. Caceres in [1]. Some concrete examples of these relationship will be provided. Also, the cardinality of some finite theories will be studied.

1.2 Justification

A relationship between propositional logic and algebraic structures has been studied. In particular, given an algebraic structure A, a one to one correspondence exists between the models associated with its propositional theory and the substructures of A.

This relationship will be studied in this project using algebraic structures such as: groups, rings, lattices and algebras; in particular, Boolean Algebras. One of the

questions that arises when working with finite algebraic structure and its propositional theory is the cardinality of these sets. An answer to this question and a formula will be provided for some of the studied structures.

1.3 Historical Background

From Caceres [1] we know that given a ring R, we can define the propositional language associated to R as follows: the logical connectives are $\{\wedge, \vee, \rightarrow, \leftrightarrow, \neg\}$, defined as usual; the set of logical symbols includes the logical connectives and the parenthesis (,); and its associated propositional theory is given by:

$$T(R) = \{S_0, S_a \wedge S_b \rightarrow S_{a-b}, S_a \rightarrow S_{ab} : (\forall a \in R)(\forall b \in R)\}$$

A one to one correspondence has been shown to exist between the ideals of R and the models associated to T(R), as presented in Theorem 3.2.13 of Caceres [1] .[1]

In Burris and Sankappanavar [2], connections similar to the one established in Theorem 3.2.13 were studied, and applied to other algebraic structures. Enderton [3] also discusses fundamental aspects of propositional theory that will be relevant to the development of this project.

Several books such as Herstein [4], Hungerford [5] and Dummit and Foote [6] were used as references to review the algebraic structure concepts and properties.

[1] A complete proof of this result will be included in Chapter 3, and all the propositional logic concepts will be defined there.

1.4 Objectives

The main objectives of this investigation can be summarized as follows:

1. Study important properties of algebraic structures: lattices and Boolean Algebras.
2. Study the relation between different algebraic structures and propositional logic.
3. Provide concrete examples of these relationships.
4. Establish some properties.
5. Present applications for these relationships.

CHAPTER 2
ALGEBRAIC STRUCTURES AND PROPERTIES

2.1 Definition of Group

The following definitions are taken from Herstein [4]. Similar definitions can be found in Abstract Algebra textbooks such as: Hungerford [5], and Dummit and Foote [6].

Definition 2.1.1. Let G be a non-empty set and $\cdot$ be a binary operation defined in G. We say that G is a **group** if it satisfies:

1. $(\forall a \in G)(\forall b \in G) \quad a \cdot b \in G$
2. $(\forall a \in G)(\forall b \in G)(\forall c \in G) \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. $(\exists e \in G)$ such that $(\forall a \in G)$, $a \cdot e = e \cdot a = a$
4. $(\forall a \in G)(\exists b \in G)$ such that $a \cdot b = b \cdot a = e$

If, in addition, $(\forall a \in G)(\forall b \in G)$, we have that $a \cdot b = b \cdot a$, we say that G is an **abelian group**.

Definition 2.1.2. A nonempty subset H of a group G is a **subgroup** of G if, under the product of G, H is a group itself. That is, H is a subset of G if and only if:
1. $a, b \in H$ implies that $a \cdot b \in H$.
2. $a \in H$ implies that $a^{-1} \in H$.

Definition 2.1.3. A subgroup N of G is a **normal subgroup** of G if for every $a \in G$ and $n \in N$, $a \cdot n \cdot a^{-1} \in N$.

2.2 Definition of Ring

Definition 2.2.1. Let R be a non-empty set, and let two operations, $+$ and $\cdot$ be defined on R, which will be referenced as addition and multiplication, respectively, such that: $(\forall a \in R)$, $(\forall b \in R)$, $(\forall c \in R)$:

1. $a + b \in R$
2. $a + b = b + a$
3. $(a + b) + c = a + (b + c)$
4. $(\exists 0 \in R)$ such that $(\forall a \in R)$, $a + 0 = a$
5. $(\forall a \in R)(\exists(-a) \in R)$ such that $a + (-a) = 0$
6. $a \cdot b \in R$
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

Then R is a **ring**.

If R satisfies that $(\exists 1 \in R)$ such that $(\forall a \in R)$, $a \cdot 1 = 1 \cdot a = a$, then R is a *ring with unit element.*

If, in addition, $(\forall a \in R)$ and $(\forall b \in R)$, $a \cdot b = b \cdot a$, then R is a *commutative ring.*

Example 2.2.2. Consider R be the set of integers and let $+$ and $\cdot$ be defined as the usual addition and multiplication of integers. Then, R is a commutative ring with unit element.

Example 2.2.3. Let R be the set of even integers and let $+$ and $\cdot$ be defined as usual. Then, R is a commutative ring without unit element.

Definition 2.2.4. A non-empty subset I of a commutative ring R is an **ideal** of R if:

1. $0 \in I$
2. $(\forall a \in R)(\forall b \in R)((a, b \in I) \rightarrow (a - b \in I))$
3. $(\forall a \in R)(\forall b \in R)((a \in I) \rightarrow (a \cdot b \in I))$

2.3 Definition of lattices

There are two different ways of defining a lattice structure. The first is algebraic, like groups and rings, and the other is based on the order of the elements.

Definition 2.3.1. A non-empty set L with two binary operations, $\wedge$ and $\vee$, that will be read as "meet" and "join", respectively, defined on L, is a **lattice** if $(\forall x \in L)(\forall y \in L)(\forall z \in L)$, it satisfies:

L1: (a) $x \vee y = y \vee x$

(b)$x \wedge y = y \wedge x$ (Commutative Laws)

L2: (a) $x \vee (y \vee z) = (x \vee y) \vee z$

(b) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (Associative Laws)

L3: (a) $x \vee x = x$

(b) $x \wedge x = x$ (Idempotent Laws)

L4: (a)$x = x \vee (x \wedge y)$

(b)$x = x \wedge (x \vee y)$ (Absorption Laws)

Example 2.3.2. Let L be the set of natural numbers $\mathbb{N}$ and define $\vee$ as the least common multiple and $\wedge$ as the greatest common divisor. It can be verified that L satisfies Definition 2.3.1.

Before including the second definition of lattices, we need to introduce the concept of partially ordered set.

Definition 2.3.3. Let A be a non-empty set. A binary relation $\leq$ defined on A is a **partial order** in A if $(\forall a \in A)(\forall b \in A)$, the following conditions hold in A:

i. $a \leq a$ (Reflexivity)

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

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

A partially ordered set or poset is a set with a partial order relation.

If, in addition, $(\forall a \in A)(\forall b \in A)$, we have $a \leq b$ or $b \leq a$ then, we say that A is a totally ordered set, or simply, A is a **chain**.
In the case that $a \leq b$ but $a \neq b$, then we denote this by $a < b$.

Some examples of partially ordered sets are:
Example 2.3.4. 1. Let *P(X)* be the power set of a non-empty set X, and let A be an arbitrary subset of X, denoted by $A \subseteq X$. It can be verified that $\subseteq$ is a partial order relation on *P(X)*.
2. Let $\mathbb{R}$ be the set of real numbers and take $\leq$ as the usual ordering in $\mathbb{R}$. Then, $\leq$ is a total order on $\mathbb{R}$.

Definition 2.3.5. Let P be a partially ordered set and $A \subseteq P$. An element $p \in P$ is an **upper bound** of A if $(\forall a \in A), a \leq p$. We say that $p \in P$ is the **least upper bound** of A or the *supremum* of A (sup A) if p is an upper bound of A, and if $(\exists b \in P)$ such that $(\forall a \in A) a \leq b$, then $p \leq b$.

Similarly, we can define the lower bound of A and the greatest lower bound or *infimum* of A (inf A).

Given $a \in P$ and $b \in P$, we say that b covers a or, equivalently, a is covered by b, denoted by $a \prec b$, if $a < b$ and if $(\exists c \in P)$ such that $a \leq c \leq b$, then $a = c$ or $c = b$.

Hasse Diagrams are used to show the relationship between elements in a finite partially ordered set. Given a poset A, we represent the elements of A by a small

circle "∘". If $a \prec b$, then the circle of a is located below the circle of b, joining them with a line segment. Some examples of Hasse Diagrams are shown below.

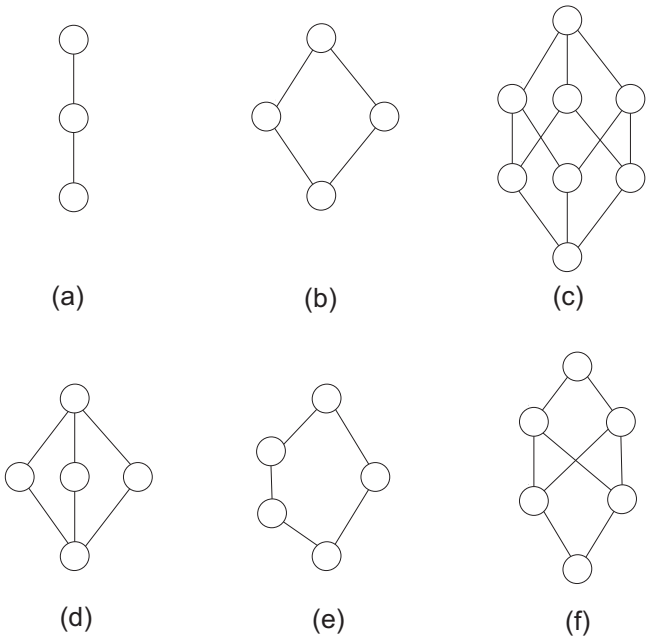

Figure 2–1: Examples of Hasse Diagrams

Now, we will introduce the second definition of a lattice.

Definition 2.3.6. A partially ordered set, L, is said to be a **lattice** if $(\forall a \in L)(\forall b \in L)$, both, sup{a, b} and inf{a, b}, are in L.

Several interesting and useful results from studies by Burris and Sankappanavar [2] are included in the following pages.

The next lemma explains the relationship between the two definitions of a lattice.

Lemma 2.3.7. Definition 2.3.1 is equivalent to Definition 2.3.6.

Proof. Let a and b be arbitrary elements of a non-empty set L satisfying Definition 2.3.1, and define $\leq$ as follows: $a \leq b$ if and only if $a = a \wedge b$ and $b = a \vee b$. We need to show that L is a partially ordered set that satisfies Definition 2.3.6.

First, L is reflexive, since $(\forall a \in L)\ a = a \wedge a$ by L3. Thus $a \leq a$.

Now, we prove that L is antisymmetric. We assume that $(\forall a \in L)(\forall b \in L)\ a \leq b$ and $b \leq a$. Then by definition of $\leq$, we have $a = a \wedge b$ and $b = b \wedge a = a \wedge b$ by L1. So, $a = b$.

Next, we must prove that L is transitive. We begin by assuming that $(\forall a \in L)(\forall b \in L)(\forall c \in L)$, $a \leq b$ and $b \leq c$. Then,

$$a = a \wedge b \text{ and } b = b \wedge c$$

So, by L2, we have that:

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

Thus, we have that $a = a \wedge c$. We conclude that $a \leq c$ and L is transitive. Therefore, L is a partially ordered set.

We proceed by showing that both, sup{a, b} and inf{a, b}, are in L.

From L4 (b) and L1 we know that $(\forall a \in L)(\forall b \in L)$,

$$a = a \wedge (a \vee b) \text{ and } b = b \wedge (a \vee b)$$

Then,

$$a \leq (a \vee b) \text{ and } b \leq (a \vee b)$$

So, as $(a \vee b)$ is an upper bound of a and b in L, we can verify that

$$(a \vee b) = \sup\{a, b\}$$

Suppose that $(\exists c \in L)$ such that $a \leq c$ and $b \leq c$. Then, $a = a \wedge c$ and $b = b \wedge c$. By L4 and L1, we obtain:

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

and

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

Therefore,

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

On the other hand,

$$(a \vee c) \vee (b \vee c) = (a \vee b) \vee c \qquad \text{(by L1 and L3)}$$

Therefore, $(a \vee b) \vee c = c$. In summary, we have that:

$$(a \vee b) \wedge c = (a \vee b) \wedge [(a \vee b) \vee c)] = a \vee b \qquad \text{(by L4)}$$

Thus, we conclude that $a \vee b \leq c$, and, therefore,

$$a \vee b = \sup\{a, b\}.$$

We will now prove that

$$a \wedge b = \inf\{a, b\}.$$

From L4 and L1, we have that $(\forall a \in L)(\forall b \in L)$,

$$a = a \vee (a \wedge b) \text{ and } b = b \vee (a \wedge b)$$

Then, we obtain $a \wedge b \leq a$ and $a \wedge b \leq b$. Therefore $a \wedge b$ is a lower bound of a and b in L. Let us now verify that

$$(a \wedge b) = \inf\{a, b\}.$$

Suppose that $(\exists c \in L)$ such that $c \leq a$ and $c \leq b$. Then, $c = a \wedge c$ and $c = b \wedge c$. But, by L2:

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

Therefore, since $c = (a \wedge b) \wedge c$, we obtain that $c \leq (a \wedge b)$.

Then,

$$a \wedge b = \inf\{a, b\}$$

Finally, as $a \vee b = \sup\{a, b\} \in L$ and $a \wedge b = \inf\{a, b\} \in L$, Definition 2.3.1 implies Definition 2.3.6.

Now we will verify that Definition 2.3.6 implies Definition 2.3.1. First, assume that a non-empty set L satisfies Definition 2.3.6 of a lattice, and let a, b and c be arbitrary elements of L. Define $\vee$ and $\wedge$ as follows:

$$a \wedge b = \inf\{a, b\} \text{ and } a \vee b = \sup\{a, b\}$$

We want to show that L satisfies Definition 2.3.1.

L1 is true, since $a \vee b = \sup\{a, b\} = \sup\{b, a\} = b \vee a$ and $a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$.

For L2, we need to show that $a \vee (b \vee c) = (a \vee b) \vee c$, that is,

$$\sup\{a, \sup\{b, c\}\} = \sup\{\sup\{a, b\}, c\}$$

Let $d = \sup\{b, c\}$, $e = \sup\{a, b\}$, $f = \sup\{e, c\}$. Then, applying the supremum definition, we obtain that $b \leq d$, $c \leq d$, $a \leq e$, $b \leq e$, $e \leq f$ and $c \leq f$. By transitivity, $a \leq f$ and $b \leq f$. Then, f is an upper bound of $\{a, b\}$. Since $c \leq f$ and $b \leq f$, we have that $d \leq f$. Therefore, f is an upper bound of $\{a, d\}$ and $\sup\{a, d\} \leq f$. So

$$\sup\{a, \sup\{b, c\}\} \leq \sup\{\sup\{a, b\}, c\}$$

Using a similar approach, we can show that

$$\sup\{\sup\{a, b\}, c\} \leq \sup\{a, \sup\{b, c\}\}$$

Therefore, by antisymmetry,

$$\sup\{a, \sup\{b, c\}\} = \sup\{\sup\{a, b\}, c\}$$

So, we can conclude that $a \vee (b \vee c) = (a \vee b) \vee c$.

In order to prove L3(a) we know that $a \vee a = \sup\{a, a\}$ by definition. Since L is a poset, $a \leq a$, then a is an upper bound of a, but $a \leq \sup\{a, a\}$. Since $\sup\{a,\ a\}$ is the least upper bound, then $\sup\{a,\ a\} \leq a$. By antisymmetry, we conclude that $a \vee a = \sup\{a, a\} = a$. Proof of L3(b) is similar.

For L4, we need to show that $a = a \vee (a \wedge b)$ and $a = a \wedge (a \vee b)$. By definition, we have:

$$a \vee (a \wedge b) = \sup\{a, \inf\{a, b\}\} = a$$

since $\inf\{a, b\} \leq a$ by definition.

On the other hand, we have:

$$a \wedge (a \vee b) = \inf\{a, \sup\{a, b\}\} = a$$

since $a \leq \sup\{a, b\}$ by definition.

We proved that L1 to L4 hold on L, so Definition 2.3.6 implies Definition 2.3.1, illustrating that these two definitions are equivalent. □

Using these definitions, we can verify that Examples (a) to (e) of Figure 2–1 are lattices. However, Example (f) is not a lattice, since c, d and e are upper bounds of a and b, but none of them is the least upper bound. That is, the $\sup\{a, b\}$ does not exist. See the figure below.

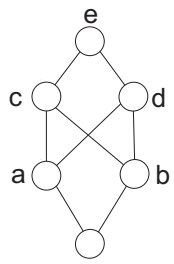

Figure 2–2: Example of a non-lattice

Now, we define the sub-structure of a lattice: a sub-lattice.

Definition 2.3.8. A non-empty subset L' of a lattice L is a **sub-lattice** of L if $(\forall a \in L')(\forall b \in L') \quad a \vee b \in L'$ and $a \wedge b \in L'$, where $\vee$ and $\wedge$ are the same operations defined for L.

For example, considering Figure 2–3, we can verify that the subset $L' = \{a, c, d, e\}$ of L is a partially ordered set, but it is not a sub-lattice of L, since $c \vee d = b$ and $b \notin L'$.

On the other hand, if we take $L' = \{b, c, d, e\}$, then L' is a sub-lattice of L.

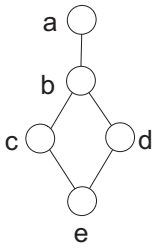

Figure 2–3: Example of a sublattice

2.3.1 Distributive and Modular Lattices

Now, we will review the concepts of distributive and modular lattices.

Definition 2.3.9. Let L be a non-empty lattice, and a, b and c be arbitrary elements of L. Then, L is a **distributive lattice** if $(\forall a \in L)(\forall b \in L)(\forall c \in L)$, it satisfies:

D1 $\quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

D2 $\quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Theorem 2.3.10. A lattice L satisfies D1 if and only if L satisfies D2.

Proof. Let us verify that if L satisfies D1, then it satisfies D2. Let x, y, z be arbitrary elements of L.

$$\begin{aligned}
x \vee (y \wedge z) &= (x \vee (x \wedge z)) \vee (y \wedge z) && \text{(by L4 (a))} \\
&= x \vee ((x \wedge z) \vee (y \wedge z)) && \text{(by L2)} \\
&= x \vee ((z \wedge x) \vee (z \wedge y)) && \text{(by L1)} \\
&= x \vee (z \wedge (x \vee y)) && \text{(by D1)} \\
&= x \vee ((x \vee y) \wedge z) && \text{(by L1)} \\
&= (x \wedge (x \vee y)) \vee ((x \vee y) \wedge z) && \text{(by L4 (b))} \\
&= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) && \text{(by L1)} \\
&= (x \vee y) \wedge (x \vee z) && \text{(by D1)}
\end{aligned}$$

Therefore, L satisfies D2. Similarly, it can be shown that if L satisfies D2, then L satisfies D1. □

In order to determine if a lattice is distributive, it suffices to prove that L satisfies one of the properties of Definition 2.3.9. [1]

Examples (a), (b) and (c) of Figure 2–1 are distributive lattices, while Examples (d) and (e), M_5 and N_5 are non-distributive lattices. Analyzing the lattice M_5, and considering a, b, c as the middle elements, as shown in Figure 2–4.

[1] Note that this process can become extremely difficult and time consuming, since we need to verify that the definition holds for every element of L.

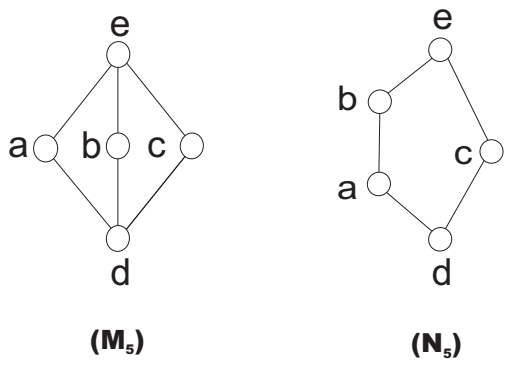

Figure 2–4: Non-distributive lattices

we have:

$$a \wedge (b \vee c) = a \wedge e = a, \text{ while } (a \wedge b) \vee (a \wedge c) = d \vee d = d$$

Then

$$a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c)$$

Therefore, M_5 is a non-distributive lattice. A similar argument can be used to show that N_5 is also a non-distributive lattice.

Definition 2.3.11. A lattice L is a **modular lattice** if $(\forall x \in L)(\forall y \in L)(\forall z \in L)$ the following law holds:

$$M : (x \leq y) \rightarrow ((x \vee (y \wedge z) = y \wedge (x \vee z)).$$

This law is known as the **modular law**.

Theorem 2.3.12. Every distributive lattice is a modular lattice.

Proof. Let L be a distributive lattice, and x, y and z be arbitrary elements of L, such that $x \leq y$. Then, $y = x \vee y$ by definition of $\leq$. By D2, we obtain:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) = y \wedge (x \vee z) \qquad \text{(by hypothesis)}$$

Therefore, L satisfies the modular law. □

N_5 in Figure 2–4 is an example of a non-modular lattice, since $a \leq b$ implies that $b = a \vee b$, but:

$$a \vee (b \wedge c) = a \vee d = a \text{ and } b \wedge (a \vee c) = b \wedge e = b$$

So,

$$a \vee (b \wedge c) \neq b \wedge (a \vee c)$$

Theorem 2.3.13 (Dedekind)**.** A lattice L is non-modular if and only if it contains a copy of N_5 as a sub-lattice.

Proof. Let L be a non-empty lattice that contains a copy of N_5 as a sub-lattice. Then, by previous remarks we conclude that L is a non-modular lattice.

Now, assume that L is a non-modular lattice. We need to show that L contains a copy of N_5 as a sub-lattice.

Since L is non-modular, there are elements a, b and c in L such that $a \leq b$, but $a \vee (b \wedge c) < b \wedge (a \vee c)$. Let $a_1 = a \vee (b \wedge c)$ and $b_1 = b \wedge (a \vee c)$.

Then

$$\begin{aligned} c \wedge b_1 &= c \wedge [b \wedge (a \vee c)] \\ &= c \wedge [(a \vee c) \wedge b] && \text{(by L1 (b))} \\ &= c \wedge [(c \vee a) \wedge b] && \text{(by L1 (a))} \\ &= [c \wedge (c \vee a)] \wedge b && \text{(by L2 (b))} \\ &= c \wedge b && \text{(by L4 (b))} \end{aligned}$$

By the definition of a_1 and b_1 , we have that $c \wedge b \leq a_1 \leq b_1$. Also, $c \wedge b = c \wedge (c \wedge b) \leq c \wedge a_1 \leq c \wedge b_1$. But $c \wedge b_1 = c \wedge b$, therefore, $c \wedge b = c \wedge a_1 = c \wedge b_1$.

Following a similar procedure, interchanging $\vee$ by $\wedge$, we can verify that $c \vee a_1 = c \vee a$, and therefore, $c \vee a_1 = c \vee b_1 = c \vee a$.

Then, the following diagram represents a copy of N_5 as a sub-lattice of L.

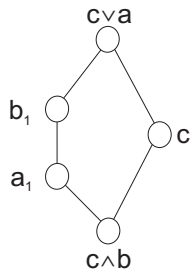

Figure 2–5: Copy of N_5

□

Theorem 2.3.14 (Birkhoff)**.** A lattice L is non-distributive if and only if it contains a copy of N_5 or M_5 as a sub-lattice.

Proof. Let L be a non-empty lattice, and suppose that it contains a copy of N_5 or M_5 as a sub-lattice. Then, by previous remarks, we conclude that L is non-distributive.

For the converse, assume that L is a non-distributive lattice that does not contain a copy of N_5 as a sub-lattice. By Theorem 2.3.13, we can state that L satisfies the modular law. We need to show that L has a copy of M_5 as a sub-lattice. Since L is non-distributive, there are elements a, b, c in L such that $(a \wedge b) \vee (a \wedge c) < a \wedge (b \vee c)$. Now, define

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

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

$$a_1 = (a \wedge e) \vee d$$

$$b_1 = (b \wedge e) \vee d$$

$$c_1 = (c \wedge e) \vee d$$

By the definition of operations, we obtain the following inequalities:

$$d \leq a_1, b_1, c_1 \leq e.$$

Since

$$\begin{aligned} a \wedge e &= a \wedge ((a \vee b) \wedge (a \vee c) \wedge (b \vee c)) \\ &= a \wedge (a \vee c) \wedge (b \vee c) && \text{(by } L4\text{)} \\ &= a \wedge (b \vee c) \end{aligned}$$

and the modular law applies to L, (that is, whenever $M : x \leq y \rightarrow x \vee (y \wedge z) = y \wedge (x \vee z)$), we state that

$$\begin{aligned} a \wedge d &= \underline{a} \wedge (\underline{(a \wedge b) \vee (a \wedge c)} \vee (b \wedge c)) \\ &= ((a \wedge b) \vee (a \wedge c)) \vee (a \wedge (b \wedge c)) && \text{(by M, since } (a \wedge b) \vee (a \wedge c) \leq a\text{)} \\ &= (a \wedge b) \vee ((a \wedge b) \wedge c) \vee (a \wedge c) && \text{(by L1 and L2)} \\ &= (a \wedge b) \vee (a \wedge c) && \text{(by L4)} \end{aligned}$$

where the underlined terms indicate where the modular law is applied. Since $(a \wedge b) \vee (a \wedge c) < a \wedge (b \vee c)$, and $a \leq (a \vee b) \wedge (a \vee c)$, we conclude that $d < e$.

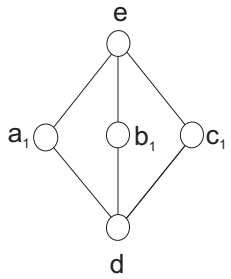

Figure 2–6: Copy of M_5

Now, we need to show that the diagram in Figure 2–6 is a copy of M_5 included in L. That is, we show that $a_1 \wedge b_1 = a_1 \wedge c_1 = b_1 \wedge c_1 = d$ and $a_1 \vee a_2 = a_1 \vee c_1 = b_1 \vee c_1 = e$. We will include two cases, since the others require similar arguments to complete

the proof. The elements where the modular law is applicable will be underlined for clarity.

From previous calculations we have that $a \wedge e = a \wedge (b \vee c)$. Also, $b \vee d = b \vee (a \wedge c)$ by applying L4 and L1. We want to show that $a_1 \wedge b_1 = d$.

$$
\begin{aligned}
a_1 \wedge b_1 &= ((a \wedge e) \vee \underline{d}) \wedge (\underline{(b \wedge e) \vee d}) \\
&= d \vee ((a \wedge e) \wedge ((b \wedge \underline{e}) \vee \underline{d})) && \text{(by M, since } d \leq ((b \wedge e) \vee d)) \text{ and L1} \\
&= d \vee ((a \wedge e) \wedge ((b \vee d) \wedge e)) && \text{(by M and since } d < e) \\
&= d \vee ((a \wedge e) \wedge (b \vee d)) && \text{(by L1 and L3)} \\
&= d \vee (a \wedge \underline{(b \vee c)} \wedge (\underline{b} \vee (a \wedge c))) && \text{(by previous remarks)} \\
&= d \vee (a \wedge (b \vee ((b \vee c) \wedge (a \wedge c)))) && \text{(by M)} \\
&= d \vee (a \wedge (b \vee (a \wedge c))) && \text{(since } a \wedge c \leq b \vee c) \\
&= d \vee (\underline{a} \wedge (\underline{(a \wedge c)} \vee b)) && \text{(by L1)} \\
&= d \vee ((a \wedge b) \vee (a \wedge c)) && \text{(by M and L1)} \\
&= d && \text{since } (a \wedge b) \vee (a \wedge c) \leq d
\end{aligned}
$$

So, we conclude that $a_1 \wedge b_1 = d$. Similar arguments can be used to prove that $a_1 \wedge c_1 = b_1 \wedge c_1 = d$.

By applying L4, we obtain the following results: $a \vee d = a \vee (b \wedge c)$ and $b \wedge e = b \wedge (a \vee c)$. Now, we will show that $a_1 \vee b_1 = e$.

$$
\begin{aligned}
a_1 \vee b_1 &= ((a \wedge e) \vee d) \vee ((b \wedge e) \vee d) \\
&= (a \wedge e) \vee d \vee (b \wedge e) && \text{(by L1 and L3)} \\
&= \underline{d} \vee (\underline{e} \wedge a) \vee (e \wedge b) && \text{(by L1)} \\
&= (\underline{e} \wedge (d \vee a)) \vee (\underline{e \wedge b}) && \text{(by M, since } d < e\text{)} \\
&= ((d \vee a) \vee (e \wedge b)) \wedge e && \text{(by M, since } e \wedge b < e\text{)} \\
&= ((a \vee (\underline{b \wedge c})) \vee (\underline{b} \wedge (a \vee c))) \wedge e && \text{(by previous remarks)} \\
&= (a \vee (b \wedge ((b \wedge c) \vee (a \vee c)))) \wedge e && \text{(by M)} \\
&= (\underline{a} \vee (b \wedge (\underline{a \vee c}))) \wedge e && \text{(since } b \wedge c \leq a \vee c\text{)} \\
&= ((a \vee c) \wedge (a \vee b)) \wedge e && \text{(by M, since } a \leq a \wedge c\text{)} \\
&= e && \text{(since } e < (a \vee c) \wedge (a \vee b)\text{)}
\end{aligned}
$$

We proved that $a_1 \vee b_1 = e$. A similar approach can be followed to show that $a_1 \vee c_1 = b_1 \vee c_1 = e$. So, we see that Figure 2–6 represents a copy of M_5 included in L. Therefore, the lattice L is non-distributive. □

Now, in order to determine if a lattice, L, is distributive, we only need to verify if a copy of M_5 or N_5 exists as a sublattice of L. For example, in Figure 2–7, the lattice included in Figure (a) is a non-distributive lattice, since it contains a copy of N_5 as a sublattice. Meanwhile, Figure (b) represents a distributive lattice.

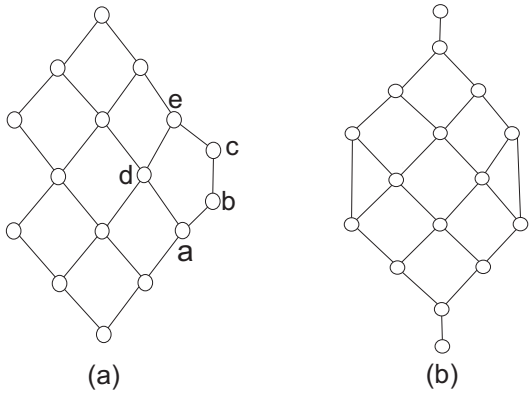

Figure 2–7: Example of Application of Birkhoff Theorem

2.4 Definition and examples of algebras

Definition 2.4.1. An **algebra** is a pair $(A; \{f_1, \cdots, f_k\})$, where A is a non-empty set and, for $i = 1, 2, \cdots, k$,

$$f_i : \underbrace{A \times A \times \cdots \times A}_{\text{n times}} \to A$$

f_i is an n-ary function.

Some examples of algebras are given below.

Example 2.4.2. 1. $(\mathbb{Z}; \{+, -, 0\})$ where $+$ is the usual addition of integers, $-a$ is the opposite of a and 0 is the identity element, is an algebra. These functions can be represented as follows:

$$f_1 : (\mathbb{Z}, \mathbb{Z}) \to \mathbb{Z}$$
$$(a, b) \mapsto a + b$$

and

$$f_2 : \mathbb{Z} \to \mathbb{Z}$$
$$a \mapsto -a$$

where $+$ is a binary operation and $-$ is a unary operation.

2. Let $\mathbb{R}$ be the set of all real numbers, then $(\mathbb{R}; \{\wedge, \vee\})$ where $a \wedge b = \min\{a, b\}$, and $a \vee b = \max\{a, b\}$ is an algebra, where both operations are binary.

2.4.1 Boolean Algebras and Boolean Rings

Definition 2.4.3. A **Boolean Algebra B** is an algebra $(B, \vee, \wedge, ', 0, 1)$ with two binary operations, "join" and "meet", denoted by $\vee, \wedge$, and a unary operation better known as a complement, $'$. We define 0 and 1 as the least and greatest elements of B, respectively. B satisfies that $(\forall x \in B)$:

B1: $(B, \vee, \wedge)$ is a distributive lattice

B2: $x \wedge 0 = 0, \qquad x \vee 1 = 1$

B3: $x \wedge x' = 0, \qquad x \vee x' = 1.$

Some examples of Boolean Algebras are now included.

Example 2.4.4. 1. $(\{0, 1\}, +, \cdot, ', 0, 1)$, where $+$ is an "or" operator, $\cdot$ is an "and" operator and $'$ is the negation. The truth value tables for these operations are included below:

$+$	0	1
0	0	1
1	1	1

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

$'$	
0	1
1	0

Using these tables, it can be easily verified that $(\{0, 1\}, +, \cdot, ', 0, 1)$ is a Boolean Algebra. This structure can be represented as a chain with two elements, where 0 is the smallest element and 1 as the largest one, as shown in Figure 2–8(a).

2. Consider A = {a, b} and $\mathscr{P}(A)$ as the power set of A. Define $\vee$ as the set union and $\wedge$ as the set intersection, 0 is the empty set and 1 is the set A. Under these conditions, this structure is a Boolean Algebra and the corresponding Hasse Diagram is included in Figure 2–8 (b).

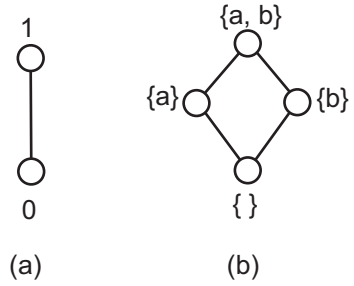

Figure 2–8: Examples of Boolean Algebras

In general, taking A as a non-empty set, $\mathscr{P}(A)$ as the power set of A and defining the operations as in previous examples, this structure always represents a Boolean Algebra.

Now, we introduce some useful properties of Boolean Algebras.

Let x and y be arbitrary elements of a Boolean Algebra B. Then, B satisfies the following properties:

B4. If $x \wedge y = 0$ and $x \vee y = 1,$ then $x' = y$

B5. $(x')' = x$

B6. $(x \vee y)' = x' \wedge y'$ and $(x \wedge y)' = x' \vee y'$ (De Morgan Laws)

Let us prove these properties.

Proof. Let x and y be arbitrary elements in B.

To prove B4, suppose that $x \wedge y = 0$ and $x \vee y = 1$. In a Boolean Algebra:

$$\begin{aligned} x' &= x' \vee 0 \\ &= x' \vee (x \wedge y) && \text{(by hypothesis)} \\ &= (x' \vee x) \wedge (x' \vee y) && \text{(by D2)} \\ &= 1 \wedge (x' \vee y) && \text{(by B3)} \\ &= x' \vee y && \text{(1 is the greatest element in B)} \end{aligned}$$

This implies that $x' \geq y$.

Also, we have:

$$\begin{aligned} x' &= x' \wedge 1 \\ &= x' \wedge (x \vee y) && \text{(by hypothesis)} \\ &= (x' \wedge x) \vee (x' \wedge y) && \text{(by D1)} \\ &= 0 \vee (x' \wedge y) && \text{(by B3)} \\ &= x' \wedge y && \text{(0 is the least element in B)} \end{aligned}$$

Then, $x' \leq y$. By anti-symmetry, we conclude that $x' = y$.

Now, we will show B5.

$$\begin{aligned} & x' \vee (x')' = 1 \\ & (x' \vee (x')') \wedge x = 1 \wedge x = x && \text{(since 1 is the greatest element)} \\ & (x' \wedge x) \vee ((x')' \wedge x) = x && \text{(by distributivity)} \\ & (x')' \wedge x = x && \text{(by B2 and B3)} \end{aligned}$$

Therefore, $x \leq (x')'$.

On the other hand:

$$\begin{aligned} & x' \vee x = 1 \\ & (x' \vee x) \wedge (x')' = 1 \wedge (x')' \\ & (x' \wedge (x')' \vee (x \wedge (x')' = (x')' = (x')' && \text{(by distributivity)} \\ & x \wedge (x')' = x && \text{(by B2 and B3)} \end{aligned}$$

So, we have that $(x')' \leq x$. Then, by antisymmetry, we conclude that $(x')' = x$.

In order to show B6, we need to prove that $(x \vee y) \wedge (x' \wedge y') = 0$ and $(x \vee y) \vee (x' \wedge y') = 1$.

By distributivity and applying the fact that 0 is the least element in B:

$$(x \vee y) \wedge (x' \wedge y') = (x \wedge x' \wedge y') \vee (y \wedge x' \wedge y') = (0 \wedge y') \vee (0 \wedge x') = 0$$

Similarly, we can show that $(x \vee y) \vee (x' \wedge y') = 1$.

Interchanging $\wedge$ and $\vee$, we can prove that $(x \wedge y)' = x' \vee y'$. □

Now, we will review the concept of Boolean Rings.

Definition 2.4.5. A ring **R** = (R, +, ·, -, 0, 1) is a **Boolean Ring** if it satisfies that $(\forall x \in R)$, $x^2 = x$.

Applying ring properties, we can show that for every Boolean Ring, the following properties hold:

Lemma 2.4.6. If R is a Boolean Ring, then it satisfies $(\forall x \in R)(\forall y \in R)$
$x + x = 0$ and $x \cdot y = y \cdot x$.

Proof. Let x and y be arbitrary elements in R. From the fact that $x^2 = x$, for all $x \in R$, we have:

$$\begin{aligned} &(x + x)^2 = x + x \\ &x^2 + x^2 + x^2 + x^2 = x + x \qquad \text{(by distributivity)} \\ &x + x = 0 \end{aligned}$$

since $x^2 = x$, and x has an additive inverse, $-x$.

Let us show that $x \cdot y = y \cdot x$.

$$
\begin{array}{ll}
(x+y)^2 = x+y & \\
x^2 + x\cdot y + y\cdot x + y^2 = x+y & \text{(by distributivity)} \\
x + x\cdot y + y\cdot x + y = x+y & \text{(since } x^2 = x\text{)} \\
x\cdot y + y\cdot x = 0 & \text{(adding the additive inverse of } x \text{ and } y\text{)} \\
x\cdot y + x\cdot y = x\cdot y + y\cdot x & \text{(since } x+x=0\text{)} \\
x\cdot y = y\cdot x &
\end{array}
$$

□

From Burris and Sankappanavar [2], we obtain the following results:

Theorem 2.4.7 (Stone)**.** a. Let $(B, \vee, \wedge, ', 0, 1)$ be a Boolean Algebra. Define $B^{\otimes} = \langle B, +, \cdot, -, 0, 1\rangle$ as an algebra, where:

$$
\begin{aligned}
a + b &= (a \wedge b') \vee (a' \wedge b) \\
a \cdot b &= a \wedge b \\
-a &= a
\end{aligned}
$$

Then, $B^{\otimes}$ is a Boolean Ring.

b. Let $\mathbf{R} = (R, +, \cdot, -, 0, 1)$ be a Boolean Ring. Define $R^{\otimes} = \langle R, \vee, \wedge, ', 0, 1\rangle$ as an algebra, where:

$$
\begin{aligned}
a \vee b &= a + b + a \cdot b \\
a \wedge b &= a \cdot b \\
a' &= 1 + a
\end{aligned}
$$

Then, $R^{\otimes}$ is a Boolean Algebra.

Sketch of proof:

In order to show (a), define B as a Boolean Algebra, and verify that the following properties hold for all a, b and c in B:

1. $a + 0 = a$
2. $a + b = a + b$
3. $a + a = 0$
4. $a + (b + c) = (a + b) + c$
5. $a \cdot 1 = 1 \cdot a = a$
6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
7. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
8. $a \cdot a = a$

We present only the proof of some of these properties for reference.

Let us prove (1).

$$\begin{aligned} a + 0 &= (a \wedge 0') \vee (a' \wedge 0) \\ &= (a \wedge 1) \vee (a' \wedge 0) \\ &= a \vee 0 \qquad \text{(since 0 and 1 are the least and greatest elements in B)} \\ &= a \end{aligned}$$

To prove (2) $a + b = b + a$, let $a \in B$ and $b \in B$ be arbitrary elements of the Boolean Algebra B. We have:

$$\begin{aligned} a + b = &\quad (a \wedge b') \vee (a' \wedge b) && \text{by definition of operation.} \\ = &\quad (b' \wedge a) \vee (b \wedge a') && \text{by commutativity of the Boolean Algebra B.} \\ = &\quad (b \wedge a') \vee (b' \wedge a) && \text{by commutativity of B.} \\ = &\quad b + a && \text{by definition of operation.} \end{aligned}$$

Now, we show (4).

$$\begin{aligned}
a + (b + c) &= (a \wedge ((b \wedge c') \vee (b' \wedge c))') \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge ((b' \vee c) \wedge (b \vee c'))) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) && \text{(By De Morgan)} \\
&= (a \wedge ((b' \wedge c') \vee (b \wedge c))) \vee ((a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)) && \text{(By distributivity)} \\
&= (a \wedge b' \wedge c') \vee (a \wedge b \wedge c) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c)
\end{aligned}$$

Since the meet and join operations are commutative, this value will not be affected by the order of the elements a, b and c. Therefore, we conclude that
$(\forall a \in B)(\forall b \in B)(\forall c \in B) \quad a + (b + c) = (a + b) + c$.

Properties (5) and (6) can be easily shown from the definitions. Now, we present a proof of (7).

$$\begin{aligned}
a \cdot b + a \cdot c &= ((a \wedge b) \wedge (a \wedge c)') \vee ((a \wedge b)' \wedge (a \wedge c)) \\
&= ((a \wedge b) \wedge (a' \vee c')) \vee ((a' \vee b') \wedge (a \wedge c)) && \text{(By De Morgan)} \\
&= (a \wedge b \wedge a') \vee (a \wedge b \wedge c') \vee (a' \wedge a \wedge c) \vee (b' \wedge a \wedge c) && \text{(By distributivity)} \\
&= (a \wedge b \wedge c') \vee (a \wedge b' \wedge c) \\
&= a \wedge ((b \wedge c') \vee (b' \wedge c)) && \text{(By distributivity)} \\
&= a \cdot (b + c)
\end{aligned}$$

In order to prove (8), let x be an arbitrary element of B. Then $x \cdot x = x \wedge x$ by definition. But $x \wedge x = x$ since B is a Boolean Algebra. Therefore, $x \cdot x = x$ for all $x \in B$.

Properties (1) to (7) show that $B^{\otimes}$ is a ring, while property (8) indicates that $B^{\otimes}$ is a Boolean Ring.

Note that $a + a = (a \wedge a') \vee (a' \wedge a) = 0 \vee 0 = 0$ for all $a \in B^{\otimes}$. Also, $a \cdot b = a \wedge b = b \wedge a = b \cdot a$, for all a and b in $B^{\otimes}$.

To show (b), assume that R is a Boolean Ring. We need to prove that the following properties hold for all a, b and c in R:

1. $a \vee b = b \vee a$
2. $a \wedge b = b \wedge a$
3. $a \vee (b \vee c) = (a \vee b) \vee c$
4. $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
5. $a \vee a = a$
6. $a \wedge a = a$
7. $a \vee (a \wedge b) = a$
8. $a \wedge (a \vee b) = a$
9. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Recall from Lemma 2.4.6, that $x + x = 0$ and $x \cdot y = y \cdot x$ for all x and y in R.

To prove (1), let a and b be arbitrary elements of R.

$$\begin{aligned} a \vee b = &\quad a + b + a \cdot b && \text{by definition of operation} \\ = &\quad b + a + b \cdot a && \text{by commutativity in the Boolean Ring R} \\ = &\quad b \vee a && \text{by definition of operation} \end{aligned}$$

This completes the proof of (1).

The proof of (2) is a direct consequence of the Boolean Ring definition.

Now, we demonstrate (3).

$$\begin{aligned} a \vee (b \vee c) &= a + (b + c + b \cdot c) + a \cdot (b + c + b \cdot c) && \text{(By definition of operation)} \\ &= a + b + c + b \cdot c + a \cdot b + a \cdot c + a \cdot b \cdot c && \text{(By distributivity)} \end{aligned} \tag{i}$$

On the other hand, we have:

$$\begin{aligned}
(a \vee b) \vee c &= (a + b + a \cdot b) + c + (a + b + a \cdot b) \cdot c && \text{(By definition of operation)} \\
&= a + b + a \cdot b + c + a \cdot c + b \cdot c + a \cdot b \cdot c && \text{(By distributivity)} \\
&= a + b + c + b \cdot c + a \cdot b + a \cdot c + a \cdot b \cdot c && \text{(By commutativity)} \qquad \text{(ii)}
\end{aligned}$$

Comparing (i) and (ii) we conclude that $a \vee (b \vee c) = (a \vee b) \vee c$.

By interchanging $\vee$ by $\wedge$ it can be shown that $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Property (4) can be easily shown by associativity in R.

Let us show (5).

$$\begin{aligned}
a \vee a = \quad & a + a + a \cdot a && \text{by definition of operation} \\
= \quad & 0 + a && \text{since } a + a = 0 \text{ and } a \cdot a = a \text{ in a Boolean Ring R} \\
= \quad & a && \text{by definition of R}
\end{aligned}$$

Property (6) can be verified using the fact that $x^2 = x$ for all $x \in R$.

Now, we will verify the absorption laws, Properties (7) and (8).

$$\begin{aligned}
a \vee (a \wedge b) &= a + a \cdot b + a \cdot (a \cdot b) && \text{(By definition of operations)} \\
&= a + a \cdot b + a \cdot b && \text{(Since } a^2 = a\text{)} \\
&= a + 0 && \text{(Since } (\forall a \in R) \quad a + a = 0 \text{)} \\
&= a
\end{aligned}$$

A similar approach can be used to prove that $a \wedge (a \vee b) = a$.

Now, let us show the distributive laws, Property (9):

$$\begin{aligned}
(a \wedge b) \vee (a \wedge c) &= a \cdot b + a \cdot c + (a \cdot b) \cdot (a \cdot c) && \text{(By definition of operations)} \\
&= a \cdot b + a \cdot c + a \cdot b \cdot c && \text{(By commutativity and } a^2 = a\text{)} \\
&= a \cdot (b + c + b \cdot c) && \text{(By distributivity in } R\text{)} \\
&= a \wedge (b \vee c)
\end{aligned}$$

From properties (1) to (8), we conclude that $R^{\otimes}$ is a lattice, and property (9) assures that it is distributive.

Now, $R^{\otimes}$ is a Boolean Algebra if the following properties hold:

10. $a \wedge 0 = 0$ and $a \vee 1 = 1$
11. $a \vee a' = 1$ and $a \wedge a' = 0$

To show (11), let a be an arbitrary element of R.

$$\begin{aligned}
a \vee a' &= a + a' + a \cdot a' && \text{(by definition)} \\
&= a + (1 + a) + a \cdot (1 + a) && \text{(since } a' = 1 + a \text{ in } R^{\otimes}\text{)} \\
&= a + 1 + a + a \cdot 1 + a \cdot a && \text{(by distributivity)} \\
&= a + a + 1 + a + a && \text{(by commutativity, } a \cdot a = a \text{ and } a \cdot 1 = a\text{)} \\
&= 1 && \text{(since } a + a = 0\text{)} \\
a \wedge a' &= a \cdot a' && \text{(by definition of operation)} \\
&= a \cdot (1 + a) && \text{(since } a' = 1 + a\text{)} \\
&= a \cdot 1 + a \cdot a && \text{(by distributivity)} \\
&= a + a && \text{(since } a^2 = a\text{)} \\
&= 0
\end{aligned}$$

The proof of (10) is similar. Therefore, we conclude that $R^{\otimes}$ is a Boolean Algebra.[2]

For a Boolean Algebra $\mathbf{B} = (B, \vee, \wedge, ', 0, 1)$, we can define an ideal and a filter as follows:

Definition 2.4.8. A subset I of a Boolean Algebra **B** is an **ideal** if:

(a) $0 \in I$

(b) If $a \in I$ and $b \in I$, then $a \vee b \in I$

(c) If $a \in I$ and $b \leq a$ then $b \in I$

Definition 2.4.9. A subset F of a Boolean Algebra **B** is a **filter** if:

(a) $1 \in F$

(b) If $a \in F$ and $b \in F$, then $a \wedge b \in F$

(c) If $a \in F$ and $b \geq a$ then $b \in F$

Now, taking **B** as a Boolean Algebra, we recall from Theorem 2.4.7 that the algebra $B^{\otimes} = \langle B, +, \cdot, -, 0, 1\rangle$ is a Boolean Ring. Then, we can define the ideals of $B^{\otimes}$ following definition 2.2.4 and definition 2.4.8.

From Burris and Sankappanavar [2], we obtain the following result:

Theorem 2.4.10. Let $\mathbf{B} = (B, \vee, \wedge, ', 0, 1)$ be a Boolean Algebra. Then, a subset I is an ideal of **B** if and only if I is an ideal of $B^{\otimes}$.

Proof. Assume that I is an ideal of B. Then, by definition of ideal, we have the following hypothesis:

1. $0 \in I$
2. If $a \in I$ and $b \in I$, then $a \vee b \in I$
3. If $a \in I$ and $b \leq a$ then $b \in I$

[2] A complete proof of this theorem is found in Burris and Sankappanavar [2], pages 138 to 141.

We need to prove that I is an ideal of $B^{\otimes}$.

1. $0 \in I$ by hypothesis.

2. Let a and b be arbitrary elements of I. Defining $+$ as in the Stone Theorem, Theorem 2.4.7, we want to show that $(a + b) \in I$. By definition of $\wedge$, we have that $a \wedge b' \leq a$ and $a' \wedge b \leq b$. Then $a \wedge b' \in I$ and $a' \wedge b \in I$, by hypothesis (3). Also, $(a \wedge b') \vee (a' \wedge b) \in I$, applying hypothesis (2). Thus, we have that $a + b = (a \wedge b') \vee (a' \wedge b) \in I$.

3. Let $a \in I$ and $b \in B$ be arbitrary elements. We need to prove that $a \cdot b \in I$. By definition of $\wedge$, $a \wedge b \leq a$. Then, $a \wedge b \in I$ by hypothesis (3). Since $a \cdot b = a \wedge b$, we conclude that $a \cdot b \in I$. Therefore, I is an ideal of $B^{\otimes}$.

On the other hand, suppose that I is an ideal of $B^{\otimes}$. Then:

1. $0 \in I$

2. If $a \in I$ and $b \in I$, then $a + b \in I$

3. If $a \in I$ and $b \in B$ then $a \cdot b \in I$

Let us verify that I is an ideal of B.

1. $0 \in I$ by hypothesis.

2. Let a and b be arbitrary elements of I. By hypothesis, $a + b \in I$ and $a \cdot b \in I$, then $a + b + a \cdot b \in I$. Since $a \vee b = a + b + a \cdot b$, then $a \vee b \in I$.

3. Let $a \in I$ and $b \in B$ be arbitrary elements, such that $b \leq a$. Then, $b = a \wedge b = a \cdot b$, by definition of operation. So, by (3), $a \cdot b \in I$, then $b \in I$. Therefore, I is an ideal of B. □

Definition 2.4.11. If $X \subseteq B$, and B is a Boolean Algebra, X' is defined as follows:

$$X' = \{a' \in B : a \in X\}$$

Lemma 2.4.12. Let B be a Boolean Algebra.

a. Let $I \subseteq B$. Then I is an ideal of B if and only if I' is a filter of B.

b. Let $F \subseteq B$. Then F is a filter of B if and only if F' is an ideal of B.

Only a proof of (b) is included. The proof of (a) is similar.

Proof. Let $F \subseteq B$, and a and b be arbitrary elements of F. Assume that F is a filter of B. Then, we have the following hypothesis:

(a) $1 \in F$

(b) If $a \in F$ and $b \in F$, then $a \wedge b \in F$

(c) If $a \in F$ and $b \geq a$ then $b \in F$

Let us verify that F' is an ideal of B.

1. Since $1 \in F$, then $0 \in F'$ by definition 2.4.11.

2. Since $a \in F$ and $b \in F$, then $a' \in F'$ and $b' \in F'$. Also, since $a \wedge b \in F$, $(a \wedge b)' \in F'$. By De Morgan, we have $(a \wedge b)' = a' \vee b'$. Therefore, $a' \vee b' \in F'$.

3. Let $a \in F'$ and $b \leq a$. Since $a \in F'$, then $a' \in F$. From the fact that $b \leq a$ if an only if $a' \leq b'$, and $a' \in F$, we establish that $b' \in F$. Therefore, $(b')' = b \in F'$.

Thus, F' is an ideal of B.

The other implication can be proved similarly. Therefore, F is a filter of B if and only if F' is an ideal of B. □

Based on the definitions provided in this chapter, we give the following examples:

Example 2.4.13. Let $C = \{1, 2, 3\}$ and A and B be arbitrary subsets of C. Define $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. Let $\mathscr{P}(C)$ be the power set of the set C. Then, we can show that $\mathscr{P}(C)$ is a Boolean Algebra, where the empty set $\emptyset$ represents the 0, the set C represents the 1. Refer to Figure 2–9 for the corresponding diagram.

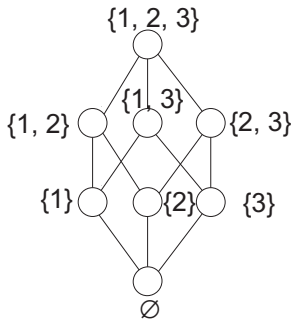

Figure 2–9: Boolean Algebra of the set C = {1, 2, 3}

We have already shown that this figure represents a distributive lattice. In order to show that for all $X \in \mathscr{P}(C)$, $X \wedge \emptyset = \emptyset$, we have that $X \wedge \emptyset = X \cap \emptyset = \emptyset$ by definition of set intersection. Also, for all $X \in \mathscr{P}(C)$, $X \vee C = X \cup C = C$ by definition of set union. Now, applying the definition of set complement, we can verify that for all $X \in \mathscr{P}(C)$, $X \wedge X' = X \cap X' = \emptyset$ and $X \vee X' = X \cup X' = C$. Therefore, $B = (\mathscr{P}(C), \cup, \cap, ', \emptyset, C)$ is a Boolean Algebra.

Moreover, using Theorem 2.4.7, since B is a Boolean Algebra, we can define $B^{\otimes}$ as the algebra $(\mathscr{P}(C), +, \cdot, -, \emptyset, C)$ such that for all A and B, subsets of C:

$$\begin{aligned} A + B &= (A \cap B') \cup (A' \cap B) \\ A \cdot B &= A \cap B \\ -A &= A \end{aligned}$$

Then, we can show that $B^{\otimes}$ is a Boolean Ring. Now, we verify some of the properties of a Boolean Ring.

First, let us prove that $(\forall A \subseteq C)$, $A + \emptyset = A$.

$$\begin{aligned} A + \emptyset = \; & (A \cap \emptyset') \cup (A' \cap \emptyset) && \text{(by definition of operation)} \\ = \; & (A \cap C) \cup \emptyset && \text{(by definition of intersection of sets)} \\ = \; & A \cup \emptyset = A \end{aligned}$$

Second, we want to prove that $(\forall A \subseteq C)(\forall B \subseteq C), \quad A + B = B + A$.

$$\begin{aligned} A + B &= (A \cap B') \cup (A' \cap B) && \text{(by definition of operation)} \\ &= (A' \cap B) \cup (A \cap B') && \text{(by commutativity)} \\ &= (B \cap A') \cup (B' \cap A) \\ &= B + A \end{aligned}$$

Finally, we verify that $A + A = \emptyset$.

$A + A = (A \cap A') \cup (A' \cap A) = \emptyset \cup \emptyset = \emptyset \quad$ since $A \cap A' = \emptyset$.

Now, we show that for all $A \subseteq C, \quad A \cdot C = A$. By definition of set intersection, we obtain that $A \cdot C = A \cap C = A$.

By definition of the $\cdot$ and $+$ operations, we can easily verify that these operations are associative and distributive.

Finally, for all $A \subseteq C, \quad A \cdot A = A \cap A = A$.

Example 2.4.14. Let C be defined as in the previous example, since $\mathscr{P}(C)$ is a ring, then we can find the ideals and filters of this set. The ideals of $\mathscr{P}(C)$ are: $\{\emptyset, \{1\}\}, \quad \{\emptyset, \{2\}\}, \quad \{\emptyset, \{3\}\}, \quad \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \quad \{\emptyset, \{1\}, \{3\}, \{1,3\}\}$ and $\{\emptyset, \{2\}, \{3\}, \{2,3\}\}$.

Following definition 2.4.11, and lemma 2.4.12, we obtain that the filters of $\mathscr{P}(C)$ are:

$\{\{1,2,3\}, \{1,3\}, \ \{1,2\}, \{1\}\}, \{\{1,2,3\}, \{1,3\}\}, \ \{\{1,2,3\}, \{1,2\}\}, \ \{\{1,2,3\}, \{1,3\}\}$

$\{\{1,2,3\}, \{2,3\}\}, \ \{\{1,2,3\}, \{2,3\}, \{1,3\}, \{3\}\}, \ \{\{1,2,3\}, \{2,3\}, \{1,2\}, \{2\}\}$.

We can verify that these sets satisfy the definition of a filter, and are the complements of the ideals.

2.5 R-Modules Definition and Examples

Now we will review the concept of R-modules, taken from Herstein [4], and provide some examples.

Definition 2.5.1. Let R be a ring. A **left R-module A** is an additive abelian group with a function

$$R \times A \to A$$

$$(r, a) \longmapsto ra$$

such that $(\forall r \in R)(\forall s \in R)(\forall a \in A)$ and $(\forall b \in A)$ we have:

a. $r(a + b) = ra + rb$

b. $(r + s)a = ra + sa$

c. $r(sa) = (rs)a$

If the ring R has an identity element, and $1 \cdot a = a, (\forall a \in A)$, we say that A is a **unitary R-module**.

Definition 2.5.2. A **right R-module A** is an additive abelian group in addition with a function

$$A \times R \to A$$

$$(a, r) \longmapsto ar$$

such that $(\forall r \in R)(\forall s \in R)(\forall a \in A)$ and $(\forall b \in A)$ we have:

a. $(a + b)r = ar + br$

b. $a(r + s) = ar + as$

c. $(as)r = a(sr)$

An example of R-modules is included below.

Example 2.5.3. Every abelian group A is a $\mathbb{Z}$-module, with

$$\mathbb{Z} \times A \to A$$

$$(r, a) \longmapsto ra$$

where $ra = \underbrace{a + a + \ldots + a}_{\text{r times}}$

Verification: For $r \in \mathbb{Z}$, $s \in \mathbb{Z}$, $a \in A$ and $b \in A$

1. Let us prove that $r(a + b) = ra + rb$.

$$\begin{aligned} r(a+b) &= \underbrace{(a+b) + (a+b) + \ldots + (a+b)}_{\text{r times}} \\ &= \underbrace{a + a + \ldots + a}_{\text{r times}} + \underbrace{b + b + \ldots + b}_{\text{r times}} && \text{since A is an abelian group} \\ &= ra + rb && \text{by definition of operation} \end{aligned}$$

2. In order to show that $(r + s)a = ra + sa$, we have:

$$\begin{aligned} (r+s)a &= \underbrace{a + a + \ldots + a}_{\text{r + s times}} \\ &= \underbrace{a + a + \ldots + a}_{\text{r times}} + \underbrace{a + a + \ldots + a}_{\text{s times}} \\ &= ra + sa && \text{(by definition of operation)} \end{aligned}$$

3. Finally, we verify that $r(sa) = (rs)a$.

$$\begin{aligned} r(sa) &= r(\underbrace{a + a + \ldots + a}_{\text{s times}}) && \text{(by definition of sa)} \\ &= \underbrace{\underbrace{a + a + \ldots + a}_{\text{s times}} + \ldots + \underbrace{a + a + \ldots + a}_{\text{s times}}}_{\text{r times}} \\ &= (rs)a \end{aligned}$$

Therefore, we have proved that A is a $\mathbb{Z}$-module, that is, we have shown that every abelian group is a $\mathbb{Z}$-module. Also, since every R-module is an abelian group, we have that every $\mathbb{Z}$-module is an abelian group.

It can be easily shown that every ring R is R-module, where $r \cdot s$ is the product operation of the ring. Also, it can be shown that if I is a left-ideal of a ring R, then I and R/I are R-modules, where $R/I = a + I,$ with $a \in R$.

Definition 2.5.4. Let A be an R-module, and $N \subseteq A$. Then N is an R**-submodule** of A if:

1. $(N, +)$ is a subgroup of A
2. $r \in R$ and $n \in N, \quad rn \in N$.

CHAPTER 3
RELATIONSHIP BETWEEN LOGIC AND ALGEBRAIC STRUCTURES

3.1 Basic concepts and notation of propositional logic

We introduce some definitions and properties that will be used to study a relationship between logic and algebraic structures. They are mainly taken from Smith, Andre and Eggen [7], Enderton [3] and Caceres [8].

We begin this chapter by constructing a language that will be used to translate English sentences into mathematics. We need to define a set of symbols, and the grammatical rules that will be applied to a finite sequence of symbols.

Define the set of symbols as follows:

Symbol	Name	Translation or use
$(,)$	Left / right parenthesis	Punctuation Marks
$'$	negation symbol	not
$\wedge$	conjunction symbol	and
$\vee$	disjunction symbol	or (inclusive)
$\rightarrow$	conditional	If . . . then . . .
$\leftrightarrow$	biconditional	if and only if
$S_1, S_2, \ldots, S_n, \ldots$	Sentential or propositional symbols	Represent atomic sentences

Table 3–1: Propositional Logic Symbols Description

The sentential symbols are called nonlogical parameters. The symbols $', \vee, \wedge, \rightarrow, \leftrightarrow$ are called the sentential connectives. The logical symbols include the parenthesis and the sentential connectives.

An expression is a finite sequence of symbols. Some examples are:

$$)) \rightarrow S_a$$

$$(S_a \wedge S_b) \leftrightarrow S_c$$

As seen in these examples, not all the expressions make sense. We need to define the grammatical rules that will be used in the language to avoid ambiguities, and create well-formed formulas, wffs.

Sentence	Translation
(S_1')	not S_1
$(S_1 \wedge S_2)$	S_1 and S_2
$(S_1 \vee S_2)$	S_1 or S_2
$(S_1 \rightarrow S_2)$	If S_1 then S_2
$(S_1 \leftrightarrow S_2)$	S_1 if and only if S_2

Table 3–2: Grammatical Rules

After defining these rules, we can make new wffs from previous formulas by concatenating the symbols using the logical symbols.

For example, let $\alpha = (S_1')$, $\beta = S_2$, and $\gamma = (S_3 \wedge S_4)$, then $\alpha \rightarrow \beta$ is given by the expression:

$$(S_1' \rightarrow S_2)$$

and $\gamma \leftrightarrow \beta$ is the expression:

$$((S_3 \wedge S_4) \leftrightarrow S_2)$$

Every atomic sentence and finite sequence of symbols that follows the rules established in this section will be called a **proposition**.

A **sentential theory** is a set of propositions.

Definition 3.1.1. A **model of a theory** is an assignment of true (T) or false (F) to the propositional letters that makes true all the propositions of a given theory.

In other words, a model of a theory is a function from the set of propositional letters S to the set $\{T, F\}$ that make true all the propositions of the theory.

Then, given two propositions α and β, the following table summarizes the truth value assignment for the wffs formed using the sentential connectives.

α	β	(α')	$(\alpha \wedge \beta)$	$(\alpha \vee \beta)$	$(\alpha \rightarrow \beta)$	$(\alpha \leftrightarrow \beta)$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Table 3–3: Truth Value Assignment

Let S be a non-empty set of propositional letters, and M be a model of S. We will denote the fact that an element $x \in S$ is true in M as $M \models x$ and, equivalently, $(x, T) \in M$. If $x \in S$ is false in M, then we denote it as $M \not\models x$, and equivalently, $(x, F) \in M$.

Definition 3.1.2. Two models A and B of a given theory are **equivalent** if they satisfy the same propositions. We will just write $A = B$.

Definition 3.1.3. Two theories T_1 and T_2 are **equivalent** if they have the same models. We will denote this by $T_1 \equiv T_2$.

3.2 Preliminary and New Results

In this section, we will establish relations between sets and basic algebraic structures such as groups, rings, lattices, R-modules, and algebras with propositional logic using the concepts already defined. Some properties and examples will be provided.

Let $S = \{S_a : a \in A\}$ be the set of propositional letters associated with a nonempty set A. Let M be an arbitrary model of S. Define $\phi(M) = \{x \in S : M \models x\}$. As

previously defined:

$$M \models x \Leftrightarrow (x, T) \in M$$

and

$$M \not\models x \Leftrightarrow (x, F) \in M$$

Let A and B be arbitrary models of S. Note that

$$A \cap B = \{(x, y) \in S \times \{T, F\} : (x, y) \in A \wedge (x, y) \in B\}$$

Now, we show that $\phi(A \cap B) = \phi(A) \cap \phi(B)$.

Let $x \in \phi(A) \cap \phi(B)$. Then, $x \in \phi(A)$ and $x \in \phi(B)$. By applying definition of ϕ, $A \models x$ and $B \models x$. So, $(x, T) \in A, (x, T) \in B$, then $(x, T) \in A \cap B$. Therefore, $A \cap B \models x$, and by definition of ϕ, $x \in \phi(A \cap B)$. Since x is arbitrary, we obtain that $\phi(A) \cap \phi(B) \subseteq \phi(A \cap B)$.

Similarly, we can show that $\phi(A \cap B) \subseteq \phi(A) \cap \phi(B)$. Therefore, we conclude that $\phi(A \cap B) = \phi(A) \cap \phi(B)$.

Based on this result, we can redefine $\phi(A \cap B)$ as follows:

$$\phi(A \cap B) = \{x \in S : (A \models x) \wedge (B \models x)\}$$

and

$$A \cap B \models x \Leftrightarrow (A \models x) \wedge (B \models x)$$

3.2.1 Sets

Now, we will study operations on models of a given set C. These definitions will be applied to algebraic structures.

Let $S = \{S_a : a \in C\}$ be the set of propositional letters associated with a nonempty set C, and for each $A \subseteq C$, define the model associated with A as follows:

$$M(A) = \{(S_a, T) \in S \times \{T, F\} : a \in A\} \cup \{(S_a, F) \in S \times \{T, F\} : a \notin A\}$$

Applying the definition of set union to arbitrary nonempty subsets of C, A and B, we have that the model associated with $A \cup B$ is:

$$M(A \cup B) = \{(S_a, T) \in S \times \{T, F\} : a \in (A \cup B)\} \cup \{(S_a, F) \in S \times \{T, F\} : a \notin (A \cup B)\}$$

Note that if $a \in (A \cup B)$, then $a \in A$ or $a \in B$. This implies that $M(A) \models S_a$ or $M(B) \models S_a$. Then, $(S_a, T) \in M(A)$ or $(S_a, T) \in M(B)$. On the other hand, if $a \notin (A \cup B)$, then $a \notin A$ and $a \notin B$. So, $M(A) \not\models S_a$ and $M(B) \not\models S_a$. Therefore, $(S_a, F) \in M(A)$ and $(S_a, F) \in M(B)$.

We can rewrite the model associated with $A \cup B$ in terms of the models $M(A)$ and $M(B)$ as follows:

$$\begin{aligned} M(A \cup B) = &\{(S_a, T) : (S_a, T) \in M(A) \vee (S_a, T) \in M(B)\} \\ &\cup \{(S_a, F) : (S_a, F) \in M(A) \wedge (S_a, F) \in M(B)\} \end{aligned}$$

By applying the definition of set intersection, the model associated with the set $A \cap B$ is:

$$M(A \cap B) = \{(S_a, T) \in S \times \{T, F\} : a \in (A \cap B)\} \cup \{(S_a, F) \in S \times \{T, F\} : a \notin (A \cap B)\}$$

If $a \in (A \cap B)$, then $a \in A$ and $a \in B$. So, $M(A) \models S_a$ and $M(B) \models S_a$. Therefore, $(S_a, T) \in M(A)$ and $(S_a, T) \in M(B)$. Meanwhile, if $a \notin (A \cap B)$, then $a \notin A$ or $a \notin B$. This implies that $(S_a, F) \in M(A)$ or $(S_a, F) \in M(B)$.

Therefore, we can rewrite the model associated with $M(A \cap B)$ in terms of $M(A)$ and $M(B)$ as follows:

$$M(A \cap B) = \{(S_a, T) : ((S_a, T) \in M(A)) \wedge ((S_a, T) \in M(B))\}$$
$$\cup \{(S_a, F) : ((S_a, F) \in M(A)) \vee ((S_a, F) \in M(B))\}$$

Using the definition of complement of a set, the model associated with $M(A')$ is:

$$M(A') = \{(S_a, T) \in S \times \{T, F\} : a \in A'\} \cup \{(S_a, F) \in S \times \{T, F\} : a \in A\}$$

We can rewrite the model $M(A')$ in terms of $M(A)$ using the same approach as the one used for $M(A \cup B)$ and $M(A \cap B)$ as follows:

$$M(A') = \{(S_a, T) : (S_a, F) \in M(A)\} \cup \{(S_a, F) : (S_a, T) \in M(A)\}$$

Example 3.2.1. Let H be the set given by $H = \{1, 2, 3, 4\}$ and A and B be the subsets of H given by $A = \{1, 2\}$ and $B = \{1, 3\}$. Then, the corresponding models for these subsets are: $M(A) = \{(S_1, T), (S_2, T), (S_3, F), (S_4, F)\}$ and $M(B) = \{(S_1, T), (S_2, F), (S_3, T), (S_4, F)\}$.

Since $A \cap B = \{1\}$, then $M(A \cap B) = \{(S_1, T), (S_2, F), (S_3, F), (S_4, F)\}$.

Following the definition of $M(A \cap B)$ in terms of $M(A)$ and $M(B)$, we obtain the same result without the need to find the intersection between the sets.

$$M(A \cap B) = \{(S_1, T), (S_2, F), (S_3, F), (S_4, F)\}$$

Similarly, since $A \cup B = \{1, 2, 3\}$, then

$$M(A \cup B) = \{(S_1, T), (S_2, T), (S_3, T), (S_4, F)\}$$

Following the definition of $M(A \cup B)$ in terms of the models associated to A and B, the same result is obtained.

Now, $A' = \{3, 4\}$, then $M(A') = \{(S_1, F), (S_2, F), (S_3, T), (S_4, T)\}$, which can be easily obtained from $M(A)$, without finding the complement of A.

From this example, we conclude that for nonempty subsets A and B of a set C, the easiest way to find the models associated with $A \cap B$, $A \cup B$ and A' is by using the models $M(A)$ and $M(B)$, instead of working with the set union, intersection or complement.

Let A and B be arbitrary subsets of a set S. Define the cartesian product as $A \times B = \{(a, b) : a \in A, b \in B\}$. The model associated with $A \times B$ is given by:

$$M(A \times B) = \{(S_{(a,b)}, T) : (a, b) \in A \times B, (S_{(a,b)}, F) : (a, b) \notin A \times B\}$$

Also, note that $M(A) \times M(B)$ is given by:

$$M(A) \times M(B) = \{((S_a, x), (S_b, y)) : (S_a, x) \in M(A), (S_b, y) \in M(B)\}$$

where $(S_i, x) \in S \times \{T, F\}$.

Consider the set $H = \{1, 2, 3, 4\}$ and the subsets $A = \{1, 2\}$ and $B = \{3, 4\}$. Then, $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$. The model associated with $A \times B$ is given by:

$$\begin{aligned} M(A \times B) = \{&(S_{(1,3)}, T), (S_{(1,4)}, T), (S_{(2,3)}, T), (S_{(2,4)}, T), (S_{(1,1)}, F), (S_{(1,2)}, F), \\ &(S_{(2,1)}, F), (S_{(2,2)}, F), (S_{(3,1)}, F), (S_{(3,2)}, F), (S_{(3,3)}, F), (S_{(3,4)}, F), \\ &(S_{(4,1)}, F), (S_{(4,2)}, F), (S_{(4,3)}, F), (S_{(4,4)}, F)\} \end{aligned}$$

The models associated with A and B are given by:

$$M(A) = \{(S_1, T), (S_2, T), (S_3, F), (S_4, F)\}$$

and

$$M(B) = \{(S_1, F), (S_2, F), (S_3, T), (S_4, T)\}$$

Then, $M(A) \times M(B)$ is given by:

$$\begin{aligned} M(A) \times M(B) = \{&((S_1, T), (S_1, F)), ((S_1, T), (S_2, F)), ((S_1, T), (S_3, T)), \\ &((S_1, T), (S_4, T)), ((S_2, T), (S_1, F)), ((S_2, T), (S_2, F)), \\ &((S_2, T), (S_3, T)), ((S_2, T), (S_4, T)), ((S_3, F), (S_1, F)), \\ &((S_3, F), (S_2, F)), ((S_3, F), (S_3, T)), ((S_3, F), (S_4, T)), \\ &((S_4, F), (S_1, F)), ((S_4, F), (S_2, F)), ((S_4, F), (S_3, T)), \\ &((S_4, F), (S_4, T))\} \end{aligned}$$

Comparing $M(A \times B)$ and $M(A) \times M(B)$, we can see that both have the same cardinality, 16 elements. The next step is to determine if there is any relationship between these two sets.

First, we define the map:

$$\phi : M(A) \times M(B) \to M(A \times B)$$
$$((S_a, x), (S_b, y)) \mapsto (S_{(a,b)}, z)$$

where x, y, z are in $\{T, F\}$, and z is true if and only if x and y are both true.

Let us show that ϕ is a surjective map.

Case 1: Let $(S_{(a,b)}, T) \in M(A \times B)$. Then, there exist $(S_a, T) \in M(A)$ and $(S_b, T) \in M(B)$, such that $\phi((S_a, T), (S_b, T)) = (S_{(a,b)}, T)$.

Case 2: Let $(S_{(a,b)}, F) \in M(A \times B)$. Then, there exist $(S_a, F) \in M(A)$ or $(S_b, F) \in M(B)$ such that $\phi((S_a, x), (S_b, y)) = (S_{(a,b)}, F)$, where x or y is false. Therefore, we conclude that ϕ is a surjective map.

Now, let $\phi((S_a, x), (S_b, y)) = \phi((S_c, z), (S_d, w))$. Then, $(S_{(a,b)}, u) = (S_{(c,d)}, v)$, where $x, y, z, w, u, v \in \{T, F\}$. Therefore, $S_{(a,b)} = S_{(c,d)}$ and $u = v$. From $S_{(a,b)} = S_{(c,d)}$ we have that $(a, b) = (c, d)$. So, $a = c$ and $b = d$.

We have two cases:

Case 1: Suppose that $u = v = T$. Then, x, y, z, w are true. So, $(S_a, T) = (S_c, T)$ and $(S_b, T) = (S_d, T)$. Therefore, we conclude that $((S_a, T), (S_b, T)) = ((S_c, T), (S_d, T))$.

Case 2: Let $u = v = F$. Then, we have that $x = F$ or $y = F$ and $z = F$ or $w = F$. Since $S_a = S_c$ and $S_b = S_d$, then the true value assignment has to be the same. If $x = F$ and $y = T$, then $z = F$ and $w = T$. So, $(S_a, F) = (S_c, F)$ and $(S_b, T) = (S_d, T)$. Therefore, $((S_a, F), (S_b, T)) = ((S_c, F), (S_d, T))$. A similar approach can be obtained for $x = F, y = F$ and $x = T, y = F$.

Now, suppose that $x = F, y = T$ and $z = T, w = F$. Then, $(S_a, F) \in M(A)$ implies that $a \notin A$, and $(S_c, T) \in M(A)$ implies that $c \in A$. But, since $S_a = S_c$, then $a = c$, which contradicts the fact that $a \notin A$ and $c \in A$. So, it is not possible that $x \neq z$ and $y \neq w$.

Finally, we can conclude that ϕ is a one to one function. We have just proved the following result:

Theorem 3.2.2. Given a set S, and two non-empty sets A and B, a bijection exists between the model $M(A) \times M(B)$ and $M(A \times B)$, given by:

$$\phi : M(A) \times M(B) \to M(A \times B)$$
$$((S_a, x), (S_b, y)) \mapsto (S_{(a,b)}, z)$$

where x, y, z are in (T, F), and z is true if and only if x and y are both true.

3.2.2 Groups

Let G be a group and $S = \{S_a : a \in G\}$ be the set of propositional letters associated with G. The set of logical symbols consists of the logical connectives $\{\wedge, \vee, ', \to, \leftrightarrow\}$ and the parenthesis as previously defined in Table 3–1.

Using the grammatical rules established in Table 3–2, define a sentential theory associated to G as

$$T(G) = \{S_e, S_a \wedge S_b \rightarrow S_{a-b} : a, b \in G\}$$

where e is the identity element of G. Let A be an arbitrary model of $T(G)$, that is, $A \models T(G)$, and define $\mu(A) = \{a \in G : A \models S_a\}$. Then, $\mu(A)$ is a subgroup of G.

Since $A \models T(G)$, then $A \models S_e$, so $e \in \mu(A)$. Now, assume that a and b are arbitrary elements of $\mu(A)$. Then, $A \models S_a$ and $A \models S_b$. So, $A \models S_a \wedge S_b$. By hypothesis, $A \models S_a \wedge S_b \rightarrow S_{a-b}$, then, $A \models S_{a-b}$. Therefore, $a - b \in \mu(A)$. So, $\mu(A)$ is a subgroup of G.

Now, let B be a subgroup of G and define $\tau(B) \models S_a$ if and only if $a \in B$. Then, $\tau(B) \models T(G)$.

Since B is a subgroup of G, then $e \in B$, so, $\tau(B) \models S_e$. Now, assume that $\tau(B) \models S_a$ and $\tau(B) \models S_b$. Then, $a \in B$ and $b \in B$ imply that $a - b \in B$, since B is a subgroup of G. We have that $\tau(B) \models S_a \wedge S_b$ and $\tau(B) \models S_{a-b}$, then, $\tau(B) \models S_a \wedge S_b \rightarrow S_{a-b}$. Therefore, $\tau(B) \models T(G)$.

Let us show that $\tau(\mu(A)) = A$, where A is a model of $T(G)$, and $\mu(\tau(B)) = B$, where B is a subgroup of G.

Let $x \in \mu(\tau(B))$ be an arbitrary element. Then, $\tau(B) \models S_x$. By definition of τ, we have that $x \in B$. Therefore, $\mu(\tau(B)) \subseteq B$. On the other hand, let x be an arbitrary element in B. Then, by definition of τ, $\tau(B) \models S_x$. So, by definition of μ, we have that $x \in \mu(\tau(B))$. Therefore, $B \subseteq \mu(\tau(B))$. So, we conclude that $\mu(\tau(B)) = B$.

Now, let us verify that $\tau(\mu(A)) = A$. Suppose that $\tau(\mu(A)) \models S_x$ for some $x \in G$. Then, $x \in \mu(A)$ by definition of τ. Also, by definition of μ, we obtain that $A \models S_x$. We have that $\tau(\mu(A)) \models S_x$ implies $A \models S_x$. On the other hand, let $A \models S_x$, for

some $x \in G$. By definition of $\mu(A)$, $x \in \mu(A)$ and by definition of τ, $\tau(\mu(A)) \models S_x$. Therefore, $\tau(\mu(A)) = A$.

We have proved the following result:

Theorem 3.2.3. Let G be a group and $T(G)$ the associated propositional theory given by:

$$T(G) = \{S_e, S_a \wedge S_b \rightarrow S_{a-b} : a, b \in G\}$$

There is a one to one correspondence between the subgroups of G and the models of the sentential theory $T(G)$.

Now, we will present a concrete example to illustrate this theorem for the group $G = \mathbb{Z}_4$.

Example 3.2.4. Let $G = (\mathbb{Z}_4, +)$, where $+$ is the addition module 4. Then $T(G)$ is given by the following set:

$$\begin{aligned} T(G) = \{&S_0, \quad S_0 \wedge S_0 \rightarrow S_0, \quad S_0 \wedge S_1 \rightarrow S_3, \quad S_0 \wedge S_2 \rightarrow S_2, \quad S_0 \wedge S_3 \rightarrow S_1, \\ &S_1 \wedge S_0 \rightarrow S_1, \quad S_1 \wedge S_1 \rightarrow S_0, \quad S_1 \wedge S_2 \rightarrow S_3, \quad S_1 \wedge S_3 \rightarrow S_2, \\ &S_2 \wedge S_0 \rightarrow S_2, \quad S_2 \wedge S_1 \rightarrow S_1, \quad S_2 \wedge S_2 \rightarrow S_0, \quad S_2 \wedge S_3 \rightarrow S_3, \\ &S_3 \wedge S_0 \rightarrow S_3, \quad S_3 \wedge S_1 \rightarrow S_2, \quad S_3 \wedge S_2 \rightarrow S_1, \quad S_3 \wedge S_3 \rightarrow S_0\} \end{aligned}$$

The subgroups of G can be easily shown to be: $H = \{0\}$, $K = \{0, 2\}$, and G. Then, the models associated with $T(G)$ are:

$$\begin{aligned} M(H) =&\{(S_0, T), (S_1, F), (S_2, F), (S_3, F)\}, \\ M(K) =&\{(S_0, T), (S_1, F), (S_2, T), (S_3, F)\}, \\ M(G) =&\{(S_0, T), (S_1, T), (S_2, T), (S_3, T)\} \end{aligned}$$

We can verify that any other assignment of true and false to the propositional letters will not satisfy all the propositions of $T(G)$. For example, let

$M(T) = \{(S_0, T), (S_1, T), (S_2, F), (S_3, F)\}$, be the assignment corresponding to the subset $T = \{0, 1\}$. We can easily show that T is not a subgroup of G, and $M(T)$ is not a model associated to $T(G)$, since, for example, the proposition $S_0 \wedge S_1 \rightarrow S_3$ is false.

From this example, we see that for a group G of order 4, $T(G)$ has 17 propositions. Analyzing the structure of $T(G)$, and taking G as a group of order n, the number of propositions of the form $S_a \wedge S_b \rightarrow S_{a-b}$ is n^2. So, including the proposition S_0, we obtain that the cardinality of $T(G)$, for a finite group G of order n, is $n^2 + 1$.

Now, let N be a subgroup of a group G. If we add the propositions of the form $S_n \rightarrow S_{a+n-a}$ to $T(G)$, where a is an arbitrary element of G and $n \in N$, we establish the following theory:

$$T(G_N) = \{S_e, S_a \wedge S_b \rightarrow S_{a-b}, S_n \rightarrow S_{a+n-a} : a, b \in G, n \in N\}$$

Let $A \models T(G_N)$ and $\mu(A) = \{a \in G : A \models S_a\}$. Then, $\mu(A)$ is a normal subgroup of G.

From Theorem 3.2.3, we know that $\mu(A)$ is a subgroup of G. Now, let $n \in \mu(A)$ and $a \in G$. Then, $A \models S_n$. Since $S_n \rightarrow S_{a+n-a}$, $A \models S_{a+n-a}$. Therefore, $a+n-a \in \mu(A)$. So, we conclude that $\mu(A)$ is a normal subgroup of G.

On the other hand, let B be a normal subgroup of G and define $\tau(B) \models S_a$ if and only if $a \in B$. Let show that $\tau(B) \models T(G_N)$.

From the fact that B is a subgroup of G, we have that $e \in B$, and for $a \in B$ and $b \in B$, $a - b \in B$. Then, by definition of models, $\tau(B) \models S_e$ and $\tau(B) \models S_a \wedge S_b \rightarrow S_{a-b}$. Now, let $x \in B$. Since B is a normal subgroup of G, we obtain that $a + x - a \in B$, for all $a \in G$. Then, $\tau(B) \models S_x$ and $\tau(B) \models S_{a+x-a}$. So,

$\tau(B) \models S_x \rightarrow S_{a+x-a}$. Therefore, we can conclude that if B is a normal subgroup of G, then $\tau(B) \models T(G_N)$.

Following a similar approach as in Theorem 3.2.3, we can show that $\tau(\mu(A)) = A$, where A is a model of $T(G_N)$, and $\mu(\tau(B)) = B$, where B is a normal subgroup of G.

Therefore, we just proved the following result:

Theorem 3.2.5. Let G be a group, N a normal subgroup of G and $T(G_N)$ its extended propositional theory, which can be compared with $T(G)$ as follows: $T(G_N) = T(G) \cup \{S_n \rightarrow S_{a+n-a} : a \in G, n \in N\}$. There is a one to one correspondence between the normal subgroups of G and the models associated with the sentential theory $T(G_N)$.

3.2.3 Rings

The next result was taken from Caceres [1].

Let R be a commutative ring, and $S = \{S_a : a \in R\}$ be the set of propositional letters associated with R. As established in previous section, the set of logical symbols consists of the logical connectives $\{\wedge, \vee, ', \rightarrow, \leftrightarrow\}$ and the parenthesis.

Using the rules established in Table 3–2, define the sentential theory associated with R as:

$$T(R) = \{S_0, S_a \wedge S_b \rightarrow S_{a-b}, S_a \rightarrow S_{ab} : (\forall a \in R)(\forall b \in R)\}$$

Let $A \subseteq S$, and define that $A \models S_a$ if and only if $(S_a, T) \in A$. If $A \models T(R)$, then $\mathbf{I}(A) = \{a \in R : A \models S_a\}$ is an ideal of R.

Since $A \models S_0$, then $0 \in \mathbf{I}(A)$. Let a and b be arbitrary elements in $\mathbf{I}(A)$. Then, $A \models S_a$ and $A \models S_b$. So, $A \models S_a \wedge S_b$. By hypothesis, we have that

$A \models S_a \wedge S_b \rightarrow S_{a-b}$, then, $A \models S_{a-b}$. Therefore, $a - b \in \mathbf{I}(A)$. Now, assume that $a \in \mathbf{I}(A)$ and $r \in R$. Then, $A \models S_a$. Since $A \models S_a \rightarrow S_{ar} (\forall r \in R)$, then $A \models S_{ar}$, and $ar \in \mathbf{I}(A)$ by definition of $\mathbf{I}(A)$. So, we conclude that $\mathbf{I}(A)$ is an ideal of R.

On the other hand, let I be an ideal of R and define $\mathbf{A}(I) \models S_a$ if and only if $a \in I$. Then, we can show that $\mathbf{A}(I) \models T(R)$.

First, since $0 \in R$ and I is an ideal, $0 \in I$ and $\mathbf{A}(I) \models S_0$. Let a and b be arbitrary elements of R. We want to show that $\mathbf{A}(I) \models S_a \wedge S_b \rightarrow S_{a-b}$. Suppose that $\mathbf{A}(I) \models S_a \wedge S_b$, then, $\mathbf{A} \models S_a$ and $\mathbf{A} \models S_b$. This implies that $a \in I$ and $b \in I$. But I is an ideal of R, so $a - b \in I$. So, $\mathbf{A}(I) \models S_{a-b}$. Therefore, since $\mathbf{A}(I) \models S_a \wedge S_b$ and $\mathbf{A}(I) \models S_{a-b}$, we conclude that $\mathbf{A}(I) \models S_a \wedge S_b \rightarrow S_{a-b}$. Finally, we want to show that $\mathbf{A}(I) \models S_a \rightarrow S_{ab}$. Let $a \in I$ and $b \in R$, then $ab \in I$ since I is an ideal of R. So, $\mathbf{A}(I) \models S_a$ and $\mathbf{A}(I) \models S_{ab}$. Therefore, we conclude that $\mathbf{A}(I) \models S_a \rightarrow S_{ab}$.

Since all the propositions in $T(R)$ are true in $\mathbf{A}(I)$, we conclude that $\mathbf{A}(I) \models T(R)$.

Following a similar approach as in Theorem 3.2.3, we can show that $\mathbf{A}(\mathbf{I}(A)) = A$ and $\mathbf{I}(\mathbf{A}(I)) = I$, where A is a model of $T(R)$ and I is an ideal of R

We have proved the following theorem:

Theorem 3.2.6. Let R be a commutative ring, and $T(R)$ its associated propositional theory. A one to one correspondence exists between the ideals of R and the models of the sentential theory $T(R)$.

Example 3.2.7. Let R be the ring given by $R = (\mathbb{Z}_4, +, \cdot)$, where $+$ is addition module 4 and $\cdot$ is multiplication module 4. We can verify that $T(R)$ is given by the

set:

$$\begin{aligned} T(R) = \{ & S_0, \quad S_0 \wedge S_0 \to S_0, \quad S_0 \wedge S_1 \to S_3, \quad S_0 \wedge S_2 \to S_2, \quad S_0 \wedge S_3 \to S_1, \\ & S_1 \wedge S_0 \to S_1, \quad S_1 \wedge S_1 \to S_0, \quad S_1 \wedge S_2 \to S_3, \quad S_1 \wedge S_3 \to S_2, \\ & S_2 \wedge S_0 \to S_2, \quad S_2 \wedge S_1 \to S_1, \quad S_2 \wedge S_2 \to S_0, \quad S_2 \wedge S_3 \to S_3, \\ & S_3 \wedge S_0 \to S_3, \quad S_3 \wedge S_1 \to S_2, \quad S_3 \wedge S_2 \to S_1, \quad S_3 \wedge S_3 \to S_0, \\ & S_0 \to S_0, \quad S_1 \to S_0, \quad S_1 \to S_1, \quad S_1 \to S_2, \quad S_1 \to S_3, \quad S_2 \to S_0, \\ & S_2 \to S_2, \quad S_3 \to S_0, \quad S_3 \to S_1, \quad S_3 \to S_2, \quad S_3 \to S_3 \} \end{aligned}$$

Analyzing this ring, we can verify that the ideals of R are given by:
$I_1 = \{0\}, \quad I_2 = \{0, 2\}, \quad I_3 = R$ and the models of $T(R)$ are:

$$\begin{aligned} M(I_1) =& \{(S_0, T), (S_1, F), (S_2, F), (S_3, F)\}, \\ M(I_2) =& \{(S_0, T), (S_1, F), (S_2, T), (S_3, F)\}, \\ M(I_3) =& \{(S_0, T), (S_1, T), (S_2, T), (S_3, T)\} \end{aligned}$$

Note that other assignments such as $M(A) = \{(S_0, T), (S_1, T), (S_2, F), (S_3, F)\}$ do not represent a model for $T(R)$, since propositions $S_0 \wedge S_1 \to S_3$ and $S_1 \to S_3$ are false. This corresponds to the fact that the set $A = \{0, 1\}$ is not an ideal of R.

As it was done for a group G and its associated sentential theory $T(G)$, we want to determine the order of $T(R)$ for a ring R of cardinality n. First, note that for the propositions of the form $\{S_0, S_a \wedge S_b \to S_{a-b}\}$, we have $n^2 + 1$ propositions. Now, we want to determine the number of propositions of the form $S_a \to S_{ab}$.

Let $R = \mathbb{Z}_n$ and $x \in \mathbb{Z}_n$ such that the greatest common divisor between x and n is d, denoted by $(x, n) = d$. Consider the set $A_{n/d} = \{0, 1, 2, \ldots, \frac{n}{d} - 1\}$. If $d = 1$, then we will have n different propositions of the form $S_x \to S_{xb}$. Suppose that $d \neq 1$.

For $0 \leq j < k < \frac{n}{d} - 1$ and $(x, n) = d \neq 1$, it can be seen that it is not possible for $xj \equiv xk \bmod n$. Suppose, by contradiction that $xj \equiv xk \bmod n$. Then, $n|(xj - xk)$. Since $(x, n) = d$, then there are t_1 and t_2 in $\mathbb{Z}_n$, such that $x = t_1 d$ and $n = t_2 d$. Then, $t_2|t_1(j-k)$. But as $(t_1, t_2) = 1$, we see that $t_2|(j-k)$. So, $t_2 < j - k < \frac{n}{d} - 1$, but $t_2 = \frac{n}{d}$. Therefore, we have that $\frac{n}{d} < j - k < \frac{n}{d} - 1$, which is a contradiction. So, we conclude that for $(x, n) = d \neq 1$, it is not possible that $xj \equiv xk \bmod n$, for $x \in \mathbb{Z}_n$. Then, $xj \neq xk$, for $0 \leq j < k < \frac{n}{d} - 1$. So, we have $\frac{n}{d}$ different propositions of the form $S_a \to S_{ab}$ for each $a \neq 0$.

We have just proven the following result:

Theorem 3.2.8. Given a finite ring $\mathbb{Z}_n$ with n elements, the cardinality of $T(\mathbb{Z}_n)$ is given by:

$$|T(\mathbb{Z}_n)| = n^2 + 2 + \sum_{a \in \mathbb{Z}_n - \{0\}} \frac{n}{(a, n)}$$

Reviewing Example 3.2.7, we see that $(1, 4) = 1$ and $(3, 4) = 1$. If $a = 1$ or $a = 3$, we have 4 different propositions. If $a = 2, (2, 4) = 2$, we have 2 additional propositions. Then, since $n = 4$, the cardinality of $T(\mathbb{Z}_4)$ is 28.

Now, if we consider $R = \mathbb{Z}_8$, then for each a in $\{1, 3, 5, 7\}$, we will have 32 propositions, since these numbers are relatively prime with 8. For $a = 2$ and $a = 6$, $(2, 8) = 2$ and $(6, 8) = 2$, we will have 8 additional propositions. Finally, for $a = 4$, $(4, 8) = 4$, we will have 2 more propositions. In summary, $|T(\mathbb{Z}_8)| = 108$.

3.2.4 Lattices

Let L be a lattice. The propositional language associated with L is defined as follows: $S = \{S_a : a \in L\}$ is the set of propositional letters, and the logical symbols are $\{\wedge, \vee, ', \to, \leftrightarrow, (,)\}$ as already defined in previous sections.

Define the sentential theory associated with L as:

$$T(L) = \{S_a \wedge S_b \to S_{a \wedge b} \wedge S_{a \vee b} : (\forall a \in L)(\forall b \in L)\}$$

Define the function

$$\mu : \text{ models of } T(L) \rightarrow \text{ Sublattices of L}$$
$$A \mapsto \mu(A)$$

where $\mu(A) = \{x \in L : A \models S_x\}$.
If $A \models T(L)$, then, $\mu(A)$ is a sublattice of L.

Let x and y be arbitrary elements in $\mu(A)$. Then, $A \models S_x$ and $A \models S_y$, which implies that $A \models S_x \wedge S_y$. But by hypothesis, $A \models S_x \wedge S_y \rightarrow S_{x\wedge y} \wedge S_{x\vee y}$, then $A \models S_{x\wedge y} \wedge S_{x\vee y}$. So, $A \models S_{x\wedge y}$ and $A \models S_{x\vee y}$. Therefore, applying definition of $\mu(A)$ we have that $x \wedge y \in \mu(A)$ and $x \vee y \in \mu(A)$. So, we obtain that $\mu(A)$ is a sublattice of L.

Now, if we define the function

$$\tau : \text{ Sublattices of L } \rightarrow \text{ Models of } T(L)$$
$$S \mapsto \tau(S)$$

where $\tau(S) \models S_x$ if and only if $x \in S$, then, if S is a sublattice of L, $\tau(S) \models T(L)$.

Let x and y be arbitrary elements of the sublattice S. Then, $x \wedge y \in S$ and $x \vee y \in S$. So, $\tau(S) \models S_x$, $\tau(S) \models S_y$, $\tau(S) \models S_{x\wedge y}$ and $\tau(S) \models S_{x\vee y}$. Therefore, $\tau(S) \models S_x \wedge S_y \rightarrow S_{x\wedge y} \wedge S_{x\vee y}$. So, we conclude that whenever S is a sublattice of a lattice L, $\tau(S) \models T(L)$.

Following a similar approach as in Theorem 3.2.3, we can verify that $\mu(\tau(S)) = S$, where S is a sublattice of L, and $\tau(\mu(A)) = A$, where A is a model of $T(L)$.

Therefore, we have proven the following result:

Theorem 3.2.9. Let L be a lattice and $T(L)$ its associated propositional theory. A one to one correspondence exists between the sublattices of L and the models of the sentential theory $T(L)$.

Example 3.2.10. Let L be the lattice represented in the following figure:

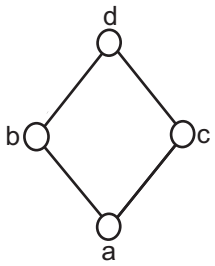

Figure 3–1: Lattice and Examples of Sublattices

Prior to presenting the corresponding propositional theory $T(L)$ associated with this lattice, recall that for all $a \in L$ and $b \in L$, $a \vee b \in L$ and $a \wedge b \in L$. Therefore, instead of writing the propositional letter $S_{a \vee b}$, we will write its equivalent propositional letter. If $a \wedge b = c$, for example, then we will write S_c instead of $S_{a \wedge b}$. That is, $S_{a \wedge b} = S_c$ if and only if $a \wedge b = c$.

Also, we will consider the commutativity of the operations in a lattice to simplify the corresponding theory. Finally, the theory $T(L)$ associated with the lattice in Figure 3–1 is given by:

$$\begin{aligned} T(L) = \{ & S_a \wedge S_a \rightarrow S_a \wedge S_a, \quad S_b \wedge S_b \rightarrow S_b \wedge S_b, \quad S_c \wedge S_c \rightarrow S_c \wedge S_c, \\ & S_d \wedge S_d \rightarrow S_d \wedge S_d, \quad S_a \wedge S_b \rightarrow S_a \wedge S_b, \quad S_a \wedge S_c \rightarrow S_a \wedge S_c, \\ & S_a \wedge S_d \rightarrow S_a \wedge S_d, \quad S_b \wedge S_c \rightarrow S_a \wedge S_d, \quad S_b \wedge S_d \rightarrow S_b \wedge S_d, \\ & S_c \wedge S_d \rightarrow S_c \wedge S_d \} \end{aligned}$$

Analyzing a lattice, we can see that every singleton[1] is a sublattice. Also, every chain is a sublattice. The following are some examples of sublattices of L:

$$A = \{a\}$$

$$B = \{a, b\}$$

$$C = \{a, c, d\}$$

The models associated with these sublattices are:

$$M(A) = \{(S_a, T), (S_b, F), (S_c, F), (S_d, F)\}$$

$$M(B) = \{(S_a, T), (S_b, T), (S_c, F), (S_d, F)\}$$

$$M(C) = \{(S_a, T), (S_b, F), (S_c, T), (S_d, T)\}$$

Meanwhile, the following set is not a sublattice of L:

$$D = \{a, b, c\}$$

since $b \vee c = d$ and $d \notin D$.

Note that $M(D) = \{(S_a, T), (S_b, T), (S_c, T), (S_d, F)\}$ is not a model for $T(L)$, since the proposition $S_b \wedge S_c \rightarrow S_a \wedge S_d$ is false.

We want to determine the cardinality of the theory associated with a lattice with n elements. From lattice theory, we have that each element in a lattice needs to be related to the others, but by commutativity, some of the propositions are repeated, and will not be counted in the theory.

From Example 3.2.10, we see that for a lattice with 4 elements, the corresponding theory will have 10 propositions: a is related to 4 elements, b is related to 3, c is

[1] A singleton is a lattice with one element.

related to 2 and d is related to itself. Then, for $n = 4$, $|T(L)| = 1 + 2 + 3 + 4 = 10$. This leads us to the following result:

Theorem 3.2.11. For a lattice with n elements, the number of propositions in $T(L)$ is given by:

$$|T(L)| = \frac{n(n+1)}{2}$$

Proof. To prove this result, mathematical induction on the order of L will be used.

For a lattice L with a single element a, $|T(L)| = 1$, that is, the lattice consists of the proposition $S_a \wedge S_a \rightarrow S_a \wedge S_a$.

Suppose, by hypothesis, that for a lattice with k elements

$$|T(L)| = \frac{k(k+1)}{2}$$

Let L be a lattice with $k+1$ elements. Then, by hypothesis, for the first k elements $T(L)$ will have $\frac{k(k+1)}{2}$ propositions. For the additional element, we will have $k+1$ propositions, since it will be related to every element in L and itself. Then, for a lattice L with $k+1$ elements, the number of propositions of $T(L)$ is given by:

$$|T(L)| = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

Therefore, by mathematical induction, we conclude that for a lattice with n elements,

$$|T(L)| = \frac{n(n+1)}{2}$$

where $T(L)$ consist of all the propositions of the form:

$$T(L) = \{S_a \wedge S_b \rightarrow S_{a \wedge b} \wedge S_{a \vee b} : (\forall a \in L)(\forall b \in L)\}$$

□

3.2.5 Algebras

In Chapter 2, we introduced the concept of an algebra as a pair $(A; \{f_1, \cdots, f_n\})$, where A is a non-empty set, and, for $1 \leq i \leq n$

$$f_i : \underbrace{A \times A \times \cdots \times A}_{\text{n times}} \to A$$

$$(a_1, a_2, \ldots, a_n) \mapsto f_i(a_1, a_2, \ldots, a_n)$$

We say that f_i is an n-ary function.

Let $\mathscr{U} = (\mathscr{A}, F)$ be an algebra. Define the set of symbols $S = \{S_{ab} : (a, b) \in A \times A\}$, and the logic connectives as usual.

Define the sentential theory associated with $\mathscr{U}$ as follows:

$$T(\mathscr{U}) = \left\{ \begin{array}{l} S_{aa}, S_{ab} \to S_{ba}, S_{ab} \wedge S_{bc} \to S_{ac}, \\ \bigwedge_{i=1}^{n} S_{a_i b_i} \to S_{f(a_1,a_2,\ldots,a_n) f(b_1,b_2,\ldots,b_n)} : \\ \text{for all } a, b, c, a_i, b_i \in A, \text{ and for all } f \text{ n-ary function} \end{array} \right\}$$

Define $\Theta(A) = \{(a, b) \in A \times A : A \models S_{ab}\}$. If $A \models T(\mathscr{U})$, then $\Theta(A)$ is a congruence of the algebra $\mathscr{U} = (\mathscr{A}, F)$. That is, $\Theta(A)$ is an equivalence relation and preserves the operations on A.

First, we need to show that $\Theta(A)$ is an equivalence relation, that is, $\Theta(A)$ is reflexive, symmetric and transitive. We will only show that $\Theta(A)$ is a transitive relation.

Let $(a, b) \in \Theta(A)$ and $(b, c) \in \Theta(A)$. Then, by definition of $\Theta(A)$, $A \models S_{ab}$ and $A \models S_{bc}$. So, $A \models S_{ab} \wedge S_{bc}$. By hypothesis, we have

$$A \models S_{ab} \wedge S_{bc} \to S_{ac}$$

then $A \models S_{ac}$. Applying definition of $\Theta(A)$, we have $(a, c) \in \Theta(A)$. Therefore, $\Theta(A)$ is a transitive relation.

Now, we will show that $\Theta(A)$ preserves the operations in A.

Let $f \in F$ be an arbitrary function and let $(a_i, b_i) \in \Theta(A)$ for $i = 1, 2, \ldots, n$. By definition of $\Theta(A)$, we have that $S \models S_{a_i b_i}$, for $i = 1, 2, \ldots, n$. Then,

$$A \models \bigwedge_{i=1}^{n} S_{a_i b_i}, \text{ and by hypothesis, } A \models \bigwedge_{i=1}^{n} S_{a_i b_i} \rightarrow S_{f(a_1,a_2,\ldots,a_n)f(b_1,b_2,\ldots,b_n)}$$

So, $A \models S_{f(a_1,a_2,\ldots,a_n)f(b_1,b_2,\ldots,b_n)}$, and, by definition of $\Theta(A)$, we have: $(f(a_1, a_2, \ldots, a_n), f(b_1, b_2, \ldots, b_n)) \in \Theta(A)$. Therefore, if $(a_i, b_i) \in \Theta(A)(\forall i)$, then $(f(a_i), f(b_i)) \in \Theta(A)(\forall i)$. We conclude that $\Theta(A)$ preserves the operation $f \in F$, and it is a congruence of the algebra $\mathscr{U} = (\mathscr{A}, F)$.

On the other hand, let $\theta \subseteq A \times A$, and define

$$\mathbf{A}(\theta) \models S_{ab} \Leftrightarrow (a, b) \in \theta$$

If θ is a congruence relation of the algebra $\mathscr{U} = (\mathscr{A}, F)$, then $\mathbf{A} \models T(\mathscr{U})$.

Let a, b, c be arbitrary elements in A. Since θ is a congruence relation, by reflexivity, we have that $(a, a) \in \theta$, then $\mathbf{A}(\theta) \models S_{aa}$. Assuming that $\mathbf{A}(\theta) \models S_{ab}$, then $(a, b) \in \theta$. Also, by symmetry, $(b, a) \in \theta$. So, $\mathbf{A} \models S_{ba}$ and $\mathbf{A} \models S_{ab} \rightarrow S_{ba}$. Now, let $\mathbf{A}(\theta) \models S_{ab}$ and $\mathbf{A}(\theta) \models S_{bc}$. Then, $(a, b) \in \theta$ and $(b, c) \in \theta$. By transitivity, we obtain that $(a, c) \in \theta$. Therefore, $\mathbf{A}(\theta) \models S_{ac}$ and $\mathbf{A}(\theta) \models S_{ab} \wedge S_{bc} \rightarrow S_{ac}$.

Let $f \in F$ be an n-ary function. We need to prove that

$$\mathbf{A} \models \bigwedge_{i=1}^{n} S_{a_i b_i} \rightarrow S_{f(a_1,a_2,\ldots,a_n)f(b_1,b_2,\ldots,b_n)}.$$

Suppose that

$$\mathbf{A} \models \bigwedge_{i=1}^{n} S_{a_i b_i}$$

Then $(a_i, b_i) \in \theta$ where $a_i, b_i \in A, i = 1, 2, \ldots, n$. Since θ is a congruence, $(f(a_1, a_2, \ldots, a_n), f(b_1, b_2, \ldots, b_n)) \in \theta$. Then, $\mathbf{A}(\theta) \models S_{f(a_1,a_2,\ldots,a_n)f(b_1,b_2,\ldots,b_n)}$.

Therefore,

$$\mathbf{A} \models \bigwedge_{i=1}^{n} S_{a_i b_i} \rightarrow S_{f(a_1,a_2,\ldots,a_n)f(b_1,b_2,\ldots,b_n)}.$$

So, $\mathbf{A}(\theta) \models T(\mathscr{U})$.

We can also prove that $\mathbf{A}(\Theta(A)) = A$, where A is a model of $T(\mathscr{U})$, and $\Theta(\mathbf{A}(\theta)) = \theta$, where θ is a congruence relation.

Therefore, we have proven the following result:

Theorem 3.2.12. Let $\mathscr{U} = (\mathscr{A}, F)$ be an algebra, where A is a non-empty set, F is a set of functions defined in A, and $T(\mathscr{U})$ its associated propositional theory. A one to one correspondence exists between the congruences of the algebra $\mathscr{U} = (\mathscr{A}, F)$ and the models of the sentential theory $T(\mathscr{U})$.

Example 3.2.13. Let $\mathscr{U} = (B, \vee, \wedge, ', 0, 1)$ be a Boolean Algebra. Define the set of logic symbols as $S = \{S_{ab} : (a, b) \in B \times B\}$, and the logic connectives as previously defined. Let a, b, c, d be arbitrary elements of the non-empty set B. The corresponding propositional theory associated with B is given by:

$$T(\mathscr{U}) = \left\{ \begin{array}{l} S_{aa}, S_{ab} \rightarrow S_{ba}, S_{ab} \wedge S_{bc} \rightarrow S_{ac}, S_{ab} \rightarrow S_{a'b'} \\ S_{ab} \wedge S_{cd} \rightarrow S_{(a\wedge c)(b\wedge d)} \wedge S_{(a\vee c)(b\vee d)} \end{array} \right\}$$

Considering the Boolean Algebra B as in Example 2.4.4, and Figure 2–8(a) and following a similar approach as in previous examples, the propositional theory $T(\mathscr{U})$ can be obtained. The propositional letters will be $S = \{S_{00}, S_{01}, S_{10}, S_{11}\}$. Let us analyze the truth value assignments that will result in a congruence for this Boolean Algebra.

Notice that since S_{aa} is a proposition in $T(\mathscr{U})$, S_{00} and S_{11} have to be true. We have four cases of truth value assignment for the remaining propositional letters, S_{01} and S_{10}.

Let S_{01} be false and S_{10} be true. By symmetry, we obtain the proposition $S_{10} \rightarrow S_{01}$. After evaluating, using Table 3–3, we conclude that this proposition is false. Therefore, this assignment does not represent a model for $T(\mathscr{U})$. Similarly, if we assign S_{01} as true and S_{10} as false, the proposition $S_{01} \rightarrow S_{10}$ is false. So, these two possibilities do not correspond to a model in $T(\mathscr{U})$.

On the other hand, if all the propositions are true, then trivially, we obtain a model for $T(\mathscr{U})$. After a short review of the propositions of $T(\mathscr{U})$, we have that if S_{01} and S_{10} are both false, this result in a model associated with $T(\mathscr{U})$.

Then, the congruences associated to the Boolean Algebra B are:

$$X = \{(0,0),(1,1)\}$$

$$Y = \{(0,0),(0,1),(1,0),(1,1)\}$$

The corresponding models are:

$$M(X) = \{(S_{00},T),(S_{01},F),(S_{10},F),(S_{11},T)\}$$

$$M(Y) = \{(S_{00},T),(S_{01},T),(S_{10},T),(S_{11},T)\}$$

3.2.6 R-Modules

Let R be a ring and RM be an arbitrary R-Module. Define the set of symbols $S = \{S_a : a \in RM\}$ and the propositional connectives as in Table 3–1. The theory associated with RM is defined as follows:

$T(RM) = \{S_0, S_a \wedge S_b \rightarrow S_{a-b}, S_a \rightarrow S_{ra} : (\forall a \in RM)(\forall b \in RM)(\forall r \in R)\}$

Let $A \models T(RM)$ and define:

$$\mu : \text{ Models of } T(RM) \rightarrow \text{ R-submodules of } RM$$

such that:

$$A \longmapsto \mu(A)$$

where

$$\mu(A) = \{a \in RM : A \models S_a\}$$

Let us show that if $A \models T(RM)$, then $\mu(A)$ is a R-submodule of RM. We can easily verify that $\mu(A)$ is a subgroup RM with respect to addition. Let $r \in R$ and $b \in \mu(A)$ be arbitrary elements. Since $b \in \mu(A)$, then $A \models S_b$. By hypothesis, $A \models S_b \rightarrow S_{rb}$. Therefore, $A \models S_{rb}$, and by definition, $rb \in \mu(A)$. So, $(\forall r \in R)(\forall b \in \mu(A))(rb \in \mu(A))$. Then, we conclude that $\mu(A)$ is a R-submodule of RM.

On the other hand, define:

$$\tau : \text{ R-submodules of } RM \rightarrow \text{ Models of } T(RM)$$

$$A \longmapsto \tau(A)$$

where $\tau(A) \models S_x$ if and only if $x \in A$, where A is a R-submodule of RM.

Let A be an arbitrary R-submodule of RM. Since A is a subgroup, then $0 \in A$ and if $a \in A$ and $b \in A$, then $a - b \in A$. So, by definition of τ see that $\tau(A) \models S_0$,

$\tau(A) \models S_a \wedge S_b \rightarrow S_{a-b}$. Now, let $r \in R$ and $a \in A$. Since A is a R-submodule, $ra \in A$. Then, by definition of τ, $\tau(A) \models S_a$ and $\tau(A) \models S_{ra} : (\forall r \in R)$.

Then, $\tau(A) \models S_a \rightarrow S_{ra}$. Therefore, $\tau(A) \models T(RM)$.

Now, we will show that $\tau(\mu(A)) = A$, where A is an arbitrary model of $T(RM)$, and $\mu(\tau(A)) = A$, where A is a R-submodule of RM. First, let $S_a \in S$ be an arbitrary propositional letter, such that $\tau(\mu(A)) \models S_a$. Then, by definition of τ, $a \in \mu(A)$. Also, by definition of μ, $A \models S_a$. Similarly, if $A \models S_a$, we can show that $\tau(\mu(A)) \models S_a$. Therefore, we conclude that $\tau(\mu(A)) \models S_a$ if and only if $A \models S_a$, so, $\tau(\mu(A)) = A$.

Let A be an arbitrary R-module of RM, and $a \in A$. By definition of τ, $\tau(A) \models S_a$, and by definition of μ, $a \in \mu(\tau(A))$. Therefore, $A \subseteq \mu(\tau(A))$. Similarly, we can prove that $\mu(\tau(A)) \subseteq A$. So, we conclude that $\mu(\tau(A)) = A$, where A is a R-submodule of RM.

Then, we just proved the following result:

Theorem 3.2.14. Let R be a ring, RM be a R-module, and $T(RM)$ its associated propositional theory. A one to one correspondence exists between the models of $T(RM)$ and the R-submodules of RM.

CHAPTER 4
CONCLUSIONS

- Given the cartesian product of two nonempty subsets, A and B, of a set C, we defined the models associated with those sets, and proved that there is a bijection ϕ from the model of $A \times B$ and the cartesian product of the models associated to A and B.
- Several interesting results of lattice structure, such as the Dedekind Theorem and Birkhoff Theorem were studied and proved. Also, for Boolean Algebras, some properties were presented. A sketch of proof for the Stone Theorem, which relates Boolean Algebras with Boolean Rings was provided.
- Given an algebraic structure $\mathscr{A}$, we can define propositional theories $T(\mathscr{A})$ such that a one to one correspondence exists between the models of $T(\mathscr{A})$ and the substructures of $\mathscr{A}$. Particularly, this relationship was studied for groups, rings, lattices, algebras and R-modules.
- The cardinality of different propositional theories was studied. In particular, a formula to calculate it was provided for finite groups, rings of the form $R = \mathbb{Z}_n$, and lattices, as follows:
  - For a group G of order n: $|T(G)| = n^2 + 1$
  - For a ring $R = \mathbb{Z}_n$

$$|T(\mathbb{Z}_n)| = n^2 + 2 + \sum_{a \in \mathbb{Z}_n - \{0\}} \frac{n}{(a, n)}$$

  - For a lattice

$$|T(L)| = \frac{n(n+1)}{2}$$

CHAPTER 5
SUGGESTIONS FOR FUTURE STUDIES

- Extend this study to include other algebraic structures, or substructures. For example, extend the propositional theory $T(R)$ for a ring R, in order to state a one to one correspondence between the models of the extended theory and the prime ideals of R.
- Extend the result for finite rings included on Theorem 3.2.8, which established a formula to find the cardinality of $T(R)$, when $R = \mathbb{Z}_n$.
- Continue the study of the cardinality of a finite theory associated with Algebras and R-Modules.

REFERENCE LIST

[1] Luis F. Cáceres. *Ultraproducts of Sets and Ideal Theories of Commutative Rings*. PhD thesis, University of Iowa, 1998.

[2] S. Burris; H.P. Sankappanavar. *A Course in Universal Algebra*. The millennium edition, 1993. Retrieved on November 30, 2005, available on www.math.uwaterloo.ca/ snburris/htdocs.html

[3] Herbert B. Enderton. *A Mathematical Introduction to Logic*. Harcourt Academic Press, California, 2001.

[4] H.I. Herstein. *Topics in Algebra*. 2nd edition, John Wiley and Sons Inc., New York, 1976.

[5] Thomas W. Hungerford. *Algebra*. Springer - Verlag New York Inc, 1974.

[6] David S. Dummit; Richard M. Foote. *Abstract Algebra*. John Wiley and Sons Inc., Third edition, New York, 2004.

[7] R. St. Andre; D. Smith; M. Eggen. *A Transition to Advanced Mathematics*. Brooks and Cole Publishing Company, Fourth edition, New York, 1997.

[8] Luis F. Cáceres. *Fundamentos de Matemáticas*. University of Puerto Rico, Mayagüez, first edition, 2003.