2

LATTICE AND BOOLEAN ALGEBRA

This chapter presents, lattice and Boolean algebra, which are basis of switching theory. Also presented are some algebraic systems such as groups, rings, and fields.

2.1 ALGEBRA

This book considers various **algebraic systems**. In this section, we present a general form of them. An algebraic system is defined by the tuple $\langle A, o_1, \ldots, o_k; R_1, \ldots, R_m; c_1, \ldots, c_k \rangle$, where, A is a non-empty set, o_i is a function $A^{p_i} \rightarrow A$, p_i is a positive integer, R_j is a relation on A, and c_i is an element of A.

Example 2.1 $\langle Z, + \rangle$ is an algebraic system consisting of a set of integers Z and addition $(+)$. $\langle Z, +, \leq \rangle$ is an algebraic system consisting of a set of integers Z, addition, and the relation "equal to or less than". ∎

2.2 LATTICE

The **lattice** is an algebraic system $\langle A, \vee, \cdot \rangle$ with two binary operations $\vee$ and $\cdot$, and arbitrary elements a, b, c in A satisfy the following four **axioms** (1)–(4):

(1) Idempotent laws: $a \vee a = a$, $a \cdot a = a$;
(2) Commutative laws: $a \vee b = b \vee a$, $a \cdot b = b \cdot a$;
(3) Associative laws: $a \vee (b \vee c) = (a \vee b) \vee c$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

T. Sasao, *Switching Theory for Logic Synthesis*

(4) Absorption laws: $a \vee (a \cdot b) = a$, $a \cdot (a \vee b) = a$.

Example 2.2

1. Let $A = \{0, 1\}$. Let $a \vee b = \max\{a, b\}$ and $a \cdot b = \min\{a, b\}$ be binary operations on A. Then, the algebraic system $\langle A, \vee, \cdot \rangle$ satisfies the axioms of the lattice.
2. Let Z be the set the integers. Let $a \vee b = \max\{a, b\}$ and $a \cdot b = \min\{a, b\}$ be binary operations on Z. Then, the algebraic system $\langle Z, \vee, \cdot \rangle$ satisfies the axioms of the lattice.
3. Let $S = \{a, b\}$. Let $\cup$ and $\cap$ be binary operations on $P(S) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$. Then, the algebraic system $\langle P(S), \cup, \cap \rangle$ satisfies the axioms of the lattice.
4. Let $A = \{1, 2, 3, 6\}$. Let $a \vee b =$(least common multiple of a and b), and $a \wedge b =$(greatest common divisor of a and b) be binary operations on A. Then, the algebraic system $\langle A, \vee, \wedge \rangle$ satisfies the axioms of the lattice. ∎

As shown in the above example, various algebraic systems satisfy the axioms of the lattice. Note that each example is a special case of the abstract algebraic system defined by the axioms. Such an example is called a **model** of the algebraic system. In general, many models satisfy the algebraic system defined by the axioms.

2.3 DISTRIBUTIVE LATTICE AND COMPLEMENTED LATTICE

The lattice $\langle A, \vee, \cdot \rangle$ satisfying the following axiom is a **distributive lattice.**

(5) Distributive laws: $a \vee (b \cdot c) = (a \vee b) \cdot (a \vee c)$, $a \cdot (b \vee c) = (a \cdot b) \vee (a \cdot c)$.

Example 2.3 The ordered set represented by the Hasse diagram in Fig. 2.1 is a distributive lattice. The ordered set represented by the Hasse diagram in Fig. 2.2 is a lattice, but not a distributive lattice. In Fig. 2.2(a), the distributive law is not satisfied since $a \cdot (b \vee c) = a \cdot 1 = a$, and $a \cdot b \vee a \cdot c = b \vee 0 = b$ ∎

Let a lattice $\langle A, \vee, \cdot \rangle$ have a maximum element 1 and a minimum element 0. For any element a in A, if there exists an element x_a such that $a \vee x_a = 1$ and $a \cdot x_a = 0$, then the lattice is a **complemented lattice.** In this case, x_a

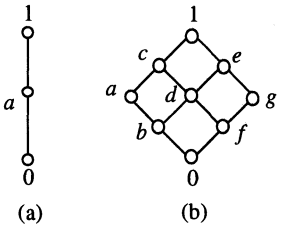

Figure 2.1 Examples of distributive lattice.

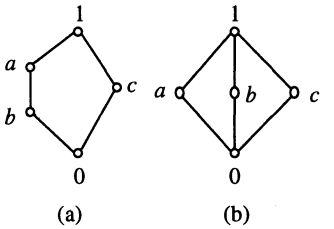

Figure 2.2 Examples of non-distributive lattice.

is a **complement** of a. A **complemented distributed lattice** is a Boolean algebra, which is introduced in the next part. In general, a complement is not unique as shown in the next.

Example 2.4

1. In Fig. 2.1(a), there is no complement for a.
2. In Fig. 2.2(a), the complement of a is c, and the complement of b is also c.
3. In Fig. 2.2(b), the complements of c are a and b. ∎

2.4 BOOLEAN ALGEBRA

2.4.1 Boolean Algebra

Let B be a set with at least two elements 0 and 1. Let two binary operations $\vee$ and $\cdot$, and a unary operation $^-$ are defined on B. The algebraic system $\langle B, \vee, \cdot, ^-, 0, 1\rangle$ is a **Boolean algebra**, if for arbitrary elements a, b and c in B the following postulates are satisfied:

(1) Idempotent laws: $a \vee a = a,\ a \cdot a = a$;
(2) Commutative laws: $a \vee b = b \vee a,\ a \cdot b = b \cdot a$;
(3) Associative laws: $a \vee (b \vee c) = (a \vee b) \vee c$,
$a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(4) Absorption laws: $a \vee (a \cdot b) = a,\ a \cdot (a \vee b) = a$;

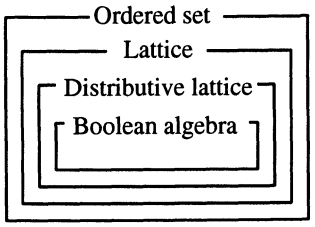

Figure 2.3 Relation of algebraic systems.

(5) Distributive laws: $a \vee (b \cdot c) = (a \vee b) \cdot (a \vee c)$,
$a \cdot (b \vee c) = (a \cdot b) \vee (a \cdot c)$;
(6) Involution: $\bar{\bar{a}} = a$;
(7) Complements: $a \vee \bar{a} = 1,\ a \cdot \bar{a} = 0$;
(8) Identities: $a \vee 0 = a,\ a \cdot 1 = a$;
(9) $a \vee 1 = 1,\ a \cdot 0 = 0$;
(10) De Morgan's laws: $\overline{a \vee b} = \bar{a} \cdot \bar{b},\ \overline{a \cdot b} = \bar{a} \vee \bar{b}$.

In the above axioms, $\vee, \cdot, and\ ^-$ are called **Boolean sum, Boolean product,** and **complement**, respectively. A Boolean algebra is a distributive lattice satisfying the conditions (6)–(10) (Fig. 2.3).

Huntington's Postulates

Boolean algebra is the algebra satisfying the ten axioms in Section 2.4.1. However, to verify whether the given algebra is Boolean algebra or not, we need only to check the following four axioms, the **Huntington's postulates.**

Identities: $a \vee 0 = a,\ a \cdot 1 = a$;
Commutative laws: $a \vee b = b \vee a,\ a \cdot b = b \cdot a$;
Distributive laws: $a \vee (b \cdot c) = (a \vee b) \cdot (a \vee c),\ a \cdot (b \vee c) = (a \cdot b) \vee (a \cdot c)$;
Complements: $a \vee \bar{a} = 1,\ a \cdot \bar{a} = 0$.

From the above four axioms, we can derive the other axioms of the Boolean algebra.

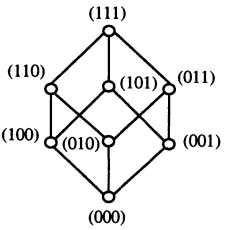

Figure 2.4
Hasse diagram of B^3.

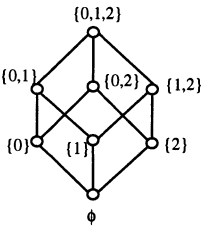

Figure 2.5
Hasse diagram of $P(\{0,1,2\})$.

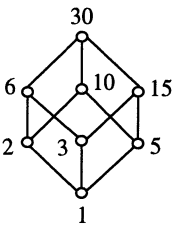

Figure 2.6
Hasse diagram of $A(30)$.

2.4.2 Models of Boolean Algebra

Boolean Algebra Over {0, 1}

Let B={0, 1}. $\langle B, \vee, \cdot, \bar{}\ , 0, 1\rangle$ is the simplest (model of the) Boolean algebra.

Boolean Algebra Over Boolean Vectors

In an n-dimensional vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$, if each element is 0 or 1, then $\boldsymbol{a}$ is an ***n*-dimensional Boolean vector**. Let $\boldsymbol{B}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \{0,1\}\}$ be the set of n-dimensional Boolean vectors. Let two elements in $\boldsymbol{B}^n$ be $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$. Define the operations $\vee, \cdot, and\ \bar{}$ as follows: $\boldsymbol{a} \vee \boldsymbol{b} = (a_1 \vee b_1, a_2 \vee b_2, \ldots, a_n \vee b_n)$, $\boldsymbol{a} \cdot \boldsymbol{b} = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$, and $\bar{\boldsymbol{a}} = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n)$.
Then, $\langle B^n, \vee, \cdot, \bar{}\ , \boldsymbol{0}, \boldsymbol{1}\rangle$ is a (model of the) Boolean algebra, where, $\boldsymbol{0} = (0, 0, \ldots, 0)$, and $\boldsymbol{1} = (1, 1, \ldots, 1)$. Fig. 2.4 is the Hasse diagram of B^3.

Boolean Algebra Over Power Set

Let A be a non-empty set, and let $P(A)$ be a power set of A. For each element of $P(A)$, if the operations $\cup, \cap$, and $\bar{}$ correspond to the union, the intersection, and the complement operation, respectively, then the algebraic system $\langle P(A), \cup, \cap, \bar{}\ , \phi, A\rangle$ is a (model of the) Boolean algebra. Fig. 2.5 shows the Hasse diagram of $P(\{0,1,2\})$.

Example 2.5 Let $A(30)$ be the set of positive integers that are divisor of 30. Let $a \vee b$ =(the least common multiple of a and b), $a \wedge b$ =(the greatest common divisor of a and b), and $\bar{a} = 30/a$ (the quotient obtained by dividing 30 by a). Then, the algebraic system $\langle A(30), \vee, \wedge, \bar{}, 1, 30\rangle$ is a (model of the) Boolean algebra. Fig. 2.6 shows the Hasse diagram of $A(30)$. ∎

Isomorphic Boolean Algebra

Note that Figs. 2.4, 2.5, and 2.6 have the same structures. In this case, these Boolean algebra are **isomorphic** to each other. Two Boolean algebras $\langle A, \vee, \cdot, \bar{}, 0_A, 1_A\rangle$ and $\langle B, \vee, \cdot, \bar{}, 0_B, 1_B\rangle$ are isomorphic iff there is the mapping $f : A \rightarrow B$, such that

1) for arbitrary $a, b \in A$, $f(a \vee b) = f(a) \vee f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$, and $f(\bar{a}) = \bar{f}(a)$, and
2) $f(0_A) = 0_B$, $f(1_A) = 1_B$ hold.

An arbitrary finite Boolean algebra is isomorphic to the Boolean algebra $\langle B^n, \vee, \cdot, \bar{}, 0, 1\rangle$, which consists of n-dimensional binary vectors, for some integer n. Therefore, if the number of the elements in the algebra is not the power of two, then it is not a Boolean algebra.

Example 2.6 Fig. 2.7 shows the Hasse diagram of B^4. ∎

2.4.3 De Morgan's Theorem

In the Boolean algebra, the De Morgan's laws or the **De Morgan's theorem** holds:
$\overline{a \cdot b} = \bar{a} \vee \bar{b}$, $\overline{a \vee b} = \bar{a} \cdot \bar{b}$.
These equations can be generalized for the n-variable case:
$\overline{x_1 \cdot x_2 \cdot \cdots \cdot x_n} = \bar{x}_1 \vee \bar{x}_2 \vee \cdots \vee \bar{x}_n$,
$\overline{x_1 \vee x_2 \vee \cdots \vee x_n} = \bar{x}_1 \cdot \bar{x}_2 \cdot \cdots \cdot \bar{x}_n$.

Definition 2.1 *Let $\langle B, \vee, \cdot, \bar{}, 0, 1\rangle$ be a Boolean algebra. The variable that takes arbitrary values in the set B is a* **Boolean variable**. *The expression that is obtained from the Boolean variables and constants by combining with the operators $\vee$, $\cdot$, $\bar{}$ and parenthesis is a* **Boolean expression**. *If a map-*

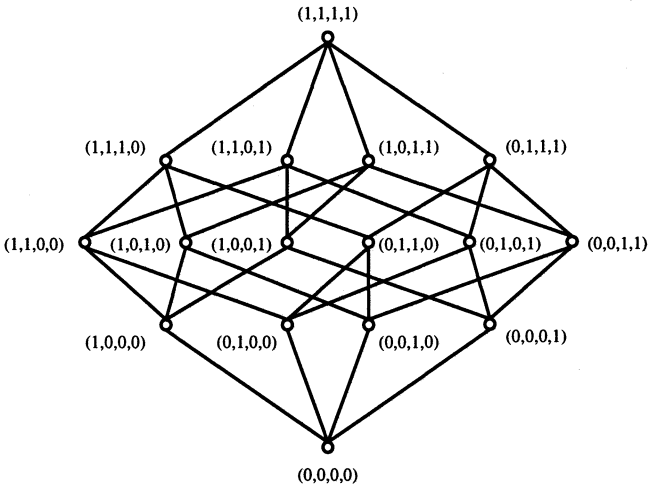

Figure 2.7 Hasse diagram of B^4.

ping $f{:}B^n \to B$ *is represented by a Boolean expression, then* f *is a* **Boolean function**. *However, not all the mappings* $f : B^n \to B$ *are Boolean functions.*

In Boolean expressions, the following **generalized De Morgan's theorem** holds.

Theorem 2.1 *Let* $F(x_1, x_2, \ldots, x_n)$ *be a Boolean expression. Then, the complement of the Boolean expression* $\overline{F}(x_1, x_2, \ldots, x_n)$ *is obtained from* F *as follows:*

1) Add the parenthesis according to the order of operations.
2) Interchange $\vee$ *with* $\cdot$.
3) Interchange x_i *with* $\bar{x}_i$.
4) Interchange 0 with 1.

Example 2.7 Let $F = x \vee \bar{y}z$. By applying the De Morgan's theorem, we have
$\overline{x \vee (\bar{y} \cdot z)} = \bar{x} \cdot (y \vee \bar{z})$. ∎

2.4.4 Principle of Duality

In the axioms of Boolean algebra (1)–(10), in an equation that contains $\vee$, $\cdot$, 0, or 1, if we interchange $\vee$ with $\cdot$, and/or 0 with 1, then the another equation holds. In general, this is true. In other words, given an equation in a Boolean algebra, the equation that is obtained from the equation by interchanging $\vee$ with $\cdot$, and/or 0 with 1 also holds. This property is the **principle of duality.**

Dual Boolean Expressions

Let A be a Boolean expression. The **dual** A^D is defined recursively as follows:

(1) $0^D = 1$.
(2) $1^D = 0$.
(3) If x_i is a variable, then ${x_i}^D = x_i (i = 1, \ldots, n)$.
(4) If A, B, and C are Boolean expressions, and $A = B \vee C$, then $A^D = B^D \cdot C^D$.
(5) If A, B, and C are Boolean expressions, and $A = B \cdot C$, then $A^D = B^D \vee C^D$.
(6) If A and B are Boolean expressions, and $A = \overline{B}$, then $A^D = \overline{(B^D)}$.

Applications of the Principle of Duality

Let A and B be Boolean expressions. The symbol $\equiv$ denotes that two expressions represent the same function. If $A \equiv B$, then $A^D \equiv B^D$. In this book, we distinguish a Boolean expression and the function represented by the expression. However, we often do not distinguish them, as in $F(x, y) = x \vee \bar{y} = \overline{(\bar{x} \cdot y)}$.

Example 2.8 Consider the identity: $xy \vee \bar{y}z = xy \vee \bar{y}z \vee xz$. If we apply the principle of duality to this equation, we have another identity: $(x \vee y)(\bar{y} \vee z) = (x \vee y)(\bar{y} \vee z)(x \vee z)$. ∎

As shown in the above example, the symbols for multiplication $\cdot$ are often omitted.

Example 2.9 Consider the Boolean algebra $B = \{0, 1, a, \bar{a}\}$. In this case, check whether the one-variable function $B \rightarrow B$ shown in Table 2.1 is a Boolean function or not. In a Boolean function, the following relation holds

Table 2.1

x	$f(x)$
0	a
1	1
a	$\bar{a}$
$\bar{a}$	1

Table 2.2

x_1	x_2	f	g	$f \vee g$	$f \cdot g$	$\bar{f}$	$\bar{g}$
0	0	0	0	0	0	1	1
0	1	1	0	1	0	0	1
1	0	1	0	1	0	0	1
1	1	0	1	1	0	1	0

(Problem 2.18): $f(x) = \bar{x}f(0) \vee xf(1)$. By assigning the values from Table 2.1, we have $f(x) = \bar{x} \cdot a \vee x \cdot 1$. Next, by assigning $x = a$, we have $f(a) = \bar{a} \cdot a \vee a \cdot 1 = 0 \vee a = a$. However, as shown in Table 2.1, $f(a) = \bar{a}$. Therefore, f is not a Boolean function. ∎

2.5 LOGIC FUNCTION

2.5.1 Two-valued Logic Function

Let $B = \{0, 1\}$. A mapping $B^n \rightarrow B$ is always represented by a Boolean expression. This mapping is a **two-valued logic function** or, a **switching function**. There are 2^n elements in B^n, and 2 elements in B. So, the total number of n-variable function is 2^{2^n}. Let us define the operations $\vee$, $\cdot$, and $\bar{}$ among logic functions as follows:

$$f \vee g = h \Leftrightarrow f(x_1, x_2, \ldots, x_n) \vee g(x_1, x_2, \ldots, x_n) = h(x_1, x_2, \ldots, x_n),$$

where x_i may take either 0 or 1, and the value of the function is computed by using the rule of the Boolean algebra $\{0, 1\}$. Similarly, $f \cdot g = h$ is also defined. And the complement of the function is defined as follows:

$$\bar{f} = g \Leftrightarrow \bar{f}(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n).$$

Example 2.10 Consider the case of n=2. The function f maps (0,1) and (1,0) to 1, and other combinations to 0 as shown in Table 2.2. On the other hand, g maps only (1,1) to 1, and other combinations to 0. In this case, $f \vee g$ maps (0,0) to 0, and other combinations to 1. $f \cdot g$ maps all the combinations to 0. $\bar{f}$ maps (0,0) and (1,1) to 1, and other combinations to 0. $\bar{g}$ maps (1,1) to 0, and other combinations to 1. ∎

2.5.2 Boolean Algebra Composed of Logic Functions

Let $\mathcal{F}_n$ be a set of n-variable logic functions. Then, $\langle \mathcal{F}_n, \vee, \cdot, \bar{}, 0, 1 \rangle$ is a Boolean algebra with 2^{2^n} elements. The constant 0 function maps all the n-tuples to 0. Similarly, the constant 1 function maps all the n-tuples to 1.

2.5.3 Recursive Definition of Logical Expressions

A **logical expression** is obtained from logic variables and constants 0 and 1, combined with operations $\vee$, $\cdot$, and $\bar{}$. In other words, a logical expression is a Boolean expression where $B = \{0, 1\}$. For a human, to check whether the given expression is a logical expression or not is easy when the expression is simple. However, when the computer program manipulates the logical expressions or when the proof of theorem is necessary, the following **recursive definition** is more convenient.

Definition 2.2

1. *Constants 0 and 1 are logical expressions.*
2. *Variables $x_1, x_2, \ldots$,and x_n are logical expressions.*
3. *If E is a logical expression, then $(\overline{E})$ is also a logical expression.*
4. *If E_1 and E_2 are logical expressions, then $(E_1 \vee E_2)$ and $(E_1 \cdot E_2)$ are also logical expressions.*
5. *The logical expressions are obtained by finite applications of 1–4. In this case, parentheses may be deleted if it does not introduce ambiguity.*

2.5.4 Evaluation of Two-valued Logical Expressions

Given a logical expression and the values of the variables, we can evaluate the value of the expression. Formally, we have the following: An **assignment mapping** $\alpha : \{x_i\} \rightarrow \{0, 1\}$ $(i = 1, \ldots, n)$ is an assignment of logic values to all logical variables. For an assignment mapping α, the **valuation mapping** $\mid F \mid_\alpha$ of a logical expression F is defined recursively to obtain the value of the logic function.

(1) $| 0 |_\alpha = 0$ and $| 1 |_\alpha = 1$.
(2) If x_i is a variable, then $| x_i |_\alpha = \alpha(x_i)$ $(i = 1, 2, \ldots, n)$.
(3) If F is a logical expression, then $| \overline{F} |_\alpha = 1 \Leftrightarrow | F |_\alpha = 0$.
(4) If F and G are logical expressions, then $| F \vee G |_\alpha = 1 \Leftrightarrow (| F |_\alpha = 1$ or $| G |_\alpha = 1)$.
(5) If F and G are logical expressions, then $| F \cdot G |_\alpha = 1 \Leftrightarrow (| F |_\alpha = 1$ and $| G |_\alpha = 1)$.

Example 2.11 Let us evaluate the value of the logical expression $F : x \vee \bar{y} \cdot z$. Let the assignment α be $\alpha(x) = 0$, $\alpha(y) = 0$, and $\alpha(z) = 1$. Then, we have $| x \vee \bar{y} \cdot z |_\alpha = 1 \Leftrightarrow (| x |_\alpha = 1$ or $| \bar{y} \cdot z |_\alpha = 1)$. Next, since $| x |_\alpha = \alpha(x) = 0$, we have $| F |_\alpha = 1 \Leftrightarrow | \bar{y} \cdot z |_\alpha = 1$. Next, note that $| \bar{y} \cdot z |_\alpha = 1 \Leftrightarrow (| \bar{y} |_\alpha = 1$ and $| z |_\alpha = 1)$. Since, $\alpha(z) = 1$, we have $| F |_\alpha = 1 \Leftrightarrow | \bar{y} |_\alpha = 1$. Finally, since $| \bar{y} |_\alpha = 1 \Leftrightarrow \alpha(y) = 0$, and $| y |_\alpha = \alpha(y) = 0$, we have $| F |_\alpha = 1$. ∎

As shown in the above example, given a logical expression F and an assignment α, we can obtain the value of $| F |_\alpha$. The computations of $| F |_\alpha$ for the given logical expression and assignment often appear in logic design.

2.5.5 Equivalence of Logical Expressions

Let F and G be logical expressions. If $| F |_\alpha = | G |_\alpha$ holds for any assignment α, then F and G are **equivalent**, denoted by the symbol $F \equiv G$. The decision of equivalence for two logical expressions is very important in logic design and verification. Numerous logical expressions of n variables exist, and they can be classified into 2^{2^n} equivalence classes by the equivalence relation $(\equiv)$.

2.6 GROUP, RING, AND FIELD

In this section, we will study group, ring, and field. In a semigroup, only addition (or a multiplication) is defined. In a group, addition and subtraction (or multiplication and division) are defined. In a ring, addition, subtraction, and multiplication are defined. In a field, addition, subtraction, multiplication, and division are defined.

In switching theory, Boolean algebra is mainly used. However, in this section, we briefly introduce other algebraic systems. We assume that in these algebraic systems, "the algebra is **closed** under the operations". In other words, let S

be a set, and let $\oplus$ and $\cdot$ be the operations. If $x, y \in S$, then $x \oplus y \in S$ and $x \cdot y \in S$. The following axioms are basic in these algebraic systems.

A1. Associative law for addition: $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.
A2. Zero element for addition: For all x, a unique 0 element exist such that $x \oplus 0 = 0 \oplus x = x$.
A3. Inverse element for addition: For any x, there exists an element y such that $x \oplus y = y \oplus x = 0$.
A4. Commutative law for addition: $x \oplus y = y \oplus x$.
M1. Associative law for multiplication: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
M2. Unit element for multiplication: For any x, a unique 1 element exists such that $x \cdot 1 = 1 \cdot x = x$.
M3. Inverse element for multiplication: For any x, an element y exist such that $x \cdot y = y \cdot x = 1$.
M4. Commutative law for multiplication: $x \cdot y = y \cdot x$.
D1. Distributive law: Multiplication over addition. $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$.
D2. Distributive law: Addition over multiplication. $(y \oplus z) \cdot x = y \cdot x \oplus z \cdot x$.

2.6.1 Semigroup

When an algebraic system $\langle S, \cdot, 1 \rangle$ satisfies the axiom M1, then it is a semigroup. If $\langle S, \oplus, 0 \rangle$ satisfies the axiom A1, then it is also a semigroup. When an algebraic system $\langle S, \cdot, 1 \rangle$ satisfies axioms M1 and M2, then it is a **semigroup with identity** or is a **monoid**. If $\langle S, \oplus, 0 \rangle$ satisfies the axioms A1 and A2, then it is also a monoid.

Example 2.12 Let the set of non-negative integers be $N = \{0, 1, \ldots\}$. Then, $\langle N, \cdot, 1 \rangle$ and $\langle N, +, 0 \rangle$ are monoids. ∎

2.6.2 Group

When an algebraic system $\langle G, \cdot, 1 \rangle$ satisfies the axioms M1, M2, and M3, then it is a **group**. When the group also satisfies M4, it is a **commutative group**, or an **Abelian group**. In this definition, addition instead of multiplication may be used. In other words, if an algebraic system satisfies axiom A1, A2, and A3, then it is also a group. In this case, if it satisfies A4, then it is a commutative group.

Table 2.3 Addition and multiplication in Z_3.

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Example 2.13

1. Let Z be the set of integers. Then, $\langle Z, +, 0\rangle$ is a commutative group.
2. Let T be the set of multiples of 3. Then, $\langle T, +, 0\rangle$ is a commutative group.
3. Let $S = \{1, -1\}$. Then, $\langle S, \cdot, 1\rangle$ is a commutative group. ∎

2.6.3 Ring

When an algebraic system $\langle R, \oplus, \cdot, 0\rangle$ satisfies the axioms A1–A4, M1, D1 and D2, then it is a **ring**. If the ring satisfies M4, then it is a **commutative ring**. If a ring satisfies M2, then it is a **ring with identity**.

Example 2.14

1. Let Z be the set of integers. Then, $\langle Z, +, \cdot, 0\rangle$ is a commutative ring with a unit element.
2. Let $R[X]$ be the set of polynomials of X whose coefficients are real numbers. Then, $\langle R[X], +, \cdot, 0\rangle$ is a commutative ring. In this case the zero element is a polynomial where all the coefficients are 0s.
3. Let M be the set of square matrices whose elements are integers. Then, $\langle M, +, \cdot, 0\rangle$ is a ring. However, it is not commutative with respect to the multiplication. For example, let

$$M_1 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \text{ and } M_2 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

Then, $M_1 \cdot M_2 \neq M_2 \cdot M_1$. ∎

2.6.4 Field

When an algebraic system $\langle F, +, \cdot, 0, 1\rangle$ satisfies the axioms A1–A4, M1, M2, M4, D1, D2 and the following axiom M3*, then it is a **field**.

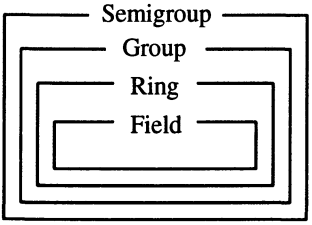

Figure 2.8 Relation of algebraic systems.

M3*. For an arbitrary non-zero element x, there exist y such that $x \cdot y = y \cdot x = 1$.

Example 2.15

1. Let Q be a set of the rational numbers. Then, $\langle Q, +, \cdot, 0, 1\rangle$ is a field.
2. Let R be a set of the real numbers. Then, $\langle R, +, \cdot, 0, 1\rangle$ is a field.
3. Let C be a set of the complex numbers. Then, $\langle C, +, \cdot, 0, 1\rangle$ is a field.
4. Let $Z_k = \{0, 1, \ldots, k-1\}$ $(k \geq 2)$. Then, $\langle Z_k, \oplus, \cdot, 0, 1\rangle$ is a field if k is a prime number. Where, addition $\oplus$ and multiplication $\cdot$ are modulo k operations. For example, when k=3, $Z_k = \{0, 1, 2\}$, and addition $\oplus$ and multiplication $\cdot$ can be defined as shown in Table 2.3.
5. Let R be the set of real numbers. Consider $R^2 = R \times R$. Let the addition $+$ and multiplication $\cdot$ in the set R^2 be $(x_1, x_2)+(y_1, y_2) = (x_1+y_1, x_2+y_2)$ and $(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)$, respectively. Then, the algebraic system $\langle R^2, +, \cdot, 0, 1\rangle$ is a commutative ring with the unit element (1, 1) for the multiplication. Also, (0, 0) is the zero element for addition. This algebraic system is not a field, since the condition M3* does not hold.
6. In the above example, if we replace the multiplication operation with $(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1 - x_2 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)$, then the algebraic system $\langle R^2, +, \cdot, 0, 1\rangle$ is a field. ∎

Fig. 2.8 shows the relations among semigroup, group, ring, and field.

Bibliographical Notes

Lattice theory is extensively described in the textbook [28]. A good, but formal reference book on Boolean algebra is [46].

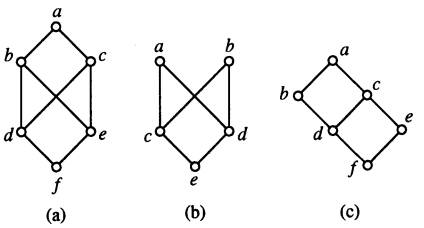

Figure 2.9

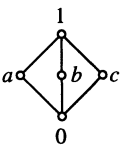

Figure 2.10

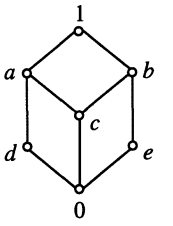

Figure 2.11

Exercises

2.1 Among the Hasse diagrams in Fig. 2.9, find a lattice. For each lattice show the operation tables.

2.2 A **modular lattice** is a lattice that satisfies the following conditions: If $x \geq z$, then $x \cdot (y \vee z) = (x \cdot y) \vee z$. Prove that the Hasse diagram in Fig. 2.10 represents a modular lattice. Is it a distributive lattice?

2.3 Does the Hasse diagram in Fig. 2.11 represent a modular lattice? Does it represent a distributive lattice?

2.4 Show that a distributive lattice is a modular lattice (See Exercise 2.2).

2.5 Let A be the set of positive integers that are divisors of 6. For $x, y \in A$, define the operations as follows:

$x \cdot y = GCD(x, y)$: The greatest common divisor of x and y.

$x \vee y = LCM(x, y)$: The least common multiple of x and y.

$\bar{x} = 6/x$: The quotient of 6 divided by x.
$I = 6$.
$O = 1$.
Show that $\langle A, \vee, \cdot, ^-, O, I\rangle$ is (a model of) a Boolean algebra.

2.6 Show the difference of a partially ordered set, a lattice, a distributive lattice, and a Boolean algebra. Show the relation between them by a Venn's diagram.

2.7 Consider the algebra on the set $A = \{0, 1, a\}$ that are defined in the following tables.

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

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

x	$\bar{x}$
0	1
1	0
a	a

Check whether each of the axioms in the Huntington's postulates holds.

2.8 Define the operations $\cdot$, $\vee$, and $^-$ (complement) so that the Boolean algebra holds on a set $A = \{0, 1, a, b\}$.

2.9 Show that the following two algebras are isomorphic each other.
Algebra 1: $\langle A, \vee, \cdot, ^-, O_A, I_A\rangle$. Let A be the set of positive integers that are divisors of 120. For $x, y \in A$, define as follows:
$x \cdot y = GCD(x, y)$: the greatest common divisor of x and y.
$x \vee y = LCM(x, y)$: the least common multiple of x and y.
$\bar{x} = 120/x$: the quotient of 120 divided by x.
$I_A = 120$, $O_A = 1$.
Algebra 2: $\langle B, \vee, \cdot, ^-, O_B, I_B\rangle$. Let $B = \{0, 1, 2, 3\} \times \{0, 1\} \times \{0, 1\}$. Then, the vector $\boldsymbol{x} = (x_1, x_2, x_3)$ that satisfies $x_1 \in \{0, 1, 2, 3\}, x_2 \in \{0, 1\}, x_3 \in \{0, 1\}$ is an element of B. Let $\boldsymbol{x} = (x_1, x_2, x_3)$ and $\boldsymbol{y} = (y_1, y_2, y_3)$ be an element of B, define the algebra as follows:
$\boldsymbol{x} \cdot \boldsymbol{y} = (\min(x_1, y_1), \min(x_2, y_2), \min(x_3, y_3))$.
$\boldsymbol{x} \vee \boldsymbol{y} = (\max(x_1, y_1), \max(x_2, y_2), \max(x_3, y_3))$.
$\bar{\boldsymbol{x}} = (3 - x_1, 1 - x_2, 1 - x_3)$.
$I_B = (3, 1, 1)$, $O_B = (0, 0, 0)$.

2.10 Verify that the $GF(4)$ shown in Table 2.4 is a field.

2.11 Let $*$ be a binary operation on the set R of real numbers. For $a, b \in R$, define $a * b = a + b - a \cdot b$ (where, $+$ and $\cdot$ denote ordinary addition and

Table 2.4 Operation table of $GF(4)$.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

multiplication, respectively). Show that the operation $*$ satisfies the associative law and the commutative law.

2.12 (M) Prove the De Morgan's laws by using the Huntington's postulates.

2.13 Modify the function in Table 2.1 to make it a Boolean function.

2.14 Show the following examples by using Hasse diagrams:
a. A partially ordered set, but not a lattice.
b. A lattice, but not a distributive lattice.
c. A distributive lattice, but not a Boolean algebra.

2.15 Let $T = \{0, 1, 2\}$. Define the binary relation $\leq$ on T^2 be as follows:

$$(x_1, y_1) \leq (x_2, y_2) \Leftrightarrow (x_1 \leq x_2) \text{ and } (y_1 \leq y_2).$$

Then, $\langle T^2, \leq \rangle$ is a partially ordered set.
a. Draw the Hasse diagram of partially ordered set.
b. Is it a lattice?
c. Is it a Boolean algebra?

2.16 In a Boolean algebra, prove the following without using truth tables: If $a \vee b = a \vee c$ and $ab = ac$, then $b = c$.

2.17 Let $Z_4 = \{0, 1, 2, 3\}$. Let addition $\oplus$ and multiplication $\cdot$ be modulo 4 operations. Is $\langle Z_4, \oplus, \cdot, 0, 1 \rangle$ a field?

2.18 (M) Let B be a Boolean algebra, and let $f : B \to B$ be a Boolean function. Then, show that

$$f(x) = \bar{x} f(0) \vee x f(1).$$

Note that the proof of Theorem 3.1 in Section 3.4 is for logic function. Show that it is true for a general Boolean function.