Introduction to Lattice Theory

D. E. RUTHERFORD
DSc DrMath

UNIVERSITY MATHEMATICAL MONOGRAPHS

Editor D. E. Rutherford DSc DrMath

OLIVER & BOYD LTD

RUTHERFORD | Introduction to Lattice Theory

2

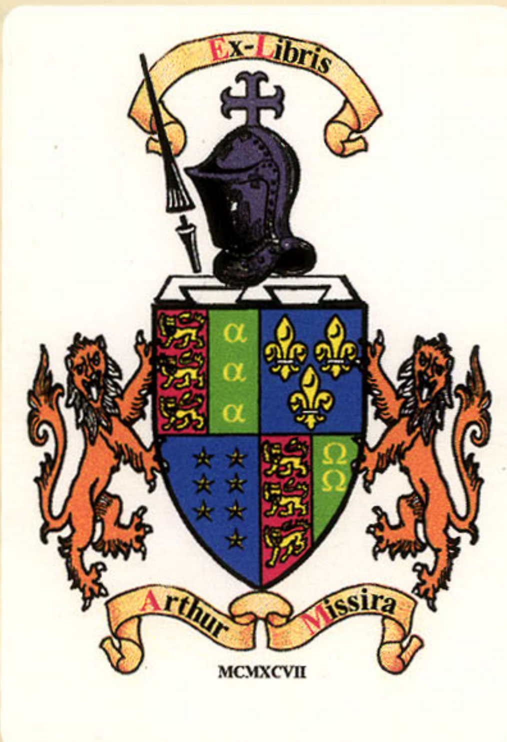
O&B

Lattice theory has many important applications not only to other branches of mathematics but also to logic and electrical engineering. Nevertheless it is also an important branch of mathematics in its own right and deserves greater emphasis in university courses than it has hitherto received.

The author's aim has been to present the basic concepts of Lattice theory in a lucid manner to those who have not studied the subject. Practically no previous mathematical knowledge is demanded, though, of course, some mathematical maturity is required. A large part of the book is devoted to the study of Boolean algebras and their applications to formal logic and the theory of switching circuits, and the application of Boolean matrices and determinants to switching circuits is given special attention. The breadth of Lattice theory is amply demonstrated by illustrations of its use in abstract algebra, geometry, topology and intuitionist logic in addition to the derivatives of Boolean algebra mentioned above.

Net price **35s**

INTRODUCTION
TO
LATTICE THEORY



UNIVERSITY MATHEMATICAL MONOGRAPHS

Editor

D. E. RUTHERFORD D.Sc., Dr.Math.

1.	*Integration, Measure and Probability* ..	H. R. Pitt, Ph.D., F.R.S.
2.	*Introduction to Lattice Theory* ..	D. E. Rutherford, D.Sc., Dr.Math.
3.	*Boundary Value Problems*	A. G. Mackie, Ph.D., F.R.S.E.
4.	*The Classical Moment Problem*	N. J. Akhiezer
5.	*Discourse on Fourier Series*	C. Lanczos, Dr.Phil., M.R.I.A.

INTRODUCTION TO LATTICE THEORY

D. E. RUTHERFORD

D.Sc., Dr.Math.

Gregory Professor of Applied Mathematics in the University of St. Andrews

OLIVER & BOYD
EDINBURGH AND LONDON

OLIVER AND BOYD LTD

Tweeddale Court
Edinburgh 1

39a Welbeck Street
London W 1

First published 1965
Reprinted with minor corrections 1966

Printed in Great Britain by
Oliver and Boyd Ltd., Tweeddale Court, Edinburgh

PREFACE

THIS volume has grown out of and has been based upon courses of lectures given in the University of St. Andrews and in the University of Notre Dame, Indiana. In the preparation of these lectures much use was made of the volumes by Garrett Birkhoff, H. Hermes, G. Nöbeling and the volume by M. L. Dubreil-Jacotin, L. Lesieur and R. Croisot and the author freely acknowledges his indebtedness to these authors. The fact that a study of lattice theory requires practically no previous mathematical knowledge, though it does of course demand considerable mathematical maturity, makes the subject a very suitable one with which to introduce undergraduates to abstract algebra, while the growing importance of the subject indicates that a reasonably elementary exposition in the English language would be a desirable addition to the existing literature. Of the books mentioned above only the well-known treatise by Birkhoff is written in English and this valuable work is directed at more sophisticated readers than those for whom the present volume is intended. The aim of the present work is therefore to provide an introduction to the simpler parts of a subject of great intrinsic beauty and to indicate some of its very numerous applications.

Many friends have assisted in the preparation of this volume. In particular, I am greatly indebted to Mr. C. G. Gibson for reading the manuscript, to Dr. T. S. Blyth for reading the proofs and to Dr. P. H. Fantham and Prof. A. D. Woozley for their valuable criticisms of certain sections of the book. All of these have made valuable suggestions of which I have taken advantage.

D. E. R.

St. Andrews, *October* 1964.

INTRODUCTION

THE theory of lattices, like group theory, provides an abstract formulation for many familiar concepts occurring in other branches of mathematics. Our intention is to define and describe the different types of lattice more commonly met with and in each case to give some indication of how they are related to other mathematical disciplines. From some points of view it might be said that Boolean algebras are the simplest and at the same time the most important lattices. Since a Boolean algebra is defined to be a lattice which is both distributive and complemented, it is logical to examine the properties of distributive lattices and of complemented lattices before Boolean algebras are investigated. Similarly, since every distributive lattice is a modular lattice the latter receives priority treatment. One could carry this process further by dealing with semi-modular lattices before modular lattices and with Brouwer algebras before Boolean algebras but because of the greater complexity of these topics, they will not be introduced in the earlier pages of this book.

It will be convenient to assume at the outset that the reader is familiar with the following logical symbols $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\in$ whose meanings are as follows:

$\wedge$ means ' and ' (conjunction of two statements)
$\vee$ means ' or ' (disjunction of two statements)
$\Rightarrow$ means ' implies that ' (logical implication)
$\Leftrightarrow$ means ' implies and is implied by ' (logical equivalence)
$\in$ means ' is an element of '

In addition we introduce the following abbreviation:

$\diamond$ means ' the proof is now complete '.

The basic ' cup ' and ' cap ' operations and the inclusion relation of lattice theory will usually be denoted by $\cup$, $\cap$ and $\geqq$ respectively, but the meanings of these symbols will depend upon the particular application of lattice theory being considered. In some cases, however, it will be desirable to use recognisably similar symbols to emphasise a distinction in meaning. For instance, in applications to set theory the symbols mentioned will more often be replaced by $\bigcup$, $\bigcap$, $\supseteq$.

Again, the signs $\rightarrow$ and $\rightarrow$ will be used to distinguish other types of implication from logical implication which is indicated by the sign $\Rightarrow$.

The illustrations I, II, III, IV of § 1 and the lattices represented by the Hasse diagrams of figs. 1, 2, 3, 4, 5 in § 3 will be referred to frequently by way of example in the course of the book. The reader should therefore remember where these are to be found.

CONTENTS

§ 1. Partially ordered sets

A **partially ordered set** or **poset** $\mathscr{P}$ is an algebraic system in which a binary relation $x \geqq y$ (read: x includes y) is defined, which satisfies the following postulates.

$\mathbf{P}_1$: For all x, $x \geqq x$. (reflexive property)

$\mathbf{P}_2$: $x \geqq y \wedge y \geqq x \Rightarrow x = y$. (antisymmetric property)

$\mathbf{P}_3$: $x \geqq y \wedge y \geqq z \Rightarrow x \geqq z$. (transitive property)

A binary relation which satisfies $\mathbf{P}_1$, $\mathbf{P}_2$, $\mathbf{P}_3$ is called an **inclusion relation** or an **order relation.** Associated with the relation $\geqq$ we can conveniently introduce the relations $\leqq$, $>$, $<$ defined as follows.

$$x \leqq y \Leftrightarrow y \geqq x;$$

$$x > y \Leftrightarrow x \geqq y \wedge x \neq y;$$

$$x < y \Leftrightarrow x \leqq y \wedge x \neq y.$$

It should be observed that the inclusion relation need not be defined for each pair of elements of $\mathscr{P}$. It is sufficient that it be defined for some pairs of elements. It should be emphasised also that $x \ngeqq y$ does not necessarily imply $x < y$.

The above abstract formulation of a poset will be clarified by considering some familiar illustrations of posets.

(I) $\mathscr{P}$ consists of all subsets of a class I (including the void set O and the class I itself); $x \geqq y$ means that the subset x includes the subset y as a subset proper or improper.

(II) $\mathscr{P}$ is the set $\mathscr{I}^+$ of all positive integers; $x \geqq y$ means that x has a factor y.

(III) $\mathscr{P}$ is the set $\mathscr{R}$ of all rational real numbers; $x \geqq y$ has its usual arithmetical meaning.

(IV) $\mathscr{P}$ is the set of all points, straight lines and planes of 3-dimensional projective geometry; $x \geqq y$ means y lies on x.

(V) $\mathscr{P}$ is the set of all human beings; $x \geqq y$ means either x and y are the same individual, or y is a descendant of x.

It is evident that a given set may form more than one poset under different inclusion relations. For instance, if we replace $\mathscr{R}$ in (III) by $\mathscr{I}^+$ then (II) and (III) give different partial orderings of the set $\mathscr{I}^+$ of all positive integers.

Any poset $\mathscr{P}$ can be represented by a **Hasse diagram** in which distinct elements of $\mathscr{P}$ are represented by distinct points and in which each relation $x \geqq y$ is represented by a line or lines which descend steadily from x to y. Nevertheless the fact that a point x is above the point y in a Hasse diagram is not sufficient to guarantee that $x \geqq y$. In fact, x and y are not related unless the diagram has at least one line which steadily descends, or steadily ascends, from one point to the other. Examples of Hasse diagrams are to be found on pp. 4, 12, etc.

Two posets $\mathscr{P}$ and $\mathscr{P}^*$ have identical structures if they can be represented by the same Hasse diagram, in which case they are said to be **isomorphic**. Expressed more formally, $\mathscr{P}$ and $\mathscr{P}^*$ are isomorphic if there is a $1-1$ correspondence $x \leftrightarrow x^*$ between the elements $x, y, \ldots$ of $\mathscr{P}$ and those $x^*, y^*, \ldots$ of $\mathscr{P}^*$ such that

$$x \geqq y \Leftrightarrow x^* \geqq y^*.$$

From $\mathbf{P}_1$, $\mathbf{P}_2$, $\mathbf{P}_3$ it quickly follows that

$\mathbf{P}_1'$: For all x, $x \leqq x$,

$\mathbf{P}_2'$: $x \leqq y \ \wedge \ y \leqq x \ \Rightarrow \ x = y$,

$\mathbf{P}_3'$: $x \leqq y \ \wedge \ y \leqq z \ \Rightarrow \ x \leqq z$.

This means that if $\geqq$ denotes one inclusion relation, then $\leqq$ denotes another. This yields the **duality principle** for posets which states that the converse of a partial ordering is itself a partial ordering. Consequently, if any theorem is true for all posets so is its dual obtained by interchanging the signs $\geqq$ and $\leqq$. If $\mathscr{P}$ is a poset, the Hasse diagram of its dual is obtained by inverting that of $\mathscr{P}$.

§ 2. Further definitions

If $\mathscr{P}$ has an element O such that $O \leqq x$ for all $x \in \mathscr{P}$, then O is called the **null element** of $\mathscr{P}$. $\mathscr{P}$ may not possess an O, but, if it does, O is unique. For, if O and O' were two null elements, then $O \leqq O'$ and $O' \leqq O$ and we can deduce from $\mathbf{P}_2$ that $O = O'$.

Dually we define the **all element** or **universal element** I of $\mathscr{P}$ such that $I \geqq x$ for all $x \in \mathscr{P}$. If I exists it is unique.

If $x > y$ but $x > z > y$ is not satisfied by any $z \in \mathscr{P}$ we say that x **covers** y. An element which covers O is called an **atom** or a **point.** Dually an element covered by I is called an **anti-atom**.

$\mathscr{P}$ is said to be **simply ordered** and is called a **chain** if

P_4: For any x and y, $x \geqq y \vee y \geqq x$.

Any two chains of n elements are isomorphic (see fig. 1 for $n = 5$).

Let $\mathscr{Q}$ be a subset of the elements of a poset $\mathscr{P}$. We call an element x of $\mathscr{P}$ an **upper bound** (u.b.) of $\mathscr{Q}$ if $x \geqq y$ for all $y \in \mathscr{Q}$. Further, an upper bound x of $\mathscr{Q}$ is said to be the **least upper bound** (l.u.b.) of $\mathscr{Q}$ if every upper bound x' of $\mathscr{Q}$ satisfies $x' \geqq x$. In particular, if any element y of $\mathscr{Q}$ is an upper bound of $\mathscr{Q}$, it must be the l.u.b. of $\mathscr{Q}$, for any other upper bound x' satisfies $x' \geqq y$. The l.u.b. of $\mathscr{Q}$ may not exist; if it exists its uniqueness follows from postulate $\mathbf{P}_2$.

Dually, we define **lower bound** (l.b.) and **greatest lower bound** (g.l.b.). The bounds so defined will have a familiar sound to readers familiar with mathematical analysis. For example if $\mathscr{Q}$ be the set of rational numbers less than unity in illustration (III) then l.u.b. of $\mathscr{Q}$ is 1 and any rational number greater than 1 is an u.b. of $\mathscr{Q}$. Again, in illustration (II) the g.l.b. of $\mathscr{Q}$ is just the H.C.F. of the integers contained in the set $\mathscr{Q}$ while any common factor is a l.b. of $\mathscr{Q}$.

It is customary to denote by $\bigcup \mathscr{Q}$ and $\bigcap \mathscr{Q}$ respectively the l.u.b. and g.l.b. of the subset $\mathscr{Q}$. We can also employ a slight modification of this notation by writing

$$\bigcup \mathscr{Q} = \bigcup_{x \in \mathscr{Q}} x, \quad \bigcap \mathscr{Q} = \bigcap_{x \in \mathscr{Q}} x.$$

Alternatively, if the context informs us that the elements of the subset $\mathscr{Q}$ are denoted by x_i we may write simply

$$\bigcup \mathscr{Q} = \bigcup x_i, \quad \bigcap \mathscr{Q} = \bigcap x_i.$$

In particular if the subset $\mathscr{Q}$ consists of a finite number n of elements $x_1, \ldots, x_n$, we may write, in analogy with the familar Σ and Π of elementary algebra,

$$\bigcup \mathscr{Q} = \bigcup_{i=1}^{n} x_i, \quad \bigcap \mathscr{Q} = \bigcap_{i=1}^{n} x_i.$$

Furthermore, we frequently call the l.u.b. of a subset the **union** of the elements which compose the subset, and correspondingly we call the g.l.b. of the subset the **intersection** or **meet** of its elements.

Even when $\mathscr{Q}$ contains only two elements of $\mathscr{P}$ a l.u.b. and a g.l.b. of $\mathscr{Q}$ need not exist in the case of the most general $\mathscr{P}$. In removing this possibility by restricting $\mathscr{P}$, we are led to define a lattice.

§ 3. First definition of a lattice

The concept of a lattice may be defined in two different ways and our next task is to formulate these definitions and to establish their equivalence. The first definition is as follows. A **lattice** is a poset such that any two elements of it possess both a l.u.b. and a g.l.b.

Let x, y be two elements of a lattice $\mathscr{L}$. Their l.u.b. or union is denoted by $x \cup y$ (read ' x union y ' or ' x cup y '), while their g.l.b. or intersection is denoted by $x \cap y$ (read ' x intersection y ' or ' x cap y '). The symbols $\cup$ and $\cap$ are sometimes referred to as ' cup ' and ' cap '. On occasion it may be desirable to employ different but recognisably similar symbols in place of $\cup$ and $\cap$ to denote l.u.b. and g.l.b.

In illustration (I), $x \cup y$ and $x \cap y$ denote the familiar set union and set intersection of set theory. For instance $x \cap y$ is the largest subset contained in both the subsets x and y.

In illustration (II) $x \cup y$ = L.C.M. (x, y), while $x \cap y$ = H.C.F. (x, y).

In illustration (III), $x \cup y = \max(x, y)$, while $x \cap y = \min(x, y)$.

Illustration (IV) does not, as it stands, form a lattice for two given points x and y have no g.l.b. However if we augment the elements of this poset to include a null element O which lies on every point and to include the whole three dimensional space I in which lies every other element, we obtain a lattice in which $x \cap y$ means the intersection of x and y in the geometrical sense and in which $x \cup y$ means the join of the elements x and y.

It is readily verified that there are only five non-isomorphic lattices with exactly five elements. Their Hasse diagrams are as follows.

FIG. 1

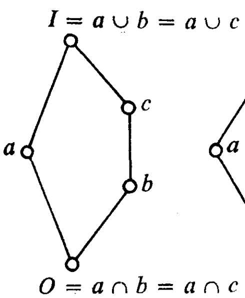


FIG. 2

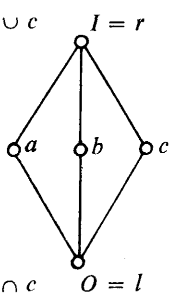


FIG. 3

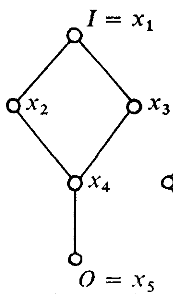


FIG. 4

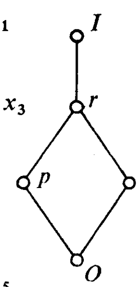


FIG. 5

We now demonstrate that the following six identities are valid for any lattice.

$\mathbf{L}_{1\cap}$: $x \cap y = y \cap x$; $\quad$ $\mathbf{L}_{1\cup}$: $x \cup y = y \cup x$, (commutative laws)

$\mathbf{L}_{2\cap}$: $x\cap(y\cap z) = (x\cap y)\cap z$; $\mathbf{L}_{2\cup}$: $x\cup(y\cup z) = (x\cup y)\cup z$, (associative laws)

$\mathbf{L}_{3\cap}$: $x\cap(x\cup y) = x$; $\mathbf{L}_{3\cup}$: $x\cup(x\cap y) = x$. (absorptive laws)

First, it is clear that $\mathbf{L}_{1\cap}$ and $\mathbf{L}_{1\cup}$ follow from our definitions of unions and intersections.

To establish $\mathbf{L}_{2\cap}$, write $s = y\cap z$ and $t = x\cap s = x\cap(y\cap z)$. Then $s\leqq y$, $s\leqq z$, $t\leqq x$, $t\leqq s$. By $\mathbf{P}_3'$, $t\leqq y$, $t\leqq z$. Thus t is a l.b. for the subset x, y, z. If r be any other l.b. of this subset, then $r\leqq x$, $r\leqq y$, $r\leqq z$ and so r is a l.b. of y and z. But s is the g.l.b. of y and z and consequently $r\leqq s$. This shows that r is a l.b. of x and s. But t is the g.l.b. of x and s, from which we conclude that $r\leqq t$. It follows that t is the g.l.b. of the subset x, y, z. In a similar manner we can show that $(x\cap y)\cap z$ is also the g.l.b. of the subset. Consequently

$$x\cap(y\cap z) = (x\cap y)\cap z,$$

which is $\mathbf{L}_{2\cap}$.

Dually, we can establish $\mathbf{L}_{2\cup}$.

These two laws permit us to drop the parentheses and to write unambiguously $x\cap y\cap z$ and $x\cup y\cup z$. Furthermore $x\cap y\cap z$ is the g.l.b. of the subset x, y, z and our arguments can clearly be extended to show that

$$x_1\cap x_2\cap\ldots\cap x_n = \text{g.l.b. of } x_1, \ldots, x_n = \bigcap_{i=1}^{n} x_i,$$

$$x_1\cup x_2\cup\ldots\cup x_n = \text{l.u.b. of } x_1, \ldots, x_n = \bigcup_{i=1}^{n} x_i.$$

We see that in the case of a finite number of elements x_i the expression $\bigcap x_i$ can be regarded as a shorthand notation for $x_1\cap\ldots\cap x_n$. In the case of infinitely many x_i however we cannot always give $\bigcap x_i$ such an interpretation and it must be thought of solely as the g.l.b. of the set of elements x_i. Corresponding remarks apply to the expression $\bigcup x_i$.

Turning now to $\mathbf{L}_{3\cap}$, write $p = x\cup y$, $q = x\cap p = x\cap(x\cup y)$. Then $p\geqq x$, $p\geqq y$, $q\leqq x$, $q\leqq p$. Since $x\geqq x$ by $\mathbf{P}_1$, it follows that x is a l.b. of x and p. But q is the g.l.b. of x and p. Consequently $x\leqq q$. Since we know that $q\leqq x$ it follows from $\mathbf{P}_2'$ that $x = q = x\cap(x\cup y)$, which is $\mathbf{L}_{3\cap}$.

Dually, we can prove $\mathbf{L}_{3\cup}$.

We obtain another important formula by replacing y in $\mathbf{L}_{3\cap}$ by $x\cap y$. By $\mathbf{L}_{3\cup}$ we get

$$x = x\cap(x\cup(x\cap y)) = x\cap x$$

and similarly its dual. Thus

$$x \cap x = x, \quad x \cup x = x \quad \text{(idempotent laws).} \tag{3.1}$$

If $x \geqq y$ then by $\mathbf{P}_1$, y is a l.b. for x and y. It is also the g.l.b. for x and y since any other l.b. must be included in y. Consequently, $x \geqq y$ implies $x \cap y = y$. Conversely, if $y = x \cap y$, then $x \geqq x \cap y = y$. Taken along with the dual result we have

$$y = x \cap y \Leftrightarrow x \geqq y \Leftrightarrow x \cup y = x. \tag{3.2}$$

§ 4. Second definition of a lattice

We now formulate our alternative definition of a lattice. A **lattice** is a set $\mathscr{L}$ of elements equipped with two binary operations denoted by $\cap$ and $\cup$ such that $\mathbf{L}_{1\cap}$, $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cap}$, $\mathbf{L}_{3\cup}$ are valid for all elements $x, y, z, \ldots$ of $\mathscr{L}$. Observe that each postulate has its dual.

It should be stressed that at this stage no properties of $\cap$ and $\cup$ are demanded other than those implied by the six postulates which they satisfy. In particular they are not yet associated with the concepts of g.l.b. and l.u.b. although we now proceed to make this association. Taking a hint from a previous result (3.2) we define $x \geqq y$ to mean $y = x \cap y$. Then by $\mathbf{L}_{3\cup}$, $x \geqq y$ implies $x \cup y = x$ and by $\mathbf{L}_{3\cap}$, $x \cup y = x$ implies that $y = (x \cup y) \cap y = x \cap y$. Accordingly, this definition maintains the validity of (3.2).

As before, the idempotent laws (3.1) are consequences of our six postulates and $\mathbf{P}_1$ is an immediate consequence of (3.1). If $x \geqq y$ and $y \geqq x$ then by (3.2), $y = x \cap y = x$, which yields $\mathbf{P}_2$. If $x \geqq y$ and $y \geqq z$ then $y = x \cap y$ and $z = y \cap z$ so that

$$x \cap z = x \cap y \cap z = y \cap z = z,$$

which implies that $x \geqq z$. This establishes $\mathbf{P}_3$ and shows that $\mathscr{L}$ is a poset in regard to the inclusion relation $\geqq$.

Since $x \geqq x \cap y$ and $y \geqq x \cap y$, it is clear that $x \cap y$ is a l.b. for x and y. If z is any other l.b., then $z \leqq x$ and $z \leqq y$, whence $z = x \cap z = y \cap z$. Then by $\mathbf{L}_{2\cap}$,

$$(x \cap y) \cap z = x \cap (y \cap z) = x \cap z = z,$$

yielding $z \leqq x \cap y$. It follows that $x \cap y$ is the g.l.b. and dually that $x \cup y$ is the l.u.b. for x and y. Since an arbitrary pair of elements have both a g.l.b. and a l.u.b., the poset forms a lattice according to the first definition.

We have now established that the two definitions of a lattice are completely equivalent, the relation between them being provided by (3.2).

Before we leave the axiomatics of the definitions we shall indicate briefly how it may be shown that the six postulates of the second definition are independent in the sense that no one of them can be deduced from the other five.

The system with the laws of composition

$$\begin{array}{c|cc} \cap & x & y \\ \hline x & x & x \\ y & y & y \end{array} \qquad \begin{array}{c|cc} \cup & x & y \\ \hline x & x & x \\ y & x & y \end{array}$$

can be shown to satisfy all the postulates except $\mathbf{L}_{1\cap}$. In this case $\mathbf{L}_{1\cap}$ cannot be a consequence of the other five. Similarly, the system with the compositions

$$\begin{array}{c|cc} \cap & x & y \\ \hline x & x & x \\ y & x & x \end{array} \qquad \begin{array}{c|cc} \cup & x & y \\ \hline x & x & y \\ y & y & y \end{array}$$

does not satisfy $\mathbf{L}_{3\cap}$ though it satisfies the others.

Consider a system of five elements y_1, y_2, y_3, y_4, y_5 having the same laws of composition as the x_1, x_2, x_3, x_4, x_5 of the lattice of fig. 4 with the exception that

$$y_2 \cap y_3 = y_3 \cap y_2 = y_5$$

instead of

$$x_2 \cap x_3 = x_3 \cap x_2 = x_4.$$

It will be found that this system satisfies all the postulates except $\mathbf{L}_{2\cap}$. Since, in fact,

$$y_2 \cap (y_3 \cap y_4) = y_2 \cap y_4 = y_4,$$

while

$$(y_2 \cap y_3) \cap y_4 = y_5 \cap y_4 = y_5,$$

it is clear that $\mathbf{L}_{2\cap}$ is not satisfied. We have shown that none of $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{3\cap}$ is deducible from the others. Dually $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cup}$ are independent of the others.

§ 5. Elementary properties

It is plain that the lattice of illustration (III) has neither an O nor an I. If, however, a lattice possesses an O and an I then from their definitions we conclude that for all x

$$O \cap x = O, \qquad O \cup x = x,$$
$$I \cap x = x, \qquad I \cup x = I.$$

It is interesting to compare these with the familiar formulae

$$0 \times x = 0, \qquad 0 + x = x,$$
$$1 \times x = x, \qquad\qquad !$$

If $x \cup y = O$, then by $\mathbf{L}_{3\cap}$ we have $x = x \cap (x \cup y) = x \cap O = O$. This result and its dual yield the important formulae

$$x \cup y = O \Rightarrow x = y = O,$$
$$x \cap y = I \Rightarrow x = y = I,$$

which may be immediately visualised by a consideration of a Hasse diagram.

Our examination of the associative laws showed that in a lattice the g.l.b. and l.u.b. of a finite subset of elements always exists. The corresponding statement is not necessarily true for infinite subsets. For instance in illustration (II) the infinite subset 1, 2, 2^2, 2^3, ... has no l.u.b. A lattice for which every subset has both a g.l.b. and a l.u.b. is said to be **complete**.

THEOREM 5.1. *A lattice without infinite chains is complete.*

Proof. Let $\mathscr{M}$ be any subset of the lattice and let $x_0, x_1, x_2, \ldots$ denote elements of $\mathscr{M}$. If x_0 is not an u.b. of $\mathscr{M}$ there is some x_1 such that $x_1 \nleqq x_0$. Then $x_0 \cup x_1 \neq x_0$. Since $x_0 \cup x_1 \geqq x_0$ we deduce that $x_0 \cup x_1 > x_0$. If $x_0 \cup x_1$ is not an u.b. of $\mathscr{M}$ there is some x_2 such that $x_2 \nleqq x_0 \cup x_1$. Then $x_0 \cup x_1 \cup x_2 \neq x_0 \cup x_1$. Since

$$x_0 \cup x_1 \cup x_2 \geqq x_0 \cup x_1$$

we deduce that $x_0 \cup x_1 \cup x_2 > x_0 \cup x_1$. If $x_0 \cup x_1 \cup x_2$ is not an u.b. of $\mathscr{M}$ there is an x_3 such that $x_3 \nleqq x_0 \cup x_1 \cup x_2$ and such that

$$x_0 \cup x_1 \cup x_2 \cup x_3 > x_0 \cup x_1 \cup x_2.$$

Thus, either the lattice has an infinite ascending chain

$$x_0 < x_0 \cup x_1 < x_0 \cup x_1 \cup x_2 < x_0 \cup x_1 \cup x_2 \cup x_3 < \ldots$$

or, at some stage this chain terminates in say $\bigcup_{i=0}^{r} x_i$ which is an u.b. for $\mathscr{M}$. In the latter case $\bigcup_{i=0}^{r} x_i$ is also a l.u.b. for $\mathscr{M}$ since any other u.b. for $\mathcal{M}$, say y, would satisfy $y \geqq x_i$, $i = 0, \ldots r$, and would consequently be an u.b. for the subset $x_0, \ldots, x_r$. Since by definition, $\bigcup_{i=0}^{r} x_i$ is the l.u.b. for this subset, it must therefore also be the l.u.b. for $\mathcal{M}$. We see therefore that every subset $\mathcal{M}$ has a l.u.b. unless the lattice has an infinite ascending chain. Dually every subset has a g.l.b. unless the lattice has an infinite descending chain. ◇

We observe also that a lattice with no O necessarily has an infinite descending chain. Consider any element x_0. We cannot have $x_0 \cap y = x_0$ for every y, since this would imply $x_0 \leqq y$ for every y and yield $x_0 = O$. It follows that given any x_0 we can find a y such that $x_0 > x_0 \cap y = x_1$, say. Similarly, we can find an infinite sequence of x_i such that

$$x_0 > x_1 > x_2 > \ldots.$$

Dually, a lattice with no I has an infinite ascending chain.

A complete lattice, however, may have infinite chains. The power set $\mathcal{P}(\mathcal{M})$ of an infinite set $\mathcal{M}$ discussed in § 19 provides an illustration.

It should be observed that the existence of an O and an I is not a sufficient condition for a lattice to be complete. For instance the set of rational numbers augmented by $+\infty (= I)$ and $-\infty (= O)$ forms a lattice if $\geqq$ has its arithmetical meaning but the subset of rationals satisfying $3 > x^2 > 2$ has neither a g.l.b. nor a l.u.b.

A **finite** lattice is one with a finite number of elements. The number of elements is called the **order** of the lattice. Clearly a finite lattice $\mathcal{L}$ has no infinite chain and is therefore complete. In particular if it consists of exactly n elements $x_1, \ldots, x_n$ then $\bigcup x_i \geqq x_j$ from which it follows that $\mathcal{L}$ has an I namely $\bigcup x_i$ and dually an O, namely $\bigcap x_i$.

On the other hand, it is possible for an infinite lattice to be complete; for instance the poset of illustration (IV) augmented by an O and an I.

A **sublattice** $\mathcal{M}$ of a lattice $\mathcal{L}$ is a subset such that

$$x \in \mathcal{M} \wedge y \in \mathcal{M} \Rightarrow x \cap y \in \mathcal{M} \wedge x \cup y \in \mathcal{M}.$$

This definition requires that a sublattice satisfies the postulates for a lattice but it should be stressed that a subset of $\mathcal{L}$ may form a lattice according to our first definition of a lattice without being a sublattice. It may happen, for example, that the g.l.b. of x and y in the subset differs from $x \cap y$ which is the g.l.b. of x and y in $\mathcal{L}$. Consider for example the subset x_1, x_2, x_3, x_5 of fig. 4. The subset forms a lattice but g.l.b. of x_2 and x_3 in the subset is x_5, whereas $x_2 \cap x_3 = x_4$.

By a **lattice polynomial** we mean an expression $f(x_1, \ldots, x_n)$ composed of lattice elements, cups and caps, and, if necessary, brackets.

THEOREM 5.2. *If* $x_i \geqq y_i$, $i = 1, \ldots, n$, *then* $f(x_1, \ldots, x_n) \geqq f(y_1, \ldots, y_n)$. An alternative way of expressing this theorem is to say that lattice polynomials are **isotone** functions of their variables.

Proof. If $x \geqq y$, then by (3.2)

$$x \cup z = (x \cup y) \cup z = x \cup (y \cup z) \geqq y \cup z$$

and

$$x \cap z \geqq y \cap (x \cap z) = (y \cap x) \cap z = y \cap z.$$

This proves the theorem if the polynomial has only one cup or cap. The general case will follow by induction if we replace x, y, z by appropriate polynomials. ◇

In illustration of this theorem we see that $x \cap (y \cup z) \geqq x \cap y$ since $y \cup z \geqq y$. Similarly $x \cap (y \cup z) \geqq x \cap z$. Thus $x \cap (y \cup z)$ is an u.b. for $x \cap y$ and $x \cap z$. Hence

$$x \cap (y \cup z) \geqq (x \cap y) \cup (x \cap z) \tag{5.1}$$

and dually

$$x \cup (y \cap z) \leqq (x \cup y) \cap (x \cup z). \tag{5.2}$$

These formulae are known as the **one-sided distributive laws.**

Since $x \cap z = z$ if $x \geqq z$, (5.1) yields the **one-sided modular law** which states that

$$x \geqq z \Rightarrow x \cap (y \cup z) \geqq (x \cap y) \cup z. \tag{5.3}$$

The one-sided distributive laws quoted above can be generalised and we shall show that in fact

$$y \cap (\bigcup x_i) \geqq \bigcup (y \cap x_i)$$

even when there are infinitely many x_i provided only that the infinite unions exist. Since $\bigcup x_i$ is the l.u.b. of the set of x_j, we have $\bigcup x_i \geqq x_j$ from which we see by the isotone property that $y \cap (\bigcup x_i) \geqq y \cap x_j$ for each x_j. Thus $y \cap (\bigcup x_i)$ is an upper bound for the set $y \cap x_j$ while $\bigcup (y \cap x_i)$ is by definition the l.u.b. for the same set. This proves what is required. The dual law is proved similarly.

MINIMAX THEOREM 5.3.

$$\bigcap_{i=1}^{m} \left(\bigcup_{j=1}^{n} x_{ij} \right) \geqq \bigcup_{j=1}^{n} \left(\bigcap_{i=1}^{m} x_{ij} \right).$$

To visualise the significance of this theorem arrange the lattice elements in a rectangular array of m rows and n columns.

$$\begin{array}{cccc} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{array}$$

and let

$$y_i = \text{l.u.b. of all } x_{ij} \text{ in the } i\text{th row} = \bigcup_{j=1}^{n} x_{ij},$$

$$z_j = \text{g.l.b. of all } x_{ij} \text{ in the } j\text{th column} = \bigcap_{i=1}^{m} x_{ij}.$$

Then the theorem states that

$$\bigcap_{i=1}^{m} y_i \geqq \bigcup_{j=1}^{n} z_j.$$

Proof: Since for all i and j, $y_i \geqq x_{ij} \geqq z_j$, it follows that $y_i \geqq$ l.u.b. of all z_j, that is to say $y_i \geqq \bigcup_j z_j$. Thus, $\bigcup_j z_i$ is a l.b. for all y_i. Consequently,

$$\bigcap_i y_i = \text{g.l.b. of all } y_i \geqq \bigcup_j z_j. \quad \diamond$$

This theorem gets its name from its application to illustration (III) in which for instance if $n = m = 2$,

$$\min(\max(p, q), \max(r, s)) \geqq \max(\min(p, r), \min(q, s)).$$

Again, in the case $n = m = 2$, we would obtain

H.C.F. (L.C.M. (p, q), L.C.M. (r, s)) has a factor
L.C.M. (H.C.F. (p, r), H.C.F. (q, s))

by applying the theorem to illustration (II).

By way of illustration, let us apply the minimax theorem to the following array:

$$\begin{matrix} z & z & y \\ z & x & x \\ y & x & y \end{matrix}$$

We obtain

$$(y \cup z) \cap (z \cup x) \cap (x \cup y) \geqq (y \cap z) \cup (z \cap x) \cup (x \cap y). \tag{5.4}$$

This formula may also be referred to as the one-sided distributive law. The reason why this formula has the same name as (5.1) and (5.2) is explained in Exercise 6.

By a **free** lattice we mean one whose elements satisfy no identities other than the six postulates of our second definition and the consequences of these. We consider briefly the free lattice generated by three elements x, y, z of which $x > z$. Using (5.3) and the isotone property, we obtain the following relations

$$x \cup y \geqq x \geqq x \cap (y \cup z) \geqq (x \cap y) \cup z \geqq z \geqq y \cap z,$$

$$x \cup y \geqq z \cup y \geqq y \geqq y \cap x \geqq y \cap z,$$

$$(y \cap x) \cup z \geqq y \cap x, \quad z \cup y \geqq x \cap (z \cup y).$$

If we replace each $\geqq$ by $>$ we can construct the following diagram.

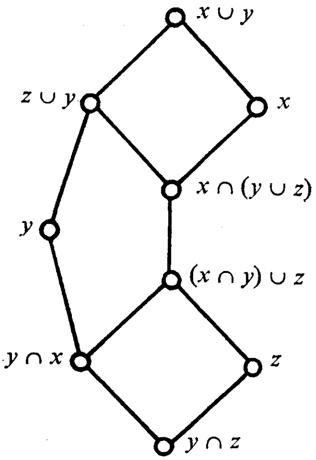


FIG. 6

Any other polynomial $f(x, y, z)$ can be shown to be one of the nine elements mentioned above. For instance $x \cup y \cup z = x \cup y$ and $y \cup (x \cap z) = y \cup z$, since by hypothesis $x > z$.

We notice that such a lattice is bound to contain a pentagonal sublattice isomorphic with the lattice of fig. 2 unless the pentagon is telescoped by a relation of the form

$$x \cap (y \cup z) = (x \cap y) \cup z.$$

The reader may verify that any other telescoping of the pentagon results in the same equation. In a free lattice, $x \cap (y \cup z)$ and $(x \cap y) \cup z$ are distinct elements. If, however, they are equal whenever $x > z$, the lattice is not free for its elements satisfy an additional identity (cf. Exercise 8).

§ 6. Modular lattices

A lattice which satisfies the postulate

M: $$x \geqq z \Rightarrow x \cap (y \cup z) = (x \cap y) \cup z$$

for all x, y, z is called a **modular** lattice. Observe that this postulate is self-dual. The equality sign on the right is of course more restricting than the corresponding inclusion sign in the one-sided modular law (5.3). The one-sided law holds for every lattice but the two-sided law holds only for modular lattices. In particular we can characterise modular lattices as follows.

THEOREM 6.1. *A lattice is modular if and only if it contains no sublattice isomorphic to the pentagonal lattice of fig.* 2.

Proof: The lattice of fig. 2 is non-modular since $c > b$ and

$$c \cap (a \cup b) = c > b = (c \cap a) \cup b.$$

Conversely, if **M** does not hold for x, y, z with $x > z$ the one-sided modular law tells us that

$$x \cap (y \cup z) > (x \cap y) \cup z$$

and so the lattice contains a sublattice of the form of fig. 6 which contains a pentagonal sublattice.

The isomorphism between fig. 2 and the pentagon of fig. 6 is obtained by setting $a = y$, $b = (x \cap y) \cup z$ and $c = x \cap (y \cup z)$. Then $a \cup b = y \cup z$ and $a \cap c = x \cap y$. ◇

THEOREM 6.2. *If*

$$a \cap b = a \cap c \wedge a \cup b = a \cup c \Rightarrow b = c$$

for every choice of elements a, b, c, then the lattice is modular.

Proof: If it were non-modular it would contain a pentagon such as fig. 2 in which $b \neq c$ although $a \cap b = a \cap c$ and $a \cup b = a \cup c$. ◇

We also have a partial converse of this theorem, namely:

THEOREM 6.3. *In a modular lattice*

$$a \cap b = a \cap c \wedge a \cup b = a \cup c \Rightarrow b = c$$

provided that either $b \geqq c$ *or* $c \geqq b$.

Proof: Suppose $b \geqq c$, then

$$b = b \cap (a \cup b) = b \cap (a \cup c) = (b \cap a) \cup c = (c \cap a) \cup c = c.$$

The case $c \geqq b$ is dealt with similarly. ◇

Observe that in the modular lattice of fig. 3, $a \cap b = a \cap c$ and $a \cup b = a \cup c$ although $b \neq c$. In this case, however, neither $b \geqq c$ nor $c \geqq b$ is true.

Of particular interest in connection with modular lattices is the concept of an **interval** $[y, x]$ of a lattice $\mathscr{L}$ consisting of all elements z such that $x \geqq z \geqq y$. It is easily verified that $[y, x]$ forms a sublattice of $\mathscr{L}$ since x and y are upper and lower bounds for the interval. This means that if z and t belong to $[y, x]$ then so do $z \cup t$ and $z \cap t$.

THEOREM 6.4. *In a modular lattice* $[x, x \cup y]$ *and* $[x \cap y, y]$ *are isomorphic.*

Proof: If $x \cup y \geqq a \geqq x$, then by the isotone property

$$y = (x \cup y) \cap y \geqq a \geqq \cap y x \cap y.$$

Thus the mapping

$$a \rightarrow a \cap y$$

maps $[x, x \cup y]$ into $[x \cap y, y]$. Dually, the mapping

$$b \rightarrow b \cup x$$

maps $[x \cap y, y]$ back again into $[x, x \cup y]$. Since the second mapping carries $a \cap y$ into

$$(a \cap y) \cup x = a \cap (y \cup x) = a,$$

it is clear that each mapping is the inverse of the other and that either of these two mappings establishes a $1-1$ correspondence between the elements of the two intervals.

Indeed, if we write $b_i = a_i \cap y$, then $a_i = b_i \cup x$ and the correspondence may be written $a_i \leftrightarrow b_i$. Since, from the isotone property,

$$a_1 \geqq a_2 \;\Rightarrow\; a_1 \cap y \geqq a_2 \cap y \;\Rightarrow\; b_1 \geqq b_2,$$

$$b_1 \geqq b_2 \;\Rightarrow\; b_1 \cup x \geqq b_2 \cup x \;\Rightarrow\; a_1 \geqq a_2,$$

it follows that

$$a_1 \geqq a_2 \;\Leftrightarrow\; b_1 \geqq b_2.$$

This establishes the isomorphism. ◇

It will be observed however that $[a, a \cup c]$ and $[a \cap c, c]$ are not isomorphic in the case of the non-modular lattice of fig. 2.

The converse of this theorem is as follows.

THEOREM 6.5. *If the intervals* $[x, x \cup y]$ *and* $[x \cap y, y]$ *of a lattice are isomorphic under the inverse mappings*

$$a \in [x, x \cup y] \rightarrow a \cap y \in [x \cap y, y]$$

$$b \in [x \cap y, y] \rightarrow b \cup x \in [x, x \cup y]$$

for all x, y, *then the lattice is modular.*

Proof: Let $z \geqq x$, then $z \cap (y \cup x) \in [x, x \cup y]$ and performing the two mappings in succession we have

$$z \cap (y \cup x) \rightarrow z \cap (y \cup x) \cap y = z \cap y \rightarrow (z \cap y) \cup x.$$

Since the second mapping is the inverse of the first,

$$z \cap (y \cup x) = (z \cup y) \cap x$$

provided $z \geqq x$. This is the required condition **M**. ◇

The isomorphism of $[x, x \cup y]$ and $[x \cap y, y]$ shows that if $x \cup y$ covers x in a modular lattice, then y covers $x \cap y$, and vice versa.

Two intervals $[a, b]$ and $[c, d]$ are said to be **similar** if elements x, y exist such that one interval is $[x, x \cup y]$ and the other is $[x \cap y, y]$.

The intervals $[a, b]$ and $[c, d]$ are said to be **projective** if a sequence of intervals

$$[a, b] = [x_1, y_1], [x_2, y_2], \ldots, [x_n, y_n] = [c, d]$$

can be found such that each pair of consecutive intervals are similar. In a modular lattice it is clear that projective intervals are isomorphic. Further, it can readily be shown that projectivity is an equivalence relation.

ZASSENHAUS'S THEOREM 6.6. *In a modular lattice if $a \geqq b$, $c \geqq d$, then $[(a \cap d) \cup b, (a \cap c) \cup b]$ and $[(b \cap c) \cup (a \cap d), a \cap c]$ are similar.*

Proof: Put $x = (a \cap d) \cup b$ and $y = a \cap c$. Then, since $a \cap c \geqq a \cap d$,

$$x \cup y = (a \cap d) \cup b \cup (a \cap c) = b \cup (a \cap c).$$

Also, by **M**,

$$x \cap y = ((a \cap d) \cup b) \cap (a \cap c) = (a \cap d) \cup (b \cap a \cap c) = (a \cap d) \cup (b \cap c).$$

The two intervals are therefore similar since they can be written $[x, x \cup y]$ and $[x \cap y, y]$. ◇

COROLLARY. *In a modular lattice the intervals $[(a \cap d) \cup b, (a \cap c) \cup b]$ and $[(b \cap c) \cup d, (a \cap c) \cup d]$ are projective.*

Proof: Both intervals are similar to the interval $[(b \cap c) \cup (a \cap d), a \cap c]$ as may be seen by interchanging a with c and b with d. ◇

A finite chain $x = a_1 \geqq a_2 \geqq \ldots \geqq a_n = y$ is a **refinement** of a second chain $x = b_1 \geqq b_2 \geqq \ldots \geqq b_m = y$ connecting x and y if every b_i is some a_j. The two chains are **equivalent** if there is a $1-1$ correspondence between the intervals $[a_{j+1}, a_j]$ and $[b_{i+1}, b_i]$ such that corresponding intervals are projective.

A finite chain $x = a_1 > a_2 > \ldots > a_n = y$ is a **composition chain** or a **maximal chain** for $[y, x]$ if each a_i covers its successor a_{i+1}. Clearly no essential refinement of a maximal chain is possible. A refinement can only be made by introducing additional equality signs.

SCHREIER'S THEOREM 6.7. *In a modular lattice any two finite chains connecting x and y have equivalent refinements.*

Proof: We obtain refinements of the chains

$$x = a_1 \geqq \ldots \geqq a_n = y,$$

$$x = b_1 \geqq \ldots \geqq b_m = y$$

by defining for $i = 1, \ldots, n-1$ and $j = 1, \ldots, m-1$,

$$a_{i,j} = (a_i \cap b_j) \cup a_{i+1}, \quad b_{j,i} = (a_i \cap b_j) \cup b_{j+1}.$$

In the first place, the isotone property shows that

$$a_{i,j} \geqq a_{i,j+1}, \quad b_{j,i} \geqq b_{j,i+1}.$$

Secondly, from the two relations

$$a_{i,m} = (a_i \cap y) \cup a_{i+1} = y \cup a_{i+1} = a_{i+1},$$

$$a_{i+1,1} = (a_{i+1} \cap x) \cup a_{i+2} = a_{i+1} \cup a_{i+2} = a_{i+1},$$

we obtain

$$a_{i+1,1} = a_{i+1} = a_{i,m}$$

and correspondingly

$$b_{j,n} = b_{j+1} = b_{j+1,1}.$$

The refinements are therefore as follows

$$x = a_{11} \geqq a_{12} \geqq \dots \geqq a_{1m} = a_{21} \geqq \dots \geqq a_{2m} = a_{31} \geqq \dots \geqq a_{n-1,m} = y,$$

$$x = b_{11} \geqq b_{12} \geqq \dots \geqq b_{1n} = b_{21} \geqq \dots \geqq b_{2n} = b_{31} \geqq \dots \geqq b_{m-1,n} = y.$$

Both refinements have $(n-1)(m-1)$ terms (excluding the equalities). The last corollary, however, shows us, by taking $a = a_i$, $b = a_{i+1}$, $c = b_j$, $d = b_{j+1}$, that $[a_{i,\,j+1}, a_{ij}]$ and $[b_{j,\,i+1}, b_{ji}]$ are projective. This provides a $1-1$ correspondence between pairs of projective intervals and consequently the two refinements are equivalent. $\diamond$

JORDAN-HÖLDER THEOREM 6.8. *Let $x = a_1 > a_2 > \dots > a_n = y$ and $x = b_1 > b_2 > \dots > b_m = y$ be two maximal chains of a modular lattice; then $n = m$ and there is a $1-1$ correspondence between $[a_{i+1}, a_i]$ and $[b_{j+1}, b_j]$ such that corresponding intervals are projective.*

Proof: Applying the previous theorem and recalling that no essential refinement of a maximal chain is possible, we see that exactly one of the signs $\geqq$ in

$$a_i = a_{i,1} \geqq a_{i,2} \geqq \dots \geqq a_{i,m} = a_{i+1}$$

can be replaced by $>$ while the others must be replaced by $=$. If $a_{i,j} > a_{i,j+1}$ then $[a_{i,j+1}, a_{i,j}]$ is projective with $[b_{j,i+1}, b_{j,i}]$ and so $b_{j,i} > b_{j,i+1}$. We conclude as above that $b_{j,k} = b_{j,k+1}$ if $k \neq i$. Thus all intervals $[a_{r,s+1}, a_{r,s}]$ and $[b_{r,s+1}, b_{r,s}]$ are either trivial, that is, isomorphic to a lattice of one element, or are isomorphic to a lattice of two elements. The $1-1$ correspondence shows that there are the same number of the latter in each chain. Accordingly $n = m$. Since we have seen that $[a_{i,j+1}, a_{i,j}] = [a_{i+1}, a_i]$ if $a_{i,j} > a_{i,j+1}$, the corresponding projective intervals are in fact $[a_{i+1}, a_i]$ and $[b_{j+1}, b_j]$. This proves the theorem. $\diamond$

This theorem informs us that if a modular lattice without infinite chains possesses both O and I, every maximal chain connecting these two elements has the same number of terms and the same number of intervals isomorphic to the lattice of two elements. The number of intervals is called the **length** of the lattice while the length of the sublattice $[O, x]$ is called the length of the element x and is denoted by $l(x)$. If $x \geqq y$ it is obvious that

$$l(x) = l(y) + \text{length } [y, x].$$

In particular, since $[x, x \cup y]$ and $[x \cap y, y]$ are isomorphic,

$$l(x \cup y) - l(x) = \text{length } [x, x \cup y] = \text{length } [x \cap y, y] = l(y) - l(x \cap y).$$

Accordingly we have the following result.

DIMENSION THEOREM 6.9. *In a modular lattice of finite length*

$$l(x) + l(y) = l(x \cup y) + l(x \cap y).$$

It should be mentioned that some authors call $l(x)$ the dimension of x while others call $l(x) - 1$ the **dimension.** We shall adopt the latter nomenclature. In the lattice obtained by augmenting the poset of illustration (IV) with O and I the geometrical dimension is $l(x) - 1$. In illustration of the dimension theorem let x be a line and y a plane then $l(x) = 2$, $l(y) = 3$. If x lies on y then $x \cup y = y$ and $x \cap y = x$ so that $l(x \cup y) = 3$ and $l(x \cap y) = 2$. In the contrary case $x \cup y = I$ while $x \cap y$ is a point z. Then $l(I) = 4$, $l(z) = 1$. These results suggest that the projective geometry of illustration (IV) with O and I added constitutes a modular lattice, which is indeed the case. In the Euclidean geometry of three dimensions there is a further possibility that x is parallel to y with the consequence that $x \cap y = O$ and $l(x \cap y) = 0$. In this case

$$l(x) + l(y) \neq l(x \cup y) + l(x \cap y),$$

showing that the lattice cannot be modular unless we augment the geometry and the lattice by supplying a plane at infinity.

§ 7. Applications to abstract algebra

For an understanding of this section the reader is expected to have some familiarity with the theory of groups and the theory of ideals.

The set of all subgroups of a given group $\mathscr{G}$ form a lattice, $\mathscr{H} \leqq \mathscr{K}$ meaning $\mathscr{H}$ is a subgroup of $\mathscr{K}$, but not a modular lattice. However the set of all normal subgroups $\mathscr{N}$, $\mathscr{M}$, ... of $\mathscr{G}$ compose a modular lattice as we shall now demonstrate. By $\mathcal{N} \cap \mathcal{M}$ we mean the set of all elements common to $\mathcal{N}$ and $\mathcal{M}$, while the l.u.b. of $\mathcal{N}$ and $\mathcal{M}$ is the set of all products nm with $n \in \mathcal{N}$ and $m \in \mathcal{M}$. In multiplicative group theory this l.u.b. is written as a product $\mathcal{N}\mathcal{M}$.

It should be stressed that although $\mathcal{N} \cap \mathcal{M}$ is the set intersection of $\mathcal{N}$ and $\mathcal{M}$ consisting of all elements common to $\mathcal{N}$ and $\mathcal{M}$, the set $\mathcal{N}\mathcal{M}$ is not the set union consisting of all elements belonging to either $\mathcal{N}$ or $\mathcal{M}$. Indeed, the set union does not in general form a subgroup. It can readily be proved that $\mathcal{N} \cap \mathcal{M}$ and $\mathcal{N}\mathcal{M}$ are both normal subgroups and it is then a matter of verification that these are the g.l.b. and l.u.b. of $\mathcal{N}$ and $\mathcal{M}$ in the poset of normal subgroups. Thus the normal subgroups of $\mathcal{G}$ compose a lattice in which $\mathcal{N} \geqq \mathcal{M}$ means that every m is an n.

To verify the modular law suppose $\mathcal{N} \geqq \mathcal{M}$. Then $\mathcal{N} \cap (\mathcal{P}\mathcal{M})$ is the set of all pm such that $pm = n$, or $p = nm^{-1}$. Then $p \in \mathcal{N}$ since $m^{-1} \in \mathcal{M} \leqq \mathcal{N}$. Consequently $p \in \mathcal{N} \cap \mathcal{P}$ and $pm \in (\mathcal{N} \cap \mathcal{P})\mathcal{M}$. Conversely $(\mathcal{N} \cap \mathcal{P})\mathcal{M}$ is the set of all qm such that $q \in \mathcal{N}$, $q \in \mathcal{P}$, $m \in \mathcal{M} \leqq \mathcal{N}$. Then $qm \in \mathcal{N}$ and $qm \in \mathcal{P}\mathcal{M}$. It follows that $qm \in \mathcal{N} \cap (\mathcal{P}\mathcal{M})$. Thus

$$\mathcal{N} \geqq \mathcal{M} \Rightarrow \mathcal{N} \cap (\mathcal{P}\mathcal{M}) = (\mathcal{N} \cap \mathcal{P})\mathcal{M},$$

which is the postulate **M** for the lattice of normal subgroups.

If

$$\mathcal{G} = \mathcal{N}_1 > \mathcal{N}_2 > \ldots > \mathcal{N}_n = e,$$
$$\mathcal{G} = \mathcal{M}_1 > \mathcal{M}_2 > \ldots > \mathcal{M}_m = e$$

are two principal series for $\mathcal{G}$, the Jordan-Hölder theorem tells us that $n = m$ and that the intervals $[\mathcal{N}_{i+1}, \mathcal{N}_i]$ and $[\mathcal{M}_{j+1}, \mathcal{M}_j]$ can be paired off in such a way that corresponding intervals are projective. To see what this means we consider two similar intervals $[\mathcal{A}, \mathcal{A}\mathcal{B}]$ and $[\mathcal{A} \cap \mathcal{B}, \mathcal{B}]$. The normal subgroup $\mathcal{A}$ of $\mathcal{A}\mathcal{B}$ separates the latter into cosets

$$\mathcal{A}\mathcal{B} = \mathcal{A} + \mathcal{A}b_2 + \ldots + \mathcal{A}b_s.$$

Selecting from both sides the elements which belong to $\mathcal{B}$,

$$\mathcal{B} = (\mathcal{A}\mathcal{B}) \cap \mathcal{B} = (\mathcal{A} \cap \mathcal{B}) + (\mathcal{A} \cap \mathcal{B})b_2 + \ldots + (\mathcal{A} \cap \mathcal{B})b_s,$$

from which it appears that the factor groups $(\mathcal{A}\mathcal{B})/\mathcal{A}$ and $\mathcal{B}/(\mathcal{A} \cap \mathcal{B})$ are isomorphic. Hence the Jordan-Hölder theorem informs us that the prime factor groups $\mathcal{N}_i/\mathcal{N}_{i+1}$ of a principal series are uniquely determined in number and structure though not in order of occurrence.

An automorphism of a finite group $\mathcal{G}$ of order r is an isomorphism of $\mathcal{G}$ with itself and can therefore be represented by a permutation of the elements $e, g_2, \ldots, g_r$ of $\mathcal{G}$. The set of all automorphisms can therefore be represented by a permutation group $\mathscr{A}$. The regular representation of $\mathscr{G}$ is also a permutation group $\mathscr{R}$ which is isomorphic with $\mathscr{G}$. Both $\mathscr{A}$ and $\mathscr{R}$ are subgroups of the symmetric group $\mathscr{S}$ of all permutations of e, g_1, $\dots g_r$. $\mathscr{A}$ and $\mathscr{R}$ generate the holomorphy group $\mathscr{K}$ of $\mathscr{G}$ which is a subgroup of $\mathscr{S}$ while $\mathscr{R}$ (or $\mathscr{G}$) can be shown to be a normal subgroup of $\mathscr{K}$. A characteristic subgroup of $\mathscr{G}$ is one which is invariant under $\mathscr{A}$ and is therefore a normal subgroup of $\mathscr{K}$. A characteristic series for $\mathscr{G}$ is part of a principal series for $\mathscr{K}$ such as

$$\mathscr{K} > \mathscr{N}_2 > \dots > \mathscr{G} > \mathscr{M}_2 > \dots > e.$$

The intervals $[\mathscr{N}_{i+1}, \mathscr{N}_i]$ correspond to the intervals determined by the principal series of $\mathscr{K}/\mathscr{G}$, so the intervals $[\mathscr{M}_{i+1}, \mathscr{M}_i]$ of the characteristic series of $\mathscr{G}$ are uniquely determined in number and structure. That is to say the factor groups $\mathscr{M}_i/\mathscr{M}_{i+1}$ are uniquely determined.

The application of the Jordan-Hölder theorem to composition series requires a more sophisticated argument which will not be reproduced here. Since the subgroups concerned may not be normal the lattice of subgroups will not be modular. On the other hand the lattice of congruence relations of the group is modular and in this lattice the Jordan-Hölder theorem may be applied.

A subset $\mathscr{N}$ of a commutative ring $\mathscr{R}$ is called an ideal of the ring if (i) n_1, $n_2 \in \mathscr{N} \Rightarrow n_1 + n_2 \in \mathscr{N}$; (ii) $n \in \mathscr{N}$, $r \in \mathscr{R} \Rightarrow rn \in \mathscr{N}$. We see from (i) that an ideal is a subgroup of the additive group of the ring and is a normal subgroup since $\mathscr{R}$ is commutative. The ideals of $\mathscr{R}$ are therefore those normal additive subgroups which satisfy the additional condition (ii). We can therefore apply to ideal theory some of the above results on normal subgroups. Then $\mathscr{N} \geqq \mathscr{M}$ means that every m is an n and $\mathscr{N} \cap \mathscr{M}$ is the set of elements common to $\mathscr{N}$ and $\mathscr{M}$. If we write $\mathscr{N} + \mathscr{M}$ to denote the set of elements of the form $n+m$, this set is the smallest ideal containing $\mathscr{M}$ and $\mathscr{N}$. We write $\mathscr{N} + \mathscr{M}$ for this l.u.b. since it differs from the set union which is usually denoted by $\mathscr{N} \cup \mathscr{M}$ in ring theory. As in the preceding section we can verify the modular law, which now takes the form

$$\mathscr{N} \geqq \mathscr{M} \Rightarrow \mathscr{N} \cap (\mathscr{P} + \mathscr{M}) = (\mathscr{N} \cap \mathscr{P}) + \mathscr{M}.$$

The ideals of $\mathscr{R}$ therefore form a modular lattice and similar intervals $[\mathscr{N} + \mathscr{M}, \mathscr{N}]$, $[\mathscr{M}, \mathscr{N} \cap \mathscr{M}]$ are isomorphic. Again, following the argument of the previous section, we conclude that the difference rings

$$(\mathscr{N} + \mathscr{M})/\mathscr{N}, \quad \mathscr{M}/(\mathscr{N} \cap \mathscr{M})$$

are isomorphic.

We illustrate this last result with the following simple example.

The only ideals of the ring of integers are of the form (n), where (n) denotes the set of all integers which are divisible by n. Then $(n)\cap(m)$ is the set of all integers divisible by both n and m, that is, the ideal (L.C.M. (n, m)), while $(n)+(m)$ is the set (H.C.F. (n, m)) of integers divisible by the H.C.F. of n and m. The residue classes of $(n)+(m)$ modulo (n) then form a ring which, we have seen, is isomorphic to the ring of residue classes of (m) modulo $(n)\cap(m)$. For instance, if $n = 10$, $m = 18$, then $(n)+(m) = (2)$ and $(n)\cap(m) = (90)$. The elements of $(n)+(m)$ are therefore the even integers any one of which can be written $10i+2j$, $j = 0, 1, 2, 3, 4$ and the jth residue class of (2) modulo (10) is the set of all integers of the form $10i+2j$ with fixed j. The ring of these residue classes is in fact isomorphic with the ring of integers modulo 5. Similarly the jth residue class of (18) modulo (90) is the set of all integers of the form $90i+18j$ and the ring of these residue classes is again isomorphic to the ring of integers modulo 5.

§ 8. Metric lattices

A real valued function $v(x)$ associated with the element x of a lattice $\mathscr{L}$ such that

$$v(x)+v(y) = v(x\cup y)+v(x\cap y)$$

is called a **valuation** of $\mathscr{L}$. The valuation is said to be **positive** if and only if

$$x>y \Rightarrow v(x)>v(y),$$

where, on the right hand side, $>$ has its arithmetical meaning.

As we have seen $l(x)$ is a positive valuation for a modular lattice of finite length. Familiar examples † of non-positive valuations are the Peano-Jordan content c (volume, area or length) of a set E,

$$c(E_1)+c(E_2) = c(E_1\cup E_2)+c(E_1\cap E_2),$$

and the more embracing measure m,

$$m(E_1)+m(E_2) = m(E_1\cup E_2)+m(E_1\cap E_2).$$

A **metric** lattice is one with a positive valuation.

† Rogosinski, *Volume and Integral* pp. 41, 64.

THEOREM 8.1. *A lattice is modular if it is metric.*

Proof: Suppose the lattice $\mathscr{L}$ is metric with a positive valuation v. Since $x > z$ implies $x \cap y \cap z = y \cap z$ and $x \cup y \cup z = x \cup y$, we have

$$\begin{aligned} v((x \cap y) \cup z) &= v(x \cap y) + v(z) - v(x \cap y \cap z) \\ &= v(x) + v(y) - v(x \cup y) + v(z) - v(x \cap y \cap z) \\ &= v(x) + v(y) + v(z) - v(x \cup y \cup z) - v(x \cap y \cap z), \\ v(x \cap (y \cup z)) &= v(x) + v(y \cup z) - v(x \cup y \cup z) \\ &= v(x) + v(y) + v(z) - v(y \cap z) - v(x \cup y \cup z) \\ &= v(x) + v(y) + v(z) - v(x \cap y \cap z) - v(x \cup y \cup z). \end{aligned}$$

So

$$v((x \cap y) \cup z) = v(x \cap (y \cup z)).$$

If, however, the lattice were non-modular, then for some $x > z$ we would have by the one-sided modular law

$$(x \cap y) \cup z < x \cap (y \cup z)$$

and consequently

$$v((x \cap y) \cup z) < v(x \cap (y \cup z))$$

providing a contradiction. It follows that $\mathscr{L}$ must be modular. ◇

The converse of this theorem holds for modular lattices of finite length for in this case a positive valuation, namely $l(x)$, always exists.

A metric lattice is so named because a **distance** $\delta(x, y)$ between the elements x and y can be defined as follows:

$$\delta(x, y) = v(x \cup y) - v(x \cap y),$$

and this distance is a real non-negative number such that

F$_1$: $\delta(x, y) = \delta(y, x)$,

F$_2$: $\delta(x, z) \leqq \delta(x, y) + \delta(y, z)$,

F$_3$: $\delta(x, y) = 0 \Leftrightarrow x = y$,

which are the postulates for a metric space (see § 37).†

We proceed to verify the above statements.

Since $x \cup y \geqq x \cap y$ it is clear that $\delta(x, y) = v(x \cup y) - v(x \cap y) \geqq 0$.

F$_1$ follows from $\mathbf{L}_{1\cup}$ and $\mathbf{L}_{1\cap}$.

Since

$$\begin{aligned} v(x \cup y) + v(y \cup z) &= v((x \cup y) \cup (y \cup z)) + v((x \cup y) \cap (y \cup z)) \\ &\geqq v(x \cup y \cup z) + v(y) \end{aligned}$$

† E. M. Patterson, *Topology* p. 26.

and

$$v(x\cap y)+v(y\cap z) = v((x\cap y)\cup(y\cap z))+v((x\cap y)\cap(y\cap z))$$
$$\leqq v(y)+v(x\cap y\cap z),$$

we have, on subtraction,

$$\begin{aligned}\delta(x, y)+\delta(y, z) &\geqq v(x\cup y\cup z)-v(x\cap y\cap z)\\ &\geqq v(x\cup z)-v(x\cap z)\\ &= \delta(x, z).\end{aligned}$$

This gives $\mathbf{F}_2$. Finally

$$x = y \Rightarrow x\cup y = x\cap y \Rightarrow v(x\cup y)-v(x\cap y) = 0.$$

On the other hand $v(x\cup y)-v(x\cap y) = 0 \Rightarrow x\cup y = x\cap y$ since the valuation is positive. Then $x = x\cap(x\cup y) = x\cap y$ and similarly $y = x\cap y$. Consequently $x = y$. Thus $\mathbf{F}_3$ is established.

§ 9. Distributive lattices

A **distributive** lattice is one which satisfies the following postulate.

$\mathbf{D}$: $$(x\cap y)\cup(y\cap z)\cup(z\cap x) = (x\cup y)\cap(y\cup z)\cap(z\cup x).$$

If $x\geqq y$ then $x\cap y = y$ and $x\cup y = x$. Substituting in $\mathbf{D}$ and using $\mathbf{L}_{3\cap}$ and $\mathbf{L}_{3\cup}$ we get immediately

$$y\cup(z\cap x) = (y\cup z)\cap x$$

which is the modular law $\mathbf{M}$. Consequently, every distributive lattice is modular, though the converse is not true.

If we take the union of both sides of $\mathbf{D}$ with x the left side becomes $x\cup(y\cap z)$ by using $\mathbf{L}_{3\cup}$, whereas the right side yields, using $\mathbf{M}$ twice,

$$x\cup\{(x\cup y)\cap(y\cup z)\cap(z\cup x)\} = \{x\cup((x\cup y)\cap(y\cup z))\}\cap(z\cup x)$$
$$= \{x\cup(y\cup z)\}\cap(x\cup y)\cap(z\cup x) = (x\cup y)\cap(x\cup z).$$

Hence $\mathbf{D}$ implies that

$\mathbf{D}_\cup$: $$x\cup(y\cap z) = (x\cup y)\cap(x\cup z)$$

and dually we obtain

$\mathbf{D}_\cap$: $$x\cap(y\cup z) = (x\cap y)\cup(x\cap z).$$

On the other hand suppose that $\mathbf{D}_\cup$ is satisfied. If we replace x in $\mathbf{D}_\cup$ by $(x\cap y)\cup(x\cap z)$ then $(x\cup y)$ is replaced by

$$(x\cap y)\cup(x\cap z)\cup y = y\cup(x\cap z) = (y\cup x)\cap(y\cup z)$$

and similarly, $x \cup z$ is replaced by $(z \cup x) \cap (z \cup y)$. Using the idempotent law to remove a superfluous term $z \cup y$, we recover **D** from $\mathbf{D}_\cup$. Dually, we can recover **D** from $\mathbf{D}_\cap$. The following important result has now been proved.

THEOREM 9.1. **D**, $\mathbf{D}_\cup$, $\mathbf{D}_\cap$ *are alternative postulates for a distributive lattice. Each implies the other two and each implies the modular law* **M**.

It is a simple matter to show by induction that $\mathbf{D}_\cup$ and $\mathbf{D}_\cap$ can be generalised to yield

$$x \cup \left(\bigcap_i^n y_i\right) = \bigcap_i^n (x \cup y_i) \; ; \; x \cap \left(\bigcup_i^n y_i\right) = \bigcup_i^n (x \cap y_i)$$

the upper suffix n indicating a finite number of terms. Either of these may be chosen as an alternative postulate, for we recover $\mathbf{D}_\cup$ and $\mathbf{D}_\cap$ by writing $y_2 = y_3 = \ldots = y_n$.

A further alternative postulate is, assuming $n \geqq 3$,

$$\bigcup_{i=1}^n \left(\bigcap_{j \neq i}^n x_j\right) = \bigcap_{i<j}^n (x_i \cup x_j),$$

which is a generalisation of **D**. To see this we first observe that when $n = 3$ this formula is a replica of **D**. We proceed by induction and assume the formula is valid for n. Observing that

$$\bigcap_j x_j \leqq \bigcap_{j \neq i} x_j \leqq \bigcup_i \left(\bigcap_{j \neq i} x_j\right)$$

and using first the generalisation of $\mathbf{D}_\cup$, then **M**, and lastly the generalisation of $\mathbf{D}_\cap$,

$$\begin{aligned}
\bigcap_{i<j}^{n+1} (x_i \cup x_j) &= \left\{\bigcap_{i<j}^n (x_i \cup x_j)\right\} \cap (x_1 \cup x_{n+1}) \cap \ldots \cap (x_n \cup x_{n+1}) \\
&= \left\{\bigcup_i^n \bigcap_{j \neq i}^n x_j\right\} \cap \left\{x_{n+1} \cup \left(\bigcap_j^n x_j\right)\right\} \\
&= \left\{\left(\bigcup_i^n \bigcap_{j \neq i}^n x_j\right) \cap x_{n+1}\right\} \cup \left\{\bigcap_j^n x_j\right\} \\
&= \bigcup_i^{n+1} \bigcap_{j \neq i}^{n+1} x_j,
\end{aligned}$$

since $\bigcap_j^n$ may be written $\bigcap_{j \neq n+1}^{n+1}$.

Conversely, if $n>3$, writing $x_3 = x_4 = \ldots = x_n$, $\bigcap_{i<j} (x_i \cup x_j)$ becomes

$$(x_1 \cup x_2) \cap (x_1 \cup x_3) \cap (x_2 \cup x_3) \cap x_3 = (x_1 \cup x_2) \cap x_3,$$

while $\bigcup_i \bigcap_{j \neq i} x_j$ takes the form

$$(x_2 \cap x_3) \cup (x_1 \cap x_3) \cup (x_1 \cap x_2 \cap x_3) = (x_2 \cap x_3) \cup (x_1 \cap x_3).$$

Thus if $n>3$ the formula implies $\mathbf{D}_\cap$, which as we know, is equivalent to $\mathbf{D}$.

It must not be assumed that the infinite distributive law

$$x \cap \left(\bigcup^{\infty} y_i \right) = \bigcup^{\infty} (x \cap y_i)$$

and its dual hold in a distributive lattice. Let us augment the infinite lattice of illustration (II) by adding one additional element 0. $\mathscr{L}$ is then the lattice of all non-negative integers in which $x \leqq y$ means that there exists an element z such that $xz = y$. Since $x0 = 0$, we conclude that $x \leqq 0$ for all x. Thus 0 is the I element of the lattice while 1 is the O element. In particular

$$2 \cap \bigcup_{k=0}^{\infty} (2k+1) = 2 \cap 0 = 2,$$

since 0 is the only upper bound for all odd integers. On the other hand

$$\bigcup_{k=0}^{\infty} 2 \cap (2k+1) = \bigcup_{k=0}^{\infty} 1 = 1.$$

Thus the infinite distributive law is invalid in this lattice although it can be shown that this lattice like that of illustration (II) is distributive. Furthermore, it can be shown that the dual law

$$x \cup \left(\bigcap^{\infty} y_i \right) = \bigcap^{\infty} (x \cup y_i)$$

does hold in the lattice mentioned above, which shows that not only can the validity of the infinite distributive laws not be derived from $\mathbf{D}$ above, but also that one of the infinite counterparts of $\mathbf{D}_\cup$ and $\mathbf{D}_\cap$ cannot be derived from the other.

Since every distributive lattice is modular a distributive lattice cannot have a sublattice isomorphic to the pentagon of fig. 2. The next theorem enables us to distinguish between distributive and non-distributive modular lattices.

THEOREM 9.2. *A modular lattice is distributive if and only if it has no sublattice isomorphic to the lattice of fig.* 3.

Proof: The distributive law asserts that

$$(a\cap b)\cup(b\cap c)\cup(c\cap a) = (a\cup b)\cap(b\cup c)\cap(c\cup a)$$

for all a, b, c whereas in the lattice of fig. 3 this is not so since the left side is the element l and the right side is the element r. Consequently this lattice is not distributive.

Conversely, write

$$l = (x\cap y)\cup(y\cap z)\cup(z\cap x),$$
$$r = (x\cup y)\cap(y\cup z)\cap(z\cup x).$$

If the lattice is not distributive then for some x, y, z we must have $l \neq r$. The one-sided distributive law (5.4) then assures us that $l<r$. Put

$$a = (r\cap x)\cup l, \quad b = (r\cap y)\cup l, \quad c = (r\cap z)\cup l.$$

Now

$$r\cap x = (x\cup y)\cap(y\cup z)\cap(z\cup x)\cap x = x\cap(y\cup z),$$

and similarly $r\cap y = y\cap(z\cup x)$. Then

$$\begin{aligned} a\cup b &= [x\cap(y\cup z)]\cup l\cup[y\cap(z\cup x)] \\ &= [x\cap(y\cup z)]\cup[y\cap(z\cup x)], \end{aligned}$$

since each term of l can be absorbed by one of the other terms of $a\cup b$. For instance $y\cap z$ is absorbed by $y\cap(z\cup x)$. Thus, using **M** twice,

$$\begin{aligned} a\cup b &= \{[x\cap(y\cup z)]\cup y\}\cap(z\cup x) \\ &= \{(x\cup y)\cap(y\cup z)\}\cap(z\cup x) \\ &= r. \end{aligned}$$

Similarly, $b\cup c = c\cup a = r$.

Since $l<r$, the modular law shows that a, b, c may also be written

$$a = r\cap(x\cup l), \quad b = r\cap(y\cup l), \quad c = r\cap(z\cup l),$$

and we can apply the dual argument of the foregoing to prove that

$$a\cap b = b\cap c = c\cap a = l.$$

Suppose $l = a$. Then $a = a\cap b$ and $b = a\cup b = r$. Similarly $c = r$. Thus $l = b\cap c = r$, which is contrary to hypothesis. In the same way we conclude that a, b, c, l, r, are all distinct and that they form a lattice isomorphic with that of fig. 3. ◇

COROLLARY. *A lattice is distributive if and only if it has no sublattice isomorphic either to that of fig.* 2 *or to that of fig.* 3.

THEOREM 9.3. *A lattice is distributive if and only if*

$$a\cap b = a\cap c \ \wedge \ a\cup b = a\cup c \Rightarrow b = c.$$

Proof. (i) If the lattice were non-distributive it would contain a five element sublattice isomorphic to one of the lattices of figs. 2, 3, in neither of which is $b = c$ although $a\cap b = a\cap c$ and $a\cup b = a\cup c$. Observe that this result amplifies a previous theorem on modular lattices.

(ii) Concerning the converse we recall that the corresponding theorem for modular lattices assumed that either $b\geqq c$ or $c\geqq b$. This assumption is no longer required if the lattice is distributive for now $a\cap b = a\cap c$ and $a\cup b = a\cup c$ implies that

$$b = b\cup(a\cap b) = b\cup(a\cap c) = (b\cup a)\cap(b\cup c) = (a\cup c)\cap(b\cup c)$$
$$= (a\cap b)\cup c = (a\cap c)\cup c = c. \quad \diamond$$

THEOREM 9.4. *A metric lattice is distributive if and only if*

$$v(x\cup y\cup z)-v(x\cap y\cap z) = v(x)+v(y)+v(z)-v(x\cap y)-v(y\cap z)-v(z\cap x),$$

for all x, y, z.

Proof: If the lattice is distributive, then

$$\begin{aligned} v(x\cup y\cup z) &= v(x)+v(y\cup z)-v(x\cap(y\cup z)) \\ &= v(x)+v(y\cup z)-v((x\cap y)\cup(x\cap z)) \\ &= v(x)+v(y)+v(z)-v(y\cap z)-v(x\cap y)-v(x\cap z) \\ &\qquad +v((x\cap y)\cap(x\cap z)), \end{aligned}$$

which gives the desired identity.

Conversely, since the lattice is metric we can retrace each step in the above argument except the statement

$$v(x\cap(y\cup z)) = v((x\cap y)\cup(x\cap z))$$

which is now a consequence of the assumed identity. Since the one-sided distributive law reads

$$x\cap(y\cup z)\geqq(x\cap y)\cup(x\cap z)$$

and since we know that the valuation v is positive we conclude that

$$x\cap(y\cup z) = (x\cap y)\cup(x\cap z)$$

which shows that the lattice is distributive. $\diamond$

The above theorem has of course a dual obtained by interchanging the cups and caps in the identity.

The following problem illustrates a practical application of the preceding theory. In a certain group of men 10 are blue-eyed, 14 are married and 16 are politicians. There is only one blue-eyed married politician but there are 21 who are either married or blue-eyed and there are 4 blue-eyed politicians. What can be said about the number of men who are either married or are politicians?

The lattice is the set of subsets of the group of men and each atom is an individual. This lattice is distributive (§ 19). An element of length l is a subset of l men. We suppose that the element x is the subset of all blue-eyed men, so that $l(x) = 10$. Also $l(y) = 14$ and $l(z) = 16$ if y is the set of married men and z is the set of politicians. The element $x \cap y$ is the set of blue-eyed married men while $x \cup y$ is the set of men who are either blue-eyed or married. Since we know that $l(x \cup y) = 21$, we deduce from

$$l(x)+l(y) = l(x \cap y)+l(x \cup y)$$

that $l(x \cap y) = 3$. We are told also that $l(x \cap z) = 4$ from which we get $l(x \cup z) = 22$ and that $l(x \cap y \cap z) = 1$. So we have

$$\begin{aligned} l(x \cup y \cup z) &= l(x \cap y \cap z)+l(x)+l(y)+l(z)-l(x \cap y)-l(x \cap z)-l(y \cap z) \\ &= 1+10+14+16-3-4-l(y \cap z). \end{aligned}$$

Thus

$$l(x \cup y \cup z)+l(y \cap z) = 34.$$

Now $l(x \cup y \cup z) \geqq l(x \cup z) = 22$, so $l(y \cap z) \leqq 34-22 = 12$. Also $l(y \cap z) \geqq l(x \cap y \cap z) = 1$. Thus

$$1 \leqq l(y \cap z) \leqq 12.$$

The relation

$$l(y)+l(z) = l(y \cap z)+l(y \cup z)$$

now gives

$$29 \geqq l(y \cup z) \geqq 18.$$

Without further information no more can be said about the number $l(y \cup z)$ of men who are either married or are politicians. It will be found that there is a possible solution of the problem for any value of $l(y \cup z)$ within the limits indicated.

§ 10. Reducibility and independence

An element x of a lattice is said to be $\cup$-**reducible**, or briefly reducible, if $x = x_1 \cup x_2$, where $x_1 < x$, $x_2 < x$. If the lattice has no infinite descending chains then any element x can be expressed as a union of a finite number of irreducible elements, say

$$x = \bigcup_{i=1}^{n} x_i;$$

for either x is itself irreducible in which case $n = 1$, or $x = x_1 \cup x_2$. If x_1 and x_2 are both irreducible then $n = 2$. If x_i is reducible then $x_i = y_1 \cup y_2$. If y_i is reducible then $y_i = z_1 \cup z_2$. This process ends after a finite number of steps since the lattice has no infinite chain of the form $x > x_i > y_i > z_i > \ldots$. When every element has been reduced as far as possible we obtain the required result.

Suppose that

$$x = \bigcup_{i=1}^{n} x_i = \bigcup_{j=1}^{m} y_j$$

are two ways of expressing x as a union of irreducible elements and write

$$t = \bigcup_{i=2}^{n} x_i, \quad z_j = y_j \cup t = y_j \cup \left(\bigcup_{i=2}^{n} x_i \right),$$

then

$$\bigcup_{j=1}^{m} z_j = \left(\bigcup_{j=1}^{m} y_j \right) \cup t = x \cup t = x.$$

Suppose the lattice is modular; then the intervals $[x_1 \cap t, x_1]$ and $[t, x_1 \cup t]$ are isomorphic. Since x_1 is irreducible in the lattice it is *a fortiori* irreducible in the first of these intervals. The isomorphism then shows that $x_1 \cup t$, that is to say x, is irreducible in the second interval. But

$$x = \bigcup_{j=1}^{m} z_j \geqq z_j \geqq t,$$

which shows that each z_j belongs to the second interval $[t, x]$. It follows that for at least one z_j, call it z_1, the $\geqq$ sign must be replaceable by the $=$ sign. Then

$$x = z_1 = y_1 \cup x_2 \cup \ldots \cup x_n.$$

It is easy to adjust the above argument to give the slightly more general result which follows.

THEOREM 10.1. *If* $x = \bigcup_{i=1}^{n} x_i = \bigcup_{j=1}^{m} y_j$ *are two representations of an element* x *as a union of irreducible elements of a modular lattice with no infinite descending chains, then for each* x_i *there exists a* y_j *such that*

$$x = x_1 \cup \ldots \cup x_{i-1} \cup y_j \cup x_{i+1} \cup \ldots \cup x_n.$$

By the above theorem, we may replace the x_i one by one until, if $m > n$, x is expressed as a union of n of the y_j. Any remaining y_j in the original expression for x are unnecessary and could have been omitted. We call an expression $\bigcup x_i$ **irredundant** if no x_i can be omitted without altering the value of the union. It is clear that if the two expressions for x in the above theorem are both irredundant then $m \ngtr n$ and correspondingly $n \ngtr m$. Consequently $n = m$.

THEOREM 10.2. *If the representations of x in the last theorem are both irredundant, then $m = n$. If the lattice is distributive then each x_i is a y_j.*

Proof: The first part has been proved already.

If the replacement for x_1 is called y_1, we have $x = x_1 \cup t = y_1 \cup t$. Then

$$x_1 = x_1 \cap x = x_1 \cap (y_1 \cup t) = (x_1 \cap y_1) \cup (x_1 \cap t).$$

Since x_1 is irreducible we have either $x_1 = x_1 \cap y_1$, or $x_1 = x_1 \cap t$ which implies $t = x_1 \cup t = x$. The second alternative however is impossible since the representations are irredundant. Hence $x_1 = x_1 \cap y_1$ and $x_1 \leqq y_1$. Similarly, if x_k is the replacement for y_1, we would have $x_1 \leqq y_1 \leqq x_k$. Since the x_i are irredundant, we must have $k = 1$ and so $x_1 = y_1$. The argument in the other cases is similar. ◇

We may clarify the significance of the last two theorems by relating them to the lattice (fig. 3) of three lines a, b, c concurrent in the point l and lying on the plane r. We have four irreducible representations of r namely $r = a \cup b = a \cup c = b \cup c = a \cup b \cup c$. In illustration of theorem 10.1, a in $a \cup b$ may be replaced by c from $a \cup c$ thereby yielding $b \cup c$. Of the four representations only the first three are irredundant. In the fourth we could delete any one of a, b, c. As stated in the second theorem, the three irredundant representations have each the same number of terms. The second part of this theorem is not applicable since the lattice is not distributive.

The lattice of illustration (II) is distributive. (See exercise 17). It is not difficult to see that the $\cup$-irreducible elements are the powers of primes. The second theorem therefore shows that a given integer can be expressed in only one way as an irredundant L.C.M. of prime powers. If the same prime occurs to different powers when the given integer is expressed as the L.C.M. of prime powers, all but the highest power are redundant and may be deleted. When this has been done the remaining irreducible elements are mutually prime so that their L.C.M. is merely their product. Our theorem therefore entails the uniqueness of factorisation of an integer.

An element y is said to be **independent** of the set $x_1, \ldots, x_m$ if $y \cap (\bigcup x_i) = O$. Otherwise y is dependent on the set. A set of elements $x_1, \ldots, x_n$ forms an **independent set** if each x_i is independent of the others, that is to say, if for all i

$$x_i \cap \left(\bigcup_{j \neq i} x_j \right) = O.$$

THEOREM 10.3. *In a modular lattice, if y is independent of an independent set $x_1, \ldots, x_n$, then $y, x_1, \ldots, x_n$ form an independent set.*

Proof: Since y is independent of the x_i it is only necessary to show that

$$x_i \cap \left(y \cup \bigcup_{j \neq i} x_j\right) = O.$$

By the modular law

$$(\bigcup x_i) \cap \left(y \cup \bigcup_{j \neq i} x_j\right) = \left((\bigcup x_i) \cap y\right) \cup \bigcup_{j \neq i} x_j = O \cup \bigcup_{j \neq i} x_j = \bigcup_{j \neq i} x_j.$$

So by the isotone property

$$x_i \cap \left(y \cup \bigcup_{j \neq i} x_j\right) \leqq \left(\bigcup x_i\right) \cap \left(y \cup \bigcup_{j \neq i} x_j\right) = \bigcup_{j \neq i} x_j.$$

Hence by (3.2) and by $\mathbf{L}_{3\cap}$,

$$x_i \cap \left(y \cup \bigcup_{j \neq i} x_j\right) = x_i \cap \left(y \cup \bigcup_{j \neq i} x_j\right) \cap \bigcup_{j \neq i} x_j = x_i \cap \bigcup_{j \neq i} x_j = O. \quad \diamond$$

§ 11. Complemented lattices

If a lattice $\mathscr{L}$ has both O and I and x, y are two elements of $\mathscr{L}$ such that

$$x \cap y = O, \quad x \cup y = I$$

then y is a **complement** of x and x is a complement of y. In general an element x may have no complement such as x_4 in fig. 4, may have several complements such as a in fig. 2 which has two complements, or a in fig. 3 which also has two complements, or may have a unique complement such as x in fig. 7.

It is patent that O and I, if they exist, are complements of each other.

If x, y are complements of each other with respect to the sub-lattice $[a, b]$, that is, if

$$x \cup y = b, \quad x \cap y = a,$$

then x, y are each a **relative complement** with respect to $[a, b]$ of the other.

A **complemented lattice** is one in which every element has at least one complement while a **relatively complemented lattice** is one in which each $[a, b]$ is a complemented lattice. For instance the lattice of fig. 2 is complemented but is not relatively complemented. In this case c has no complement in $[I, b]$ though in the whole lattice I, a, c, b, O have respective complements O, b or c, a, a, I.

THEOREM 11.1. *If x and y are complements with respect to a modular lattice $\mathscr{L}$ and if $a \geqq x \geqq b$, then x has a relative complement with respect to $[a, b]$, namely $a \cap (y \cup b)$.*

Proof: By the modular law,

$$a \cap (y \cup b) = (a \cap y) \cup b.$$

Also, since $a \geqq x \geqq b$,

$$x \cap a \cap (y \cup b) = x \cap (y \cup b) = (x \cap y) \cup b = O \cup b = b$$

and

$$x \cup (a \cap y) \cup b = x \cup (y \cap a) = (x \cup y) \cap a = I \cap a = a. \ \diamond$$

COROLLARY. *A modular complemented lattice is relatively complemented.*

We now obtain another characterisation of distributive lattices.

THEOREM 11.2. *A lattice is distributive if and only if such relative complements as exist are unique.*

Proof: If y_1, y_2 were two complements of x then

$$x \cap y_1 = x \cap y_2 = O,$$

$$x \cup y_1 = x \cup y_2 = I.$$

In a distributive lattice we have seen (Theorem 9.3) that these relations imply $y_1 = y_2$. A similar argument applies to relative complements.

Conversely, if relative complements are unique the lattice has no sublattice isomorphic to the lattices of fig. 2 and fig. 3. By the corollary to theorem 9.2, this means that the lattice is distributive. $\diamond$

It should be stressed, however, that not all the elements of a distributive lattice, as for instance that of fig. 1, need have complements.

Since in a distributive lattice complements are unique we may without ambiguity denote the complement of x by x'. Then since

$$x \cap x' = O, \quad x \cup x' = I$$

we see that

$$(x')' = x.$$

§ 12. Boolean algebras

A complemented distributive lattice is called a **Boolean algebra.** Boolean algebras were the first lattices to be investigated. They arose in the study by George Boole of formal logic and indeed are in some ways the most interesting type of lattices. The elements of a Boolean algebra satisfy the six postulates for a lattice, $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{3\cap}$, $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cup}$ (pp. 4, 5), the distributive postulate **D** (p. 22) and the following postulate **C**.

C. For any element x there is a complement x' such that

$$x \cap x' = O, \quad x \cup x' = I.$$

Since the lattice is distributive, complements are unique and we have taken this into account in employing the notation x' for the complement of x. Again, since the lattice is distributive it is also modular and the postulate **M** (p. 12) is therefore automatically satisfied. The alternative forms $\mathbf{D}_\cap$, $\mathbf{D}_\cup$ of **D** must also hold. The duality of unions and intersections in the six lattice postulates extends to the formula **D** which is self-dual. It also extends to **C** since I is the l.u.b. of all the elements of the lattice and has O the g.l.b. of all the elements as its dual, and vice versa. Postulate **C** also requires that O and I elements exist in the Boolean algebra. From their definition it is clear that O and I are complements. Thus

$$O' = I, \quad I' = O.$$

As we have already seen

$$(x')' = x,$$

from which we see that

$$x = y \Leftrightarrow x' = y',$$

by considering the uniqueness of complements.

Since a Boolean algebra is distributive, all the properties of modular and of distributive lattices are properties of a Boolean algebra. Likewise, all the properties of a complemented lattice are properties of a Boolean algebra. These need not be restated here. Our present concern is with those properties of Boolean algebras which do not extend to other lattices.

THEOREM 12.1. *In a Boolean algebra*

$$(x \cap y)' = x' \cup y', \quad (x \cup y)' = x' \cap y'.$$

Proof: Since

$$(x \cap y) \cup (x' \cup y') = (x \cup x' \cup y') \cap (y \cup x' \cup y') = (I \cup y') \cap (I \cup x') = I \cap I = I$$

and

$$(x \cap y) \cap (x' \cup y') = (x \cap y \cap x') \cup (x \cap y \cap y') = (O \cap y) \cup (O \cap x)$$
$$= O \cup O = O,$$

it is clear that $x' \cup y'$ is the complement of $x \cap y$. Dually, $x' \cap y'$ is the complement of $x \cup y$. ◇

The formulae stated in theorem 12.1 are sometimes called **de Morgan's laws.** From these laws we can prove that

$$x \leqq y \Leftrightarrow x' \geqq y',$$

since

$$x \leqq y \Leftrightarrow x \cup y = y \Leftrightarrow x' \cap y' = (x \cup y)' = y' \Leftrightarrow x' \geqq y'.$$

THEOREM 12.2. *In a Boolean algebra*

$$x \leqq y \Leftrightarrow x \cap y' = O \Leftrightarrow x' \cup y = I.$$

Proof: By the isotone property,

$$x \leqq y \Rightarrow x \cap y' \leqq y \cap y' = O \Rightarrow x \cap y' = O.$$

Conversely, if $x \cap y' = O$, then

$$x \cup y = (x \cup y) \cap I = (x \cup y) \cap (y' \cup y) = (x \cap y') \cup y = O \cup y = y,$$

from which it follows that $x \leqq y$.
Also

$$x \cap y' = O \Leftrightarrow x' \cup y = (x \cap y')' = O' = I. \ \diamond$$

THEOREM 12.3. *The infinite distributive laws hold in a complete Boolean algebra.*

Proof: As was shown in § 5,

$$y \cap (\bigcup x_i) \geqq \bigcup (y \cap x_i)$$

even when there are infinitely many terms in the unions. These unions certainly exist since the lattice is complete. Let $z = \bigcup (y \cap x_i)$. Then $y \cap x_i \leqq z$ and

$$x_i \leqq y' \cup x_i = y' \cup (y \cap x_i) \leqq y' \cup z$$

for each i. Hence

$$\bigcup x_i \leqq y' \cup z,$$

and so

$$y \cap (\bigcup x_i) \leqq y \cap (y' \cup z) = y \cap z \leqq z.$$

That is to say

$$y \cap (\bigcup x_i) \leqq \bigcup (y \cap x_i).$$

We therefore have by $\mathbf{P}_2$ the infinite distributive law

$$y \cap (\bigcup x_i) = \bigcup (y \cap x_i).$$

Its dual may be obtained in the same way. $\diamond$

§ 13. Canonical form of a Boolean polynomial

We wish to have a criterion by which we can decide whether two polynomials of a free Boolean algebra with n generators $x_1, \ldots, x_n$

are equal or not. The reader is reminded that the adjective "free" here means that the elements x_i satisfy no identities other than those implied by the postulates for the Boolean algebra. The required criterion is obtained by constructing a canonical form for each polynomial and by showing that two polynomials have the same canonical form if and only if the polynomials are equal.

A typical Boolean polynomial will be an expression involving elements $x, y, z, \ldots$, their complements $x', y', z', \ldots$, cups, caps and parentheses. By the repeated use of de Morgan's laws it can be arranged that no primes denoting complements remain outside any parentheses. At this stage each prime is attached to a single letter. Next, by the repeated use of $\mathbf{D}_\cap$ it can be arranged that no cap remains outside parentheses. At this stage our polynomial has been expressed as a union of terms, each term being an intersection of primed and unprimed letters. Since $x \cap x' = O$, a term which contains both an element and its complement may be replaced by O. Such a term may then be deleted unless every term is replaceable by O in which case the polynomial is the null element. If a term now contains any letter or any primed letter more than once, all but one of this letter or primed letter may be deleted, since $x \cap x = x$ and $x' \cap x' = x'$.

If a non-null term T contains neither x nor x' it can be replaced by two terms one of which contains x and the other x', for

$$T = T \cap I = T \cap (x \cup x') = (T \cap x) \cup (T \cap x').$$

Repeating this process as often as may be necessary, a non-null polynomial is eventually expressed as a union of terms each of which is a **minimal polynomial** of the form

$$X_1 \cap X_2 \cap \ldots \cap X_n$$

in which each X_i is either x_i or x_i'. Finally to obtain the canonical form we delete any term T at its second or subsequent occurrence, since $T \cup T = T$. For instance, if $n = 2$ any non-null polynomial has a canonical form which is the union of some or all of the minimal polynomials

$$x_1 \cap x_2, \quad x_1 \cap x_2', \quad x_1' \cap x_2, \quad x_1' \cap x_2'.$$

It is patent that polynomials having the same canonical form are equal. It remains to be shown that distinct canonical forms cannot be equal. We first observe that if two minimal polynomials T and S are distinct then $T \cap S = O$ since for some i one must contain x_i and the other x_i'. Suppose then that

$$T_1 \cup T_2 \cup \ldots \cup T_t = S_1 \cup S_2 \cup \ldots \cup S_s$$

in which the T_j are all distinct and the S_i are all distinct. Then $S_i \leqq T_1 \cup T_2 \cup \ldots \cup T_t$, which implies that

$$S_i = S_i \cap (T_1 \cup T_2 \cup \ldots \cup T_t) = (S_i \cap T_1) \cup \ldots \cup (S_i \cap T_t).$$

If S_i were distinct from each T_j the right side would be O giving a contradiction; it follows that S_i is some T_j. Thus every S is a T and likewise every T is an S. There is therefore a $1-1$ correspondence between the S_i and the T_j, $s = t$ and $S_1, \ldots S_s$ are merely $T_1, \ldots, T_t$ in a possibly different order. Disregarding this order we see that a given polynomial can have only one canonical form.

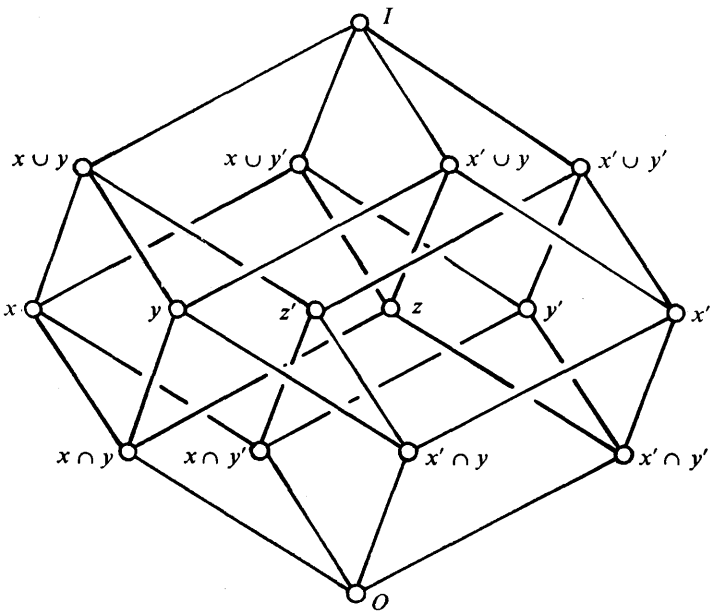


FIG. 7

For n generators there are 2^n possible minimal polynomials each of which can either be present or absent in a given canonical form. There are therefore 2^{2^n} possible distinct canonical forms and consequently a free Boolean algebra with n generators has exactly 2^{2^n} different elements. We exhibit in fig. 7 the Boolean algebra of 16 elements generated by two elements x and y. In this figure we write

$$z = (x \cap y) \cup (x' \cap y') = (x \cup y') \cap (x' \cup y),$$

$$z' = (x' \cup y') \cap (x \cup y) = (x' \cap y) \cup (x \cap y'),$$

for the sake of convenience in printing. The reader will easily verify relations such as

$$x = (x \cap y) \cup (x \cap y'),$$
$$x' = (x' \cap y') \cup (x' \cap y),$$
$$x \cup y' = (x \cap y) \cup (x \cap y') \cup (x' \cap y'),$$

which exhibit on the right the canonical form of the elements on the left.

It should be emphasised that if a Boolean algebra with n generators is not free then it will have less than 2^{2^n} elements. For instance if the generating elements x and y of the lattice of fig. 7 satisfy the additional relation $x \geqq y'$, that is to say $x \cap y' = y'$ the lattice telescopes into that of fig. 8. Indeed this relation identifies the two elements at the ends of any line of fig. 7 parallel to that joining $x \cap y'$ and y'.

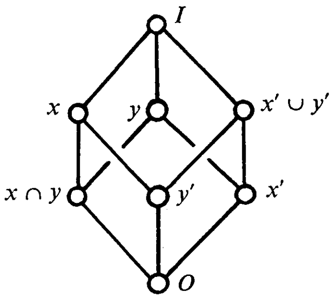


FIG. 8

It will be observed with interest that figs. 7 and 8 are the projections onto a plane of respectively a four- and a three-dimensional cube.

The reader will recognise that a dual canonical form is also possible whereby any element is represented as an intersection of **maximal polynomials** of the type $X_1 \cup X_2 \cup \ldots \cup X_n$ where once more X_i represents either x_i or x_i'. Indeed, the minimal polynomials are the atoms and the maximal polynomials are the anti-atoms of the lattice. The canonical form of an element a is merely the union of all the atoms of the sublattice formed by the interval $[O, a]$.

Another procedure for determining the canonical form of a Boolean polynomial $f(x_1, \ldots, x_n)$ is based on the following result.

EXPANSION THEOREMS 13.1. *In a Boolean algebra*

$$f(x_1, \ldots, x_n) = \{x_1 \cap f(I, x_2, \ldots, x_n)\} \cup \{x_1' \cap f(O, x_2, \ldots, x_n)\}$$

$$f(x_1, \ldots, x_n) = \{x_1 \cup f(O, x_2, \ldots, x_n)\} \cap \{x_1' \cup f(I, x_2, \ldots, x_n)\}.$$

Proof: We have seen that f is a union of minimal polynomials. All those in which x_1 occurs can be grouped together and their union may be written

$$\bigcup (x_1 \cap X_2 \cap \ldots \cap X_n) = x_1 \cap \{\bigcup (X_2 \cap \ldots \cap X_n)\},$$

while the union of those in which x'_1 occurs may be written

$$\bigcup(x'_1\cap Y_2\cap\ldots\cap Y_n) = x'_1\cap\{\bigcup(Y_2\cap\ldots\cap Y_n)\}$$

then

$$f(x_1, \ldots, x_n) = \{x_1\cap(\bigcup(X_2\cap\ldots\cap X_n))\}\cup\{x'_1\cap(\bigcup(Y_2\cap\ldots\cap Y_n))\}.$$

Putting $x_1 = I$ and $x_1 = O$ in turn in this formula yields

$$f(I, x_2, \ldots, x_n) = \bigcup(X_2\cap\ldots\cap X_n),$$
$$f(O, x_2, \ldots, x_n) = \bigcup(Y_2\cap\ldots\cap Y_n).$$

Consequently

$$f(x_1, \ldots, x_n) = \{x_1\cap f(I, x_2, \ldots, x_n)\}\cup\{x'_1\cap f(O, x_2, \ldots, x_n)\}.$$

The other formula is established dually. ◇

A repeated use of the first expansion theorem will provide the canonical form in terms of minimal polynomials. For instance,

$$\begin{aligned} f(x_1, x_2) &= \{x_1\cap f(I, x_2)\}\cup\{x'_1\cap f(O, x_2)\} \\ &= \{x_1\cap x_2\cap f(I, I)\}\cup\{x_1\cap x'_2\cap f(I, O)\}\cup\{x'_1\cap x_2\cap f(O, I)\} \\ &\qquad \cup\{x'_1\cap x'_2\cap f(O, O)\}. \end{aligned}$$

Now each of $f(I, I), f(I, O), f(O, I), f(O, O)$ is either I or O. So if we delete any term with O and suppress every I, as we may, we are left with a union of distinct minimal polynomials which is the canonical form of $f(x_1, x_2)$. The general case is entirely similar.

In the light of the preceding argument it is apparent that to establish an identity between two polynomials $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ of any Boolean algebra it is sufficient to verify that $f(\delta_1, \ldots, \delta_n) = g(\delta_1, \ldots, \delta_n)$ where the δ_i are elements of the Boolean algebra which consists of only two elements O and I. Thus, in the case $n = 2$, we can assert that $f(x_1, x_2) = g(x_1, x_2)$ provided we can establish the four relations

$$f(I, I) = g(I, I), f(I, O) = g(I, O), f(O, I) = g(O, I), f(O, O) = g(O, O).$$

Again using the distributive law and the expansion theorem it is easy to deduce that

$$x_1\cap f(x_1, \ldots, x_n) = x_1\cap f(I, x_2, \ldots, x_n),$$
$$x'_1\cap f(x_1, \ldots, x_n) = x'_1\cap f(O, x_2, \ldots, x_n)$$

and the dual formulae

$$x_1\cup f(x_1, \ldots, x_n) = x_1\cup f(O, x_2, \ldots, x_n),$$
$$x'_1\cup f(x_1, \ldots, x_n) = x'_1\cup f(I, x_2, \ldots, x_n).$$

These formulae are sometimes useful.

§ 14. Boolean rings

An interesting feature of Boolean algebras is that they can be fashioned into commutative rings by interpreting intersections as products, that is, by writing

$$xy = x \cap y,$$

and by defining the sum of two elements x and y as

$$x+y = (x \cap y') \cup (x' \cap y).$$

It is clear that the commutative and associative laws of multiplication are merely $\mathbf{L}_{1\cap}$ and $\mathbf{L}_{2\cap}$. The all-element I plays the part of an identity since

$$xI = Ix = x.$$

Furthermore, every element is idempotent since $xx = x$. The commutative law of addition follows immediately from our definition of addition and from $\mathbf{L}_{1\cup}$. Further,

$$\begin{aligned}(x+y)+z &= ((x+y) \cap z') \cup ((x+y)' \cap z) \\ &= [((x \cap y') \cup (x' \cap y)) \cap z'] \cup [(x \cap y')' \cap (x' \cap y)' \cap z] \\ &= [(x \cap y' \cap z') \cup (x' \cap y \cap z')] \cup [(x' \cup y) \cap (x \cup y') \cap z] \\ &= (x \cap y' \cap z') \cup (x' \cap y \cap z') \cup (x' \cap y' \cap z) \cup (y \cap x \cap z)\end{aligned}$$

which is seen to be symmetric in x, y, z. Consequently,

$$(x+y)+z = (y+z)+x = x+(y+z).$$

Addition is therefore associative.

Again the null element O is a zero since

$$x+O = (x \cap O') \cup (x' \cap O) = (x \cap I) \cup O = x.$$

Every element is its own additive inverse, since

$$x+x = (x \cap x') \cup (x' \cap x) = O \cup O = O.$$

Since $2x = O$ for all x, the ring is of characteristic 2 and it is therefore unnecessary to distinguish between subtraction and addition. We have still to establish the distributive law. In fact

$$\begin{aligned}xy+xz &= ((xy) \cap (xz)') \cup ((xy)' \cap (xz)) \\ &= (x \cap y \cap (x' \cup z')) \cup ((x' \cup y') \cap x \cap z) \\ &= (x \cap y \cap z') \cup (y' \cap x \cap z) \\ &= x \cap [(y \cap z') \cup (y' \cap z)] \\ &= x[y+z].\end{aligned}$$

The Boolean algebra therefore forms a ring with an identity element in which every element is idempotent.

A **Boolean ring** is a ring in which every element is idempotent, that is $xx = x$ for every x. In particular

$$x+y = (x+y)^2 = x^2+xy+yx+y^2 = x+xy+yx+y,$$

which shows that $xy+yx = O$. Put $y = x$ and we get

$$x+x = xx+xx = O,$$

showing that the ring is of characteristic 2. Then $yx = -xy = +xy$ which implies that the ring is also commutative. We have therefore shown that the Boolean algebra is a Boolean ring. We now show that every Boolean ring with an identity element I and zero O is a Boolean algebra in which $x \cap y$ means xy and $x \cup y$ means $x+y+xy$. $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{1\cup}$ are immediate consequences of these definitions. Also

$$(x\cup y)\cup z = (x\cup y)+z+(x\cup y)z = x+y+xy+z+xz+yz+xyz.$$

The symmetry of this last expression along with $\mathbf{L}_{1\cup}$ establishes $\mathbf{L}_{2\cup}$. Again,

$$x\cap(y\cup x) = x(x+y+xy) = x^2+xy+x^2y = x+2xy = x,$$

$$x\cup(y\cap x) = x+yx+xyx = x+2yx = x,$$

which yield $\mathbf{L}_{3\cap}$ and $\mathbf{L}_{3\cup}$ respectively. Similarly

$$x\cap(y\cup z) = x(y+z+yz) = xy+xz+xyxz = (xy)\cup(xz) = (x\cap y)\cup(x\cap z)$$

which establishes that the lattice is distributive. Finally if we write $x' = I+x$, then

$$x\cup x' = x+x'+xx' = x+(I+x)+x(I+x) = I+4x = I$$

while

$$x\cap x' = xx' = x(I+x) = 2x = O,$$

showing that the lattice is complemented. The Boolean ring thus satisfies all the postulates for a Boolean algebra.

THEOREM 14.1. *There is a* $1-1$ *correspondence between Boolean rings with an identity and Boolean algebras in which*

$$x+y = (x\cap y')\cup(x'\cap y),\quad x\cup y = x+y+xy,\quad x\cap y = xy,\quad x' = I+x.$$

Proof: Start with a Boolean ring in which addition is written $x+y$. Construct from it a Boolean algebra in which $x\cup y$ is defined to be $x+y+xy$ and x' is defined to be $I+x$. Finally construct from the algebra a Boolean ring in which addition is defined by

$$x\oplus y = (x\cap y')\cup(x'\cap y).$$

Then, since $xx' = O$,

$$\begin{aligned} x \oplus y &= (xy') \cup (x'y) = (xy') + (x'y) + xy'x'y \\ &= x(I+y) + (I+x)y + O \\ &= x + y + 2xy \\ &= x + y. \end{aligned}$$

Thus not only multiplication but also addition is the same in the two rings which are therefore identical. In particular, $I \oplus x = x' = I + x$. The two constructions are thus the inverses of each other. This demonstrates that the correspondence is $1-1$. $\diamond$

Before we leave this section we shall examine the relationship of the inclusion relation to ring terminology. We know that in the lattice

$$x \geqq y \Leftrightarrow x \cap y = y \Leftrightarrow x \cup y = x.$$

Thus, in the ring

$$x \geqq y \Leftrightarrow xy = y \Leftrightarrow x + y + xy = x.$$

The last statement may be written $y + xy = O$, which is merely a reformulation of $xy = y$. In particular

$$Ix = x \Leftrightarrow I \geqq x,$$

$$xO = O \Leftrightarrow x \geqq O$$

and

$$xx = x \Leftrightarrow x \geqq x.$$

§ 15. Morphisms

The concepts of homomorphisms and isomorphisms in lattice theory are, of course, analogous to those concepts in other branches of algebra but it is desirable to give a precise formulation of their definitions since in lattice theory they occur in varying contexts. Consider a mapping ϕ which associates any element x of a lattice $\mathscr{X}$ with a unique element $\phi(x) = y$ of a lattice $\mathscr{Y}$. The mapping ϕ of $\mathscr{X}$ into $\mathscr{Y}$ is called a **union-homomorphism** if

$$x_1 \cup x_2 = x_3 \Rightarrow \phi(x_1) \cup \phi(x_2) = \phi(x_3).$$

It is an **intersection-homomorphism** if

$$x_1 \cap x_2 = x_3 \Rightarrow \phi(x_1) \cap \phi(x_2) = \phi(x_3).$$

It is an **ordering-homomorphism** if

$$x_1 \geqq x_2 \Rightarrow \phi(x_1) \geqq \phi(x_2).$$

Suppose ϕ is an intersection-homomorphism, then

$$\begin{aligned} x_1 \geqq x_2 &\Rightarrow x_1 \cap x_2 = x_2 \\ &\Rightarrow \phi(x_1 \cap x_2) = \phi(x_2) \\ &\Rightarrow \phi(x_1) \cap \phi(x_2) = \phi(x_2) \\ &\Rightarrow \phi(x_1) \geqq \phi(x_2). \end{aligned}$$

Thus every intersection-homomorphism is an ordering-homomorphism and dually so is every union-homomorphism, though the converses of these statements do not hold.

Not every intersection-homomorphism is a union-homomorphism but a mapping which is both a union- and an intersection-homomorphism is called a **lattice-homomorphism**. In each of the above instances a homomorphism is called an **isomorphism** if ϕ is a mapping of $\mathscr{X}$ onto $\mathscr{Y}$ and if the implications in the above definitions are reversible, that is, if $\Rightarrow$ can be replaced by $\Leftrightarrow$. It is easy to show that in each form of isomorphism

$$\begin{aligned} \phi(x_1) = \phi(x_2) &\Rightarrow x_1 = x_2, \\ \phi(x_1) \geqq \phi(x_2) &\Rightarrow x_1 \geqq x_2. \end{aligned}$$

An isomorphism is a $1-1$ mapping, that is to say, for any $y \in \mathscr{Y}$ there exists a unique $x \in \mathscr{X}$ such that $y = \phi(x)$. In other words, in an isomorphism the inverse mapping $x = \phi^{-1}(y)$ exists.

It will now be shown that the four types of isomorphism coincide. Suppose ϕ is an ordering-isomorphism; then

$$\begin{aligned} \phi(x_1 \cap x_2) \geqq \phi(x_3) &\Leftrightarrow x_1 \cap x_2 \geqq x_3 \\ &\Leftrightarrow x_1 \geqq x_3 \wedge x_2 \geqq x_3 \\ &\Leftrightarrow \phi(x_1) \geqq \phi(x_3) \wedge \phi(x_2) \geqq \phi(x_3) \\ &\Leftrightarrow \phi(x_1) \cap \phi(x_2) \geqq \phi(x_3). \end{aligned}$$

If we choose $x_3 = x_1 \cap x_2$ the left side is true. Consequently

$$\phi(x_1) \cap \phi(x_2) \geqq \phi(x_1 \cap x_2).$$

If we choose $\phi(x_3) = \phi(x_1) \cap \phi(x_2)$, i.e., $x_3 = \phi^{-1}(\phi(x_1) \cap \phi(x_2))$, the right side is true and so

$$\phi(x_1 \cap x_2) \geqq \phi(x_1) \cap \phi(x_2).$$

Hence, by $\mathbf{P}_2$,

$$\phi(x_1 \cap x_2) = \phi(x_1) \cap \phi(x_2),$$

so that ϕ is also an intersection-isomorphism. Dually it is a union-isomorphism and since it is both it is a lattice-isomorphism. In the case of an isomorphism the prefix is evidently unnecessary. If the prefix is omitted from a homomorphism it is intended that the prefix lattice- is to be understood.

A homomorphism of a lattice with itself is sometimes called an **endomorphism.**

It is easily verified that $\phi(x) = x \cap a$, in which a is a fixed element defines an intersection-endomorphism. If the lattice is distributive this $\phi(x)$ is also a union-endomorphism and is therefore a lattice-endomorphism. Indeed

$$\phi(x_1 \cup x_2) = (x_1 \cup x_2) \cap a = (x_1 \cap a) \cup (x_2 \cap a) = \phi(x_1) \cup \phi(x_2).$$

Dually, $\psi(x) = x \cup a$ is a union-endomorphism which is a lattice-endomorphism if the lattice is distributive.

If the mapping ϕ is a lattice-homomorphism then the set of elements $\phi(x)$ of $\mathscr{Y}$ forms a sub-lattice of $\mathscr{Y}$ since the several lattice postulates are easily established. For example, for $\mathbf{L}_{3\cap}$, we have

$$\phi(x_1) \cap (\phi(x_2) \cup \phi(x_1)) = \phi(x_1) \cap \phi(x_2 \cup x_1) = \phi(x_1 \cap (x_2 \cup x_1)) = \phi(x_1).$$

In particular in a distributive lattice the set of elements $x \cap a$, a fixed, constitutes the sub-lattice consisting of the interval $[O, a]$ while the set of elements $x \cup a$ constitutes the sub-lattice $[a, I]$.

Fixed Point Theorem 15.1. *If ϕ denotes an endomorphism of a complete lattice $\mathscr{L}$ then $\phi(a) = a$ for some $a \in \mathscr{L}$.*

Proof: Let $\mathscr{M}$ denote the set of elements x of $\mathscr{L}$ for which $x \leqq \phi(x)$. $\mathscr{M}$ is non-void since O belongs to $\mathscr{M}$. Since $\mathscr{L}$ is complete, $\bigcup_{x \in \mathscr{M}} x$ exists and we denote this element by a. Since ordering is preserved by the endomorphism, $x \leqq \phi(x) \leqq \phi(a)$ is a consequence of $x \leqq a$. It follows that $a = \bigcup x \leqq \phi(a)$, showing that a is itself an element of $\mathscr{M}$ and is indeed, according to its definition, the greatest element of $\mathscr{M}$. However $\phi(a)$ is also an element of $\mathscr{M}$, since $a \leqq \phi(a)$ implies that $\phi(a) \leqq \phi(\phi(a))$. Hence $\phi(a) \leqq a$. Consequently $\phi(a) = a$. ◇

§ 16. Direct products

Let $\mathscr{X}$ and $\mathscr{Y}$ be two lattices. The set of ordered pairs (x, y) with $x \in \mathscr{X}$, $y \in \mathscr{Y}$ form a lattice if we define

$$(x_1, y_1) \cup (x_2, y_2) = (x_1 \cup x_2, y_1 \cup y_2),$$
$$(x_1, y_1) \cap (x_2, y_2) = (x_1 \cap x_2, y_1 \cap y_2).$$

The verification of postulates $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{3\cap}$, $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cup}$ may be left to the reader. The lattice so constructed is called the **direct product** of $\mathscr{X}$ and $\mathscr{Y}$ and may be denoted by $\mathscr{X} \times \mathscr{Y}$. For instance, if

$\mathscr{X}$ and $\mathscr{Y}$ have Hasse diagrams of fig. 10 and fig. 9 then $\mathscr{X}\times\mathscr{Y}$ has 12 elements and has the Hasse diagram of fig. 11.

FIG. 9

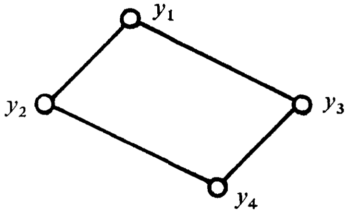


FIG. 10

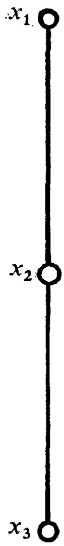
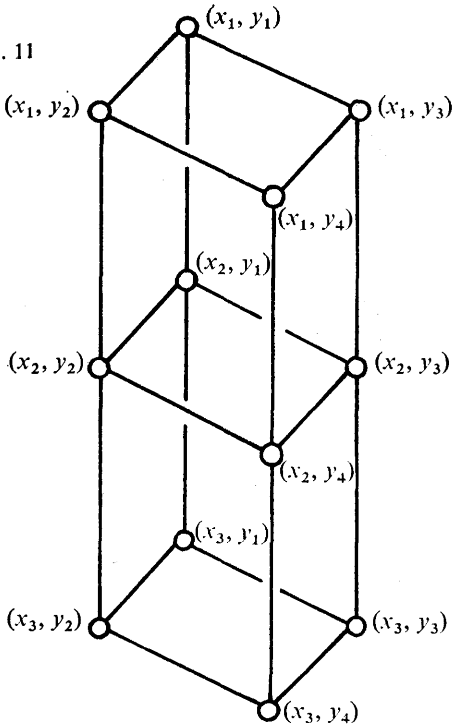


FIG. 11



The inclusion relation in $\mathscr{X}\times\mathscr{Y}$ is easily seen to be

$$(x_1, y_1)\geqq(x_2, y_2) \Leftrightarrow x_1\geqq x_2 \wedge y_1\geqq y_2.$$

It will be recognised that $\mathscr{X}\times\mathscr{Y}$ and $\mathscr{Y}\times\mathscr{X}$ have identical structures, for it is merely a matter of nomenclature whether a given element of the direct product is called (x, y) or (y, x).

The concept of a direct product can easily be extended to embrace the product of any number of lattices. For instance, if $\mathscr{Y}$ is itself the direct product of $\mathscr{U}$ and $\mathscr{V}$ then $\mathscr{X} \times \mathscr{Y} = \mathscr{X} \times \mathscr{U} \times \mathscr{V}$ and a typical element of this direct product might be written (x, u, v). It is left to the reader to verify that the operation $\times$ is associative.

It is of interest to enquire whether a given lattice is isomorphic to a direct product of two lattices. Since the order of a direct product is the product of the orders of the component lattices it follows that a lattice of prime order such as those of fig. 2 and fig. 3 cannot be expressed as direct products. We shall show, however, that every distributive lattice $\mathscr{L}$ of order greater than 2 is either a direct product or a sub-lattice of a direct product. If a is a fixed element of $\mathscr{L}$ other than O or I then the set of elements $a \cap x$ forms a sub-lattice of $\mathscr{L}$, namely the interval $[O, a]$. The set of elements $a \cup x$ is also a sub-lattice namely $[I, a]$. Thus the set of ordered pairs

$$X = (a \cup x, a \cap x)$$

is a subset of the direct product of these two sub-lattices. Further

$$X = Y \Leftrightarrow x = y$$

by a property of distributive lattices. There is therefore a $1-1$ correspondence between the ordered pairs X and the elements x of the lattice. Again

$$\begin{aligned} X \cup Y &= (a \cup x, a \cap x) \cup (a \cup y, a \cap y) \\ &= (a \cup x \cup a \cup y, (a \cap x) \cup (a \cap y)) \\ &= (a \cup (x \cup y), a \cap (x \cup y)), \end{aligned}$$

and dually

$$X \cap Y = (a \cup (x \cap y), a \cap (x \cap y)).$$

Thus the set of pairs X forms a sub-lattice of the direct product $[a, I] \times [O, a]$ and $\phi(x) = X$ determines an isomorphism between the lattice $\mathscr{L}$ and this sub-lattice. We can express this by saying that $\mathscr{L}$ is isomorphic with a **sub-direct product** of $[a, I]$ and $[O, a]$.

If $[O, a]$ is of order greater than 2 the process can be repeated by choosing a fixed element b of $[O, a]$ other than a or O, and $[O, a]$ can then be expressed as a sub-direct product of $[b, a]$ and $[O, b]$. We can repeat the process on $[a, I]$, or on $[b, a]$, or on $[O, b]$, and so on until, in the case of a lattice $\mathscr{L}$ of finite order, $\mathscr{L}$ has been expressed as a sub-direct product of a finite number n of intervals each of order 2. Each of these intervals is then isomorphic to the two element lattice consisting only of 0 and 1, and each element of this sub-direct product may be written as an ordered n-tuple each of whose components are 0 or 1. Furthermore $\mathscr{L}$ is of length n.

These points should be clarified by the following illustration in which the theory is applied to the distributive lattice of fig. 12. For the first decomposition we fix a and take

$$\begin{aligned} I &= (a \cup i, a \cap i) = (i, a) \\ A &= (a \cup a, a \cap a) = (a, a) \\ B &= (a \cup b, a \cap b) = (a, b) \\ C &= (a \cup c, a \cap c) = (i, d) \\ D &= (a \cup d, a \cap d) = (a, d) \\ O &= (a \cup o, a \cap o) = (a, o) \end{aligned}$$

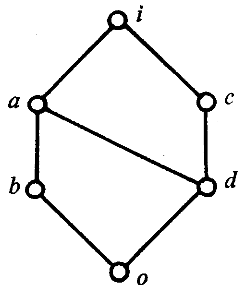


FIG. 12

then I, A, B, C, D, O is a lattice isomorphic with $\mathscr{L}$.

The direct product of $[a, i]$ and $[o, a]$ contains, however, eight elements, namely the six pairs already mentioned and in addition the pairs (i, b) and (i, o). The given lattice $\mathscr{L}$ is not a direct product but is a sub-direct product of $[a, i]$ and $[o, a]$. Of these intervals the first is of order 2 and the second of order 4. Select from $[o, a]$ an element, say, b not equal to a or o and take

$$\begin{aligned} \alpha &= (b \cup a, b \cap a) = (a, b) \\ \beta &= (b \cup b, b \cap b) = (b, b) \\ \delta &= (b \cup d, b \cap d) = (a, o) \\ \omega &= (b \cup o, b \cap o) = (b, o). \end{aligned}$$

Since $\alpha, \beta, \delta, \omega$ form a lattice isomorphic with a, b, d, o, we see that $[o, a]$ is isomorphic with $[b, a] \times [o, b]$ and so $\mathscr{L}$ is isomorphic with a sub-lattice of $[a, i] \times [b, a] \times [o, b]$. The elements of this sub-lattice are the ordered triplets

$$(i, a, b), \quad (a, a, b), \quad (a, b, b), \quad (i, a, o), \quad (a, a, o), \quad (a, b, o).$$

Each component of the direct product is now a sub-lattice of order 2 and since the position in the triplet determines which of these sub-lattices is involved, we can represent each of them by the two elements 1 and 0. In this case the ordered triplets become

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

The full direct product would contain the additional triplets $(1, 0, 1)$ and $(1, 0, 0)$.

We may call such a set of n-tuples, isomorphic with a finite distributive lattice $\mathscr{L}$, a **representation** of $\mathscr{L}$.

It has been shown that any finite distributive lattice is isomorphic with a sub-direct product of 2-element lattices. A Boolean algebra, however, is actually a direct product of 2-element lattices. To see this it is only necessary to verify that the lattice of ordered pairs X is isomorphic with the direct product $[a, I] \times [O, a]$. We know that it is isomorphic with a sub-lattice of this direct product so it is sufficient to show that for every element (b, c), $b \in [a, I]$, $c \in [O, a]$ of the direct product, an element x of the Boolean algebra exists such that $a \cup x = b$, $a \cap x = c$. We observe however that $b \geqq a \geqq c$. Since a Boolean algebra is complemented, it is also relatively complemented and therefore a has a relative complement, namely $b \cap (a' \cup c)$ in the interval $[c, b]$. Thus, choosing $x = b \cap (a' \cup c)$ we obtain without much difficulty

$$a \cup x = b, \quad a \cap x = c.$$

It follows that each constituent decomposition yields a direct product and consequently the Boolean algebra is a direct product of 2-element lattices. Its representation therefore consists of all possible n-tuples of 0s and 1s. Thus a Boolean algebra of length n has exactly 2^n distinct elements. Another consequence of these arguments is that the Hasse diagram of this Boolean algebra has the form of an n-dimensional cube.

§ 17. Propositional calculus

We now turn our attention to the applications of Boolean algebra to two-valued logic and in particular to the calculus of propositions. Historically, lattice theory had its beginnings in the investigations of Boole into the formalism of logic. By a **proposition** we mean a statement which in some clearly defined sense is either true (T) or false (F). Thus of the two propositions

Grass is green,

Fish grow on trees,

the first is T and the second is F. With the help of the words 'and' ($\wedge$), 'or' ($\vee$), 'not' ($\sim$) compound propositions such as

Grass is not green

Grass is green and fish grow on trees,

can be constructed from simpler ones, and the truth values T or F of compound propositions may be calculated from those of simpler ones of which they are composed by means of the **logical matrices.**

These matrices are to be regarded as statements of the axioms upon which the propositional calculus is based. They are as follows:

$\sim$	
T	F
F	T

$\wedge$	T	F
T	T	F
F	F	F

$\vee$	T	F
T	T	T
F	T	F

Thus ' grass is green and fish grow on trees ' is F because F appears in row T and column F of the matrix for $\wedge$.

It is usual to denote propositions by p, q, ... and propositions compounded from these by

$$p \wedge q, \quad p \vee q, \quad \sim p, \quad p \wedge (\sim q), \quad p \wedge (q \vee r),$$

and so on. By way of clarification it should be stated that $\vee$ denotes the inclusive ' or ' (Latin *vel*) so that $p \vee q$ means 'p or q or both '. The exclusive ' or ' (Latin *aut*) corresponds to the $+$ of Boolean rings. We could write $p+q$, to mean 'p or q but not both '. The reader may think that it is obvious that propositions form a distributive lattice when $p \wedge q$ and $p \vee q$ are interpreted as the intersection and union respectively of the propositions p and q, for the several postulates appear to be satisfied. For instance, the two sides of the distributive law

$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$$

have the same meaning. We wish, however, to elucidate the significance of the phrase ' have the same meaning ' and we now turn to this task.

A proposition which cannot be constructed from other simpler propositions exclusively with the help of $\wedge$, $\vee$, $\sim$ may be called an **elementary proposition.** In general the truth value of a compound proposition can be determined from the logical matrices and from the truth values of the elementary propositions composing it. There are however certain compound propositions whose truth value can be determined without a knowledge of the truth values of the elementary propositions. For instance

Shakespeare wrote Hamlet or Shakespeare did not write Hamlet

is T whether or not Shakespeare wrote Hamlet. In the above compound proposition we can replace the elementary proposition ' Shakespeare wrote Hamlet ' by any other proposition p without altering its truth value. Thus

$$p \vee (\sim p) \text{ is } T \text{ for all } p.$$

Similarly

$$p \wedge (\sim p) \text{ is } F \text{ for all } p.$$

These results can be calculated from the logical matrices alone. Such computations are conveniently set out in the form of **truth tables.** In such a table all possible combinations of truth values for the elementary propositions involved are tabulated to the left of the double line. The columns to the right of the double line are then computed in succession from the logical matrices. The truth tables for $p \vee (\sim p)$ and for $p \wedge (\sim p)$ may be set down together as follows.

p	$\sim p$	$p \vee (\sim p)$	$p \wedge (\sim p)$
T	F	T	F
F	T	T	F

A proposition q, such as $p \vee (\sim p)$, is said to be **formally true** and is called a **tautology** if every proposition q^* obtained from q by replacing its elementary propositions by arbitrary propositions is T. Correspondingly q is said to be **formally false** and is called an **absurdity** or a **contradiction** if every q^* is F. We observe that this notation permits us to write

$$(p \wedge q)^* = p^* \wedge q^*, \quad (p \vee q)^* = p^* \vee q^*, \quad (\sim p)^* = \sim(p^*).$$

We now introduce the symbol $\leftrightarrow$ by defining $p \leftrightarrow q$ to be an abbreviation for the proposition $(p \wedge q) \vee ((\sim p) \wedge (\sim q))$. The following computation

p	q	$p \wedge q$	$\sim p$	$\sim q$	$(\sim p) \wedge (\sim q)$	$p \leftrightarrow q$
T	T	T	F	F	F	T
T	F	F	F	T	F	F
F	T	F	T	F	F	F
F	F	F	T	T	T	T

shows that $\leftrightarrow$ has the logical matrix

$\leftrightarrow$	T	F
T	T	F
F	F	T

We see that $p \leftrightarrow q$ is T if and only if p and q have equal truth values. There is the further possibility that the proposition $p \leftrightarrow q$ is formally true in which case we call p, q **equivalent** propositions and write $p \equiv q$. With this definition of $\equiv$ we can prove that

(i) $p \equiv p$,

(ii) if $p \equiv q$ then $q \equiv p$,

(iii) if $p \equiv q$ and $q \equiv r$ then $p \equiv r$,

(iv) if $p \equiv q$ then $\sim p \equiv \sim q$,

(v) if $p \equiv q$ then $p \wedge r \equiv q \wedge r$,

(vi) if $p \equiv q$ then $p \vee r \equiv q \vee r$,

(vii) $p \wedge q \equiv q \wedge p$,

(viii) $p \vee q \equiv q \vee p$.

In each case an indirect proof can be constructed. We exhibit the details for (iii) and leave the others as exercises for the reader. Suppose $p \not\equiv r$. Then $p^* \leftrightarrow r^*$ is F for some choice of p^* and r^* and so for this choice p^*, r^* have different truth values. If we suppose p^* is T and r^* is F, then $p \equiv q$ states that $p^* \leftrightarrow q^*$ is T for every q^* and consequently each q^* like p^* is T. Further $q \equiv r$ states that $q^* \leftrightarrow r^*$ is T from which we see that r^* like q^* is T in contradiction to the supposition that r^* is F. Since a similar contradiction arises if we suppose that p^* is F and r^* is T the validity of (iii) has been demonstrated.

If $p_1 \equiv p_2$ and $q_1 \equiv q_2$, then from (v) and (vii)

$$p_1 \wedge q_1 \equiv p_2 \wedge q_1 \equiv q_1 \wedge p_2 \equiv q_2 \wedge p_2 \equiv p_2 \wedge q_2.$$

Using (iii) we obtain

(ix) if $p_1 \equiv p_2$ and $q_1 \equiv q_2$ then $p_1 \wedge q_1 \equiv p_2 \wedge q_2$.

Similarly, from (iii), (vi) and (vii),

(x) if $p_1 \equiv p_2$ and $q_1 \equiv q_2$ then $p_1 \vee q_1 \equiv p_2 \vee q_2$.

The results (i), (ii), (iii) show that $\equiv$ is an equivalence relation which we might well have denoted by $=$. Our object however has been to elucidate the meaning of this kind of equality and for this purpose we think the notation $\equiv$ more suggestive. It is in this sense that the postulates for a distributive lattice are satisfied by interpreting $\vee$ and $\wedge$ as union and intersection. For instance the distributive law takes the form

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

and its validity can be demonstrated by showing that each side has the same truth value whatever the truth values of p, q, r may be. This is done in the following truth table

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

In clarification of the meanings of $p \leftrightarrow q$ and $p \equiv q$ we point out that there are different categories of propositions. We can consider elementary propositions as being in the lowest category. The statement $p \leftrightarrow q$ is in a higher category since it is a proposition about propositions namely that p, q have the same truth value. $p \equiv q$ is in a higher category still, since it is a proposition about a proposition about propositions namely that $p \leftrightarrow q$ is formally true.

The equivalence relation mentioned separates all propositions into equivalence classes and we may denote by $\bar{p}$ the class to which the proposition p belongs. That is, the propositions p and q belong to the same class if and only if $p \equiv q$. Expressing this in another way, $\bar{p} = \bar{q}$ if and only if $p \equiv q$. The results (iv), (ix) and (x) show that the operations $\sim$, $\wedge$, $\vee$ are stable in relation to the equivalence relation and that the equivalence relation is indeed a congruence relation which enables us to define unambiguously the following operations on the set of equivalence classes:

$$\begin{aligned} \bar{p} &= \bar{q}' && \text{if and only if} \quad p \equiv \sim q, \\ \bar{p} &= \bar{q} \cap \bar{r} && \text{if and only if} \quad p \equiv q \wedge r, \\ \bar{p} &= \bar{q} \cup \bar{r} && \text{if and only if} \quad p \equiv q \vee r. \end{aligned}$$

If, for example (ix) were not true, then for some p_1, q_1, p_2, q_2 we would have $p_1 \equiv q_1$, $p_2 \equiv q_2$, $p_1 \wedge p_2 \not\equiv q_1 \wedge q_2$ with the consequence that $\bar{p}_1 = \bar{q}_1$, $\bar{p}_2 = \bar{q}_2$, $\overline{p_1 \wedge p_2} \neq \overline{q_1 \wedge q_2}$, and we could not define

$$\bar{p}_1 \cap \bar{p}_2 = \overline{p_1 \wedge p_2}$$

without involving an ambiguity.

We observe that the statement

$$p \vee (\sim p) \leftrightarrow q \vee (\sim q)$$

is always T since each side has the same truth value T for all p, q.

Thus

$$p \vee (\sim p) \equiv q \vee (\sim q)$$

and we may denote the congruence class to which $p \vee (\sim p)$ belongs by I. Thus

$$I = \overline{p \vee (\sim p)} = \bar{p} \cup \overline{(\sim p)} = \bar{p} \cup \bar{p}'.$$

In the same way

$$p \wedge (\sim p) \equiv q \wedge (\sim q),$$

since each side is always F, and we can write

$$O = \overline{p \wedge (\sim p)} = \bar{p} \cap \overline{(\sim p)} = \bar{p} \cap \bar{p}'.$$

In fact I is the class of all tautologies and O is the class of all contradictions.

THEOREM 17.1. *The classes $\bar{p}$, $\bar{q}$, ..., O, I of propositions form a Boolean algebra in relation to the operations $\cap$, $\cup$, $'$, defined above.*

Proof: We need not give a detailed proof for each postulate. We have already seen in (vii) that $p \wedge q \equiv q \wedge p$ so we obtain $\mathbf{L}_{1\cap}$ from

$$\bar{p} \cap \bar{q} = \overline{p \wedge q} = \overline{q \wedge p} = \bar{q} \cap \bar{p}.$$

The other postulates for a distributive lattice are proved in a similar manner. For instance we can show by constructing a truth table that $p \equiv p \wedge (p \vee q)$ from which we get

$$\bar{p} = \overline{p \wedge (p \vee q)} = \bar{p} \cap \overline{(p \vee q)} = \bar{p} \cap (\bar{p} \cup \bar{q})$$

which is $\mathbf{L}_{3\cap}$. Further,

$$\bar{p} \cup I = \bar{p} \cup (\bar{p} \cup \bar{p}') = (\bar{p} \cup \bar{p}) \cup \bar{p}' = \bar{p} \cup \bar{p}' = I.$$

and dually, $\bar{p} \cap O = O$. These formulae imply that I is the all element and that O is the null element. The relations $\bar{p} \cup \bar{p}' = I$, $\bar{p} \cap \bar{p}' = O$ now demonstrate that the lattice is complemented since each class $\bar{p}$ has a complement $\bar{p}'$. Thus the lattice is a Boolean algebra. ◇

We may also introduce the logical symbol for material implication ($\rightarrow$) by defining $p \rightarrow q$ (if p then q) to mean $(\sim p) \vee q$. It should be emphasised that $p \rightarrow q$ does not indicate a relation of premise and conclusion but only that q is not F if p is T. In particular $p \rightarrow q$ is T if p is F which leads to the somewhat unexpected result that every proposition is implied (materially) by any false proposition. For instance

6 is a prime $\rightarrow$ Homer was a Greek.

The proposition $p \rightarrow q$ is an element of the class $\bar{p}' \cup \bar{q}$ of the Boolean algebra and the proposition $(p \rightarrow q) \wedge (q \rightarrow p)$ belongs to the class $(\bar{p}' \cup \bar{q}) \cap (\bar{q}' \cup \bar{p})$ which is identical with $(\bar{p} \cap \bar{q}) \cup (\bar{p}' \cap \bar{q}')$ and is the class containing the proposition $(p \wedge q) \vee ((\sim p) \wedge (\sim q))$ which was defined to be $p \leftrightarrow q$.

A proposition of the form $p \rightarrow q$ may be T or F, but in deducing a true theorem from given axioms we are permitted to employ such a proposition only if it is always T, that is to say, only if $p \rightarrow q$ is a tautology belonging to the class I. This means that $\bar{p}' \cup \bar{q} = I$, or that $\bar{p} \leqq \bar{q}$. In other words, in order that $p \rightarrow q$ be a tautology it is necessary and sufficient that $\bar{q} \in [\bar{p}, I]$. The totality of valid deductions from a proposition or set of axioms p are therefore those propositions belonging to the classes of the interval $[\bar{p}, I]$.

If we now define '$p \Rightarrow q$' to mean 'the statement $p \rightarrow q$ is a tautology' then $p \Rightarrow q$ will mean that statement q is a valid (possibly mathematical) deduction from the statement p. This is the sense in which the symbol $\Rightarrow$ is used in other sections of this book. The statement $p \Rightarrow q$ is read 'p logically implies q', whereas $p \rightarrow q$ is read 'p materially implies q'.

Likewise, if we define '$p \Leftrightarrow q$' to mean 'the statement $p \leftrightarrow q$ is a tautology' then the symbol $\Leftrightarrow$ has the same meaning as it does elsewhere in this book. Indeed $\Leftrightarrow$ and $\equiv$ have exactly the same meaning, but to avoid ambiguity it was thought desirable to use $\equiv$ in place of $\Leftrightarrow$ in the present section.

It is worth mentioning that the formalism of the propositional calculus can all be expressed in the terminology of Boolean rings. Thus the propositions $p \vee q$, $p \wedge q$, $\sim p$, $p \rightarrow q$ belong respectively to the classes $\bar{p}+\bar{q}+\bar{p}\bar{q}$, $\bar{p}\bar{q}$, $I+\bar{p}$, $I+\bar{p}+\bar{p}\bar{q}$, where $\bar{p}+\bar{q}$ denotes the class containing the proposition $(p \wedge (\sim q)) \vee (q \wedge (\sim p))$. For instance, to prove that

$$\{[p \rightarrow (q \vee r)] \wedge (\sim q)\} \Leftrightarrow \{(p \rightarrow r) \wedge (\sim q)\}$$

we observe that the proposition on the left belongs to the class

$$\begin{aligned}
&[I+\bar{p}+\bar{p}(\bar{q}+\bar{r}+\bar{q}\bar{r})](I+\bar{q}) \\
&\qquad = I+\bar{p}+\bar{p}\bar{q}+\bar{p}\bar{r}+\bar{p}\bar{q}\bar{r}+\bar{q}+\bar{p}\bar{q}+\bar{p}\bar{q}+\bar{p}\bar{r}\bar{q}+\bar{p}\bar{q}\bar{r} \\
&\qquad = I+\bar{p}+\bar{p}\bar{q}+\bar{p}\bar{r}+\bar{p}\bar{q}\bar{r}+\bar{q} \\
&\qquad = (I+\bar{p}+\bar{p}\bar{r})(I+\bar{q})
\end{aligned}$$

which is the class containing the proposition on the right.

Again, since the Boolean ring is of characteristic 2, it is easily verified that

$$I+(I+\bar{p}+\bar{p}\bar{q})+(I+\bar{p}+\bar{p}\bar{q})[I+(\bar{r}+\bar{p}+\bar{r}\bar{p})+(\bar{r}+\bar{p}+\bar{r}\bar{p})(\bar{r}+\bar{q}+\bar{r}\bar{q})] = I.$$

It follows that

$$(p \rightarrow q) \rightarrow [(r \vee p) \rightarrow (r \vee q)]$$

is a tautology. We may therefore express this in the form

$$(p \rightarrow q) \Rightarrow [(r \vee p) \rightarrow (r \vee q)].$$

§ 18. The truth ideal

We recall that a non-empty subset $\mathscr{J}$ of a commutative ring $\mathscr{A}$ is called an ideal of $\mathscr{A}$ if and only if $j_1, j_2 \in \mathscr{J} \Rightarrow j_1 + j_2 \in \mathscr{J}$ and $j \in \mathscr{J},\ x \in \mathscr{A} \Rightarrow xj \in \mathscr{J}$. Such an ideal is called a prime ideal if $xy \in \mathscr{J} \Rightarrow$ either $x \in \mathscr{J}$ or $y \in \mathscr{J}$. Analogously an **intersection-ideal** ($\cap$-ideal) $\mathscr{J}$ of a lattice $\mathscr{L}$ is a non-empty subset of $\mathscr{L}$ such that

$\mathbf{J}_1$: $$j_1, j_2 \in \mathscr{J} \Rightarrow j_1 \cap j_2 \in \mathscr{J},$$

$\mathbf{J}_2$: $$j \in \mathscr{J}, x \in \mathscr{L} \Rightarrow x \cup j \in \mathscr{J},$$

and $\mathscr{J}$ is a **prime** $\cap$-ideal if, in addition,

$\mathbf{J}_3$: $$x \cup y \in \mathscr{J} \Rightarrow x \in \mathscr{J} \vee y \in \mathscr{J}.$$

Replacing j in $\mathbf{J}_2$ by $x \cap y$, we obtain

$$x \cap y \in \mathscr{J} \Rightarrow x = x \cup (x \cap y) \in \mathscr{J}.$$

On the other hand, replacing x by $x \cup j$ and y by j in this last result, we obtain

$$j = (x \cup j) \cap j \in \mathscr{J} \Rightarrow x \cup j \in \mathscr{J},$$

which is $\mathbf{J}_2$. Thus, $\mathbf{J}_2$ is equivalent to the postulate

$\mathbf{J}_2'$: $$x \cap y \in \mathscr{J} \Rightarrow x \in \mathscr{J}.$$

The postulates for a prime $\cap$-ideal may therefore be reformulated as follows

$\mathbf{J}_1, \mathbf{J}_2'$: $$x \in \mathscr{J} \ \wedge\ y \in \mathscr{J} \Leftrightarrow x \cap y \in \mathscr{J}$$

$\mathbf{J}_2, \mathbf{J}_3$: $$x \in \mathscr{J} \ \vee\ y \in \mathscr{J} \Leftrightarrow x \cup y \in \mathscr{J}.$$

THEOREM 18.1. *The classes of true propositions form a prime $\cap$-ideal $\mathscr{T}$ of the Boolean algebra of classes of propositions.*

Proof: According to the logical matrices $p \wedge q$ is T if and only if p is T and q is T while $p \vee q$ is T if and only if p is T or q is T. Consequently if $\mathscr{T}$ denotes the set of all classes of true propositions, then

$$\bar{p} \in \mathscr{T} \ \wedge\ \bar{q} \in \mathscr{T} \Leftrightarrow \bar{p} \cap \bar{q} \in \mathscr{T},$$

$$\bar{p} \in \mathscr{T} \ \vee\ \bar{q} \in \mathscr{T} \Leftrightarrow \bar{p} \cup \bar{q} \in \mathscr{T}.$$

In other words, $\mathscr{T}$ is a prime $\cap$-ideal. ◇

Dually the classes of false propositions form a prime $\cup$-ideal $\mathscr{F}$ of the same Boolean algebra. That is,

$$\bar{p} \in \mathscr{F} \ \wedge\ \bar{q} \in \mathscr{F} \Leftrightarrow \bar{p} \cup \bar{q} \in \mathscr{F},$$

$$\bar{p} \in \mathscr{F} \ \vee\ \bar{q} \in \mathscr{F} \Leftrightarrow \bar{p} \cap \bar{q} \in \mathscr{F}.$$

Since every proposition is either true or false, the two ideals $\mathscr{T}$ and $\mathscr{F}$ are complementary not only in the sense that one contains the complements of the other but also in the sense that between them they account for all the classes of the Boolean algebra.

We now construct a homomorphism of the Boolean algebra onto the two element lattice with elements 0 and 1 as follows: define

$$\phi(\bar{p}) = 1 \text{ if } \bar{p} \in \mathscr{T}, \quad \phi(\bar{p}) = 0 \text{ if } \bar{p} \in \mathscr{F}.$$

To see that this is a lattice homomorphism we observe that if $\bar{p}, \bar{q} \in \mathscr{T}$, then $\bar{p} \cup \bar{q}, \bar{p} \cap \bar{q} \in \mathscr{T}$, so that

$$\phi(\bar{p} \cup \bar{q}) = 1 = 1 \cup 1 = \phi(\bar{p}) \cup \phi(\bar{q}),$$
$$\phi(\bar{p} \cap \bar{q}) = 1 = 1 \cap 1 = \phi(\bar{p}) \cap \phi(\bar{q}).$$

If $\bar{p} \in \mathscr{T}$, $\bar{q} \in \mathscr{F}$ then $\bar{p} \cup \bar{q} \in \mathscr{T}$, $\bar{p} \cap \bar{q} \in \mathscr{F}$, whence

$$\phi(\bar{p} \cup \bar{q}) = 1 = 1 \cup 0 = \phi(\bar{p}) \cup \phi(\bar{q}),$$
$$\phi(\bar{p} \cap \bar{q}) = 0 = 1 \cap 0 = \phi(\bar{p}) \cap \phi(\bar{q}).$$

If $\bar{p} \in \mathscr{F}$, $\bar{q} \in \mathscr{T}$, a similar argument applies.

Lastly, if $\bar{p}, \bar{q} \in \mathscr{F}$, then $\bar{p} \cup \bar{q}, \bar{p} \cap \bar{q} \in \mathscr{F}$, yielding

$$\phi(\bar{p} \cup \bar{q}) = 0 = 0 \cup 0 = \phi(\bar{p}) \cup \phi(\bar{q}),$$
$$\phi(\bar{p} \cap \bar{q}) = 0 = 0 \cap 0 = \phi(\bar{p}) \cap \phi(\bar{q}).$$

The above formulae establish the homomorphism.

To demonstrate whether a particular proposition p is T or F it is sufficient to determine whether $\phi(\bar{p})$ is 1 or 0. We observe that if $\phi(\bar{p}) = 1$ then $\phi(\bar{p} \cap \bar{q}) = \phi(\bar{q}) = \phi(I \cap \bar{q})$ and $\phi(\bar{p} \cup \bar{q}) = 1 = \phi(I \cup \bar{q})$. It is therefore permissible in a computation of $\phi(\bar{r})$ to replace any true statement p by I and dually any false statement by O.

The following example (*Math. Gazette*, 36, p. 186) is instructive. Of three counters A, B, C, one is red, one is blue and one is white. Of the three following statements one is T and two are F:

'A is red', 'B is not red', 'C is not blue'.

Determine the colour of each counter.

Adopting the notation A_r = 'A is red' etc., the three statements are A_r, $\sim B_r$, $\sim C_b$. It is unnecessary to distinguish between the statement A_r and the equivalence class to which it belongs so we write A_r for $\bar{A}_r$ and A_r' for $\overline{\sim A_r}$. According to hypothesis, $\phi(H) = 1$, where

$$H = (A_r \cap B_r \cap C_b) \cup (A_r' \cap B_r' \cap C_b) \cup (A_r' \cap B_r \cap C_b'),$$

but the conditions of the problem state that

$$A_r' = A_b \cup A_w, \ B_r' = B_b \cup B_w, \ C_b' = C_r \cup C_w.$$

We can therefore transform H so that it takes the form

$$(A_r \cap B_r \cap C_b) \cup ((A_b \cup A_w) \cap (B_b \cup B_w) \cap C_b) \cup ((A_b \cup A_w) \cap B_r \cap (C_r \cup C_w)).$$

Expressing the right hand side as a union of intersections, we have

$$H = \bigcup (A_x \cap B_y \cap C_z).$$

However, any term in this union with repetitions amongst the x, y, z can be replaced by O since, for example, $\phi(A_r \cap B_r) = 0$, implying that A and B cannot both be red. The only remaining term in H is $A_b \cap B_r \cap C_w$ and $\phi(H) = 1$ implies that $A_b \wedge B_r \wedge C_w$ is T. Thus, A is blue, B is red and C is white.

§ 19. Power sets

One of the most important examples of a Boolean algebra is the illustration (I) of the set $\mathscr{P}(\mathscr{M})$ of all subsets of a given set $\mathscr{M}$. The set $\mathscr{P}(\mathscr{M})$ is called the **power set** of the set $\mathscr{M}$ and is understood to include the void subset $\mathcal{O}$ as well as the whole set $\mathscr{M}$ as subsets. The power set forms a Boolean algebra in relation to set union and set intersection which we now define in terms of the logical symbols $\vee$ and $\wedge$. Let a, b, ... denote elements of $\mathscr{P}(\mathscr{M})$, that is to say, subsets of $\mathscr{M}$, and let x, y, ... be the elements of $\mathscr{M}$. We define unions, intersections and complements in $\mathscr{P}(\mathscr{M})$ as follows:

$$\begin{aligned} x \in a \cap b &\Leftrightarrow x \in a \ \wedge \ x \in b, \\ x \in a \cup b &\Leftrightarrow x \in a \ \vee \ x \in b, \\ x \in a' &\Leftrightarrow \sim (x \in a). \end{aligned}$$

The postulates for a Boolean algebra are easily verified by employing Boolean logic. For instance the validity of $\mathbf{D}_\cup$ for $\mathscr{P}(\mathscr{M})$ can be demonstrated as follows.

$$\begin{aligned} x \in a \cup (b \cap c) &\Leftrightarrow (x \in a) \ \vee \ (x \in b \ \wedge \ x \in c) \\ &\Leftrightarrow (x \in a \ \vee \ x \in b) \ \wedge \ (x \in a \ \vee \ x \in c) \\ &\Leftrightarrow (x \in a \cup b) \ \wedge \ (x \in a \cup c) \\ &\Leftrightarrow x \in (a \cup b) \cap (a \cup c). \end{aligned}$$

Consequently

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c).$$

The six postulates $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{3\cap}$, $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cup}$ can be obtained in a similar manner.

Again

$$x \in a \cap a' \Leftrightarrow x \in a \ \wedge \ \sim(x \in a).$$

If p denotes the proposition $x \in a$ then the statement on the right is $p \wedge \sim p$, which is an absurdity. Thus $x \in a \cap a'$ is F for every $x \in \mathscr{M}$. In other words the subset $a \cap a'$ contains no elements of $\mathscr{M}$. This means that $a \cap a'$ is the void subset. Thus

$$a \cap a' = \emptyset.$$

Further

$$x \in a \cup a' \Leftrightarrow x \in a \ \vee \ \sim(x \in a).$$

Since the statement on the right is a tautology, $x \in a \cup a'$ is T for every x. Hence $a \cup a'$ is the whole set $\mathscr{M}$ and

$$a \cup a' = \mathscr{M}.$$

Set inclusion can now be defined as follows

$$a \supseteq b \Leftrightarrow a \cup b = a.$$

Now $a \cup b = a$ means $x \in a \ \vee \ x \in b \Leftrightarrow x \in a$. In other words, $x \in a \ \vee \ x \in b$ has the same truth value as $x \in a$. But $x \in a \ \vee \ x \in b$ is T if $x \in b$ is T, so $x \in a$ is T if $x \in b$ is T. That is to say, $a \supseteq b$ means every element of b is an element of a. Clearly $\mathscr{M} \supseteq a \supseteq \emptyset$ for every a, from which it is apparent that $\mathscr{M}$ is the all element of $\mathscr{P}(\mathscr{M})$ and $\emptyset$ is its null element. The relations

$$a \cup a' = \mathscr{M}, \quad a \cap a' = \emptyset$$

show that every subset a has a complement a'. Since we have already shown that $\mathscr{P}(\mathscr{M})$ is a distributive lattice, we have proved that it is also a Boolean algebra.

It will now be shown that $\mathscr{P}(\mathscr{M})$ is a complete lattice. Consider a set of elements a_i of $\mathscr{P}(\mathscr{M})$, that is to say, a set of subsets of $\mathscr{M}$, and suppose that x_{ij} denote the elements of $\mathscr{M}$ which belong to the particular subset a_i. Let u denote the subset of $\mathscr{M}$ consisting of all x_{ij}, in which the suffix i ranges over all the subsets of the set and j ranges over all the elements of a_i. Then $x_{ij} \in a_i \Rightarrow x_{ij} \in u$ which means $a_i \subseteq u$. Clearly u is an upper bound of the set of subsets a_i. Let v be any other upper bound. Then $a_i \subseteq v$, which means

$$x_{ij} \in a_i \Rightarrow x_{ij} \in v.$$

Since v contains all x_{ij}, we have $x_{ij} \in u \Rightarrow x_{ij} \in v$, or $u \subseteq v$. This proves that u is the least upper bound. We write $u = \bigcup a_i$.

Again, let n denote the subset of $\mathscr{M}$ consisting of those x_{ij} which belong to every a_i. Then $x \in n \Rightarrow x \in a_i$, or $n \subseteq a_i$. Thus n is a lower bound of the set of subsets a_i. Let m be any other lower bound.

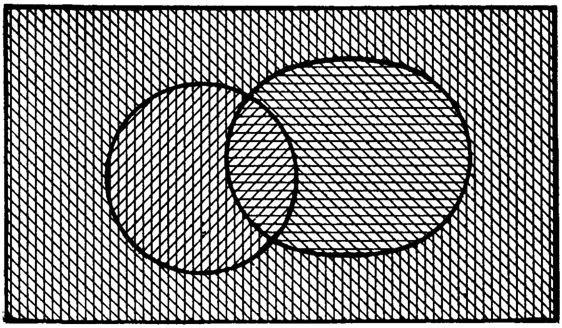


FIG. 13

Then $m \subseteq a_i$, or $x \in m \Rightarrow x \in a_i$. So every element of m belongs to every a_i. That is, $x \in m \Rightarrow x \in n$, or $m \subseteq n$. Consequently n is the greatest lower bound and we write $n = \bigcap a_i$.

Since least upper bounds and greatest lower bounds exist for any set of elements a_i, the lattice $\mathscr{P}(\mathscr{M})$ is complete.

The algebra of sets can be illustrated graphically by **Venn diagrams** of which fig. 13 is an example. We shall describe the shading in fig. 13 geographically, referring to vertical shading as N-S shading, to horizontal shading as E-W shading, and so forth. Let $\mathscr{M}$ be the set of points within the rectangle of fig. 13 and let a be the subset of points shaded SW-NE within or on the circle. Then a' is the subset of points shaded SE-NW outside the circle. If b be the subset of points shaded E-W within or on the oval then b' is the subset of points shaded N-S outside this oval. Further, $a \cup b$ is the subset shaded either SW-NE or

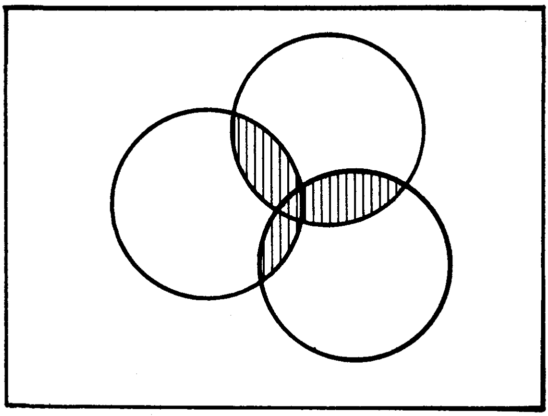


FIG. 14

E-W within either the circle or the oval or on one of the boundaries, while $a \cap b$ is the subset shaded both SW-NE and E-W within or on both curves. Relations such as $(a \cup b)' = a' \cap b'$ can be interpreted geometrically without difficulty for the subset of points not in $a \cup b$ is the same as the subset which is not in a and not in b. It is the subset shaded both N-S and SE-NW. The relation $a \supseteq b$ would mean that the oval lay within the circle. Although the power set $\mathscr{P}(\mathscr{M})$ is a very special power set if $\mathscr{M}$ is the set of points within a given rectangle, such a power set can be used to visualise the algebraic properties of any power set. For instance if a, b, c each denote the subsets within or on one of the three circles of fig. 14, the shaded portion is represented either by $(a \cap b) \cup (b \cap c) \cup (c \cap a)$ or by $(a \cup b) \cap (b \cup c) \cap (c \cup a)$ and the diagram therefore illustrates the distributive law **D**.

It will further be noticed that each minimal polynomial corresponds to an elementary area. For instance the four differently shaded areas of fig. 13 correspond to $a \cap b$, $a' \cap b$, $a \cap b'$, $a \cap b'$. Again $(a \cap b') \cup (a' \cap b)$, or in the notation of Boolean rings $a+b$ is the subset of points which belongs either to a or to b but not to both.

§ 20. Switching circuits

By a switching circuit we mean a piece of electrical apparatus between the terminals of which may be one or more switches of different sorts. These switches may be hand operated, or may be operated by the circuit itself, or by other circuits. Since we are only concerned with whether or not a current flows in the circuit when a potential difference is applied between two of the terminals we do not take into account the magnitude of the current nor the magnitudes of the component resistances. At any instant a given switch a is supposed to be either open ($a = 0$) or closed ($a = 1$). By means of electrical relays it is possible to arrange that a number of other switches are open when a is open and are closed when a is closed. We shall denote each of these by a so that a really denotes a class of switches which are either simultaneously open or simultaneously closed. Again another set of switches a' can be operated by relays so that each switch a' is open when a is closed and is closed when a is open. In the accompanying diagrams the lines indicate conductors while the lettered gaps in these conductors denote switches. The boxes containing letters denote relays which may be used to operate other switches. Fig. 15 denotes a circuit containing a single switch a and a relay. A current flows in this circuit only when $a = 1$ and, when it does so, it operates the relay which may be used to operate other

FIG. 15

switches a and also to operate switches a'. The circuit of fig. 16 has two switches a and b in series and will be denoted by $a \cap b$ (electrical

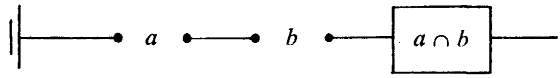


FIG. 16

engineers denote this by ab). Since this circuit is closed if and only if a and b are both closed,

$$\left.\begin{aligned} a \cap b = 1 &\Leftrightarrow a = 1 \wedge b = 1, \\ a \cap b = 0 &\Leftrightarrow a = 0 \vee b = 0. \end{aligned}\right\} \tag{20.1}$$

When the relay of this circuit operates a switch c such that $c = 1$ when $a \cap b = 1$ and $c = 0$ when $a \cap b = 0$, it is natural to write $c = a \cap b$. In effect, this means that not only can a single letter denote a class of switches but a single letter or a single formula can denote a class of equivalent circuits all of which are open simultaneously or all closed simultaneously.

In a similar manner a circuit containing two switches a and b in parallel will be denoted by $a \cup b$ (fig. 17) and it is easy to see that

$$\left.\begin{aligned} a \cup b = 1 &\Leftrightarrow a = 1 \vee b = 1 \\ a \cup b = 0 &\Leftrightarrow a = 0 \wedge b = 0. \end{aligned}\right\} \tag{20.2}$$

(Since many electrical engineers write $a+b$ for $a \cup b$ the reader should beware of confusing this type of addition with addition in a Boolean ring.)

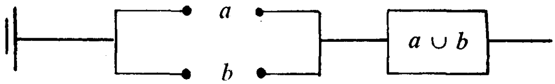


FIG. 17

As our notation suggests, the component circuits, or rather the classes of equivalent circuits, are the elements of a Boolean algebra. The verification of the postulates of a distributive lattice is accomplished in exactly the same manner as was done in the propositional calculus by means of truth tables. For instance, the two circuits of fig. 18

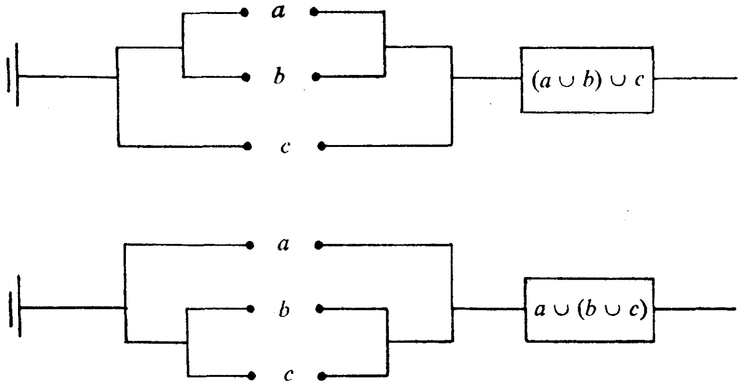


FIG. 18

are either simultaneously open or simultaneously closed, as is demonstrated by the accompanying truth table.

a	b	c	$a \cup b$	$(a \cup b) \cup c$	$b \cup c$	$a \cup (b \cup c)$
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	1	0	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Thus the circuit $(a \cup b) \cup c$ is equivalent to the circuit $a \cup (b \cup c)$ and $\mathbf{L}_{2\cup}$ is valid. We adopted the convention that $a = 1$ denoted that the switch or circuit a was closed, but we may in fact denote a short circuit by 1 (fig. 19). Thus we may interpret $a = 1$ to mean that a is temporarily equivalent to a short circuit. Similarly we interpret $a = 0$ to mean that a is temporarily equivalent to an open circuit (fig. 19), which is labelled 0.

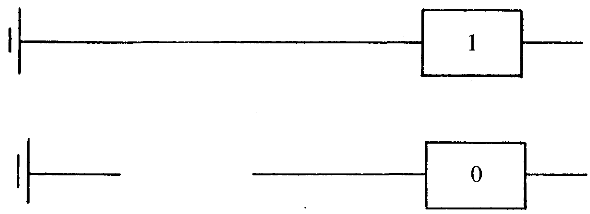


FIG. 19

Since it is easily verified that $a \cup 1 = 1$, $a \cap 0 = 0$, it is clear that 1 is the all element and 0 is the null element of the lattice. An examination of the circuits of fig. 20 reveals that

$$a \cup a' = 1, \quad a \cap a' = 0,$$

from which it is clear that each class a has complement a'. So the lattice is a Boolean algebra.

In the circuits of figs. 16 and 17 the switches a and b might be operated manually since they may be operated independently. The circuit of fig. 20 denoted by $a \cup a' = 1$ reveals a different situation for the operation of a' is determined by that of a and the one cannot be manipulated independently of the other. This relationship is expressed by the formula $a \cup a' = 1$. We now mention some other circuits in which the relationship between the switches is expressed by an equation in the Boolean algebra. Consider a circuit with two switches a, b related by the equation

$$a \cup b = a$$

or by one of the equivalent formulae $a \geqq b$, $a \cap b = b$. Since $1 \geqq a \geqq b$, it follows that $b = 1 \Rightarrow a = 1$. Thus b cannot be closed until a is closed and whenever a is open b must be open. We need not concern ourselves here with the mechanical construction of such a circuit which can be achieved in various ways but it is plain that such a device would have practical value. Indeed the idea can be extended to a **sequential system** of circuits a, b, c, ... such that $a \geqq b \geqq c$... of which the last can be closed only when a, b, c, ... have been closed in alphabetical order.

Another circuit of special interest contains three switches a, b, c satisfying

$$b = a \cap (b \cup c).$$

Since this relation implies $a \geqq b$, this circuit is a modification of the previous one. Assume initially that $a = 1$; then the closing of c ensures that $c = 1$, $b \cup c = 1$, $b = a \cap (b \cup c) = 1$, b closes. However, b must open immediately we open a. This is known as a **lock-in** circuit. We can suppose that a is a break switch which is normally held closed by a spring and that c is a make switch normally held open by a spring. The switch b is operated by a relay. To close b we have only to press c momentarily. Then b stays closed until a is pressed momentarily, but when this is done b opens and stays open until c is pressed again. The circuit is illustrated in fig. 21.

The two principal objects in applying Boolean algebra to switching problems is first to design a circuit with a prescribed function and

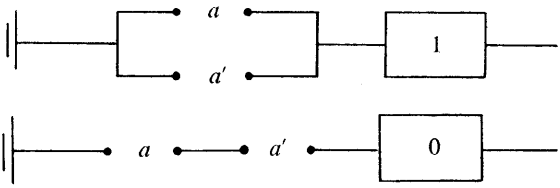


FIG. 20

secondly to simplify a circuit without altering its function. As an illustration of the first type of problem we consider the construction of a binary adder which yields the sum of three digits a, b, c in the binary scale. One of these digits, say c, will be a ' carry in ' from a previous column. Since a, b, c are each 0 or 1 their sum must be one of the four integers 0, 1, 2, 3 which in the binary scale take the forms 00, 01, 10, 11. If we denote this sum in the binary scale by xy, then x is the ' carry out ' digit which is inserted into the next column. The summation to be performed and the required values of x, y are as follows

$$\begin{array}{r} a \\ b \\ \underline{c} \\ xy \end{array}$$

a	b	c	x	y
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Thus employing the formulae 20·1 and 20·2

$$\begin{aligned} y = 1 \Leftrightarrow\ & (a = 0 \wedge b = 0 \wedge c = 1) \vee (a = 0 \wedge b = 1 \wedge c = 0) \\ & \vee (a = 1 \wedge b = 0 \wedge c = 0) \vee (a = 1 \wedge b = 1 \wedge c = 1) \\ \Leftrightarrow\ & (a' = 1 \wedge b' = 1 \wedge c = 1) \vee (a' = 1 \wedge b = 1 \wedge c' = 1) \\ & \vee (a = 1 \wedge b' = 1 \wedge c' = 1) \vee (a = 1 \wedge b = 1 \wedge c = 1) \\ \Leftrightarrow\ & (a' \cap b' \cap c = 1) \vee (a' \cap b \cap c' = 1) \\ & \vee (a \cap b' \cap c' = 1) \vee (a \cap b \cap c = 1) \\ \Leftrightarrow\ & (a' \cap b' \cap c) \cup (a' \cap b \cap c') \cup (a \cap b' \cap c') \cup (a \cap b \cap c) = 1. \end{aligned}$$

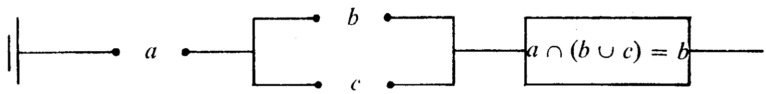


FIG. 21

Consequently,

$$y = (a'\cap b'\cap c)\cup(a'\cap b\cap c')\cup(a\cap b'\cap c')\cup(a\cap b\cap c).$$

Similarly

$$x = (a'\cap b\cap c)\cup(a\cap b'\cap c)\cup(a\cap b\cap c')\cup(a\cap b\cap c),$$

which simplifies to

$$x = (a\cap b)\cup(b\cap c)\cup(c\cap a).$$

The following networks may therefore be used (fig. 22):

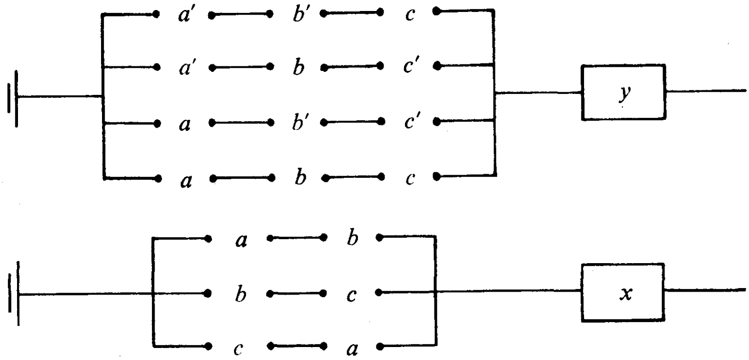


FIG. 22

The problem of simplifying a circuit is largely one of reducing a given Boolean polynomial to an equivalent expression which is simpler in form in the sense that fewer letters are required in writing it down. Thus the first of the two expressions for x above requires 12 letters or switches while the second only requires 6. A further alternative employing only 5 switches would be given by the formula

$$x = [a\cap(b\cup c)]\cup(b\cap c).$$

There are of course also certain technical considerations which must be taken into account in determining which of two circuits should be regarded as the simpler. It is beyond the scope of this book to deal with such questions in greater detail though some aspects of the problem will be considered in the next section.

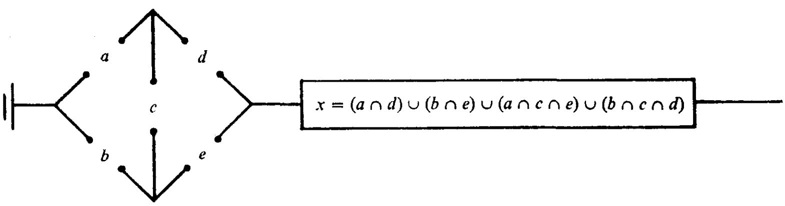


FIG. 23

§ 21. Bridge circuits

The circuits discussed in the previous section have all been of the series-parallel type. If bilateral elements are used which conduct current in both directions it may be possible to simplify a given circuit by using a bridge circuit such as that of fig. 23. In this circuit we suppose that when c is closed current can flow in either direction through this switch. The bridge circuit illustrated employs only five switches though a series-parallel circuit for x would require at least eight corresponding to

$$x = [a \cap (e \cup (c \cap d))] \cup [b \cap (d \cup (c \cap e))]$$

or ten corresponding to the formula for x in the figure. The appropriate formula for such a bridge circuit can be obtained by enumerating the possible paths of the current and by taking the union of the Boolean functions for the different paths. Alternatively a more methodical procedure is described in § 24.

A device for the construction of non-series-parallel circuits is the **disjunctive tree** which employs transfer switches in which the operation of a and a' is effected by a single spring. Consider the case of three variables (three classes of switches) a, b, c and suppose that $f(a, b, c)$ is the Boolean function for a class of circuits. Using the expansion theorem (§ 13) twice, we find that $f(a, b, c)$ can be written

$$[a \cap b \cap f(1, 1, c)] \cup [a \cap b' \cap f(1, 0, c)] \\ \cup [a' \cap b \cap f(0, 1, c)] \cup [a' \cap b' \cap f(0, 0, c)].$$

Now $f(1, 1, c)$, $f(1, 0, c)$, $f(0, 1, c)$, $f(0, 0, c)$ all belong to the four element lattice generated by c which is composed of the elements 0, c, c', 1. The required circuit is therefore realised by marrying the disjunctive tree for a and b (fig. 24*a*) with the network of fig. 24b.

There is, of course, no need to include the open circuit 0 in fig. 24b except for diagrammatic purposes. Whatever the nature of $f(a, b, c)$ at most eight switches or four transfer switches are required. By way of illustration we take

$$f(a, b, c) = (a' \cap b' \cap c) \cup (a' \cap b \cap c') \cup (a \cap b' \cap c') \cup (a \cap b \cap c)$$

which is the formula for the digit y of the binary adder investigated in the previous section. It is easily verified that

$$f(1, 1, c) = c, f(1, 0, c) = c', f(0, 1, c) = c', f(0, 0, c) = c.$$

To obtain the required circuit (fig. 25) it is only necessary to connect the circuits $a \cap b$ and $a' \cap b'$ with c and to connect $a \cap b'$ and $a' \cap b$ with c'. The short circuit 1 in fig. 24b is not required.

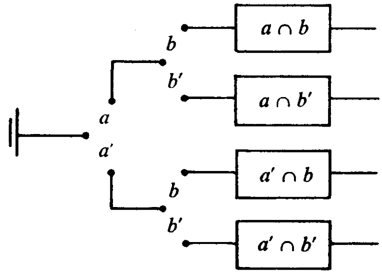


FIG. 24a

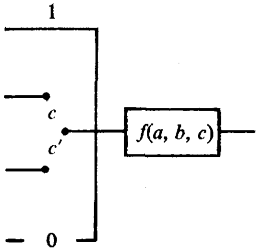


FIG. 24b

The circuit of fig. 25 is clearly more economical than the series-parallel circuit of fig. 22 for the same Boolean function. The method described may be applied to any number of variables but as the number rises the complexities of the computation rapidly increase.

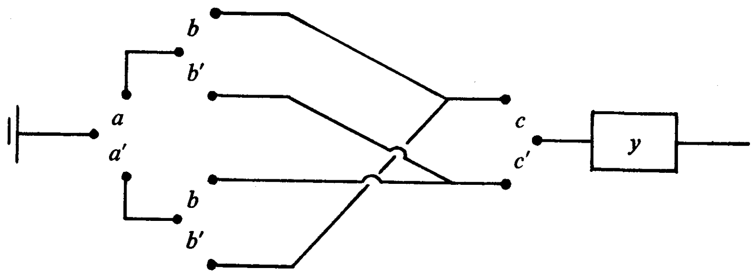


FIG. 25

§ 22. Boolean matrices

In this section we shall consider the set $\mathscr{M}$ of square matrices X of order n whose elements x_{ij} belong to a Boolean algebra $\mathscr{B}$. It will be convenient to denote by 0 and 1 the null and all elements of $\mathscr{B}$. If we define unions and intersections of Boolean matrices according to the formulae

$$X \cup Y = [x_{ij} \cup y_{ij}], \quad X \cap Y = [x_{ij} \cap y_{ij}],$$

it can easily be verified that $\mathscr{M}$ forms a distributive lattice with respect to $\cup$ and $\cap$. This is an immediate consequence of the fact that $\mathscr{B}$ is a distributive lattice. Further, the matrices

$$O = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & 0 \end{bmatrix}, \qquad I = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ . & . & \dots & . \\ 1 & 1 & \dots & 1 \end{bmatrix}$$

are evidently the null and all elements of $\mathscr{M}$. Defining $X \geqq Y$ to mean $X \cup Y = X$ it is patent that

$$X \geqq Y \Leftrightarrow x_{ij} \geqq y_{ij} \text{ for all } i, j.$$

It is also readily established that $[x'_{ij}]$, which we denote by X', is the complement of X. Since $\mathscr{M}$ is complemented it forms a Boolean algebra. [The matrix X' must not be confused with the transpose of X which we shall denote by X^T.]

In this Boolean algebra $\mathscr{M}$ of matrices we can also define matrix multiplication as follows:

$$XY = \left[\bigcup_{k=1}^{n} (x_{ik} \cap y_{kj}) \right].$$

It is evident that the matrix

$$\Phi = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \cdot & \cdot & \dots & \cdot \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

plays the part of a multiplicative unit. As we have seen, $\mathscr{M}$ is a Boolean algebra of matrices in which an additional operation of multiplication is defined, but $\mathscr{M}$ can also be regarded from another point of view. If $\cup$ and $\cap$ in $\mathscr{B}$ be interpreted as addition and multiplication then $X \cup Y$ and XY are the familiar sum and product of two matrices. The matrix ring so obtained has a zero matrix O and a unit matrix Φ. The associative and distributive laws hold, for instance

$$X(Y \cup Z) = (XY) \cup (XZ).$$

In this matrix ring we have an additional operation $X \cap Y$ defined, but multiplication is not in general distributive with respect to this operation.

Consider next the subset $\mathscr{S}$ of $\mathscr{M}$ consisting of all matrices X with the property that $X \geqq \Phi$, that is, such that all diagonal elements are 1. A typical matrix of $\mathscr{S}$ is of the form

$$X = \begin{bmatrix} 1 & x_{12} & \dots & x_{1n} \\ x_{21} & 1 & \dots & x_{2n} \\ \cdot & \cdot & \dots & \cdot \\ x_{n1} & x_{n2} & \dots & 1 \end{bmatrix}.$$

The subset $\mathscr{S}$ is closed with respect to $\cap$ and $\cup$, since

$$x_{ii} = y_{ii} = 1 \Rightarrow x_{ii} \cap y_{ii} = x_{ii} \cup y_{ii} = 1.$$

Indeed $\mathscr{S}$ is a distributive lattice with null element Φ and all element I.

In fact $\mathscr{S}$ is a sub-lattice of $\mathscr{M}$, and furthermore, $\mathscr{S}$ is an $\cap$-ideal of $\mathscr{M}$ since (§ 18),

$$x_{ii} = y_{ii} = 1 \Leftrightarrow x_{ii} \cap y_{ii} = 1.$$

To take another view of the matter, $\mathscr{S}$ is the interval $[\Phi, I]$ of $\mathscr{M}$. Again, $\mathscr{S}$ is itself a Boolean algebra for any element X of $\mathscr{S}$ has a relative complement $X^{\ddagger}$ in $[\Phi, I]$, where

$$X^{\ddagger} = I \cap (X' \cup \Phi) = X' \cup \Phi = \begin{bmatrix} 1 & x'_{12} & \dots & x'_{1n} \\ x'_{21} & 1 & \dots & x'_{2n} \\ \cdot & \cdot & \dots & \cdot \\ x'_{n1} & x'_{n2} & \dots & 1 \end{bmatrix}.$$

We observe also that $\mathscr{S}$ is closed with respect to matrix multiplication for if $x_{ii} = y_{ii} = 1$, then $\bigcup_k (x_{ik} \cap y_{ki}) \geqq x_{ii} \cap y_{ii} = 1$. Consequently $XY \in \mathscr{S}$ if $X, Y \in \mathscr{S}$. The Boolean algebra $\mathscr{S}$ is more important from the point of view of practical applications than is the Boolean algebra $\mathscr{M}$.

LUNTS'S THEOREM 22.1. *If $X \in \mathscr{S}$, then $X \leqq X^2 \leqq \dots \leqq X^{n-1} = X^n$.*

Proof: If $X, Y \in \mathscr{S}$, then by the isotone property $XY \geqq X\Phi$. Consequently $XY \geqq X$. In particular $XX \geqq X$, $X^2X \geqq X^2$, ... Thus

$$X \leqq X^2 \leqq X^3 \leqq \dots \leqq X^{n-1} \leqq X^n.$$

It is therefore sufficient to prove that $X^n \leqq X^{n-1}$. Since $\mathscr{S}$ is closed with respect to multiplication, the diagonal elements of X^n and X^{n-1} are the same, for they are each 1.

Let $(X^r)_{ij}$ denote the ijth element of X^r. Then $(X^n)_{ij}$ is a union of terms such as $x_{ik_1} \cap x_{k_1k_2} \cap \dots \cap x_{k_{n-1}j}$. If $i \neq j$ there must be repetitions amongst the $n+1$ suffixes $i, k_1, \dots, k_{n-1}, j$. A moment's consideration will show that such a term contains (in the typographical sense) and is included in (in the mathematical sense) a shorter term which is equal to a term of $(X^{n-1})_{ij}$. For instance, for $n = 5$, observing that the suffix 3 is repeated in the left member,

$$x_{43} \cap x_{31} \cap x_{15} \cap x_{53} \cap x_{32} \leqq x_{43} \cap x_{32} = x_{43} \cap x_{32} \cap x_{22} \cap x_{22}.$$

Since each term of $(X^n)_{ij}$ is included in a term of $(X^{n-1})_{ij}$ the isotone property shows that $(X^n)_{ij} \leqq (X^{n-1})_{ij}$. Consequently $X^n \leqq X^{n-1}$, which is what we set out to prove. ◇

§ 23. Boolean determinants

We define the determinant of a Boolean matrix X of order n as follows:

$$|X| = \bigcup_{\sigma} (x_{1i_1} \cap \ldots \cap x_{ni_n})$$

in which the union is taken over all possible permutations

$$\sigma = \begin{pmatrix} 1, & 2, & \ldots, & n \\ i_1, & i_2, & \ldots, & i_n \end{pmatrix}.$$

For example,

$$\begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix} = (x_{11} \cap x_{22}) \cup (x_{12} \cap x_{21}).$$

In some ways this definition is more akin to the permanent of elementary algebra than to the determinant, but since there is nothing corresponding to negative signs in Boolean algebra such a distinction is superficial. A Boolean determinant has some properties which remind us of those of ordinary permanents and determinants. For instance, the interchange of two rows or of two columns leaves $|X|$ unaltered. Again, $|X|$ can be expanded by a given row (or column). Thus expansion by the ith row yields

$$|X| = (x_{i1} \cap |X_{i1}|) \cup \ldots \cup (x_{in} \cap |X_{in}|),$$

in which the cofactor $|X_{ij}|$ of x_{ij} is the determinant of the matrix X_{ij} of order $n-1$ obtained by deleting from X the row and column containing x_{ij}. An immediate consequence of the expansion formula is that $|X| \geqq x_{ij} \cap |X_{ij}|$. As in elementary algebra the adjoint or adjugate matrix adj X of X is defined to be the matrix which has $|X_{ji}|$ in the ith row and jth column.

Since $|X|$ is a Boolean polynomial in the elements of X it follows from the isotone property that $X \geqq Y \Rightarrow |X| \geqq |Y|$. Also

$$X \geqq Y \Rightarrow X_{ij} \geqq Y_{ij} \Rightarrow |X_{ij}| \geqq |Y_{ij}| \Rightarrow \operatorname{adj} X \geqq \operatorname{adj} Y.$$

As in elementary algebra, the addition theorem holds. For instance

$$\begin{vmatrix} x_1 \cup y_1, & z_1 \\ x_2 \cup y_2, & z_2 \end{vmatrix} = \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix} \cup \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}.$$

Again, the extraction of a common factor from a row or column is permissible as in the example

$$\begin{vmatrix} x \cap y_1, & z_1 \\ x \cap y_2, & z_2 \end{vmatrix} = x \cap \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}.$$

In the remainder of this section we shall restrict our attention to matrices X belonging to the subset $\mathscr{S}$. That is, we shall suppose that $x_{11} = \ldots = x_{nn} = 1$.

We recall † that any permutation can be expressed as a product of cycles. Suppose, for instance, that

$$\sigma = \begin{pmatrix} 1 \ldots 9 \\ i_1 \ldots i_9 \end{pmatrix} = (h_1 h_2 h_3)(k_1 k_2)(l_1 l_2 l_3 l_4).$$

Then $x_{1i_1} \cap \ldots \cap x_{9i_9}$ takes the form

$$(x_{h_1h_2} \cap x_{h_2h_3} \cap x_{h_3h_1}) \cap (x_{k_1k_2} \cap x_{k_2k_1}) \cap (x_{l_1l_2} \cap x_{l_2l_3} \cap x_{l_3l_4} \cap x_{l_4l_1}).$$

If the term on the left involves x_{ji}, then j, i must appear as consecutive suffixes in one of the cycles. Suppose for convenience that this is the 3-cycle $(h_1 h_2 h_3)$; then the term on the right would take the form

$$(x_{ji} \cap x_{ih} \cap x_{hj}) \cap (x_{k_1k_2} \cap x_{k_2k_1}) \cap (x_{l_1l_2} \cap x_{l_2l_3} \cap x_{l_3l_4} \cap x_{l_4l_1}).$$

Recalling the expansion formula, it is plain that $| X_{ji} |$ is obtained from $| X |$ by replacing x_{ji} by 1 and every other x_{jk} in the jth row by 0. To evaluate $| X_{ji} |$ we write down each term of $| X |$ containing x_{ji}, delete x_{ji} and take the union of the modified terms. In the above illustration the modified term would be

$$(x_{ih} \cap x_{hj}) \cap (x_{k_1k_2} \cap x_{k_2k_1}) \cap (x_{l_1l_2} \cap x_{l_2l_3} \cap x_{l_3l_4} \cap x_{l_4l_1}),$$

which is included in $x_{ih} \cap x_{hj}$, which is a term of $(X^2)_{ij}$. In the general case any modified term would be included in a term $x_{ih_1} \cap x_{h_1h_2} \cap \ldots \cap x_{h_rj}$ for some $r < n$. Thus, since $X \in \mathscr{S}$, any modified term would, by Theorem 22.1, be included in a term of $(X^{n-1})_{ij}$. Accordingly each term of $| X_{ji} |$ is included in a term of $(X^{n-1})_{ij}$. Thus,

$$| X_{ji} | \leqq (X^{n-1})_{ij}.$$

On the other hand, any term of $(X^{n-1})_{ij}$ is of the form

$$x_{ih_1} \cap x_{h_1h_2} \cap \ldots \cap x_{h_{n-2}j}.$$

If there are no repetitions amongst the n suffixes i, h_1, ..., h_{n-2}, j, this is a term of $| X_{ji} |$ corresponding to the permutation

$$\sigma = \begin{pmatrix} i & h_1 & \ldots & h_{n-2} & j \\ h_1 & h_2 & \ldots & j & i \end{pmatrix}.$$

† Ledermann, *Theory of finite groups* p. 66.

If repetitions occur the term of $(X^{n-1})_{ij}$ is included in a shorter term which, by an argument not unlike that used in Lunts's theorem, is equal to a term of $|X_{ji}|$. For instance, for $n = 6$

$$x_{43} \cap x_{31} \cap x_{15} \cap x_{53} \cap x_{32} \leqq x_{43} \cap x_{32} = x_{43} \cap x_{32} \cap x_{11} \cap x_{55} \cap x_{66},$$

the term on the right being a term of $|X_{24}|$ corresponding to the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$. This argument shows that $(X^{n-1})_{ij} \leqq |X_{ji}|$. Consequently $|X_{ji}| = (X^{n-1})_{ij}$ for all i, j. We may formulate this result as follows:

THEOREM 23.1. *If* $X \in \mathscr{S}$, *then* adj $X = X^{n-1}$.

Combining this last result with Lunts's theorem we obtain the following.

COROLLARY. *If* $X \in \mathscr{S}$ *then* X *is idempotent if and only if* $X =$ adj X.

Proof: If $X = X^2$, then $X = X^2 = X^3 = \ldots = X^{n-1} = \text{adj } X$.
If $X = \text{adj } X$, then $X \leqq X^2 \leqq \ldots \leqq X^{n-1} = \text{adj } X = X$.

Consequently $X = X^2$. ◇

Another consequence of this result is that adj X is idempotent if $X \in \mathscr{S}$, for $(\text{adj } X)^2 = X^{2(n-1)} = X^{n-1} = \text{adj } X$, since $X^n = X^{n-1}$.

In the case of a matrix $X \in \mathscr{S}$ a process closely allied to pivotal condensation can be employed to evaluate the elements of adj X. It is necessary to choose an element on the leading diagonal as pivot and we choose in fact $x_{nn} (= 1)$. If we denote by Y the matrix whose ijth element is

$$\begin{vmatrix} x_{ij} & x_{in} \\ x_{nj} & x_{nn} \end{vmatrix} = x_{ij} \cup (x_{in} \cap x_{nj}),$$

then

$$X^2 = \left[\bigcup_k (x_{ik} \cap x_{kj}) \right] \geqq [x_{ij} \cup (x_{in} \cap x_{nj})] = Y.$$

So

$$\text{adj } X = \text{adj } (X^2) \geqq \text{adj } Y.$$

Consequently, if $i, j \neq n$, we obtain, recalling the expansion formula,

$$|X_{ij}| \geqq |Y_{ij}| \geqq y_{nn} \cap |Y_{ij,nn}| = |Y_{ij,nn}|,$$

where $y_{nn} = x_{nn} \cup (x_{nn} \cap x_{nn}) = x_{nn} = 1$ and where $Y_{ij,nn}$ is the submatrix obtained from Y by deleting the ith and nth rows and the jth and nth columns. Employing $n-2$ applications of the addition theorem $|Y_{ij,nn}|$ can be expressed as a union of 2^{n-2} terms $n-1$ of which compose the expansion of $|X_{ij}|$ by its last row. For instance, if $n = 4, i = 1, j = 2$,

$$|Y_{12,44}| = \begin{vmatrix} x_{21}\cup(x_{24}\cap x_{41}), & x_{23}\cup(x_{24}\cap x_{43}) \\ x_{31}\cup(x_{34}\cap x_{41}), & x_{33}\cup(x_{34}\cap x_{43}) \end{vmatrix}$$

$$= \begin{vmatrix} x_{21} & x_{23} \\ x_{31} & x_{33} \end{vmatrix} \cup \left\{x_{41}\cap \begin{vmatrix} x_{24} & x_{23} \\ x_{34} & x_{33} \end{vmatrix}\right\} \cup \left\{x_{43}\cap \begin{vmatrix} x_{21} & x_{24} \\ x_{31} & x_{34} \end{vmatrix}\right\}$$

$$\cup \left\{x_{41}\cap x_{43}\cap \begin{vmatrix} x_{24} & x_{24} \\ x_{34} & x_{34} \end{vmatrix}\right\}$$

$$= \begin{vmatrix} x_{21} & x_{23} & x_{24} \\ x_{31} & x_{33} & x_{34} \\ x_{41} & x_{43} & x_{44} \end{vmatrix} \cup(x_{41}\cap x_{43}\cap x_{24}\cap x_{34})$$

$$= X_{12}\cup(x_{41}\cap x_{43}\cap x_{24}\cap x_{34}).$$

Thus $|Y_{ij,nn}| \geqq |X_{ij}|$ and consequently, if $i, j \neq n$,

$$|X_{ij}| = |Y_{ij,nn}| = |Y_{nn,ij}|.$$

This means that the elements in the first $n-1$ rows and first $n-1$ columns of adj X are identical with those of adj Y_{nn}. A practical application of this result will be described in the next section.

§ 24. Multi-terminal networks

We consider briefly the applications of the two previous sections to a network of switches with m terminals $P_1, P_2, \ldots, P_m$. Denote by z_{ij} the Boolean function for the circuit which could carry current from P_i to P_j without passing through any other terminal. In the case in which the switches are bilateral, carrying current in both directions, we will have $z_{ij} = z_{ji}$, but we may also consider unilateral switches formed by diodes, so that in general this symmetry is not present. We also write $z_{ii} = 1$, indicating that a terminal P_i can always be regarded as connected to itself by a short circuit. The m^2 Boolean functions z_{ij} thus form a Boolean matrix Z belonging to the subset $\mathscr{S}$ of such matrices which have 1 in each position on the leading diagonal. Z is called the **reduced connection matrix** of the network. Correspondingly, let f_{ij} be the Boolean function for the circuit joining P_i to P_j by any route whatever. The matrix F so obtained also belongs to $\mathscr{S}$ and is called the **output matrix** of the network. We consider the problem of finding F when Z is given. Consider the ijth element of Z^2. This is

$$(z_{i1}\cap z_{1j})\cup\ldots\cup(z_{im}\cap z_{mj})$$

and is clearly the Boolean function for all paths from P_i to P_j each passing through at most one other terminal. Similarly, the ijth element of Z^3 is $\bigcup_{k_1,k_2}(z_{ik_1}\cap z_{k_1k_2}\cap z_{k_2j})$ which is the Boolean function for all paths from P_i to P_j each passing through at most two other terminals. In the same way the ijth element of Z^{m-1} gives all possible paths from P_i to P_j, since there are only $m-2$ other terminals. Consequently $F = Z^{m-1}$, and, utilising previous results,

$$F = \operatorname{adj} Z.$$

Now the adjugate of any matrix of $\mathscr{S}$ is idempotent and so

$$F = F^2,$$

which entails

$$F = \operatorname{adj} F.$$

To evaluate F from Z it is unnecessary to evaluate $Z^2, Z^3, \ldots, Z^{m-1}$ in turn. In view of Lunts's theorem that $Z^{m-1} = Z^m$ it is sufficient to evaluate Z^2, Z^4, Z^8, Z^{16}, ... until we find two equal powers of Z: these must each be equal to $Z^{m-1} = F$. Alternatively F is obtained by computing adj Z. This would be a suitable method if only one matrix element $f_{ij} = |Z_{ji}|$ were required.

If the network is comparatively simple there should be no difficulty in determining each z_{ij} but in more complicated bridge circuits uncertainty may arise as to whether all possible routes from P_i to P_j have been taken into account. It is however possible to insert a sufficient number $n-m$ of additional terminals $P_{m+1}, \ldots, P_n$ into the network to ensure that between any two of the terminals $P_1, \ldots, P_n$ the connection is a series-parallel one. The reduced connection matrix X for the augmented system of n terminals can then be systematically evaluated. The augmented output matrix adj $X = X^{n-1}$ will then give the output $|X_{ji}|$ of the circuit from P_i to P_j and must therefore contain F as the sub-matrix composed of the first m rows and columns of adj X. In general the matrix X will be uncomfortably large for the computation of adj X but since only the elements of the sub-matrix F are required the method of pivotal condensation described earlier may be applied.

The artificial terminals $P_n, P_{n-1}, \ldots, P_{m+1}$ can be successively eliminated. Thus eliminating P_n we have $|X_{ij}| = |Y_{nn,ij}|$ provided neither i nor j is equal to n. In fact we can replace adj X by adj Y_{nn} without altering the sub-matrix F. This has reduced by one the order of the matrix whose adjugate is to be computed. Successively eliminating the other artificial terminals in the same manner we eventually replace X, a matrix of order n, by one of order m and the adjugate can then be found in the manner already described. Alternatively f_{ij} can be calculated by eliminating all terminals except P_i and P_j.

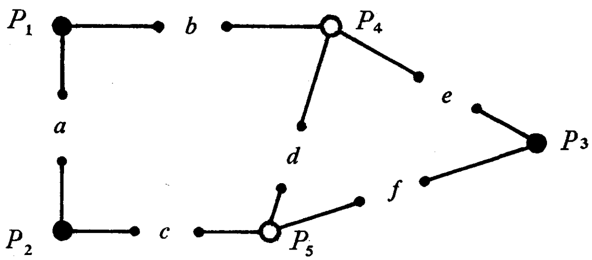


FIG. 26

In illustration consider the network of fig. 26. We suppose P_1, P_2, P_3 are actual terminals and that P_4, P_5 are artificial terminals. Then

$$Z = \begin{bmatrix} 1 & a\cup(b\cap c\cap d) & b\cap(e\cup(f\cap d)) \\ a\cup(b\cap c\cap d) & 1 & c\cap(f\cup(d\cap e)) \\ b\cap(e\cup(f\cap d)) & c\cap(f\cup(d\cap e) & 1 \end{bmatrix}.$$

Now $F = Z^2$; for instance

$$\begin{aligned} f_{12} &= [1\cap(a\cup(b\cap c\cap d))]\cup[(a\cup(b\cap c\cap d))\cap 1]\cup \\ &\qquad \cup[(b\cap(e\cup(f\cap d)))\cap(c\cap(f\cup(d\cap e)))] \\ &= a\cup(b\cap c\cap d)\cup(b\cap e\cap f\cap c). \end{aligned}$$

Alternatively $F = \operatorname{adj} Z$, so

$$f_{12} = |Z_{21}| = \begin{vmatrix} a\cup(b\cap c\cap d), & b\cap(e\cup(f\cap d)) \\ c\cap(f\cup(d\cap e)), & 1 \end{vmatrix},$$

which gives the same formula as before.

As a further alternative we can compute the matrix X for the augmented system. This is

$$X = \begin{bmatrix} 1 & a & 0 & b & 0 \\ a & 1 & 0 & 0 & c \\ 0 & 0 & 1 & e & f \\ b & 0 & e & 1 & d \\ 0 & c & f & d & 1 \end{bmatrix}.$$

Eliminating P_5 by the pivot underlined in X, we get

$$Y_{55} = \begin{bmatrix} 1 & a & 0 & b \\ a & 1 & c\cap f & c\cap d \\ 0 & c\cap f & 1 & e\cup(d\cap f) \\ b & c\cap d & e\cup(d\cap f) & \underline{\underline{1}} \end{bmatrix}.$$

Eliminating P_4 by the pivot underlined in Y_{55} we get

$$\begin{bmatrix} 1 & a\cup(b\cap c\cap d) & b\cap(e\cup(d\cap f)) \\ a\cup(b\cap c\cap d) & 1 & (c\cap f)\cup(c\cap d\cap(e\cup(d\cap f))) \\ b\cap(e\cup(d\cap f)) & (c\cap f)\cup(c\cap d\cap(e\cup(d\cap f))) & \underline{\underline{1}} \end{bmatrix}$$

which is easily seen to be the matrix Z. We can now calculate f_{12} as before, or else remove P_3 by the pivot marked and obtain f_{12} in the first row and second column of the resulting matrix of order two.

§ 25. Brouwer algebras

A lattice $\mathscr{L}$ with an O is called a Brouwer algebra if it is closed with respect to an operation denoted by ' $\rightarrow$ ' which satisfies

B: $$x \leqq y \rightarrow z \Leftrightarrow x \cap y \leqq z$$

for all $x, y, z \in \mathscr{L}$.

The operation $\rightarrow$ unlike $\cup$ and $\cap$ is neither commutative nor associative as we shall presently demonstrate by means of a counter-example.

Since $x \cap O = O$, then any x satisfies $x \leqq O \rightarrow O$. From this it appears that $O \rightarrow O$ is the all element I of $\mathscr{L}$. Again since $I \cap x = x$, it follows that $I \leqq x \rightarrow x$. Thus for any x,

$$x \rightarrow x = I.$$

THEOREM 25.1. *A Brouwer algebra is a distributive lattice.*

Proof: Let $\bigcup(y \cap x_i) = r$. Then $y \cap x_i \leqq r$ and $x_i \leqq y \rightarrow r$. Consequently $\bigcup x_i \leqq y \rightarrow r$ and $(\bigcup x_i) \cap y \leqq r$. Since the reverse inequality $(\bigcup x_i) \cap y \geqq \bigcup(y \cap x_i)$ is given by the one-sided distributive law, we obtain

$$y \cap (\bigcup x_i) = \bigcup(y \cap x_i)$$

which provides the distributive law $\mathbf{D}_\cap$. $\diamond$

The above proof is also valid in the case where the x_i belong to an infinite set provided that the infinite unions exist. We may say then that the infinite analogue of $\mathbf{D}_\cap$ is valid in a Brouwer algebra in the cases where it is meaningful. Although the dual distributive law $\mathbf{D}_\cup$ can be derived from $\mathbf{D}_\cap$, we cannot assume that the infinite analogue of $\mathbf{D}_\cup$ is valid in a Brouwer algebra even when the appropriate infinite intersections exist.

Consider now the set of all elements x_i of a Brouwer algebra such that for given y and z

$$x_i \cap y \leqq z, \quad \text{or} \quad x_i \leqq y \to z.$$

This set may of course be infinite. However, $y \to z$ is clearly one of the set since $y \to z \leqq y \to z$ and is at the same time an upper bound of the set. It follows that $y \to z$ is the l.u.b. of the set. That is to say

$$y \to z = \bigcup x_i.$$

Again, since $z \cap y \leqq z$, we see that $z \cap y$ is a member of the, possibly infinite, set of elements $x_i \cap y$. Also $z \cap y$ is an upper bound of this set since $x_i \cap y = (x_i \cap y) \cap y \leqq z \cap y$. It follows that it is the l.u.b. of the set, or

$$z \cap y = \bigcup (x_i \cap y).$$

We are therefore assured that in a Brouwer algebra $\bigcup x_i$ and $\bigcup (x_i \cap y)$ exist even when these unions are infinite.

THEOREM 25.2. *A lattice $\mathscr{L}$ with an O element is a Brouwer algebra if and only if for every $y, z \in \mathscr{L}$ the set of x_i such that $x_i \cap y \leqq z$ has a greatest element.*

Proof: As we have just seen, if $\mathscr{L}$ is a Brouwer algebra the set of x_i has a greatest element $y \to z$ which is the l.u.b. of the x_i.

If the set of x_i has a greatest element x^*, then x^* is the l.u.b. of the set. That is, $x^* = \bigcup x_i$. Define $y \to z = x^*$. Then if $x_i \cap y \leqq z$, that is to say if x_i is an element of the set, then $x_i \leqq x^* = y \to z$. Conversely, if $x_i \leqq y \to z = x^*$, then $x_i \cap y \leqq x^* \cap y \leqq z$ so that x_i must be an element of the set. Thus $x_i \cap y \leqq z \Leftrightarrow x_i \leqq y \to z$, which shows that $\mathscr{L}$ must be a Brouwer algebra. ◇

The non-distributive lattices of figs. 2 and 3 cannot be Brouwer algebras. Each of these has three elements x_i, namely O, a, b such that $x_i \cap c \leqq b$ but in neither case does the set of x_i contain a greatest element.

Any finite distributive lattice is a Brouwer algebra for let x_i, $i = 1, \ldots, n$ be all the elements which satisfy $x_i \cap y \leqq z$; then

$$(\bigcup x_i) \cap y = \bigcup (x_i \cap y) \leqq z,$$

which shows that $\bigcup x_i$ is one of the set and is therefore the greatest element for the set.

The lattice of six elements illustrated in fig. 27 is a finite distributive lattice and therefore provides a convenient illustration of a Brouwer

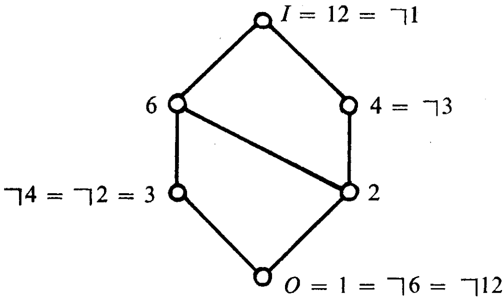


FIG. 27

algebra. It is in fact the lattice of the factors of 12. The reader will easily verify that $x \to y$ is given by the following table,

$\to$	12	6	4	3	2	1
12	12	6	4	3	2	1
6	12	12	4	3	4	1
4	12	6	12	3	6	3
3	12	12	4	12	4	4
2	12	12	12	3	12	3
1	12	12	12	12	12	12

It is at once apparent from this table that the operation $\to$ is non-commutative. Since $6 \to (4 \to 2) = 6 \to 6 = 12$ and $(6 \to 4) \to 2 = 4 \to 2 = 6$, the operation $\to$ is non-associative.

We now establish some relations which are valid in a Brouwer algebra. From $x \to y \leqq x \to y$ we get $(x \to y) \cap x \leqq y$, which yields at once

$$(x \to y) \cap x \leqq y \cap x.$$

In a similar manner $x \cap y \leqq x \cap y$ yields

$$x \leqq y \to (x \cap y).$$

Since $I \cap x \leqq y \Leftrightarrow I \leqq x \to y$, we have

$$x \leqq y \Leftrightarrow x \to y = I. \tag{25.1}$$

If $x \leqq y$, then from a previous result $(z \to x) \cap z \leqq x \cap z \leqq y \cap z \leqq y$. Whence

$$x \leqq y \Rightarrow (z \to x) \leqq (z \to y).$$

An immediate consequence of this is that $z \to (x \cap y) \leqq z \to x$ and similarly $z \to (x \cap y) \leqq z \to y$. Consequently

$$z \to (x \cap y) \leqq (z \to x) \cap (z \to y).$$

Again, $y \to z = \bigcup t_i$, where $t_i \cap y \leqq z$ and $x \to z = \bigcup s_j$, where $s_j \cap x \leqq z$. If $x \leqq y$, then $t_i \cap x \leqq t_i \cap y \leqq z$ and so every t is an s. So, $\bigcup s_j \geqq \bigcup t_i$. That is to say,

$$x \leqq y \Rightarrow (x \to z) \geqq (y \to z). \tag{25.2}$$

THEOREM 25.3. *Every Boolean algebra is a Brouwer algebra.*

Proof: If x, y, z are elements of a Boolean algebra, then

$$x \leqq y' \cup z \Rightarrow x \cap y \leqq (y' \cup z) \cap y = z \cap y \leqq z.$$

Conversely

$$x \cap y \leqq z \Rightarrow x \leqq y' \cup x = y' \cup (x \cap y) \leqq y' \cup z.$$

Thus,

$$x \cap y \leqq z \Leftrightarrow x \leqq y' \cup z.$$

The Boolean algebra therefore becomes a Brouwer algebra by defining $y \to z = y' \cup z$. ◇

On the other hand, not every Brouwer algebra is a Boolean algebra for the Brouwer algebra of fig. 27 is not Boolean.

§ 26. Pseudo-complements

We have seen that a Brouwer algebra is distributive. If it is complemented it is simply a Boolean algebra and every element x has a unique complement x'. We can, however, modify the concept of complement so that it is applicable to any Brouwer algebra whether it is complemented or not. In fact we define the **pseudo-complement** or **Brouwer complement** $\neg x$ of an element x of a Brouwer algebra to be

$$\neg x = x \to O.$$

We shall show that in the case of a Boolean algebra $\neg x = x'$. Since $\neg x$ is the greatest element t such that $t \cap x = O$, it is clear from the relation $x' \cap x = O$ that $\neg x \geqq x'$. On the other hand,

$$x' = x' \cup O = x' \cup (\neg x \cap x) = x' \cup \neg x,$$

which shows that $\neg x \leqq x'$. Consequently $\neg x = x'$.

As a particular case of (25.2) we have $x \to O \geqq y \to O$ if $x \leqq y$. Hence

$$x \leqq y \Rightarrow \neg x \geqq \neg y, \tag{26.1}$$

Since $\neg x = x \to O$, it follows that $\neg x \cap x \leqq O$ for all x, or,

$$\neg x \cap x = O,$$

while $x \cap \neg x = O \Rightarrow x \leqq \neg x \to O = \neg\neg x$. Thus for all x,

$$x \leqq \neg\neg x.$$

Consequently, replacing x by $\neg x$ we get $\neg x \leqq \neg\neg\neg x$. On the other hand, replacing y by $\neg\neg x$ in (26.1), we see that $\neg x \geqq \neg\neg\neg x$. We see then that, for all x,

$$\neg x = \neg\neg\neg x. \tag{26.2}$$

Again

$$\neg O = O \rightarrow O = I,$$

while $\neg I = I \rightarrow O$ shows that

$$\neg I = \neg I \cap I = O.$$

In distinction to the formulae $x = x''$ and $x \cup x' = I$ of Boolean algebras the formulae $x = \neg\neg x$ and $x \cup \neg x = I$ are not in general true in Brouwer algebras. For instance in fig. 27 we see that $\neg\neg 2 = \neg 3 = 4$ and $2 \cup \neg 2 = 6 \neq 12$.

THEOREM 26.1. *A Brouwer algebra is a Boolean algebra if and only if* $x \cup \neg x = I$ *for all* x.

Proof: If the lattice is a Boolean algebra, we have seen that $\neg x = x'$. Then $x \cup \neg x = x \cup x' = I$.

If $x \cup \neg x = I$, then $\neg x$ is a complement of x for we already know that $x \cap \neg x = O$. The lattice is therefore a complemented distributive lattice and consequently is a Boolean algebra. ◇

THEOREM 26.2. *A Brouwer algebra is a Boolean algebra if and only if* $x = \neg\neg x$ *for all* x.

Proof: If the lattice is Boolean, then $x' = \neg x$ and

$$x = x'' = \neg x' = \neg\neg x.$$

If $x = \neg\neg x$ for all x, let $y = \neg(x \cup \neg x) = (x \cup \neg x) \rightarrow O$, or $y \cap (x \cup \neg x) = (y \cap x) \cup (y \cap \neg x) = O$. Thus $y \cap x = O$ and $y \cap \neg x = O$, from which we get $y \leqq x \rightarrow O = \neg x$ and $y \leqq \neg x \rightarrow O = \neg\neg x$. Hence $y \leqq \neg x \cap \neg\neg x = O$, since $z \cap \neg z = O$ for all z and in particular for $z = \neg x$. Since we have proved that $y = \neg(x \cup \neg x) = O$, we conclude that $I = \neg O = \neg\neg(x \cup \neg x) = x \cup \neg x$. The previous theorem now shows that the lattice is a Boolean algebra. ◇

§ 27. Intuitionist logic

Boolean logic as formulated in the calculus of propositions, although mathematically sound, has some features which from the philosophical point of view may be considered unsatisfactory. Amongst these are the two tautologies

$$O \Rightarrow p,$$

$$(p \Rightarrow q) \vee (q \Rightarrow p).$$

The intuitionist logic constructed by L. E. J. Brouwer as an alternative to Boolean logic eliminates the second though not the first of these tautologies. In this logic it is assumed that propositions compose a Brouwer algebra in which $\cap$ or $\wedge$ is interpreted as 'and', $\cup$ or $\vee$ as 'or', $\neg$ as 'not (in the intuitionist sense)', $\rightarrow$ as 'implies (in the intuitionist sense)', I as a tautology, and O as an absurdity. Since $I \cap O = O \leqq p$ for any p, it follows that $I = O \rightarrow p$. Thus the statement $O \rightarrow p$, meaning that any proposition p is implied by an absurdity, is still a tautology in intuitionist logic.

An examination of the Brouwer algebra of fig. 5 reveals that in this particular case $p \rightarrow q = q$ and $q \rightarrow p = p$. Thus

$$(p \rightarrow q) \vee (q \rightarrow p) = q \vee p = r \neq I.$$

It follows that

$$(p \rightarrow q) \vee (q \rightarrow p)$$

cannot be a tautology in intuitionist logic.

It has already been shown (25.1) that $p \rightarrow q = I \Leftrightarrow p \leqq q$. Hence $p \rightarrow q$ is a tautology if and only if $p \leqq q$. It follows that, just as in Boolean logic the totality of propositions deducible from a given proposition p constitutes the interval $[p, I]$. In particular, since $p \leqq \neg\neg p$, it is a tautology that

$$p \rightarrow \neg\neg p,$$

but it is not a tautology that

$$\neg\neg p \rightarrow p.$$

For instance, in the lattice of fig. 27,

$$\neg\neg 2 \rightarrow 2 = \neg 3 \rightarrow 2 = 4 \rightarrow 2 = 6 \neq I.$$

This has important consequences in mathematical reasoning for it prohibits the use of *reductio ad absurdum* arguments. We cannot for instance argue that an object is red because it has been proved to be not (not red). The object may, of course, be red but it has not been proved to be so if we accept intuitionist logic as the basis of our argument.

Again, as has already been shown by a counter-example,

$$p \vee \neg p$$

is not a tautology. We cannot argue that an object is either red or not red. The rule of *tertium non datur* is thus eliminated from intuitionist logic, although we can use as a substitute the tautology

$$\neg\neg(p \vee \neg p)$$

which was established in the proof of Theorem 26.2.

We have emphasised the respects in which Brouwer's logic differs from that of Boole but, needless to say, in many respects they are in agreement. For instance

$$\neg(p \wedge \neg p)$$

is a tautology which embodies the law of contradiction. Intuitionists therefore accept the principle that any proposition which implies its own contradiction is absurd.

§ 28. De Morgan's laws in Brouwer algebras

We now examine the counterparts of De Morgan's laws in Brouwer algebras. Since $x \leqq x \cup y$, we have $\neg x \geqq \neg(x \cup y)$ and similarly $\neg y \geqq \neg(x \cup y)$. Consequently $(\neg x) \cap (\neg y) \geqq \neg(x \cup y)$. On the other hand

$$\begin{aligned}(\neg x) \cap (\neg y) \cap (x \cup y) &= [(\neg x) \cap (\neg y) \cap x] \cup [(\neg x) \cap (\neg y) \cap y] \\ &= O \cup O = O.\end{aligned}$$

Hence $(\neg x) \cap (\neg y) \leqq (x \cup y) \rightarrow O = \neg(x \cup y)$. Thus, corresponding to $(x \cup y)' = x' \cap y'$, we have

$$\neg(x \cup y) = (\neg x) \cap (\neg y). \tag{28.1}$$

Similarly, since $x \geqq x \cap y$, we have $\neg(x \cap y) \geqq \neg x$ and $\neg(x \cap y) \geqq \neg y$, from which it follows that

$$\neg(x \cap y) \geqq (\neg x) \cup (\neg y). \tag{28.2}$$

However, in the lattice of fig. 5 we can show that

$$\neg p = q, \quad \neg q = p, \quad q \cup p = r, \quad q \cap p = O, \quad \neg O = I,$$

so that in this case $\neg(p \cap q) > (\neg p) \cup (\neg q)$. It is clear then that we cannot in general replace $\geqq$ by $=$ in (28.2).

Let us write

$$z = \neg(x \cap y) \cap \neg\neg x \cap \neg\neg y.$$

Then, clearly

$$z \cap (x \cap y) = O,$$

which yields

$$z \cap x \leqq y \rightarrow O = \neg y,$$

while from the definition of z, $z \leqq \neg\neg y$ and so $z \cap x \leqq \neg\neg y$. Thus $z \cap x \leqq \neg y \cap \neg\neg y = O$, or $z \leqq x \rightarrow O = \neg x$. Again, from the definition of z, we have $z \leqq \neg\neg x$. Consequently,

$$z \leqq \neg x \cap \neg\neg x = O.$$

We have therefore shown that

$$\neg(x \cap y) \cap \neg\neg x \cap \neg\neg y = O,$$

or

$$\neg(x \cap y) \leqq (\neg\neg x \cap \neg\neg y) \rightarrow O = \neg(\neg\neg x \cap \neg\neg y).$$

On the other hand, using (26.2), (28.1) and (28.2), we can see that

$$\neg(x \cap y) = \neg\neg\neg(x \cap y) \geqq \neg\neg(\neg x \cup \neg y) = \neg(\neg\neg x \cap \neg\neg y).$$

Consequently, by $\mathbf{P}_2$ and (28.1),

$$\neg(x \cap y) = \neg(\neg\neg x \cap \neg\neg y) = \neg\neg(\neg x \cup \neg y).$$

If we now introduce a new operation ' $\Cup$ ' by defining

$$x \Cup y = \neg\neg(x \cup y),$$

it will be seen that

$$\neg(x \Cup y) = \neg\neg\neg(x \cup y) = \neg(x \cup y) = \neg x \cap \neg y,$$

$$\neg(x \cap y) = \neg\neg(\neg x \cup \neg y) = \neg x \Cup \neg y.$$

The formulae

$$\neg(x \Cup y) = \neg x \cap \neg y, \quad \neg(x \cap y) = \neg x \Cup \neg y$$

are easily remembered since they exhibit the same symmetry as de Morgan's laws. From these we easily deduce that

$$\neg\neg(x \Cup y) = \neg(\neg x \cap \neg y) = \neg\neg x \Cup \neg\neg y,$$

$$\neg\neg(x \cap y) = \neg(\neg x \Cup \neg y) = \neg\neg x \cap \neg\neg y.$$

Consider the subset $\mathscr{B}$ of elements belonging to a Brouwer algebra $\mathscr{L}$ which satisfy

$$x = \neg\neg x.$$

Then $\mathscr{B}$ is closed with respect to the operations $\Cup$ and $\cap$, for if $x = \neg\neg x$ and $y = \neg\neg y$, then

$$x \Cup y = \neg\neg x \Cup \neg\neg y = \neg\neg(x \Cup y),$$

$$x \cap y = \neg\neg x \cap \neg\neg y = \neg\neg(x \cap y).$$

Indeed we can show that $\mathscr{B}$ is a distributive lattice with respect to the operations $\Cup$ and $\cap$. It is clear that $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{1\Cup}$ are valid. Also

$$(x \Cup y) \Cup z = \neg\neg((x \Cup y) \Cup z) = \neg(\neg(x \Cup y) \cap \neg z) = \neg(\neg x \cap \neg y \cap \neg z).$$

The symmetry of the expression on the extreme right along with the commutative laws shows that

$$(x \uplus y) \uplus z = x \uplus (y \uplus z)$$

which is $\mathbf{L}_{2\uplus}$. The reader may verify in a similar manner that the postulates $\mathbf{L}_{3\cap}$, $\mathbf{L}_{3\uplus}$ and $\mathbf{D}_{\uplus}$ are also satisfied.

Moreover,

$$x \uplus \neg x = \neg\neg(x \cup \neg x) = \neg(\neg x \cap \neg\neg x) = \neg O = I,$$

while

$$x \cap \neg x = O.$$

It follows that $\mathscr{B}$ is complemented since $\neg x \in \mathscr{B}$ on account of the identity $\neg x = \neg\neg\neg x$. We therefore have the following result.

THEOREM 28.1. *The subset $\mathscr{B}$ of elements x of a Brouwer algebra $\mathscr{L}$ which satisfy $x = \neg\neg x$ form a Boolean algebra with respect to the operations $\uplus$ and $\cap$.*

We see immediately that the mapping defined by $\phi(x) = \neg\neg x$ is a lattice homomorphism of the Brouwer algebra $\mathscr{L}$ onto the Boolean algebra $\mathscr{B}$ since

$$\phi(x \uplus y) = \neg\neg(x \uplus y) = \neg\neg x \uplus \neg\neg y = \phi(x) \uplus \phi(y),$$
$$\phi(x \cap y) = \neg\neg(x \cap y) = \neg\neg x \cap \neg\neg y = \phi(x) \cap \phi(y),$$
$$\phi(\neg x) = \neg\neg\neg x = \neg\phi(x).$$

§ 29. Atomic lattices

We previously defined an atom as an element which covers O. An **atomic** lattice is one in which each element other than O includes at least one atom. Evidently, every finite lattice is atomic but infinite lattices with an O exist which are not atomic. One of these is described at the end of this section. Any power set $\mathscr{P}(\mathscr{M})$ is an atomic lattice since the one element subsets of $\mathscr{M}$ are clearly atoms of $\mathscr{P}(\mathscr{M})$ and every subset of $\mathscr{M}$ excepting the void subset, includes at least one atom. For clarity we shall denote atoms by $p, q, \ldots$ and arbitrary elements of the lattice by $x, y, z, \ldots$. In the following discussion we consider atomic lattices which have the additional property that each element has a unique complement.

We shall show that in such a lattice, $x > y$ implies that there exists an atom p such that $p \leqq x$, $p \cap y = O$. The isotone property shows that if $x > y$, then $y' \cup x \geqq y' \cup y = I$. Then $y' \cap x \neq O$, for otherwise

$x = y$ by the uniqueness of the complements. So there exists an atom p such that $p \leqq y' \cap x$. That is, $p \leqq x$ and $p \leqq y'$. Thus

$$p \cap y \leqq y' \cap y = O$$

and consequently $p \nleqq y$.

Suppose next that x and z contain exactly the same atoms. That is to say

$$p \leqq x \Leftrightarrow p \leqq z,$$

then x and $x \cap z$ contains exactly the same atoms. But if $x \neq z$, then either $x \cap z < x$ or $x \cap z < z$. However, if $x \cap z < x$ we have just seen that x contains an atom p not contained in $x \cap z$. The contradiction shows that the supposition $x \neq z$ is false. Since the argument in the other case is similar, we see that if x and z contain the same atoms then $x = z$. We express this result as follows.

THEOREM 29.1. *In an atomic lattice in which each element has a unique complement, two elements are equal if and only if they contain the same atoms.*

We next show that the complement p' of an atom p is an anti-atom, that is to say an element covered by I. It is clear that $p' \neq I$ for otherwise $p = I \cap p = p' \cap p = O$. Suppose that $p' < x \leqq I$. Then $p \cup x \geqq p \cup p' = I$. Since $p \cap x \leqq p$ we must have either $p \cap x = p$ or $p \cap x = O$. The latter alternative is impossible since the uniqueness of complements would yield the contradiction $x = p'$. Thus $p \cap x = p$ and $p \cup x = x$. Comparing the two values obtained for $p \cup x$ we see that $x = I$, showing that no x satisfies $p' < x < I$. Consequently p' is an anti-atom.

Let p, q be two atoms. Then $q \cup p'$ must be p' or I and $q \cap p'$ must be q or O from the property of atoms and anti-atoms. However the three statements $q \leqq p'$, $q \cup p' = p'$, $q \cap p' = q$ are equivalent, so either $q \leqq p'$, or $q \cup p' = I$ and $q \cap p' = O$. In the latter case we have $q = p$ from the uniqueness of complements. We can reword this as follows: if $q \neq p$ then $q \leqq p'$.

Suppose $p \cap x = O$. Then x does not include the atom p; it must however include an atom q. Since $q \neq p$, we have $q \leqq p'$. Consequently $q \leqq x \cap p'$. Since $q \leqq x \cap p'$ implies $q \leqq x$, we see that when $p \cap x = O$ then x and $x \cap p'$ contain the same atoms. As we have just seen, this means that $x = x \cap p'$ that is to say $p' \geqq x$.

If $p \cap x = p \cap y = O$, then $p' \geqq x$ and $p' \geqq y$. Consequently $p' \geqq x \cup y$. Now this is incompatible with $p \leqq x \cup y$, for otherwise $p \leqq p'$ and

$p = p \cap p' = O$. Since $p \geqq p \cap x$ we must have either $p \cap x = p$ or $p \cap x = O$ and similarly either $p \cap y = p$ or $p \cap y = O$. If we are given that $p \leqq x \cup y$, then we must exclude the possibility that $p \cap x = p \cap y = O$. It follows that $p \leqq x \cup y$ implies that either $p \cap x = p$ or $p \cap y = p$, that is to say either $p \leqq x$ or $p \leqq y$. Since $p \leqq x$ or $p \leqq y$ implies $p \leqq x \cup y$, we have the result

$$p \leqq x \cup y \Leftrightarrow p \leqq x \ \vee \ p \leqq y. \tag{29.1}$$

The relation

$$p \leqq x \cap y \Leftrightarrow p \leqq x \ \wedge \ p \leqq y$$

follows from the definition of $x \cap y$ as the g.l.b. of x and y.

Consider now the power set $\mathscr{P}(\mathscr{M})$ of the set $\mathscr{M}$ of all atoms belonging to an atomic lattice $\mathscr{L}$ with unique complements. Let $[x]$ denote the subset of $\mathscr{M}$ consisting of all atoms p such that $p \leqq x$. Then the above formulae take the form

$$[x \cup y] = [x] \cup [y],$$

$$[x \cap y] = [x] \cap [y],$$

in which $\cup$ and $\cap$ denote set unions and set intersections. In other words the subsets $[x]$, $[y]$, ... are closed with respect to $\cup$ and $\cap$, and the set of all such subsets form a sublattice of $\mathscr{P}(\mathscr{M})$. Moreover

$$\phi(x) = [x]$$

defines an isomorphism ϕ between the elements x of $\mathscr{M}$ and the subsets $[x]$ which are the elements of the sublattice. That ϕ is a homomorphism has just been demonstrated. That it is also an isomorphism follows from the fact that if x and z contain the same atoms, then $x = z$; that is to say

$$[x] = [z] \Leftrightarrow x = z.$$

Since the power set $\mathscr{P}(\mathscr{M})$ is a distributive lattice, so is any sublattice of $\mathscr{P}(\mathscr{M})$. The isomorphism which we have established, therefore shows that any atomic lattice $\mathscr{L}$, in which each element has a unique complement, is necessarily distributive and is therefore a Boolean algebra. If, in addition, $\mathscr{L}$ is complete we can show that $\mathscr{L}$ is isomorphic to the whole power set $\mathscr{P}(\mathscr{M})$.

To see this, consider any element of $\mathscr{P}(\mathscr{M})$, say the subset $\mathscr{N}$ of $\mathscr{M}$ consisting of the atoms p_i. Since $\mathscr{L}$ is complete, $\bigcup p_i$ exists as an element of $\mathscr{L}$. If $q \leqq \bigcup p_i$, then either q is one of the p_i or, as we showed a moment ago, $p_i \leqq q'$ for each p_i. The second alternative is impossible since it would give

$$q \leqq \bigcup p_i \leqq q'.$$

We see then that $\mathscr{N} = [\bigcup p_i]$ since $[\bigcup p_i]$ contains no atoms other than the atoms p_i. Thus not only does every x determine an element of $\mathscr{P}(\mathscr{M})$ but every element of $\mathscr{P}(\mathscr{M})$ determines an element of $\mathscr{L}$. We may sum up the foregoing as follows.

THEOREM 29.2. *Any atomic lattice in which every element has a unique complement is a Boolean algebra and is isomorphic to a sublattice of the power set of the set of atoms. If the atomic lattice is complete it is isomorphic to the power set itself.*

Since a power set is complete and atomic and, being a Boolean algebra, also has unique complements, we see that the only complete atomic lattices with unique complements, that is, the only complete atomic Boolean algebras are, apart from isomorphism, the power sets, and vice versa.

It must be mentioned that Boolean algebras exist which are not atomic lattices. We describe one in outline only. Let $\mathscr{M}$ be an infinite set and define $a \equiv b$ to mean that two of its subsets a and b differ only in a finite number of elements. It can be shown that $a \equiv b$ is a congruence relation which separates $\mathscr{P}(\mathscr{M})$ into equivalence classes $\bar{a}$, $\bar{b}$. Thus

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b.$$

These classes form a Boolean algebra $\mathscr{B}$ in which $\bar{a} \cup \bar{b} = \overline{a \cup b}$, $\bar{a} \cap \bar{b} = \overline{a \cap b}$. Any finite subset of $\mathscr{M}$ belongs to the class $\bar{O}$, so if $\mathscr{B}$ has an atom $\bar{p}$ then p must be an infinite subset of $\mathscr{M}$. We can however separate p into two disjoint infinite subsets say q and r. Since q is an infinite subset, $q \not\equiv O$ and consequently $\bar{O} < \bar{q}$. From $q \cup r = p$, we deduce that $\bar{q} \leqq \bar{p}$, but this relation can be strengthened to yield $\bar{q} < \bar{p}$ since we know that $q \not\equiv p$. Hence $\bar{O} < \bar{q} < \bar{p}$, which demonstrates that $\bar{p}$ cannot be an atom after all. Indeed $\mathscr{B}$, though Boolean, has no atoms.

We remark here that a lattice $\mathscr{L}$ which is not atomic must have an infinite descending chain. If $\mathscr{L}$ has no O, this has been proved already (§ 5). Suppose $\mathscr{L}$ has an O and that x_0 includes no atom. Since x_0 is not itself an atom, there exists x_1 such that $x_0 > x_1 > O$. Then x_1 cannot include an atom for otherwise x_0 would include the same atom. Repeating the argument on x_1, x_2, ... we obtain the infinite chain $x_0 > x_1 > x_2 > \dots$.

Similarly, if the dual of $\mathscr{L}$ is not atomic then $\mathscr{L}$ must have an infinite ascending chain.

We conclude from these arguments that if $\mathscr{L}$ has no infinite chains then both $\mathscr{L}$ and its dual are atomic.

§ 30. Semi-modular lattices

A lattice is called **semi-modular** † if it has no infinite chains and if, for all x, y:

S: $\quad x$ and y cover $x \cap y \Rightarrow x \cup y$ covers x and y.

Suppose that x covers $x \cap z$ and construct a maximal chain (fig. 28)

$$x \cap z = t_0 < t_1 < \ldots < t_n = z$$

for $[x \cap z, z]$ such that t_{i+1} covers t_i. Evidently

$$(x \cup t_i) \cup t_{i+1} = x \cup t_{i+1}.$$

Now, applying **S** repeatedly, x and t_1 cover $x \cap z$, so $x \cup t_1$ as well as t_2 covers t_1, so $x \cup t_2$ and t_3 cover t_2, ..., so $x \cup z$ $(= x \cup t_n)$ covers z $(= t_n)$. It follows then that

S*: $\quad x$ covers $x \cap z \Rightarrow x \cup z$ covers z

is a consequence of **S**. Since, however, **S*** clearly implies **S**, it is evident that **S** and **S*** are equivalent postulates.

It is to be observed that a similar argument to the above also shows that $x \cup t_{i+1}$ covers $x \cup t_i$, and indeed that

$$x = x \cup t_0 < x \cup t_1 < \ldots < x \cup t_n = x \cup z$$

is a maximal chain for $[x, x \cup z]$ which has the same length as the above chain for $[x \cap z, z]$.

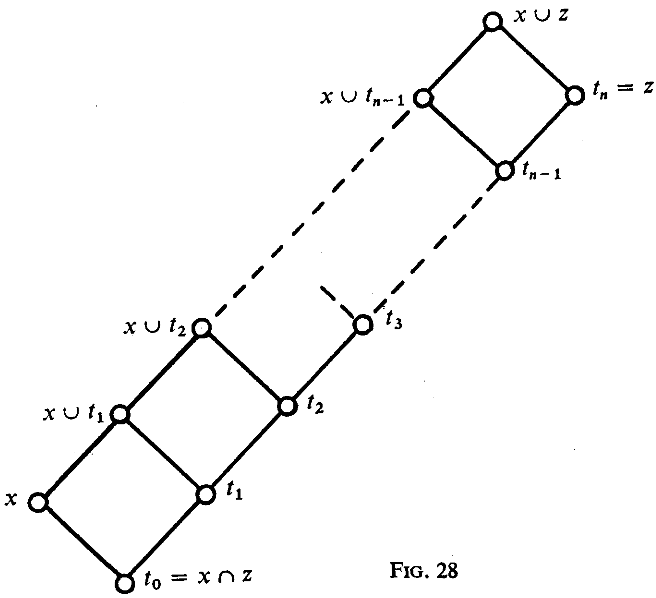


FIG. 28

† The term semi-modular is sometimes used in a more general sense than that employed here. See G. Szász, *Einführung in die Verbandstheorie* § 45.

THEOREM 30.1. *In a semi-modular lattice all maximal chains for a given interval* $[y, x]$ *are of the same length.*

Proof: If x covers y, the theorem is obviously true since the only maximal chain is of length 1. We use an inductive argument and assume that the theorem is true for any interval possessing a maximal chain of length $n-1$. Suppose then that

$$y<t_1<\ldots<t_{n-1}<x,$$
$$y<s_1<\ldots<s_{m-1}<x$$

are two maximal chains for $[y, x]$. First suppose that $s_1 \leqq t_{n-1}$. Then by the induction hypothesis, the maximal chains

$$y<t_1<\ldots<t_{n-1},$$
$$y<s_1<\ldots<t_{n-1},$$
$$s_1<\ldots<t_{n-1}<x,$$
$$s_1<\ldots<s_{m-1}<x$$

are all of the same length $n-1$. Hence $m = n$. Secondly, if $s_1 \nleqq t_{n-1}$ then s_1 covers $s_1 \cap t_{n-1}$ since $s_1 \cap t_{n-1} = y$. In this case the semi-modular law **S** shows that

$$s_1<s_1 \cup t_1<\ldots<s_1 \cup t_{n-1} = x$$

is a maximal chain for $[s_1, x]$ of length $n-1$ (replace x by s_1 and n by $n-1$ in fig. 28). By the induction hypothesis,

$$s_1<s_2<\ldots<s_{m-1} = x$$

is also of length $n-1$ and so in this case also $m = n$. ◇

The theorem just proved shows that in a semi-modular lattice, just as in a modular lattice, the length of an interval may be defined unambiguously and, correspondingly, the length $l(x)$ of an element is defined as the length of $[O, x]$. However, the semi-modular lattice of fig. 29 cannot be modular since its sub-lattice consisting of the elements I, a, c, q, O is isomorphic to the lattice of fig. 2. On the other hand a modular lattice of finite length is necessarily semi-modular for the isomorphism of the intervals $[x, x \cup y]$ and $[x \cap y, y]$ entails that $x \cup y$ covers x if y covers $x \cap y$, which is postulate **S***.

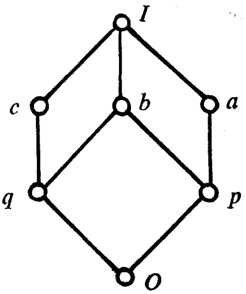


FIG. 29

In a semi-modular lattice the dimension theorem is weakened to take the following form.

THEOREM 30.2. *In a semi-modular lattice*

$$l(x)+l(y) \geqq l(x \cup y)+l(x \cap y).$$

Proof: It is sufficient to prove the equivalent formula

$$\text{length } [x, x \cup y] \leqq \text{length } [x \cap y, y].$$

Let $x \cap y = t_0 < t_1 < \ldots < t_n = y$ be a maximal chain for $[x \cap y, y]$. We shall prove that

$$\text{length } [x \cup t_i, x \cup t_{i+1}] \leqq \text{length } [t_i, t_{i+1}],$$

so that, by addition,

$$\text{length } [x \cup t_0, x \cup t_n] \leqq \text{length } [t_0, t_n],$$

which is equivalent to the desired result.

Since $t_{i+1} \geqq t_{i+1} \cap (x \cup t_i) \geqq t_i$ and since t_{i+1} covers t_i, there are two possibilities. In the first, $t_{i+1} \cap (x \cup t_i) = t_i$ and so, by **S***, $(x \cup t_i) \cup t_{i+1}$ covers $x \cup t_i$, that is to say $x \cup t_{i+1}$ covers $x \cup t_i$. In this case

$$\text{length } [x \cup t_i, x \cup t_{i+1}] = 1 = \text{length } [t_i, t_{i+1}].$$

In the second case $t_{i+1} \cap (x \cup t_i) = t_{i+1}$, which yields

$$x \cup t_i = t_{i+1} \cup (x \cup t_i) = x \cup t_{i+1}.$$

In this case

$$\text{length } [x \cup t_i, x \cup t_{i+1}] = 0 < 1 = \text{length } [t_i, t_{i+1}]. \quad \diamond$$

In fig. 29 we observe that $l(a)+l(c) = 2+2 = 4$, while

$$l(a \cup c)+l(a \cap c) = l(I)+l(O) = 3+0 = 3.$$

It follows that the inclusion sign in theorem 30.2 cannot in general be replaced by an equality sign.

THEOREM 30.3. *A lattice is modular if it and the dual lattice are both semi-modular.*

Proof: If the lattice is semi-modular, then

$$l(x)+l(y) \geqq l(x \cup y)+l(x \cap y),$$

where $l(x) = \text{length } [O, x]$. If its dual is also semi-modular, then

$$m(x)+m(y) \geqq m(x \cap y)+m(x \cup y),$$

where $m(x) = \text{length } [x, I] = h-l(x)$ and $h = \text{length } [O, I]$. The last inequality may therefore be rearranged to yield

$$l(x)+l(y) \leqq l(x \cup y)+(x \cap y).$$

Consequently,

$$l(x)+l(y) = l(x \cup y)+l(x \cap y).$$

Since $l(x)$ is a positive valuation, the lattice is evidently metric and therefore, by a previous theorem, modular. ◇

COROLLARY. *A lattice without infinite chains is modular if and only if*

$$x \text{ covers } x \cap z \Leftrightarrow x \cup z \text{ covers } z.$$

The reader will not fail to observe the relationship of this result to theorem 6.4.

§ 31. Atoms in a semi-modular lattice

Since, by definition, a semi-modular lattice has no infinite descending chain, such a lattice must be atomic and we wish now to consider the properties of the atoms in a semi-modular lattice. As before, we use the letters p, q, r to denote atoms. Since $p \cap z \leqq p$, there are only two possibilities. Either $p \cap z = p$, in which case $p \leqq z$, or $p \cap z = O$ and in the latter case p covers $p \cap z$. Applying postulate $\mathbf{S}^*$ to the case where x is an atom p we have

$\mathbf{G}_1$: $$p \cap z = O \Rightarrow p \cup z \text{ covers } z.$$

We now show that $\mathbf{G}_1$ is equivalent to the postulate

$\mathbf{G}_1^*$: $$x \geqq z \Rightarrow x \cap (p \cup z) = (x \cap p) \cup z.$$

We observe that $\mathbf{G}_1^*$ is weaker than the modular law $\mathbf{M}$ since the equality on the right need not hold unless p is an atom.

Suppose that $\mathbf{G}_1$ is true and that $x \geqq z$. For any atom p either $p \leqq x$ or $p \cap x = O$. But

$$\begin{aligned} p \leqq x &\Rightarrow p \cup z \leqq x \cup z = x \\ &\Rightarrow x \cap (p \cup z) = p \cup z = (x \cap p) \cup z. \end{aligned}$$

In the other case $p \cap x = p \cap z = O$, which imply that $p \cup x$ covers x and $p \cup z$ covers z. Now $z \leqq x \cap (p \cup z) \leqq p \cup z$. Further $p \cup z = x \cap (p \cup z)$ would give $x \cup p \cup z = x$ contradicting the fact that $x \cup p$ covers x. It follows, therefore, that

$$x \cap (p \cup z) = z = O \cup z = (x \cap p) \cup z.$$

Thus $\mathbf{G}_1 \Rightarrow \mathbf{G}_1{}^*$.

Conversely, suppose that $p \cap z = O$ and that $p \cup z \geqq x \geqq z$. If $p \leqq x$, then $p \cup z \leqq x$ and, by $\mathbf{P}_2$, $x = p \cup z$. But if $p \cap x = O$, then by $\mathbf{G}_1^*$

$$x = x \cap (p \cup z) = (x \cap p) \cup z = z.$$

Since it has been shown that any x satisfying $p \cup z \geqq x \geqq z$ must be either $p \cup z$ or z, it is clear that $p \cup z$ covers z. Thus $\mathbf{G}_1^* \Rightarrow \mathbf{G}_1$ and consequently $\mathbf{G}_1 \Leftrightarrow \mathbf{G}_1^*$.

Consider now a set of atoms $p_1, \ldots, p_n$. Since $p_i \cap \left(\bigcup_{j \neq i} p_j \right)$ must have one of the values p_i and O, either the atoms form an independent set, or else for at least one value of i

$$p_i \cap \left(\bigcup_{j \neq i} p_j \right) = p_i,$$

from which it follows that $p_i \leqq \bigcup_{j \neq i} p_j$ is the condition that p_i be dependent on the other p_j. If this be so, then

$$\bigcup_j p_j = p_i \cup \left(\bigcup_{j \neq i} p_j \right) = \bigcup_{j \neq i} p_j.$$

In this case $\bigcup_j p_j$ contains at least one redundant term p_i. We conclude that if $\bigcup_j p_j$ is an irredundant representation of x as a union of (irreducible) atoms, then $p_1, \ldots, p_n$ must form an independent set.

In the light of these results we reconsider the theorems of § 10. In the proofs of theorem 10.1 and of the first half of theorem 10.2 the only use made of the modular law was in showing that the intervals $[x_1 \cap t, x_1]$ and $[t, x_1 \cup t]$ were isomorphic. If, however, the x_i are atoms, which we now call p_i, the semi-modular law is sufficient to display the isomorphism between $[p_1 \cap t, p_1]$ and $[t, p_1 \cup t]$, where t now stands for $\bigcup_{j \neq 1} p_j$. For either $p_1 \cap t = p_1$, in which case both intervals are of zero length and $p_1 \cup t = t$ showing that p_1 is redundant, or else $p_1 \cap t = O$ in which case (by $\mathbf{G}_1$) $p_1 \cup t$ covers t and both intervals are of length 1. In the light of these remarks we may state the following.

THEOREM 31.1. *If* $x = \bigcup_{i=1}^{n} p_i = \bigcup_{j=1}^{m} q_j$ *are two representations in a semi-modular lattice of an element x as a union of atoms, then for each p_i there exists a q_j such that*

$$x = p_1 \cup \ldots \cup p_{i-1} \cup q_j \cup p_{i+1} \cup \ldots \cup p_n.$$

Further, if the p_i form an independent set and the q_j form an independent set, then $n = m$.

Again, in the case of theorem 10.3 it will be realised that the argument is still valid in a semi-modular lattice if we replace y by an atom p for then $\mathbf{G}_1^*$ takes the place of $\mathbf{M}$ in the proof. We formulate this as follows.

THEOREM 31.2. *In a semi-modular lattice, if p is independent of an independent set $q_1, \ldots, q_n$, then $p, q_1, \ldots, q_n$ form an independent set.*

As a corollary of the above theorems we can now establish the following.

EXCHANGE LEMMA 31.3. *If p, $q_1, \ldots, q_n$, r are atoms of a semi-modular lattice such that p is dependent on $q_1, \ldots, q_n$, r but independent of $q_1, \ldots, q_n$, then r is dependent on $p, q_1, \ldots, q_n$.*

Proof: The enunciation does not state that $q_1, \ldots, q_n$ are independent but, if not, we may omit any which are redundant in the expression $\bigcup q_i$ since this is the only combination of the q_i which will be mentioned. We may therefore suppose that $q_1, \ldots, q_n$ form an independent set. In the light of the last theorem the hypothesis states that $p, q_1, \ldots, q_n$ also forms an independent set. Since p is dependent on $q_1, \ldots, q_n, r$, then $p \leqq (\bigcup q_i) \cup r$, whence

$$p \cup (\bigcup q_i) \cup r = (\bigcup q_i) \cup r.$$

If r were independent of $p, q_1, \ldots, q_n$ and *a fortiori* of $q_1, \ldots, q_n$ then both $p, q_1, \ldots, q_n, r$ and $q_1, \ldots, q_n, r$ would be independent sets and the above equation would give two representations of the same element as unions of independent atoms, one with $n+2$ terms and the other with $n+1$ terms. As we have seen, this is impossible since both representations must have the same number of terms. Consequently r must be dependent on $p, q_1, \ldots, q_n$. $\diamond$

§ 32. Geometric lattices

As we have already mentioned in the previous section $\mathbf{G}_1$ is deducible from the semi-modular postulate $\mathbf{S}$. The converse, however, is not true. Consider the lattice formed by adjoining one additional element a satisfying $O < p_1 < a < I$ to the Boolean algebra of 16 elements (writing $p_1 = x' \cap y'$, $p_2 = x' \cap y$, $p_3 = x \cap y'$, $p_4 = x \cap y$, the Boolean algebra of 16 elements is the lattice of fig. 7) which has four atoms p_1, p_2, p_3, p_4. Now $\mathbf{G}_1$ is satisfied in this lattice since $p_i \cap a = O$, $p_i \cup a = I$ for $i = 2, 3, 4$, and since $\mathbf{G}_1$ is necessarily valid within the Boolean algebra itself. On the other hand a and $p_1 \cup p_2$ cover $a \cap (p_1 \cup p_2)$ which is the element p_1, but $I = a \cup (p_1 \cup p_2)$ does not cover $p_1 \cup p_2$ since $I > p_1 \cup p_2 \cup p_3 > p_1 \cup p_2$. It follows that $\mathbf{S}$ is not deducible from $\mathbf{G}_1$ alone.

A lattice without infinite chains is called a **geometric lattice** if it satisfies $\mathbf{G}_1$ and $\mathbf{G}_2$.

$\mathbf{G}_2$: Every non-null element is a union of a finite number of atoms.

The condition that the lattice has no infinite chains restricts our attention to geometries of finite dimensions. We shall not in this book consider geometries of infinite dimensions.

THEOREM 32.1. *A geometric lattice is semi-modular.*

Proof: From $\mathbf{G}_2$ it follows that if x and y contain the same atoms then $x = y$ and if x covers y there must be at least one atom p such that $p \leqq x$, $p \cap y = O$. Then from $\mathbf{G}_1$, $p \cup y$ covers y. But $p \cup y \leqq x$ since $p \leqq x$ and $y \leqq x$. Thus $y < p \cup y \leqq x$. Since however x covers y, we obtain $p \cup y = x$.

Now replacing y in the above argument by $x \cap z$ we obtain the following result. If x covers $x \cap z$ then an atom p exists such that $p \cap x \cap z = O$ which yields $p \cap z = O$ since $p \leqq x$, and such that $p \cup (x \cap z) = x$ which yields

$$x \cup z = p \cup (x \cap z) \cup z = p \cup z.$$

Since $p \cap z = O$, it follows from $\mathbf{G}_1$ that $p \cup z$ covers z and it follows that if x covers $x \cap z$ then $x \cup z$ covers z. Thus $\mathbf{S}^*$ is satisfied. ◇

The converse of this theorem does not hold since semi-modular lattices exist in which $\mathbf{G}_2$ is not valid. For instance the lattice of fig. 29 is semi-modular but neither a nor c are unions of points.

We observe the relationship between the postulates $\mathbf{G}_1$, $\mathbf{G}_2$, $\mathbf{S}$:

$$\mathbf{G}_1 \wedge \mathbf{G}_2 \Rightarrow \mathbf{S} \Rightarrow \mathbf{G}_1.$$

As we have seen, neither of the implications is reversible.

As the name suggests, geometric lattices have obvious connections with geometries of finite dimensions. The elements of such a lattice are linear varieties together with the null element O and the whole space I. The geometrical points are the atoms, the 'straight' lines cover points, planes cover lines and so forth. We interpret $x \leqq y$ to mean x lies on y or y passes through x. Then $x \cap y$ is the geometrical intersection of x and y while $x \cup y$ is the join of x and y, that is, the smallest linear variety passing through both x and y.

Since a geometric lattice is semi-modular each element x has a length $l(x)$ associated with it. Points are of length 1, lines of length 2, planes of length 3, etc. In geometry, however, it is more usual to refer to the dimension of an element x which is $l(x) - 1$.

Two distinct points determine a unique line (put $z = q$ in $\mathbf{G}_1$), but three distinct points do not necessarily determine a unique plane since the points may be collinear. This raises the question of independence and we therefore review some previous results in the light of their geometrical significance.

A geometric lattice is semi-modular and atomic. Every element is a union of points and is therefore a union of independent points. Suppose $x = p_1 \cup \ldots \cup p_r$, where the p_i form an independent set. Then

$$p_i \cap \left(\bigcup_{j \neq i} p_j \right) = O$$

and by the isotone property

$$p_i \cap (p_1 \cup p_2 \cup \ldots \cup p_{i-1}) = O.$$

Thus, from $\mathbf{G}_1$, $p_1 \cup \ldots \cup p_i$ covers $p_1 \cup \ldots \cup p_{i-1}$. It follows that

$$O < p_1 < p_1 \cup p_2 < \ldots < p_1 \cup \ldots \cup p_r = x$$

is a maximal chain of length r for $[O, x]$. It follows that the length $l(x)$ of an element x is the maximum number r of independent points contained in x. Such a set of independent points $p_1, \ldots, p_r$ is called a **basis** for x and a basis $p_1, \ldots, p_n$ for I is a basis for the geometry of dimension $n-1$.

Consider the sub-lattice generated by a basis $p_1, \ldots, p_n$ for a geometry. Since

$$p_i \cap \left(\bigcup_{j \neq i} p_j \right) = O, \quad p_i \cup \left(\bigcup_{j \neq i} p_j \right) = I,$$

the element $\bigcup_{j \neq i} p_j$ is a complement of p_i both in the whole lattice and in the sub-lattice generated by the basis. Suppose y is any complement of p_i in the sub-lattice. Then y, like any other element of the lattice is a union of some subset of the basic elements. This subset cannot include p_i itself, since otherwise we would have $p_i \cap y = p_i$ in contradiction to $p_i \cap y = O$. The subset, however, must include every other basic element, for otherwise the relation $p_i \cup y = I = \bigcup p_j$ would show that some p_j was redundant and that the points of the basis were not independent. We conclude that complementation is unique in the sub-lattice though not in the whole lattice. Since complementation is unique in this atomic sub-lattice, the sub-lattice is a Boolean algebra and is isomorphic to the power set of the basis. In illustration, three non-collinear points p_1, p_2, p_3 form a basis for a two-dimensional geometry. The sub-lattice generated by the basis consists of O, p_1, p_2, p_3, the lines $p_1 \cup p_2$, $p_2 \cup p_3$, $p_3 \cup p_1$ and the plane $I = p_1 \cup p_2 \cup p_3$. The Hasse diagram is that of fig. 8 with the elements labelled x', y', $x \cap y$ renamed p_1, p_2, p_3 respectively. The line joining p_1 and p_2, that is, the line $p_1 \cup p_2$, is the element labelled $x' \cap y'$. In the power set of the basis however $p_1 \cup p_2$ is the subset consisting of only two points p_1 and p_2. The isomorphism thus relates the whole line joining p_1 and p_2 to the subset of two points p_1 and p_2. Similarly it relates the whole plane to the set of three points p_1, p_2, p_3.

In regard to the same illustration the exchange lemma could be interpreted as follows. Suppose q is dependent on p_1, p_2, p_3 (q lies on the plane $p_1 \cup p_2 \cup p_3$) but is independent of p_1, p_2 (q does not lie on the line $p_1 \cup p_2$) then p_3 is dependent on q, p_1, p_2 (p_3 lies on the plane $q \cup p_1 \cup p_2$). Notice that q is not an element of the sub-lattice generated by p_1, p_2, p_3. Both q and p_3 are complements of the line $p_1 \cup p_2$ in the lattice but p_3 is its only complement in the sub-lattice.

In any geometric lattice two independent (distinct) points p_1, p_2 determine a unique line $p_1 \cup p_2$, but the dual of this fact need not be true. For instance, in two-dimensional geometry two distinct lines need not intersect in a unique point. Parallel lines in Euclidean geometry provide a familiar example. In a projective geometry of n dimensions two primes (or anti-atoms) of dimensions $n-1$ intersect in a linear variety of dimension $n-2$. This leads us to define a **projective** lattice as a lattice without infinite chains in which $\mathbf{G}_1$, $\mathbf{G}_2$ and their duals are valid. Since both such a lattice and its dual must be semi-modular the lattice is modular by a previous theorem.

In a geometric lattice we have

$$l(x)+l(y) \geqq l(x \cup y)+l(x \cap y),$$

since the lattice is semi-modular, but in a projective lattice we have

$$l(x)+l(y) = l(x \cup y)+l(x \cap y).$$

The significance of these formulae has already been illustrated in the remarks following the dimension theorem (§ 6).

Let $p_1, \ldots, p_r$ be a basis for x. Then x is of length r and we can construct a maximal chain

$$x < x_1 < \ldots < x_{n-r} = I$$

of length $n-r$ if the geometry is of dimension n. Since x_1 covers x there must be a point q_1 such that $q_1 \cap x = O$, $q_1 \leqq x_1$. Then $x_1 \geqq q_1 \cup x \geqq x$. But $q_1 \cup x$ covers x by $\mathbf{G}_1$ and x_1 covers x by hypothesis. So $x_1 = x \cup q_1$. Similarly we find a point q_2 such that $x_2 = x_1 \cup q_2 = x \cup q_1 \cup q_2$, and eventually points $q_1, \ldots, q_{n-r}$ such that

$$x \cup q_1 \cup \ldots \cup q_{n-r} = I.$$

Then $p_1, \ldots, p_r, q_1, \ldots, q_{n-r}$ form a basis for the geometry and the sub-lattice generated by these points is a Boolean algebra. Hence x has a complement

$$x' = q_1 \cup \ldots \cup q_{n-r},$$

from which it is clear that

$$x = q'_1 \cap \ldots \cap q'_{n-r},$$

in which

$$q'_i = (\bigcup p_k) \cup \left(\bigcup_{j \neq i} q_j \right).$$

Observe that q'_i is of dimension $n-1$ and is therefore a prime. Thus in any geometric lattice every element is an intersection of primes (anti-atoms). This however is the dual of $\mathbf{G}_2$, so we see that the dual of $\mathbf{G}_2$ is valid in any geometric lattice.

If a denotes a prime, we may express the dual of $\mathbf{G}_1$ as

$\mathbf{G}_3$: $$a \cup z = I \Rightarrow z \text{ covers } a \cap z.$$

Thus a projective lattice is one without infinite chains satisfying $\mathbf{G}_1$, $\mathbf{G}_2$ and $\mathbf{G}_3$.

§ 33. Algebraic geometry

In the previous section the elements of a geometric lattice were referred to as linear varieties. The adjective 'linear' may or may not be taken in a strictly algebraic sense according to the nature of the geometry under consideration. In the present section we wish to consider varieties which are not linear, such as circles, parabolas, etc. but it is now assumed that all such elements are defined algebraically.

If $\mathscr{F}$ is a field and $\xi_1, \ldots, \xi_n$ be n elements of an algebraic extension of $\mathscr{F}$ then $\xi = (\xi_1, \ldots, \xi_n)$ is called a **point** in n-dimensional space and the ξ_i are its co-ordinates. The elements of the polynomial ring $\mathscr{F}[x_1, \ldots, x_n]$ are polynomials $f = f(x) = f(x_1, \ldots, x_n)$. A point ξ is called a **zero** of the polynomial f if $f(\xi_1, \ldots, \xi_n) = 0$. The set of common zeros of a given system of polynomials $f_1, \ldots, f_r$ is called an **algebraic manifold** or **variety**. For instance, if $\mathscr{F}$ is the real field, the variety determined by

$$f_1 = x^2+y^2+z^2-1, f_2 = x$$

is a circle lying in the YZ plane. The polynomials $f_1, \ldots, f_r$ generate an ideal (see § 7 and § 18), denoted by $(f_1, \ldots, f_r)$, of $\mathscr{F}[x_1, \ldots, x_n]$ which consists of all polynomials

$$g_1 f_1 + \cdots + g_r f_r, \quad g_i \in \mathscr{F}[x_1, \ldots, x_n].$$

Every common zero of the f_i is a zero of every element of this ideal and we may say that the manifold is determined by the ideal. In fact every ideal of $\mathscr{F}[x_1, \ldots, x_n]$ determines a manifold and it can be shown† that every ideal is generated by a finite number of polynomials which determine the manifold. As was shown in § 7 these ideals form a modular lattice in which $a \geqq b$ means that the ideal a contains every polynomial of the ideal b. We denote by $m(a)$ the manifold determined by the ideal a. It is, however, possible for different ideals to determine the same manifold. For instance, if $\mathscr{F}$ is the real field then the ideal $a = (x, y^2)$ determines the same manifold in three dimensional space as does the ideal $b = (x, y)$ namely the z axis. Since in this case b contains polynomials, for instance y, not contained in a, it is possible for $b \geqq a$ but $m(b) = m(a)$.

Amongst all the ideals defining a given manifold m there is one of special importance, namely, that which contains every polynomial but no others which has a zero at each point of m. This ideal we denote by $j(m)$ and it is clear that it is the ideal sum (or lattice union) of all the ideals which define m. The ideal $j(m)$ is therefore the largest ideal determining m and it may be called the **associated ideal** of m. In this way we associate with each manifold m_r an ideal j_r which determines m_r and is determined by it. If we write $m_r \subset m_s$ to denote that every point of m_r is a point of m_s and that m_s contains at least one point which is not a point of m_r, then

$$m_r \subset m_s \Leftrightarrow j_r > j_s.$$

We observe, for example, that a point of m_s which is not a point of m_r cannot be a zero of every polynomial of j_r, while every point of m_r must be a zero of every polynomial of j_s. It follows from the above that $\supseteq$ is an inclusion relation and that the manifolds form a lattice in which the operations coincide with set unions and intersections. It is not difficult to prove that the above relation leads to

$$m_r = m_s \cap m_t \Leftrightarrow j_r = j(m(j_s + j_t)) \Rightarrow j_r \geqq j_s + j_t,$$
$$m_r = m_s \cup m_t \Leftrightarrow j_r = j_s \cap j_t.$$

In other words,

$$j(m_s \cap m_t) \geqq j(m_s) + j(m_t),$$
$$j(m_s \cup m_t) = j(m_s) \cap j(m_t).$$

The details are left to the reader as an exercise.

It is plain that the lattice of the manifolds m_r is isomorphic to the dual of the lattice of the associated ideals j_r. The former being a lattice of subsets of a set is distributive. So is the lattice of the associated ideals j_r, since the distributive law **D** is self dual. Since the lattice of all ideals of $\mathscr{F}[x_1, \ldots, x_n]$ is known to have no infinite ascending chains,

† See, N. H. McCoy, *Rings and Ideals* Chapt. IX.

the same must be true of its sub-lattice of associated ideals j_r. Thus the lattice of manifolds has no infinite descending chains. Each manifold therefore, according to theorem 10.2 has a unique representation as a union of $\cup$-irreducible manifolds.

THEOREM 33.1. *If j is the ideal associated with the manifold m then m is $\cup$-irreducible if and only if j is a prime ideal of the polynomial ring.*

Proof: (i) Suppose m is reducible. Then

$$m = m_1 \cup m_2, \quad m \supset m_1, \quad m \supset m_2.$$

Consequently

$$j = j_1 \cap j_2, \quad j < j_1, \quad j < j_2.$$

So j_1 contains a polynomial f_1 not in j and j_2 contains a polynomial f_2 not in j. Now $f_1 f_2$ is a polynomial of both j_1 and j_2 and therefore of $j_1 \cap j_2$ or of j. Since $f_1 f_2 \in j, f_1 \notin j, f_2 \notin j$, it follows that j cannot be prime.

(ii) If j is not prime, it contains a polynomial $f_1 f_2$ such that $f_1 \notin j, f_2 \notin j$. Let m_1 consist of all points of m which are also zeros of f_1 and let m_2 consist of all points of m which are also zeros of f_2. Then $m_1 \subset m$, since $f_1 \notin j$, and $m_2 \subset m$. Consequently $m \supseteq m_1 \cup m_2$. Since $f_1 f_2 \in j$, every point ξ of m satisfies the equation

$$f_1(\xi) f_2(\xi) = 0,$$

which implies either $f_1(\xi) = 0$ or else $f_2(\xi) = 0$. That is, either ξ is a point of m_1 or ξ is a point of m_2. Then $m \subseteq m_1 \cup m_2$. It follows that $m = m_1 \cup m_2$ with $m \subset m_1$ and $m \subset m_2$. In other words m is reducible. ◇

In the light of this theorem we conclude that every manifold has a unique representation as the union of manifolds determined by prime ideals.

§ 34. Closure

In this and the following sections we shall consider the relationship between certain topological concepts in the light of the theory of lattices. An endomorphism $\phi(x) = \bar{x}$ of the poset $\mathscr{P}$ which maps an element x of $\mathscr{P}$ onto the element $\bar{x}$ of $\mathscr{P}$ is called a **closure operation** of $\mathscr{P}$ if the three following axioms are satisfied

$\mathbf{K}_0$: $$x \leqq y \Rightarrow \bar{x} \leqq \bar{y},$$

$\mathbf{K}_1$: $$x \leqq \bar{x},$$

$\mathbf{K}_2$: $$\bar{\bar{x}} = \bar{x}.$$

The element $\bar{x}$ is called the **closure** of x and x is said to be **closed** if $x = \bar{x}$. Thus, by $\mathbf{K}_2$, the closure of any element is closed. Further by $\mathbf{K}_0$ if $x \leqq y = \bar{y}$, then $\bar{x} \leqq \bar{y} = y$. So $\bar{x}$ is included in every closed element which includes x. Since $\bar{x}$ is itself a closed element which includes x, we see that the closure of x is the smallest closed element which includes x.

If $\mathscr{P}$ has an I element then $\bar{I} \geqq I$ which shows that $\bar{I} = I$ and that I, if it exists, is closed. If the intersection y of a set of closed elements x_i exists, then for all x_i,

$$y = \bigcap_j x_j \leqq x_i = \bar{x}$$

and consequently, by $\mathbf{K}_0$ and $\mathbf{K}_2$

$$\bar{y} \leqq \bar{\bar{x}}_i = \bar{x}_i = x_i.$$

This shows that

$$\bar{y} \leqq \bigcap x_i = y.$$

Since $\bar{y} \geqq y$ by $\mathbf{K}_1$, we see that $\bar{y} = y$ and that the intersection of any number of closed elements, if it exists, is also a closed element.

If we now stipulate that $O \in \mathscr{P}$ and that any two elements x, y of $\mathscr{P}$ have a least upper bound $x \cup y$, we can formulate the two following postulates.

$\mathbf{K}_3$: $$\overline{x \cup y} = \bar{x} \cup \bar{y}.$$

$\mathbf{K}_4$: $$\bar{O} = O.$$

From $\mathbf{K}_3$ it is easy to see that

$$x \leqq y \Rightarrow y = y \cup x \Rightarrow \bar{y} = \overline{y \cup x} = \bar{y} \cup \bar{x} \Rightarrow \bar{x} \leqq \bar{y}.$$

Thus $\mathbf{K}_0$ is a consequence of $\mathbf{K}_3$, though the converse does not hold as will presently be demonstrated by means of a counter-example.

The postulates $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ constitute the **Kuratowski axioms of closure.**

In a Brouwer algebra we have shown that $x \leqq \neg\neg x$ which is $\mathbf{K}_1$ if we take $\neg\neg x$ to be the closure $\bar{x}$ of x. Since $\neg x = \neg\neg\neg x$, we obtain $\neg\neg x = \neg\neg\neg\neg x$, or $\bar{x} = \bar{\bar{x}}$, which is $\mathbf{K}_2$. Again

$$x \leqq y \Rightarrow \neg x \geqq \neg y \Rightarrow \neg\neg x \leqq \neg\neg y \Rightarrow \bar{x} \leqq \bar{y},$$

which verifies $\mathbf{K}_0$. Thus the endomorphism $\phi(x) = \neg\neg x$ defines a closure operation in the Brouwer algebra. Furthermore

$$\bar{O} = \neg\neg O = \neg I = O,$$

so that $\mathbf{K}_4$ is also satisfied. Consider however the lattice of fig. 5. It is easily verified that $\neg p = q$, $\neg q = p$, whence $\neg\neg p = p$, $\neg\neg q = q$. Thus $\bar{p} \cup \bar{q} = \neg\neg p \cup \neg\neg q = p \cup q = r$, while

$$\overline{p \cup q} = \bar{r} = \neg\neg r = \neg O = I.$$

In this instance $\mathbf{K}_3$ is not satisfied. Consequently $\mathbf{K}_3$ cannot be a consequence of $\mathbf{K}_0$, $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_4$.

The relationship $\overline{x \cup y} \geqq \bar{x} \cup \bar{y}$, of which the above illustration provides an example, is true in general as we now show. Since $x \cup y \geqq x$, then $\overline{x \cup y} \geqq \bar{x}$. Likewise $\overline{x \cup y} \geqq \bar{y}$, so $\overline{x \cup y} \geqq \bar{x} \cup \bar{y}$.

As a further illustration, the closure operation $\bar{n} = n$ if n is even, $\bar{n} = n+1$ if n is odd, defined on the chain of integers in which $\geqq$ has its arithmetical meaning and which has 0 as the least element, clearly satisfies $\mathbf{K}_0$, $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_4$, while $\mathbf{K}_3$ follows from the identity $\overline{\max(l, m)} = \max(\bar{l}, \bar{m})$ which is established without difficulty.

An important consequence of $\mathbf{K}_3$ is that

$$x = \bar{x} \wedge y = \bar{y} \Rightarrow \overline{x \cup y} = \bar{x} \cup \bar{y} = x \cup y.$$

In other words the union of two closed elements is closed. This result can be extended by induction to show that the union of a finite number of closed elements is closed.

It will now be assumed that the poset $\mathscr{P}$ is a Boolean algebra in which a closure operation is defined satisfying the Kuratowski axioms and we shall show how the duality in the Boolean algebra can be extended to the closure operation. Accordingly, we define the **interior** $\underset{\sim}{x}$ of an element x to be the complement of the closure of the complement of x, that is to say,

$$\underset{\sim}{x} = (\overline{x'})'$$

and say that x is **open** if and only if $x = \underset{\sim}{x}$. In some ways it is more convenient to write the relation defining $\underset{\sim}{x}$ in the equivalent form

$$(\underset{\sim}{x})' = (\overline{x'}).$$

Thus, by $\mathbf{K}_0$

$$x' \geqq y' \Rightarrow (\overline{x'}) \geqq (\overline{y'}) \Rightarrow (\underset{\sim}{x})' \geqq (\underset{\sim}{y})'.$$

Taking complements of both sides, we obtain

$\mathbf{K}_0^*$: $$x \leqq y \Rightarrow \underset{\sim}{x} \leqq \underset{\sim}{y}.$$

Since $(\underset{\sim}{x})' = (\overline{x'}) \geqq x'$ by $\mathbf{K}_1$, we get

$\mathbf{K}_1^*$: $$x \geqq \underset{\sim}{x}.$$

Again, by $\mathbf{K}_2$,

$$(\underset{\sim}{\underset{\sim}{x}})' = (\overline{(\underset{\sim}{x})'}) = (\overline{\overline{x'}}) = (\overline{x'}) = (\underset{\sim}{x})',$$

so, taking complements,

$\mathbf{K}_2^*$: $$\underset{\sim}{x} = \underset{\sim}{\underset{\sim}{x}}.$$

Next, by $\mathbf{K}_3$,

$$(\underline{x\cap y})' = \overline{((x\cap y)')} = \overline{(x'\cup y')} = \overline{(x')}\cup\overline{(y')} = (\underline{x})'\cup(\underline{y})' = (\underline{x}\cap\underline{y})'.$$

Taking complements of both sides, we have

$\mathbf{K}_3^*$: $$\underline{x\cap y} = \underline{x}\cap\underline{y}.$$

Lastly, by $\mathbf{K}_4$,

$$(\underline{I})' = \overline{(I')} = \bar{O} = O = I',$$

and so, taking complements once more,

$\mathbf{K}_4^*$: $$\underline{I} = I.$$

It is evident therefore that, in a Boolean algebra, each closure postulate implies its own dual and that $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$ regarded as postulates are equivalent to $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$. There is therefore a dual statement or theorem derived from $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$ corresponding to every one derived from $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$. For instance, dual to

$$\underline{I} = I = \bar{I},$$

we have

$$\bar{O} = O = \underline{O},$$

showing that the elements O and I have the property of being both open and closed. Dual to the defining relation

$$(\underline{x})' = \overline{(x')},$$

we have

$$(\bar{x})' = \underline{(x')},$$

the latter being obtained from the former by first substituting x' for x and then taking complements of both sides.

The endomorphism defined by $\phi(x) = \underline{x}$ may be called an **interior operation** if $\mathbf{K}_0^*$, $\mathbf{K}_1^*$, $\mathbf{K}_2^*$ are satisfied. From what we have seen, each closure operation in a Boolean algebra defines an interior operation and conversely it may be shown that each interior operation determines a closure operation. If the closure operation satisfies the Kuratowski axioms, then the resulting interior operation satisfies the duals of the Kuratowski axioms. It follows that interior operations are the duals of closure operations and open elements are duals of closed elements. Indeed, if x is open then x' is closed, and vice versa, since

$$x = \underline{x} \Rightarrow x' = (\underline{x})' = \overline{(x')}.$$

As a consequence of duality, we can state without further proof that $\underline{x}$ is the greatest open element contained in x, that the union, if it exists, of any number of open elements is open, and that the intersection of a finite number of open elements is open.

Any lattice, or indeed any poset in which every pair of elements has a least upper bound, can be given the closure operation $\bar{x} = a \cup x$ in which a is a fixed element, for the verification of $\mathbf{K}_0$, $\mathbf{K}_1$, $\mathbf{K}_2$ is trivial. It is easy to see that $\mathbf{K}_3$ is also satisfied. Assuming that the poset has an O element, we have

$$\bar{O} = a \cup O = a$$

so that $\mathbf{K}_4$ is not satisfied unless $a = O$. This shows that $\mathbf{K}_4$ is independent of the other postulates. However, if we modify the specification to read

$$\bar{x} = a \cup x, \quad x > O,$$
$$\bar{O} = O,$$

we have a closure operation satisfying $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ applicable to any lattice with an O. The dual statements $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$ need not hold for an arbitrary lattice and indeed they may not even have a meaning,

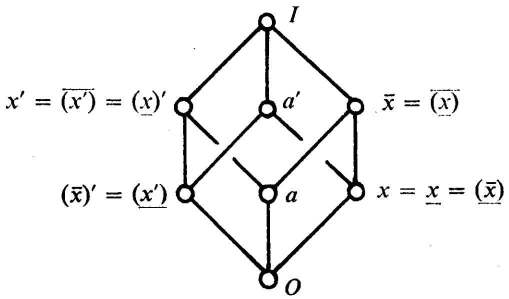


FIG. 30

but we have shown that in a Boolean algebra the one set entails the other. It is not difficult to see that in such a case the above closure operation yields the interior operation

$$\underline{x} = a' \cap x, \quad x < I,$$
$$\underline{I} = I.$$

There is, of course, no reason why the interior of the closure of x should be the same as the closure of the interior of x, but we can confirm that in general $\underline{(\bar{x})}$ and $\overline{(\underline{x})}$ are distinct elements by applying the above closure and interior operations to the lattice of fig. 30.

§ 35. Kuratowski spaces

A complete Boolean algebra together with a closure operation satisfying $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$, or dually an interior operation satisfying

$\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$, defined on it may be called a **Kuratowski space** or a **topological space**. It has been shown that in such a space $\mathscr{P}$, the set $\mathscr{C}$ of all open elements has the following properties

$$\mathbf{T}_1: \qquad I \in \mathscr{C},$$

$$\mathbf{T}_2: \qquad c_i \in \mathscr{C} \Rightarrow \bigcap_{i=1}^{n} c_i \in \mathscr{C},$$

$$\mathbf{T}_3: \qquad c_i \in \mathscr{C} \Rightarrow \bigcup c_i \in \mathscr{C},$$

in which $\bigcup c_i$ denotes the union of either a finite or an infinite number of elements.

We now take a different point of view and suppose that $\mathscr{C}$ is any subset of the elements of a complete Boolean algebra $\mathscr{P}$ such that $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ are satisfied. We define anew, for each element x of $\mathscr{P}$, the element $\underline{x}$ by

$$\underline{x} = \bigcup_{c_i \leqq x} c_i,$$

and we shall show that $\phi(x) = \underline{x}$ is an interior operation such that $\underline{x}$ is the interior of x in the sense of the previous definition. Anticipating this result we call the elements x open if and only if $x = \underline{x}$. It is clear from the above definition that

$$\underline{c} = c$$

if $c \in \mathscr{C}$. Thus all the elements of $\mathscr{C}$ are open. On the other hand if x is open then $x = \underline{x} = \bigcup_{c_i \leqq x} c_i$ and $\mathbf{T}_3$ shows that x is then an element of $\mathscr{C}$. So is in fact every open element of $\mathscr{P}$. From $\mathbf{T}_3$ it follows that $\underline{x}$ is open and that $\mathbf{K}_2^*$ is satisfied. From $\mathbf{T}_1$ it is clear that I is open and that $\mathbf{K}_4^*$ is valid. Since

$$\underline{x} = \bigcup_{c_i \leqq x} c_i \leqq x,$$

$\mathbf{K}_1^*$ holds.

Again,

$$\underline{x \cap y} = \bigcup_{c_i \leqq x \cap y} c_i \leqq \bigcup_{c_i \leqq x} c_i = \underline{x}$$

and similarly $\underline{x \cap y} \leqq \underline{y}$, from which it follows that

$$\underline{x \cap y} \leqq \underline{x} \cap \underline{y}.$$

On the other hand, since the infinite distributive laws are valid in a complete Boolean algebra,

$$\underline{x} \cap \underline{y} = \left(\bigcup_{c_i \leqq x} c_i\right) \cap \left(\bigcup_{c_j \leqq y} c_j\right) = \bigcup_{\substack{c_i \leqq x \\ c_j \leqq y}} (c_i \cap c_j).$$

Now, any term $c_i \cap c_j$ of this union satisfies $c_i \cap c_j \leqq x \cap y$ by the isotone property, so

$$\underline{x} \cap \underline{y} \leqq \bigcup_{c_k \leqq x \cap y} c_k = \underline{x \cap y}.$$

We have therefore established that, by $\mathbf{P}_2$,

$$\underline{x \cap y} = \underline{x} \cap \underline{y},$$

which is $\mathbf{K}_3^*$, and this implies $\mathbf{K}_0^*$.

We have seen that with this new definition of interior $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ imply $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$ and these in turn imply $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ if we define

$$\bar{x} = ((\underline{x'}))'.$$

This means that any subset $\mathscr{C}$ of elements of $\mathscr{P}$ which satisfy $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ defines an interior operation in which $\mathscr{C}$ is the set of all open elements and which fashions $\mathscr{P}$ into a Kuratowski space.

Let $\psi(x) = \underset{\approx}{x}$ denote an arbitrary interior operation satisfying $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$. This interior operation defines a set $\mathscr{C}$ of open elements c_i with the property that $c_i = \underset{\approx}{c}_i$ and such that the elements of $\mathscr{C}$ satisfy $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$. The set $\mathscr{C}$ in turn defines an interior operation

$$\phi(x) = \underline{x} = \bigcup_{c_i \leqq x} c_i$$

satisfying $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$. We have already seen that the open elements defined by $\phi(x) = \underline{x}$ are precisely all the elements of $\mathscr{C}$ and no others. We shall now show that $\underset{\approx}{x} = \underline{x}$. Since $\underset{\approx}{x}$ belongs to $\mathscr{C}$ by $\mathbf{K}_2^*$ and $\underset{\approx}{x} \leqq x$ by $\mathbf{K}_1^*$, it is clear that $\underset{\approx}{x} \leqq \underline{x}$. On the other hand, $c_i \leqq x$ implies that $c_i = \underset{\approx}{c}_i \leqq \underset{\approx}{x}$, whence $\underline{x} \leqq \underset{\approx}{x}$. This shows that $\underline{x} = \underset{\approx}{x}$ and that the two interior operations are indeed identical. In other words $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ and $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$ are equivalent sets of postulates when applied to a complete Boolean algebra.

A set of elements $\mathscr{C}$, belonging to a complete Boolean algebra $\mathscr{P}$, satisfying $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$ is commonly called a **topology** of $\mathscr{P}$. Thus, a topology may be regarded as a kind of texture imparted to $\mathscr{P}$ by $\mathscr{C}$. Since, as we have seen, this texture may equally well be determined by an interior operation satisfying $\mathbf{K}_1^*$, $\mathbf{K}_2^*$, $\mathbf{K}_3^*$, $\mathbf{K}_4^*$, or, alternatively, by a closure operation satisfying $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$, we may, without ambiguity, refer to the topology $\phi(x) = \underline{x}$, or to the topology $\phi(x) = \bar{x}$. In other words, we extend the meaning of the word ‘ topology ’ so that it refers to the texture superimposed on $\mathscr{P}$ rather than to the set $\mathscr{C}$ which determines this texture.

§ 36. Neighbourhoods

It will now be assumed that the complete Boolean algebra $\mathscr{P}$ is also atomic. As was shown in § 29 this means that $\mathscr{P}$ is isomorphic with the power set of its atoms and that any element of $\mathscr{P}$ is the union of the atoms which it contains. It has already been shown that a topology satisfying $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ defines and is defined by a subset $\mathscr{C}$ of open elements satisfying $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$. In this section we wish to show that, assuming $\mathscr{P}$ is now atomic, the topology may be fully determined by a structure of sub-systems of $\mathscr{C}$ and we now describe such structures of which there may be many, which have this property. First of all consider a fixed atom p and consider a system $\mathscr{N}_p$ of open elements such that if p is contained in an open element c then there is at least one element n_p of $\mathscr{N}_p$ such that

$$p \leqq n_p \leqq c.$$

Then n_p is a **neighbourhood** of p and $\mathscr{N}_p$ is a system of neighbourhoods for the atom p.

If one system of neighbourhoods $\mathscr{N}_p$ is in this way assigned to each atom p, we may call such a set of systems of neighbourhoods a **neighbourhood structure** of $\mathscr{P}$ and denote this structure by $\mathscr{N}$. The topological space will in general have many neighbourhood structures and it certainly has one, namely, that in which $\mathscr{N}_p$ is the set of all open elements containing p.

Suppose then that a neighbourhood structure $\mathscr{N}$ is given. We deduce its more important properties.

Since I is an open element which contains every atom p, for any p we can find an n_p such that

$$p \leqq n_p \leqq I.$$

Consequently,

$\mathbf{H}_1$: Every atom p has at least one neighbourhood n_p.

If the atom p has two neighbourhoods n_1 and n_2, then $p \leqq n_1$, $p \leqq n_2$ so that $p \leqq n_1 \cap n_2$. But $n_1 \cap n_2$ is open since n_1 and n_2 are both open; so a neighbourhood n_3 of p can be found such that $p \leqq n_3 \leqq n_1 \cap n_2$ We formulate this as follows.

$\mathbf{H}_2$: If n_1 and n_2 are two neighbourhoods of p then there is a neighbourhood n_3 of p such that $n_3 \leqq n_1$, $n_3 \leqq n_2$.

Suppose the atom q is included in the neighbourhood n_p of p. Since n_p is open we can find a neighbourhood n_q of q such that $q \leqq n_q \leqq n_p$. Thus,

$\mathbf{H}_3$: If q is included in n_p then q has a neighbourhood n_q such that $n_q \leqq n_p$.

Conversely, suppose a system $\mathcal{N}_p$ of elements which we call neighbourhoods is associated with each atom p in such a way that $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ are satisfied. As before, we call the set $\mathcal{N}$ of all such systems a neighbourhood structure and we shall prove that $\mathcal{N}$ determines a topology in which the elements of $\mathcal{N}$ are all open. We define $\bar{x}$ to be the union of all atoms p which have the property that $x \cap n_p > O$ for every neighbourhood n_p of p. Suppose $p \leqq x$. For every n_p, and by $\mathbf{H}_1$ there is at least one, we have $p \leqq n_p$ and consequently $O < p \leqq x \cap n_p$. This shows that $p \leqq \bar{x}$ according to the above definition of $\bar{x}$. Thus every atom of x is an atom of $\bar{x}$. In other words

$$x \leqq \bar{x},$$

since we are dealing with a power set. $\mathbf{K}_1$ is thus established.

Suppose $\bar{x} \cap n_p > O$. Since $\mathscr{P}$ is atomic we can find an atom q such that $q \leqq \bar{x} \cap n_p$. Thus $q \leqq n_p$ and by $\mathbf{H}_3$ we have an n_q such that $q \leqq n_q \leqq n_p$ with the result that $x \cap n_q \leqq x \cap n_p$. We also have $q \leqq \bar{x}$ which means that $x \cap n_q > O$. Combining these results we get

$$\bar{x} \cap n_p > O \;\Rightarrow\; x \cap n_p > O. \tag{36.1}$$

Now if $p \nleqq \bar{x}$ then by definition $x \cap n_p = O$ for some n_p and it has ust been shown (36.1) that this implies $\bar{x} \cap n_p = O$ which means that $p \nleqq \bar{\bar{x}}$. In other words $p \leqq \bar{\bar{x}} \Rightarrow p \leqq \bar{x}$, or $\bar{x} \geqq \bar{\bar{x}}$. But an immediate consequence of $\mathbf{K}_1$ is $\bar{x} \leqq \bar{\bar{x}}$. So, by $\mathbf{P}_2$,

$$\bar{x} = \bar{\bar{x}},$$

which is $\mathbf{K}_2$.

Again $x \cap n_p > O$ implies $(x \cup y) \cap n_p > O$. So $p \leqq \bar{x}$ implies $p \leqq \overline{x \cup y}$; that is, $\bar{x} \leqq \overline{x \cup y}$. Similarly $\bar{y} \leqq \overline{x \cup y}$, and consequently

$$\bar{x} \cup \bar{y} \leqq \overline{x \cup y}.$$

If $p \leqq (\bar{x} \cup \bar{y})'$ then $p \leqq (\bar{x})' \cap (\bar{y})' \leqq (\bar{x})'$. Accordingly, p is not contained in $\bar{x}$ and so for some neighbourhood n_1 of p we have $x \cap n_1 = O$. Similarly for some n_2 of p we have $y \cap n_2 = O$. By $\mathbf{H}_2$ there is an n_3 of p such that $n_3 \leqq n_1$, $n_3 \leqq n_2$. So $x \cap n_3 = y \cap n_3 = O$ and, by the distributive law $(x \cup y) \cap n_3 = O$. Thus p is not contained in $\overline{x \cup y}$ but $p \leqq (\overline{x \cup y})'$. It follows that $(\bar{x} \cup \bar{y})' \leqq (\overline{x \cup y})'$ and consequently that

$$\bar{x} \cup \bar{y} \geqq \overline{x \cup y}.$$

Together with the previous relation this gives

$$\bar{x} \cup \bar{y} = \overline{x \cup y},$$

which is $\mathbf{K}_3$.

Lastly $\bar{O}$ is the union of all atoms p such that $O \cap n_p > O$. There is no such p, so

$$\bar{O} = O,$$

which is $\mathbf{K}_4$.

It follows from these results that in a complete atomic Boolean algebra a structure satisfying the postulates $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ determines a Kuratowski space in which $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ are valid. We have still to show that the neighbourhoods are open elements in regard to the topology introduced. Suppose $p \leqq n_q$. By $\mathbf{H}_3$ there exists an n_p such that $p \leqq n_p \leqq n_q$. Now if $x \cap n_p = O$, then, by definition, $p \nleqq \bar{x}$ and $p \leqq (\bar{x})'$. In particular, $(n_p)' \cap n_p = O$, so

$$p \leqq (\overline{(n_p)'})' = \underline{n_p}.$$

Since, by $\mathbf{K}_0^*$, $n_p \leqq n_q \Rightarrow \underline{n_p} \leqq \underline{n_q}$, we see that $p \leqq n_q \Rightarrow p \leqq \underline{n_p} \leqq \underline{n_q}$. That is to say, $n_q \leqq \underline{n_q}$, but by $\mathbf{K}_1^*$ we have $n_q \geqq \underline{n_q}$. Hence $n_q = \underline{n_q}$ and every neighbourhood is an open element.

Frequently a topological space has further restrictions placed upon it. Such a space is called a **Hausdorff space** if the neighbourhood axioms $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ are supplemented by

$\mathbf{H}_4$: If p, q are distinct atoms then neighbourhoods n_p and n_q exist such that

$$n_p \cap n_q = O.$$

We know that O and I are open elements in any topology and it is patent that the system $\mathscr{C}$ consisting only of O and I satisfy the conditions $\mathbf{T}_1$, $\mathbf{T}_2$, $\mathbf{T}_3$. This system therefore defines a topology in which O and I are the only open elements and in which $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ must be valid. Their validity is indeed easy to verify since each atom has only one neighbourhood namely I. It is clear that in this topology $\mathbf{H}_4$ is not satisfied, from which it follows that $\mathbf{H}_4$ is not a consequence of $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$.

§ 37. Metric spaces

In this section $\leqq$ is used both in its arithmetical sense and as an inclusion relation. The context determines which meaning is intended.

The topological spaces we now consider were among the first to be investigated. As in the previous section we consider a complete atomic Boolean algebra $\mathscr{P}$ which, as we know, is isomorphic to the power set of its atoms. We assume that for each pair of atoms (or points) a real number $\delta(p, q)$ satisfying

$$0 \leqq \delta(p, q) < +\infty$$

is assigned such that

$\mathbf{F}_1$: $$\delta(p, q) = \delta(q, p),$$

$\mathbf{F}_2$: $$\delta(p, r) \leqq \delta(p, q) + \delta(q, r),$$

$\mathbf{F}_3$: $$p = q \Leftrightarrow \delta(p, q) = 0.$$

The Boolean algebra is then called a **metric space** and $\delta(p, q)$ is called the **distance** between p and q, or, alternatively, the **metric** of the space $\mathscr{P}$. The postulates $\mathbf{F}_1$, $\mathbf{F}_2$, $\mathbf{F}_3$ were first formulated by Frechet. If $x \neq O$, we can define further

$$\delta(x, p) = \delta(p, x) = \underset{q \leqq x}{\text{g.l.b.}} \{\delta(p, q)\}.$$

We may introduce the following endomorphism of $\mathscr{P}$

$$\bar{O} = O$$

$$\bar{x} = \bigcup_{\delta(x,p) = 0} p, \quad \text{if } x \neq O$$

and show that this is a topology. $\mathbf{K}_4$ is satisfied by definition. If $p \leqq x$ then $\delta(x, p) = 0$, by $\mathbf{F}_3$, and consequently $p \leqq \bar{x}$. Thus

$$x \leqq \bar{x}$$

which is $\mathbf{K}_1$.

If $q \leqq \bar{\bar{x}}$, then $\delta(\bar{x}, q) = 0$; that is, g.l.b. $\delta(p, q) = 0$ with $p \leqq \bar{x}$. In other words, for a given positive ε there exists a p_1 such that

$$\delta(p_1, q) < \varepsilon, \quad p_1 \leqq \bar{x}.$$

Similarly $p_1 \leqq \bar{x}$ implies that for the same ε there exists an atom p_2 such that

$$\delta(p_1, p_2) < \varepsilon, \quad p_2 \leqq x.$$

By $\mathbf{F}_2$, we have for a given ε

$$\delta(q, p_2) \leqq \delta(q, p_1) + \delta(p_1, p_2) < 2\varepsilon, \quad p_2 \leqq x.$$

Hence $\delta(q, x) = 0$ and $q \leqq \bar{x}$. Thus every atom of $\bar{\bar{x}}$ is contained in $\bar{x}$ and $\bar{\bar{x}} \leqq \bar{x}$. However $\bar{x} \leqq \bar{\bar{x}}$ by $\mathbf{K}_1$ and so

$$\bar{\bar{x}} = \bar{x}$$

which is $\mathbf{K}_2$.

Lastly, suppose $q \leqq \overline{x \cup y}$. Then $\delta(x \cup y, q) = 0$, which tells us that g.l.b. $\delta(p, q) = 0$ with $p \leqq x \cup y$. This means that there exists a $p_n \leqq x \cup y$ such that $\delta(p_n, q) < 1/n$ for all positive integers n. Now by (29.1)

$p_n \leqq x \cup y$ entails either $p_n \leqq x$ or $p_n \leqq y$. Consequently either there is an infinity of p_n such that

$$p_n \leqq x, \quad \delta(p_n, q) < 1/n,$$

or an infinity of p_n such that

$$p_n \leqq y, \quad \delta(p_n, q) < 1/n.$$

But if $\delta(p_n, q) < 1/n$ for an infinity of integers n, then g.l.b. $(\delta(p_n, q)) = 0$. So either $\delta(x, q) = 0$ or $\delta(y, q) = 0$. Then either $q \leqq \bar{x}$ or $q \leqq \bar{y}$. In either case $q \leqq \bar{x} \cup \bar{y}$ and so

$$\overline{x \cup y} \leqq \bar{x} \cup \bar{y}.$$

If $q \leqq \bar{x}$ then $\delta(x, q) = 0$ and g.l.b. $(\delta(p, q)) = 0$ with $p \leqq x$. Since $x \leqq x \cup y$ we see that g.l.b. $(\delta(p, q)) = 0$ with $p \leqq x \cup y$, so $\delta(x \cup y, q) = 0$ and $q \leqq \overline{x \cup y}$. Thus $\bar{x} \leqq \overline{x \cup y}$ and similarly $\bar{y} \leqq \overline{x \cup y}$. Consequently

$$\bar{x} \cup \bar{y} \leqq \overline{x \cup y},$$

which, together with the previous result gives

$$\bar{x} \cup \bar{y} = \overline{x \cup y},$$

which is $\mathbf{K}_3$.

Since the above endomorphism satisfies $\mathbf{K}_1$, $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$ it is a topology and shows that a metric space becomes a Kuratowski space when this topology is imposed on it. If $\mathbf{F}_3$ is replaced by the weaker postulate

$\mathbf{F}'_3$: $$\delta(p, p) = 0,$$

all the above arguments are valid. In this case the space is called a **quasi-metric space** and such a space is also a Kuratowski space. Not every Kuratowski space can be endowed with a metric or a quasi-metric.

An alternative approach is to observe that a neighbourhood structure satisfying $\mathbf{H}_1$, $\mathbf{H}_2$, $\mathbf{H}_3$ is given for a metric space by defining the ε-neighbourhood of p to be

$$n_p(\varepsilon) = \bigcup q, \quad \delta(p, q) < \varepsilon$$

in which ε is a positive real number. The neighbourhood structure is then the set of all $n_p(\varepsilon)$ for all atoms p and for all ε. By $\mathbf{F}_3$ or $\mathbf{F}'_3$, $p \leqq n_p(\varepsilon)$ so $\mathbf{H}_1$ is satisfied. If $n_p(\varepsilon_1)$ and $n_p(\varepsilon_2)$ are two neighbourhoods of p then $n_p(\eta)$ where $\eta = \min(\varepsilon_1, \varepsilon_2)$ has the property that $n_p(\eta) \leqq n_p(\varepsilon_1)$ and $n_p(\eta) \leqq n_p(\varepsilon_2)$ so $\mathbf{H}_2$ is satisfied. Suppose now $q \leqq n_p(\varepsilon)$, then $\delta(p, q) = \varepsilon - \eta$ where $0 < \eta < \varepsilon$, assuming $q \neq p$. Then $n_q(\eta) \leqq n_p(\varepsilon)$, since, if $r \leqq n_q(\eta)$, we have $\delta(r, q) < \eta$ and by $\mathbf{F}_2$

$$\delta(r, p) \leqq \delta(r, q) + \delta(p, q) < \eta + \varepsilon - \eta = \varepsilon,$$

i.e. $r \leqq n_p(\varepsilon)$. So $\mathbf{H}_3$ is also satisfied.

Furthermore, suppose $\delta(p,q) = 3\varepsilon > 0$, that is, $p \neq q$. Then $n_p(\varepsilon) \cap n_q(\varepsilon) = 0$ since otherwise there would be an atom r such that $r \leqq n_p(\varepsilon)$, $r \leqq n_q(\varepsilon)$ so that $\delta(r, p) < \varepsilon$, $\delta(r, q) < \varepsilon$. Then by $\mathbf{F}_2$

$$\delta(p, q) \leqq \delta(r, p) + \delta(r, q) < 2\varepsilon$$

contradicting the previous assumption. It follows that a metric space satisfies $\mathbf{H}_4$ and is therefore a Hausdorff space. Since not every Kuratowski space is a Hausdorff space it follows that not every Kuratowski space can be given a metric or quasi-metric.

We conclude by illustrating the content of the foregoing sections with one of the simplest possible examples. The power set of the points on the real line, which we take to be the ξ axis, forms a complete atomic Boolean algebra. If $\delta(p, q)$ is the Euclidean distance between p and q then $\delta(x, q)$ is, loosely speaking, the distance of q from the nearest point of the set of points x. Strictly, $\delta(x, q)$ is the g.l.b. of the distances of the points p of x from q. The closure $\bar{x}$ of the set x is then the set of points each of which is infinitely near a point of x, and includes all the points of x together with the limit points of x. For instance if x is the set of points $\{a < \xi \leqq b\}$ then $\bar{x} = \{a \leqq \xi \leqq b\}$, $x' = \{(\xi \leqq a) \vee (\xi > b)\}$, $\overline{x'} = \{(\xi \leqq a) \vee (\xi \geqq b)\}$, $\underset{\sim}{x} = ((\overline{x'}))' = \{a < \xi < b\}$. Any union of open intervals such as $\underset{\sim}{x}$ is open and any finite intersection of them is also open. As ε-neighbourhoods of the point p with co-ordinate ξ_1 we have the open intervals $\{\xi_1 - \varepsilon < \xi < \xi_1 + \varepsilon\}$. The system of such intervals forms only a subset of the set of all open sets, for the union of two such intervals is open though it need not itself be such an interval since it may consist of two disjoint portions.

EXERCISES

1. Prove that a poset $\mathscr{P}$ forms a lattice if $I \in \mathscr{P}$ and if every non-void subset of $\mathscr{P}$ has a g.l.b.

2. Show that there are only fifteen non-isomorphic lattices with exactly six elements. How many are self dual?

3. Prove that in any lattice

$$[(x \cap y) \cup (x \cap z)] \cap [(x \cap y) \cup (y \cap z)] = x \cap y,$$

$$(x \cap z) \cup (y \cap t) \leqq (x \cup y) \cap (z \cup t).$$

4. Obtain the one-sided distributive laws (5·1) and (5·2) as special cases of the minimax theorem.

5. Prove that if some x_{pq} in the proof of the minimax theorem has the property that it includes every element in its own row and is included in every element in its own column then

$$\bigcap_i \left(\bigcup_j x_{ij} \right) = \bigcup_j \left(\bigcap_i x_{ij} \right).$$

   Show that the converse of this result holds provided the lattice is a chain. Show also, by means of a counter-example, that the converse does not hold in general, for instance in the lattice of illustration (II).

6. Show that (5·1), (5·2), (5·4) are equivalent statements as follows. Replace x in (5·1) by $(x \cup y) \cap (x \cup z)$ to obtain (5·4). Replace x in (5·4) by $x \cup y$ to obtain (5·2). Dually deduce (5·1) from (5·2).

7. Verify that in *any* telescoping of the pentagon of fig. 6 the identity $x \cap (y \cup z) = (x \cap y) \cup z$ is satisfied.

8. Prove that a lattice is modular if and only if, for all x, y, z,

$$x \cup (y \cap (x \cup z)) = (x \cup y) \cap (x \cup z).$$

9. Prove that a lattice is modular if and only if, for all x, y, z,

$$[x \cup (y \cap z)] \cap (y \cup z) = [x \cap (y \cup z)] \cup (y \cap z).$$

10. If for certain elements x, y, z of a modular lattice the formula $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$ is true, prove that

$$y \cap (z \cup x) = (y \cap z) \cup (y \cap x)$$

   and that $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$. Deduce that in a modular lattice $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$ and $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$ provided two of the three elements x, y, z are ends of a chain.

11. Prove the converse of Zassenhaus's theorem that if the intervals $[(a \cap d) \cup b,\ (a \cap c) \cup b]$, $[(b \cap c) \cup (a \cap d),\ a \cap c]$ are similar whenever $a \geqq b$, $c \geqq d$, then the lattice is modular.

12. If $a_1 \geqq b_1$ and $a_2 \geqq b_2$, show that in any lattice
$$\theta \equiv (a_1 \cap a_2) \cup b_1 = (a_1 \cap b_2) \cup (a_2 \cap b_1)$$
if and only if $\theta = a_1 \cap a_2 = (a_1 \cap b_2) \cup b_1$.

13. Let $\mathscr{V}$ denote a finite dimensional vector space. We write $\mathscr{W}_1 \leqq \mathscr{W}_2$ to denote that every vector of the subspace $\mathscr{W}_1$ belongs to the subspace $\mathscr{W}_2$. Show that the set of all subspaces of $\mathscr{V}$ forms a modular lattice with respect to the inclusion relation defined above.

14. Use theorem 9.4 to show that the lattice of fig. 3 is not distributive.

15. Prove that the lattice of positive integers, in which $\geqq$ has its arithmetical meaning, is distributive.

16. If $(x \cup y) \cap (z \cup (x \cap y)) = (x \cap y) \cup (y \cap z) \cup (z \cap x)$ for all x, y, z, prove that the lattice is distributive. (Hint: first prove the lattice is modular.)

17. Use theorem 11·2 to show that the lattice of factors of a given integer (illustration (II)) is distributive.

18. A complemented lattice is such that if x' denotes any complement of x then $x' \geqq y \Leftrightarrow x \cap y = O$. Prove that complements are unique and that the lattice is distributive.

19. Prove that in a Boolean algebra
$$(y \cup z') \cap (z \cup x') \cap (x \cup y') = (y' \cup z) \cap (z' \cup x) \cap (x' \cup y).$$

20. In a Boolean algebra prove that

(a) $y \leqq x' \Leftrightarrow x \cap y = O$

(b) $y \geqq x' \Leftrightarrow x \cup y = I$

(c) $x = y \Leftrightarrow (x \cap y') \cup (x' \cap y) = O$

(d) $x = O \Leftrightarrow y = (x \cap y') \cup (x' \cap y)$.

21. Of 1000 people, 816 like apples, 723 bananas, 645 cherries while 562 like both apples and bananas, 463 both apples and cherries, 470 both bananas and cherries, but only 310 like all three fruits. How many people like none of them? How many like apples but dislike both bananas and cherries? [1, 101]

22. Prove that the set of all idempotents $e_1, e_2, \ldots$ of a commutative ring forms a distributive lattice in which $e_1 \leqq e_2$ means $e_1 e_2 = e_2$, $e_1 \cup e_2$ means $e_1 e_2$ and $e_1 \cap e_2$ means $e_1 + e_2 - e_1 e_2$. Prove also that the zero of the ring is the I element of the lattice. Show further, that if the ring has an identity element 1, the lattice is a Boolean algebra with $O = 1$ and $e_i' = 1 - e_i$.

23. For a given Boolean algebra $\mu(x)$ is a non-negative real number such that
$$x \cap y = O \Rightarrow \mu(x \cup y) = \mu(x) + \mu(y).$$
Prove that $\mu(x)$ is a valuation for the lattice. Show that this valuation is positive if $\mu(x) = 0 \Rightarrow x = O$.

24. We define 'subtraction' in a Boolean algebra by denoting by $x - y$ the relative complement of y in $[O, x \cup y]$. Prove that
(a) $x - (x - (x - y)) = x - y = (x - y) - y$,
(b) $(x - y) \cup (y - x) = (x \cup y) - (x \cap y)$,
(c) $x - (y - z) = (x - y) \cup (x \cap z)$.
Express each of the basic operations of union, intersection and complementation in terms of subtraction only.

25. Prove that in a Boolean algebra $x \cap (y \cup (z \cap (x' \cup (y' \cap z))))$ is equal to
$$(x \cup y \cup z) \cap (x' \cup y \cup z) \cap (x \cup y' \cup z) \cap (x \cup y \cup z') \cap (x \cup y' \cup z')$$
by expressing both polynomials in canonical form.

26. The elements x, y, z of a Boolean ring satisfy $x + y + z = 0$, $xy + yz + zx = 1$. Prove that $x \cup y = 1, x' \cup y' = z, x \cap y = 1 + x + y$.

27. ϕ, ψ are two ordering-homomorphisms of a lattice $\mathscr{L}_1$ into a lattice $\mathscr{L}_2$. Show that $\phi \cup \psi$ and $\phi \cap \psi$ are also ordering-homomorphisms if we define
$$(\phi \cup \psi)x = \phi(x) \cup \psi(x),$$
$$(\phi \cap \psi)x = \phi(x) \cap \psi(x).$$
Show that the set of all such homomorphisms form a lattice in relation to the operations $\cup$, $\cap$.
Show also that the set of all ordering-homomorphisms $\phi_a(x) = x \cap a$ of a distributive lattice $\mathscr{L}$ into itself forms a distributive lattice $\mathscr{V}$ in relation to $\cup$, $\cap$. If $\mathscr{L}$ has a null element and an all element, find the null and all elements of $\mathscr{V}$.

28. Verify the postulates $\mathbf{L}_{1\cap}$, $\mathbf{L}_{2\cap}$, $\mathbf{L}_{3\cap}$, $\mathbf{L}_{1\cup}$, $\mathbf{L}_{2\cup}$, $\mathbf{L}_{3\cup}$ in the case of the direct product $\mathscr{X} \times \mathscr{Y}$ of two lattices $\mathscr{X}$ and $\mathscr{Y}$.

29. Prove that the direct product of two metric lattices is a metric lattice.

30. Establish the formulae (i), (ii), (iv)...(viii) on p. 49.

31. If p, q, r, s denote propositions, prove that the statements

(a) $[(p \leftrightarrow q) \leftrightarrow (r \wedge \sim s)] \leftrightarrow [(\sim p \leftrightarrow r) \leftrightarrow (q \wedge s)]$

(b) $(p \leftrightarrow q) \wedge (r \leftrightarrow s)$

are logically equivalent. [Hint: the minimax theorem provides a neat solution.]

32. Each of the objects A, B, C is either green or red or white. Of the following statements one is true and four are false.

(1) B is not green and C is not white.

(2) C is red and (4) is true.

(3) Either A is green or B is red.

(4) Either A is red or (1) is false.

(5) Either A is white or B is green.

Determine the colour of each object.

33. Using ring notation for the calculus of propositions show that the set of all false propositions forms a prime ideal of the Boolean ring. (See § 18 for definition of a prime ideal of a ring.)

34. The formula for y cited in fig. 22 was obtained by listing the alternatives in which $y = 1$ and using the formulae (20·1a) and (20·2a). Re-obtain this formula for y by listing the alternatives in which $y = 0$ and using formulae (20.1b) and (20.2b).

35. A, B are two telephones which are arranged so that B cannot be called unless A is engaged but B is not cut off when A puts down the receiver. Furthermore a light C is switched on whenever both A and B are engaged but does not switch off until both A and B are disengaged. Construct suitable circuits and obtain Boolean equations representing the circuits for B and C.

36. a, b, c are binary digits. Design as simple a circuit as possible to calculate $ab+c$ and to represent the answer in the binary scale. Apply the result to designing a circuit to calculate the product xy when x, y are integers in the binary scale each having not more than two digits.

37. Prove that the Boolean matrix equation $XA = B$ has a solution $X = (B'A^T)'$ if and only if $B \leq (B'A^T)'A$. Illustrate this result (due to R. D. Luce) with the case in which

$$A = \begin{bmatrix} a' & a & a' \\ a & a' & a' \\ a' & a' & a \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

38. If X is the Boolean matrix

$$\begin{bmatrix} a & a'\cap b & a'\cap b' \\ a'\cap b' & a & a'\cap b \\ a'\cap b & a'\cap b' & a \end{bmatrix},$$

prove that $|X| = 1$ and that $X^3 = \Phi$.

39. Tabulate the values of $x \rightarrow y$ for the lattice of fig. 5.

40. Prove that in a Brouwer algebra

$$(a \rightarrow b) \rightarrow a \leqq (a \rightarrow b) \rightarrow b.$$

41. If $\mathscr{L}$ be the lattice of factors of $a^n b^m$ where a, b are different primes and $x \leqq y$ means x is a factor of y, show that $\mathscr{L}$ is a Brouwer algebra in which

$$(x \rightarrow y) \cup (y \rightarrow x) = I.$$

42. A given Brouwer algebra is closed with respect to the operation $\leftarrow$ defined by $x \geqq y \leftarrow z \Leftrightarrow x \cup y \geqq z$ which is dual to the operation $\rightarrow$. Show that if

$$x \rightarrow O = x \leftarrow I$$

for all x, then the Brouwer algebra is a Boolean algebra.

43. A. A. Monteiro defines a Brouwer algebra as a system closed with respect to three binary operations $\cup$, $\cap$, $\rightarrow$ such that

$\mathbf{A}_0$: An element O exists such that $O \cap x = O$ for all x,

$\mathbf{A}_1$: $x \rightarrow x = y \rightarrow y$,

$\mathbf{A}_2$: $(x \rightarrow y) \cap y = y$,

$\mathbf{A}_3$: $x \cap (x \rightarrow y) = x \cap y$,

$\mathbf{A}_4$: $x \rightarrow (y \cap z) = (x \rightarrow z) \cap (x \rightarrow y)$,

$\mathbf{A}_5$: $(x \cup y) \rightarrow z = (x \rightarrow z) \cap (y \rightarrow z)$.

Deduce these formulae from the definition in § 25 of a Brouwer algebra. Defining $I = x \rightarrow x$ deduce from $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$ alone that $I \cap x = x$, $x \cap I = x \cap x$, $I \rightarrow x = x$, $x \cap y = y \cap x$, $x \cap x = x$, $x \cap I = x$, $x \cap y = x \Leftrightarrow x \rightarrow y = I$, $x \cap y = I \Rightarrow x = I$. (These are the first steps in proving that the definition of § 25 follows from $\mathbf{A}_0, \ldots, \mathbf{A}_5$).

44. Prove that the following ten statements (Heyting's postulates) are intuitionist tautologies.

(i) $x \rightarrow x \wedge x$,

(ii) $x \wedge y \rightarrow y \wedge x$,

(iii) $x \rightarrow (y \rightarrow x)$,

(iv) $x \to (x \vee y)$,

(v) $[x \wedge (x \to y)] \to y$,

(vi) $\neg x \to (x \to y)$,

(vii) $(x \to y) \to [(x \wedge z) \to (y \wedge z)]$,

(viii) $[(x \to y) \wedge (y \to z)] \to (x \to z)$,

(ix) $[(x \to z) \wedge (y \to z)] \to [(x \wedge y) \to z]$,

(x) $[(x \to y) \wedge (x \to \neg y)] \to \neg x$.

45. Show that in intuitionist logic

$$(x \vee y) \to \{[(x \to y) \wedge (y \to x)] \to (x \wedge y)\}$$

is a tautology.

46. In a Brouwer algebra, prove that the set of elements x satisfying $\neg\neg x = I$ forms an $\cap$-ideal. Show that it is not in general a prime $\cap$-ideal by providing a counter-example from the lattice of factors of 12.

47. Show that if $y \cap z < x < z < x \cup y$ in a semi-modular lattice then there exists an element t such that $y \cap z < t \leqq y$ and $x = (x \cup t) \cap z$.

48. Prove that in a two-dimensional projective lattice the following statement holds. If p, q, r, s, t are distinct points (atoms) such that $p \leqq q \cup r$, $p \leqq s \cup t$, then a point w exists such that $w \leqq q \cup s$, $w \leqq r \cup t$.

Prove the same result for a three-dimensional projective lattice.

49. Prove that in a topological space an element x is open if and only if $y \geqq x \Rightarrow \underline{y} \geqq x$.

50. Prove that in a topological space $x \cup y = I \Rightarrow \bar{x} \cup \underline{y} = I$ and that $x \cap y = O \Rightarrow \bar{x} \cap \underline{y} = O$. Prove also that $\underline{x} \cup \bar{y} = \overline{\underline{x \cup y}} \cup \bar{y}$ and deduce that the set of all open elements form a Brouwer algebra in which $x \to y = x' \cup y$.

51. Defining the **frontier** $f(x)$ of an element x belonging to a topological space to be $\bar{x} \cap \overline{(x')}$, prove that (i) $f(x) = f(x')$, (ii) $\bar{x} = x \cup f(x)$, (iii) $\underline{x} = x \cap (f(x))'$, (iv) $f(x \cup y) \cup f(x \cap y) \leqq f(x) \cup f(y)$. Show also that $f(x) = O$ if and only if x is both open and closed.

INDEX

PRINTED IN GREAT BRITAIN BY
OLIVER AND BOYD LTD.,
EDINBURGH

UNIVERSITY MATHEMATICAL MONOGRAPHS

Mathematicians the world over are familiar with the University Mathematical Texts series. These books were designed as inexpensive volumes suitable for undergraduate students. This new, related series of University Mathematical Monographs will cater for the most part for the more mature mathematician, but certain volumes of an elementary character which could not conveniently be published as University Mathematical Texts will also be included. The high standard of mathematical and typographical presentation set by the Texts will be maintained.

TITLES IN THE SERIES

1. **Integration, Measure and Probability**
   H. R. PITT PhD FRS
   25s
2. **Introduction to Lattice Theory**
   D. E. RUTHERFORD DSc DrMath
   35s
3. **Boundary Value Problems**
   A. G. MACKIE PhD FRSE
   50s
4. **The Classical Moment Problem**
   N. I. AKHIEZER
   70s
5. **Discourse on Fourier Series**
   C. LANCZOS DrPhil MRIA
   63s

To be published shortly

6. **Differential and Integral Calculus**
   F. ERWE
7. **Lectures on Modern Algebra**
   P. DUBREIL and **M.-L. DUBREIL-JACOTIN**

RUTHERFORD

Introduction to Lattice Theory

2

O&B