ANNALS OF MATHEMATICS
Vol. 40, No. 3, July, 1939

THE LATTICE THEORY OF OVA

BY MORGAN WARD AND R. P. DILWORTH[1]

(Received December 21, 1938; revised March 24, 1939)

I. INTRODUCTION

1. In a series of previous papers,[2] we have developed the theory of residuated lattices; that is, lattices over which a multiplication and associated residuation may be defined with the same properties as in polynomial ideal theory. Here we reverse our procedure and start with a system closed under a single suitably restricted operation of multiplication (see section 3). Following E. T. Bell, (Bell 1), we call such a system an "ovum."[3] By the adjunction of properly defined ideals of various kinds (distinguished sub-sets of the ovum), we imbed the ovum in a residuated lattice, incidentally generalizing many of the imbedding theorems of MacNeille 1. The Noether lattices introduced in W-D enables us to describe concisely the arithmetical behavior of ova. In particular, the recent results of A. H. Clifford in these Annals (Clifford 1) come under our general theory. An interesting new result is the following "fundamental theorem of the arithmetic of finite ova." *By the adjunction of a finite number of ideals, every finite ovum may be imbedded in a residuated lattice in which every element, and in particular the elements of the ovum, may be uniquely represented as a cross-cut of primary elements.*

2. The plan of this paper is as follows. After some set-theoretic preliminaries, we define and discuss in the third and fourth divisions of the paper two types of distinguished subsets of an ovum, its product ideals and ovoid ideals. (The reader is referred to the paper Clifford 2 in these Annals for the literature and history of ovoid ideals.) In the concluding division of the paper, we give the arithmetical theory of ovoid ideals, obtaining the following general result: *If the lattice of ovoid ideals is modular and if the ascending chain axiom holds, then all of the decomposition theorems of Emmy Noether for the ideals of commutative rings hold.*

3. We shall use the lattice terminology of our previous papers. If $\mathfrak{S}$ is a lattice of elements $A, B, \cdots$ and unit element E over which a multiplication is

---

[1] Portions of this paper have been revised in accordance with suggestions of Dr. A. H. Clifford, who kindly read it in manuscript.

[2] The papers relevant to the present investigation are Ward 1, 2 and the joint paper Ward-Dilworth 1, which we cite here as W-D.

[3] Bell does not postulate the existence of a unit in his general definition. Other terms are "commutative groupoid" (G. Birkhoff 2), "semi-group" A. H. Clifford 2. For a recent discussion of finite ova, see Poole 1.

defined (Ward 1), we write $X \supset Y$, $Y \subset X$ for X contains Y and (X, Y), $[X, Y]$, XY or $X \cdot Y$ for the union, cross-cut and product respectively of the elements X and Y.

Assume that $\mathfrak{S}$ is completely closed relative to union; that is, every subset of elements of $\mathfrak{S}$ has a union. Then if for every subset Ω of elements A of $\mathfrak{S}$ and any fixed element B, the union of the set of elements BA is the product of B and the union of the A, we say that multiplication is "completely distributive" relative to union. It is easily shown that multiplication is completely distributive relative to union if and only if the union of the products of all pairs of elements of any two sets of $\mathfrak{S}$ is the product of the unions of the sets.[4] Complete distributivity is of importance because of the following theorem.

THEOREM 3.1. *Let $\mathfrak{S}$ be a lattice which is completely closed relative to union over which a commutative and associative multiplication may be defined distributive with respect to union, and let the unit element of the lattice also be the unit with respect to multiplication. Then a necessary and sufficient condition that any two elements of $\mathfrak{S}$ may have a residual is that multiplication be completely distributive relative to union.*

PROOF. The sufficiency of the condition is established in Ward 1. To prove the necessity, assume that every two elements of $\mathfrak{S}$ have a residual: specifically, given A and B, there exists an element $R = A:B$ such that $A \supset RB$; $A \supset XB$ implies $R \supset X$. It is shown in Ward 1 how the ordinary properties of the residual then follow and in particular,

$$\text{(i) } A:BC = (A:B):C \qquad \text{(ii) } A \supset B \text{ if and only if } A:B = E.$$

Now let Ω be any set of elements A of $\mathfrak{S}$, and B, a fixed element of $\mathfrak{S}$. Let U and V denote respectively the union of all A and of all BA. It suffices to show that $V = BU$. Since $U \supset A$, $BU \supset BA$ for $A \in \Omega$ (Ward 1). Hence $BU \supset V$. But $V \supset BA$, $A \in \Omega$. Hence by (ii) and (i), $E = V:BA = (V:B):A$ or $V:B \supset A$. Hence $V:B \supset U$ or $V \supset BU$, $V = BU$.

4. We understand by an "ovum" a set O of elements $a, b, c, \cdots$ over which a binary relation $x = y$ called "equality" and a binary operation xy called multiplication are well-defined subject to the following conditions: (i) Equality is an equivalence relation; (ii) O is closed under multiplication and multiplication is associative and commutative; (iii) O contains a unit e such that $ae = ea = a$, any a in O; (iv) If $a = b$, then $ac = bc$, $ca = cb$ any c in O. In short, an ovum is a system satisfying all the usual postulates for an Abelian group save the existence of inverses.[5]

---

[4] MacNeille 1 has an example showing that complete closure relative to union and distributivity of multiplication relative to union for finite sets does not imply complete distributivity.

[5] The unit e may be dispensed with by strengthening slightly the conditions on the residual introduced later. The non-commutative case will be treated by R. P. Dilworth elsewhere.

For example, any lattice over which a multiplication is defined with the properties in Ward 1 is an ovum with respect to the multiplication whose unit element is the unit of the lattice.

If U and V are subsets of O, we denote by $U + V$ and $U \cap V$ their set-theoretic union and cross-cut. Here as usual if U and V have no elements in common, $U \cap V$ is the set-theoretic null class Z containing no elements of O but contained in every other subset.

If u lies in U, we write $u \in U$. If Ω is any class of subsets A of O, we write $\sum A$ for the set-theoretic union of the A in Ω. $U \supset V$, $V \subset U$ and $U = V$ denote set-theoretic inclusion and equality.

If U and V are any two subsets, their *set product* UV is by definition the set of all products uv, $u \in U$ and $v \in V$. If U consists of a single element u, we write uV for UV. It is clear that the subsets of O form an ovum with respect to the operation of multiplication so defined, and if $A \supset B$, then $AC \supset BC$ for any C. The following theorem is a direct consequence.

THEOREM 4.1. *The operation of multiplication of subsets is completely distributive with respect to set theoretic union.*

In particular $C(A + B) = CA + CB$ for any three sets A, B and C. On the other hand, $C(A \cap B) \neq CA \cap CB$ in general.

A set H is called a sub-ovum of O if $H^2 \subset H$. A sub-ovum is called "proper" if it contains the unit element e of O and the zero element z whenever the latter exists. Here z is defined by the property $az = z$ for every a of O.

Let $\bar{O}$ be a proper sub-ovum of O, fixed throughout all that follows. An element a of O is said to "divide" an element b of O (relative to $\bar{O}$) if there exists an element c of $\bar{O}$ such that $ac = b$. We write $a \mid b$. If $a \mid b$ and $b \mid a$, a and b are said to be equivalent (relative to $\bar{O}$); we write then $a \backsim b$. The division relation $\mid$ partially orders O, and $\backsim$ is an equivalence relation. Moreover $e \mid a$ for every element a of $\bar{O}$, and if z exists, $a \mid z$ for every a of O.

II. THE PRODUCT IDEALS OF AN OVUM

5. The first type of distinguished subset of O which we shall consider is the product ideal.

DEFINITION 5.1. *A subset S' is called a product ideal (relative to $\bar{O}$) if $\bar{O}S' = S'$.*

If in addition $\bar{O} \supset S'$, S' is said to be integral. Clearly O itself is a product ideal. Hence given any subset A of O, there is a least product ideal A' containing it. We call A' the ideal generated by A. If A consists of a single element a, we write $A' = (a)$.

If the ovum contains a zero element z, then $z \in S'$ every S' and the ideal (z) is the set Z consisting of z alone. Hence $S' \supset Z$ for every product ideal S'. If O contains no zero element, we count the null set Z as a product ideal. It is easily seen that the product ideals of $O(\bar{O})$ are closed under the operations of set-theoretic cross-cut and union.

We denote the union and cross-cut of a set Ω by $\mu\Omega$ and $\kappa\Omega$ respectively. The following theorem is now evident:

THEOREM 5.1. *The set of all product ideals and the set of all integral product ideals of any ovum both form distributive lattices which are completely closed with respect to union and cross-cut.*

THEOREM 5.2. *The set of all integral product ideals of an ovum form a residuated lattice completely closed relative to union and cross-cut.*

PROOF. Since the union and cross-cut operations on ideals in $\bar{O}$ are the set-theoretic operations on the ideals qua classes of elements, it is evident that the ideals form a completely closed distributive lattice. The postulates for a multiplication in a lattice are

M 1 *If $\bar{O}$ contains A', B', then $\bar{O}$ contains $A'B'$.*
M 2 *If $A' = B'$, then $A'C' = B'C'$.*
M 3 $A'B' = B'A'$.
M 4 $(A'B')C' = A'(B'C')$.
M 5 $A'O' = A'$ any A'. (Here $O' = \bar{O}$).
M 6 $A'(B', C') = (A'B', A'C')$.

These postulates are clearly all satisfied. We shall denote this lattice by $\mathfrak{R}$. We also have from theorems 3.1 and 4.1

M7 *$\mathfrak{R}$ is completely closed with respect to union, and the product of the unions of any two classes of ideals of $\mathfrak{R}$ is the union of the set-products of all pairs of elements in the classes.*

Hence (Ward 1) a residuation $X':Y'$ may be defined over $\mathfrak{R}$ with the properties R 1–R 6 given in W-D, §4, so that the ideals of $\bar{O}$ form a residuated lattice by definition.

It is impossible to prove that the lattice of *all* product ideals of O may be residuated, for the unit element O of the lattice is not the unit with respect to multiplication, so that M 5 is not satisfied. All the remaining postulates are satisfied. A similar situation occurs in defining the product of two modules of a ring of algebraic integers (Dedekind 1). M 5 is arithmetically important, as it assures that $A' \supset A'B'$.

If a is any element of $\bar{O}$, the product ideal (a) is clearly the set $a\bar{O}$ of all multiples of a in $\bar{O}$. We call (a) an (integral) principal ideal.

THEOREM 5.3. *If A' is an integral principal ideal and $A' \supset B'$, then there exists an integral ideal C' such that $A'C' = B'$.*

PROOF. By hypothesis, $A' = a\bar{O}$. Since $A' \supset B'$, every element of B' is of the form aq, where q lies in a certain fixed class Q of $\bar{O}$. Then

$$B' = \sum_Q aq\bar{O} = \sum a\bar{O}q\bar{O} = a\bar{O}\sum q\bar{O} = A'C'$$

where C' is the ideal $\sum q\bar{O}$.

It follows from M 7 in the proof of theorem 5.5, and W-D, lemma 13.1, that we may take $C' = B':A'$.[6]

[6] There may be several ideals C' such that $A'C' = B'$.

6. It may be shown by simple examples that if the ovum $\bar{O}$ contains an infinite number of non-equivalent elements, no chain conditions need be satisfied in $\mathfrak{R}$, or in other words integral product ideals are in general expressible only as unions of an infinite number of elements of $\bar{O}$. If however $\bar{O}$ contains only a finite number of non-equivalent elements, then $\mathfrak{R}$ is a finite lattice satisfying the following conditions:[7]

N 1. *$\mathfrak{R}$ is residuated.*

N 2. *The ascending chain condition holds in $\mathfrak{R}$.*

D 3. *Every element of $\mathfrak{R}$ is the union of a finite number of principal ideals.*

D 4. *The principal ideals of $\mathfrak{R}$ are closed under multiplication.*

Hence by theorem 5.3 and theorem 14.2 of W-D, $\mathfrak{R}$ is a Noether lattice. Since $\mathfrak{R}$ is also a distributive lattice, we may state the following theorem.

THEOREM 6.1. *If $\bar{O}$ contains only a finite number of principal product ideals, then every element of $\bar{O}$ is expressible as a cross-cut of a finite number of primary product ideals in essentially one way only.*

If in particular O itself has only a finite number of elements, and we take $\bar{O} = O$, we have the "fundamental theorem of the arithmetic of finite ova" stated in the introduction.

III. The Ovoid Ideals of an Ovum

7. The second type of distinguished subset of O which we shall consider is the ovoid ideal. There is little gain in defining division in O relative to a proper subovum $\bar{O}$, and for the remainder of the paper we identify $\bar{O}$ with O as in Clifford 2.

DEFINITION 7.1. *Let A be any set of elements of O. The cross-cut of all the residuals $(s):(t)$ of principal product ideals (s), (t) such that $(s):(t)$ contains A is called the ovoid ideal generated by A.*

We write $\mathfrak{a} = (A)$ (Clifford 2). Evidently $\mathfrak{a}$ is a product ideal containing both A and A'. It is easily shown that this definition is equivalent to the definition in Clifford 2. It seems to us somewhat easier to grasp.

O itself is an ovoid ideal $\mathfrak{o}$, and the ovoid ideals form a semi-ordered set with respect to the relation $(\mathfrak{x}) \supset (\mathfrak{y})$ of set-theoretic inclusion. We use small German letters for ovoid ideals.

As in part II, a special convention is made for the null ideal. If the ovum contains a zero element z, the set $\mathfrak{z}$ consisting of the single element z is an ovoid ideal contained in every other ideal. If the ovum contains no zero element, we count the null set as an ovoid ideal $\mathfrak{z}$ contained in every other.

The following properties of ovoid ideals are obvious from the definition:

(7.1) $\quad (A) \supset A, \quad A \supset B \quad$ implies $\quad (A) \supset (B), \quad ((A)) = (A).$

LEMMA 7.1. (Clifford 2) *If the subset A consists of a single element a, the ovoid ideal (A) is the principal product ideal $(a) = aO$.*

---

[7] The letters N 1, N 2, D 3, D 4 refer to the like-designated conditions in W-D.

THEOREM 7.1. *The set-theoretic cross-cut of any class of ovoid ideals is an ovoid ideal.*

PROOF. Let Ω be a class of ovoid ideals $\mathfrak{a}$, and let K be the set-theoretic cross-cut of the $\mathfrak{a}$. (K exists, since $\mathfrak{a} \supset \mathfrak{z}$). Then $\mathfrak{a} \in \Omega$ implies $\mathfrak{a} \supset K$. Hence by (7.1), $(\mathfrak{a}) \supset (K)$, $\mathfrak{a} \supset (K)$. Hence $K \supset (K)$, $K = (K)$.

We may now define the union of any set of ovoid ideals $\mathfrak{b}$ as the cross-cut of the non-empty set Ω of all ideals $\mathfrak{a}$ such that $\mathfrak{b} \supset \mathfrak{a}$, all $\mathfrak{b}$. It is easy to prove from (7.1):

LEMMA 7.2. (Clifford 2) *The union of any set of ovoid ideals is the ovoid ideal generated by their set theoretic sum.*

We may now state one of our fundamental theorems.

THEOREM 7.2. *The set of ovoid ideals of any ovum form a completely closed lattice relative to the relation of set-theoretic inclusion.*

8. We now pass to the multiplicative properties of the lattice of ovoid ideals. The set product of two ovoid ideals need not be an ovoid ideal. We accordingly define the product of two ovoid ideals to be the ideal generated by their set product. To distinguish this new product from the set product, we use a dot, writing

$$(A)\cdot(B) = ((A)(B)), \quad \text{or} \quad \mathfrak{a}\cdot\mathfrak{b} = (\mathfrak{a}\mathfrak{b}). \tag{8.1}$$

This multiplication is readily shown to satisfy postulates M 1–M 5 of section 5, where the unit element is the unit ideal $\mathfrak{o}$.

THEOREM 8.1. *The operation of multiplication of ovoid ideals is completely distributive with respect to union.*

PROOF. Let Ω be any set of ovoid ideals $\mathfrak{a}$, and let $\mathfrak{b}$ be any fixed ovoid ideal. Let $\mathfrak{u}$ be the union of the ideals $\mathfrak{a}$, and $\mathfrak{v}$ the union of the ideals $\mathfrak{b}\cdot\mathfrak{a}$. Then by lemma 7.2 $\mathfrak{u} = (\sum \mathfrak{a})$, $\mathfrak{v} = (\sum \mathfrak{b}\cdot\mathfrak{a})$. We wish to show that $\mathfrak{b}\cdot\mathfrak{u} = \mathfrak{v}$. We need the following lemma due to A. H. Clifford: (Clifford 2).

LEMMA 8.1. *If A and B are any two subsets of O, then the product of the ovoid ideals which they generate is the ideal generated by their set product:*

$$(A)\cdot(B) = (AB). \tag{8.2}$$

By (8.2), $\mathfrak{b}\cdot\mathfrak{u} = (\mathfrak{b}\sum \mathfrak{a}) = (\sum \mathfrak{b}\mathfrak{a})$ by theorem 4.1. But by lemma 7.2 $(\sum \mathfrak{b}\mathfrak{a}) = (\sum (\mathfrak{b}\mathfrak{a})) = (\sum \mathfrak{b}\cdot\mathfrak{a}) = \mathfrak{v}$

It follows that M 7 and M 6 of section 5 are satisfied. Hence we have

THEOREM 8.2. *The set of all ovoid ideals of O form a completely closed residuated lattice.*

We denote this lattice by $\mathfrak{S}$.

If (a) and (b) are principal ovoid ideals, it is easily shown that $(a)\cdot(b) = (a)(b) = (ab)$. Hence we have

LEMMA 8.2. *The principal ovoid ideals of O are closed under multiplication, and form an ovum within the lattice $\mathfrak{S}$ which is simply isomorphic with O.*

In W-D, an element $\mathfrak{a}$ of a residuated lattice $\mathfrak{S}$ was defined to be "principal" provided that $\mathfrak{a} \supset \mathfrak{b}$ if and only if there existed a lattice element $\mathfrak{c}$ such that $\mathfrak{ac} = \mathfrak{b}$.

THEOREM 8.3. *Every principal ideal of the lattice of all ovoid ideals of an ovum is a principal element of the lattice.*

PROOF. Let $\mathfrak{a} = (a)$ and $\mathfrak{a} \supset \mathfrak{b}$. Consider the set C of all elements c such that $ac \in \mathfrak{b}$ and let $\mathfrak{c} = (C)$. Then $\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{c}$. For since $\mathfrak{b} \supset aC$, $(\mathfrak{b}) \supset (aC)$ or $b \supset \mathfrak{a} \cdot \mathfrak{c}$. Since $\mathfrak{a} \supset \mathfrak{b}$ and $\mathfrak{a} = (a)$, if $b \in \mathfrak{b}$ then $b = ca$, $c \in O$. Hence $aC \supset \mathfrak{b}$ so that $(aC) \supset \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{c} \supset \mathfrak{b}$, $\mathfrak{a} \cdot \mathfrak{c} = \mathfrak{b}$.

IV. THE ARITHMETICAL PROPERTIES OF OVA

9. We shall now consider the arithmetical properties of the lattice $\mathfrak{S}$. In W-D, we have called a lattice a "Noether lattice" if it satisfies the three conditions.

N 1. *The lattice $\mathfrak{S}$ may be residuated.*

N 2. *The ascending chain condition holds in $\mathfrak{S}$.*

N 3. *Every irreducible of $\mathfrak{S}$ is primary.*

In such a lattice the decomposition theorems first proved by Emmy Noether for the ideals of a commutative ring with chain condition hold. We also proved there that sufficient conditions[8] that any lattice be a Noether lattice are N 1, N 2 and

D 2 *$\mathfrak{S}$ is modular.*

D 3′ *There exists a set $\mathfrak{P}$ of principal elements of $\mathfrak{S}$ such that every other element is the union of a finite number of elements of $\mathfrak{P}$.*

D 4′ *The set $\mathfrak{P}$ is closed under multiplication.*

In the present case, N 1 is satisfied by theorem 8.2, and D 4′ is satisfied for $\mathfrak{P}$ the principal ideals of $\mathfrak{S}$ by lemma 8.2. Clifford has shown that N 2 implies D 3′ (Theorem 8.4; Clifford 2, theorem 2.1). Hence we may state the fundamental result:

THEOREM 9.1. *The lattice of ovoid ideals of any ovum is a Noether lattice provided that*

N 2. *The ascending chain condition holds in $\mathfrak{S}$,*

D 2. *$\mathfrak{S}$ is modular.*

If we assume that $\mathfrak{S}$ is distributive instead of modular, we have an analogue of theorem 6.1 on product ideals; namely

THEOREM 9.2. *If the lattice of ovoid ideals of an ovum satisfies the conditions*

N 2. *The ascending chain condition holds in $\mathfrak{S}$,*

D 6. *$\mathfrak{S}$ is distributive,*

then every element of the lattice, and in particular the principal ideals corresponding

---

[8] The more restrictive conditions D 3 and D 4 quoted in section 6 are stated in W-D. But an examination of the proof of theorem 14.2 of W-D will show that D3′ and D4′ are sufficient.

to elements of the ovum, may be uniquely represented as a cross-cut of primary elements, each belonging to a different prime.

If we assume that every ovoid ideal is principal, then D 6 is satisfied by W-D theorem 16.2. Hence we may state:

THEOREM 9.3. *The conclusions of theorem* 9.2 *hold provided that the lattice of ovoid ideals satisfies the conditions*

N 2. *The ascending chain condition holds in* $\mathfrak{S}$,

D 7. *Every ovoid ideal is principal.*

10. The two simplest types of distributive lattice are arithmetical lattices and semi-arithmetical lattices. An arithmetical lattice is one which is a direct product[9] of simple chain lattices and in which N 2 holds. It is quite easy to show that the fundamental theorem of arithmetic[10] holds in a lattice if and only if the lattice is arithmetical. Such lattices have been thoroughly investigated by F. Klein (Klein 1).

The notion of a semi-arithmetical lattice was introduced by one of us in a recent paper in these Annals. (Ward 2.) A semi-arithmetical lattice is a distributive lattice in which the ascending chain condition holds and in which every element may be uniquely represented as a cross-cut of irreducible elements *co-prime in pairs*. If the semi-arithmetical lattice is residuated, it follows that every element may be uniquely represented as a *product* of irreducible elements; for if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, their product equals their cross-cut. Conversely, it is not difficult to show that if every element of a lattice may be uniquely represented as a product of irreducible elements, co-prime in pairs, then the lattice is semi-arithmetical; in other words a residuated semi-arithmetical lattice is the most general type of lattice in which a unique multiplicative decomposition of elements may be defined.

We can therefore replace condition D 6 by conditions that $\mathfrak{S}$ be semi-arithmetical or arithmetical to obtain still more special types of decomposition in $\mathfrak{S}$. The investigations of Clifford viewed from this standpoint give convenient sets of conditions that the lattice be arithmetical.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA.

REFERENCES

E. T. BELL	1	Am. Math. Monthly 37 (1930) pp. 400–418.
GARRETT BIRKHOFF	1	Bull. Am. Math. Soc. 40 (1934) pp. 613–619.
	2	These Annals (2) 35 (1934) pp. 351–360.
A. H. CLIFFORD	1	Bull. Am. Math. Soc. 40 (1934) pp. 326–330.
	2	These Annals (2) 39 (1938) pp. 594–610.

[9] For the notion of a direct product of lattices, see Garrett Birkhoff 1.

[10] Every lattice element is then uniquely representable as a cross-cut or product of co-prime powers of divisor free elements. (Klein 1.)

R. DEDEKIND	1	Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed.
L. E. DICKSON	1	Trans. Am. Math. Soc. 6 (1905) p. 205.
F. KLEIN	1	Math. Annalen 106 (1932) pp. 114–134.
H. M. MACNEILLE	1	Trans. Am. Math. Soc. 42 (1937) pp. 416–460.
A. R. POOLE	1	Am. Math. Journ. 59 (1937) pp. 23–32.
M. WARD AND R. P. DILWORTH		Trans. Am. Math. Soc. (reference later).
M. WARD	1	Duke Math. Journ. 3 (1937) pp. 627–636.
	2	These Annals (2) 39 (1938) pp. 558–568.