ANNALS OF MATHEMATICS
Vol. 39, No. 3, July, 1938

STRUCTURE RESIDUATION

BY MORGAN WARD

(Received Dec. 27, 1937)

I. INTRODUCTION

1. Given any two elements A and B of a structure[1] Σ, we define the residual of B with respect to A relative to cross-cut as an element $R = A : B$ of Σ with the properties

(1.1) $A \supset [A : B, B]$,

(1.2) $A \supset [X, B]$ implies that $A : B \supset X$ for any element X of Σ.

The residual $S = A - B$ of B with respect to A relative to union is defined dualistically by

$$(A - B, B) \supset A,$$

$(X, B) \supset A$ implies that $X \supset A - B$ for any element X of Σ.

The properties of these two operations may be summarized as follows: We define a structure as *residually closed* (relative to cross-cut) if any two elements in it have a residual with the properties (1.1), (1.2). *Every residually closed structure is distributive.*[1] A structure will be said to be *distributively closed*[2] (relative to cross-cut) if given any two sets Θ and Φ of elements of Σ, and the set Γ of all cross-cuts of elements of Θ with elements of Φ, the union of Γ is the cross-cut of the unions of Θ and Φ.

Every distributively closed structure is residually closed.[3] Sufficient conditions that a structure Σ be distributively closed are (i) Σ contains an all element O_0; (ii) Σ is distributive; (iii) the ascending chain condition holds in Σ. Thus every finite distributive structure is residually closed. Similar results hold by duality for residuation with respect to union.

2. The results of a recent paper (Ward [1]) in which I have considered residuation in a structure over which a multiplication is defined which is distributive with respect to union apply to the present case on identifying multiplication with cross-cut. The assumption $(A, B) = A : (A : B)$ analyzed there is a

---

[1] We use the terminology of Ore's recent memoir in these Annals (Ore, [1]), save for the substitution of the term "distributive structure" for Ore's "arithmetic structure," and the interchange of the symbols $(\cdots)$ and $[\cdots]$.

[2] MacNeille [1] uses the term "lattice with completely distributive products."

[3] Compare MacNeille [1] lemma 7.6. MacNeille's "product complement" A' is our "residual of A with respect to E_0."

necessary and sufficient condition that a structure residually closed with respect to cross-cut and containing a unit element E_0 may be a Boolean algebra.

If Σ is a distributive structure containing an all element in which the ascending chain condition holds, then the general decomposition theorems for Dedekind structures become almost trivial (Ore [1] page 415); every element of Σ save O_0 has a unique representation as the cross-cut of a finite number of prime elements none of which divides any other. A very interesting situation arises however if the accompanying structure residuation has any one of the three equivalent properties[4]

$$A : [B, C] = (A : B, A : C),\ (B, C) : A = (B : A, C : A),\ (A : B, B : A) = O_0 .$$

In this case, the primes in the canonical representation of any element as a cross-cut may be chosen relatively prime in pairs. The primes themselves are not necessarily powers of irreducible elements as in common arithmetic, but they may be associated with such powers in a relatively simple manner.

I propose here the name "semi-arithmetical structure (or lattice)" for these systems. A simple example is the set of numbers 1, 2, 3, 6 and 12 with $[\cdots]$ and $(\cdots)$ the L.C.M. and G.C.D. operations. We may remark that *every finite distributive structure may be represented as a finite set of positive integers closed under* L.C.M. *and* G.C.D. I have constructed a proof of this fact by induction; but it is also an immediate consequence of the recent result of Mac Neille's [1] allowing us to imbed any distributive structure in a Boolean algebra. Conversely, it implies Mac Neille's theorem for the case of a finite structure.

II. Properties of Residually Closed Structures

3. We define a structure following Ore as a system Σ of elements $A, B, C, \cdots$ over which there is a well defined division relation $X \supset Y$ such that

Postulate I. $A \supset A$; $A \supset B$ *and* $B \supset C$ *imply* $A \supset C$.

Postulate II. *For each pair of elements* A, B *of* Σ *there exist elements* D *and* M *such that*: $D \supset A, D \supset B$; $S \supset A$, $S \supset B$ *implies* $S \supset D$. $A \supset M$, $B \supset M$; $A \supset T$, $B \supset T$ *implies* $M \supset T$.

If $A \supset B$, $B \supset A$ we write $A = B$. We write $M = [A, B]$ $D = (A, B)$ reversing Ore's usage.

We shall now examine the consequences of assuming

Postulate III. (a). Σ *is residually closed relative to cross-cut*; *or* (b) Σ *is residually closed relative to union.*

Assume III a. Then taking $B = A$ in (1.1), we see that Σ contains an all element $O_0 = A : A$ dividing every other element. Similarly on assuming II b, we see that Σ contains a unit element $E_0 = A - A$ divisible by every other element. Since all properties of residuation relative to union may be obtained

[4] The first two equalities are the third and fourth "distributive laws for residuation" analyzed at length in Ward [1].

by a similar dualizing, we shall confine ourselves to stating results only for residuation relative to cross-cut.

We list here for reference some elementary properties of residuation. We use $\rightarrow$ for "implies that", $\cdots + \cdots$ for "both $\cdots$ and $\cdots$" and $\backsim$ for "implies and is implied by."

(i) $A : B \supset A$.

(ii) $A \supset B \rightarrow A : C \supset B : C + C : B \supset C : A$.

(iii) $A = B \rightarrow A : C = B : C + C : A = C : B$.

(iv) $A \supset B \backsim A : B = O_0$.

(v) $A : A = O_0 + A : O_0 = A$.

(vi) $A : B \supset C \backsim A \supset [B, C]$.

(vii) $A : (A : B) \supset (A, B)$.

(viii) $A : [B, C] = (A : B) : C = (A : C) : B$.

(ix) $A : B = (A : B) : B$.

(x) $[A, B] : B = A : B$.

(xi) $A : B = R \rightarrow R : B = R$.

(xii) If $A : B = A$, then $A \supset [X, B] \backsim A \supset X$.

(xiii) $R = A : B + S = A : R \rightarrow R = A : S$.

(xiv) If $B^{(1)} = B$, $B^{(n+1)} = A : B^{(n)}$, then

$$B^{(2n)} = B^{(2)}, B^{(2n+1)} = B^{(3)}, \qquad (n = 1, 2, 3, \cdots).$$

(xv) $A : B = A : (A, B)$.

(xvi) $(A, B) = O_0 \rightarrow A : B = A$.

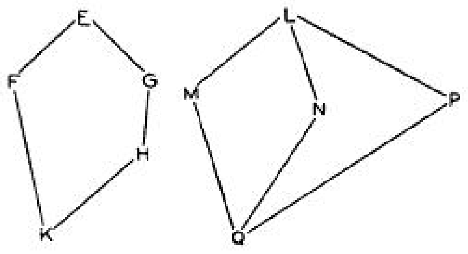
These rules all readily follow from the definition (1.1), (1.2) and postulates I, II, III a. Consider for example (xv). Since $(A, B) \supset B$, $A : B \supset A : (A,B)$ by (ii). By (vii), $A : (A : B) \supset (A, B)$. Therefore by (ii) again, $A : (A, B) \supset A : \{A : (A : B)\}$. But by (xiii), $A : \{A : (A : B)\} = A : B$. Hence $A : (A, B) \supset A : B$ by (iii), giving (xv).

THEOREM 3.1. *If Σ is residually closed relative to cross-cut, then Σ is a distributive structure.*

PROOF. All structures of order less than five are easily seen to be distributive. If Σ is not a Dedekind structure, it is known (Dedekind [1] p. 255) that Σ contains a sub-structure Γ of order five which is not a Dedekind structure. Similarly, if Σ is not distributive but is a Dedekind structure, it contains a sub-structure Λ of order five which is not distributive. (Birkhoff [1] p. 617.) The types of these sub-structures are well known; their lattice diagrams are given in the illustration (see next page). (Klein [1] pp. 222–223).

Suppose that Σ is not a Dedekind structure. Consider the residual $H : G$

of the elements G and H of the sub-structure Γ. Since $H \supset [F, G]$, $H : G \supset F$ by (1.2). Also $H : G \supset H$ by rule (i). Therefore $H : G \supset (H, F)$ or $H : G \supset E$. Then by rule (vi), $H \supset [G, E]$ or $H \supset G$ which is false.



Γ Λ

The structure Σ must therefore be Dedekindian. If it is non-distributive, consider the residual $M : N$ of the elements M and N in the sub-structure Λ. Since $M \supset [N, P]$, $M : N \supset P$ by (1.2). Also $M : N \supset M$ by rule (i). Therefore $M : N \supset (M, P)$ or $M : N \supset L$. Then by rule (vi), $M \supset [N, L]$ or $M \supset N$ which is false.

Hence every structure of order greater than four which is residually closed must be distributive, and the proof is complete.

4. Theorem 3.1 allows us to apply all the results obtained in Ward [1] for residuation in a structure closed with respect to multiplication. For on identifying cross-cut with the multiplication defined there, the three conditions given for a multiplication $X \cdot Y$ are satisfied (Ward [1] section 3); namely

$A \cdot B$ is in Σ if A, B are in Σ; $A \cdot (B \cdot C) = (A \cdot B) \cdot C$; $A \cdot B = B \cdot A$.

$O_0 \cdot A = A$ for every A in Σ.

$A \cdot (B, C) = (A \cdot B, A \cdot C)$.

In particular, if when $B \supset A$ we define the quotient of A by B as an element A/B of Σ such that

$$(4.1) \qquad A = \left[B, \frac{A}{B}\right], \qquad A = [B, X] \text{ implies that } \frac{A}{B} \supset X,$$

it follows that if the quotient A/B exists it equals the residual $A : B$. But more is true; namely

THEOREM 4.1. *If $B \supset A$, the quotient A/B always exists and equals the residual $A : B$.*

PROOF. By (1.1), $A \supset [A : B, B]$. But $B \supset A$ and $A : B \supset A$ by rule (i). Hence $[A : B, B] \supset A$, $A = [A : B, B]$. Also if $A = [B, X]$, $A \supset [B, X]$ so that $A : B \supset X$ by (1.2). Therefore $A : B = A/B$ by the definition (5.1).

We obtain as a corollary the following important rule of manipulation[5]:

$$\text{(xvii)} \qquad B \supset A \backsim A = [A : B, B].$$

[5] We may observe that (xvii) shows that postulate D of Ward [1] is always satisfied in a residually closed structure.

We also have the two "distributive laws" (Ward [1], section III)

$$\text{LI} \qquad M : (A_1, A_2, \cdots, A_n) = [M : A_1, \cdots, M : A_n]$$

$$\text{LII} \qquad [A_1, A_2, \cdots, A_n] : M = [A_1 : M, \cdots, A_n : M].$$

The remaining two distributive laws

$$\text{LIII} \qquad (A_1, \cdots, A_n) : M = (A_1 : M, \cdots, A_n : M)$$

$$\text{LIV} \qquad M : [A_1, \cdots, A_n] = (M : A_1, \cdots, M : A_n)$$

are not generally valid. We shall analyze their meaning and validity when we come to discuss the arithmetical properties of residually closed structures.

A large portion of Ward [1] was devoted to analyzing the consequences of assuming*

POSTULATE C. *If $A \supset B$, there exists an element F such that $A = B : P$.* This assumption was shown to be equivalent to assuming the rule

$$(4.2) \qquad (A, B) = A : (A : B).$$

In case Σ has a unit element E_0, this last rule implies that Σ is a Boolean algebra. For consider $A' = E_0 : A$ for any element A of Σ. We have $(A, A') = A' : (A' : A) = E_0 : A : \{(E_0 : A) : A\} = O_0$ by rules (iii), (iv) and (v). Also since $A \supset E_0$, $[A, A'] = E_0$ by rule (xvii). Finally $(A')' = E_0 : (E_0 : A) = (E_0, A) = A$. Thus A' is the negative of A. Conversely in a Boolean algebra $A : B = (A, B')$ (Dilworth [1]), and (4.2) is easily seen to be satisfied.

III. DISTRIBUTIVELY CLOSED STRUCTURES

5. Let Σ^* denote the class of all sub-sets of elements of Σ. If Θ and Φ are any two such sub-sets, we define $[\Theta, \Phi]$ and (Θ, Φ) to be the least sub-sets containing respectively all elements $[T, F]$ and (T, F), T in Θ, F in Φ. The operations $[\cdots]$ and $(\cdots)$ thus defined over Σ^* are commutative and associative and if Σ contains an all element or a unit element so does Σ^*, but the resulting algebra is not a structure since the operations are obviously not indempotent.

If every element of Θ divides every element of Φ, we write $\Theta \supset \Phi$. If $\Phi \supset \Phi$, $[\Theta, \Phi] = \Phi$, $(\Theta, \Phi) = \Phi$ but not conversely. If Θ consists of a single element T, we write when convenient $\Phi \supset T$, $T \supset \Phi$, $[T, \Phi]$ or (T, Φ) for $\Phi \supset \Theta, \Theta \supset \Phi$, $[\Theta, \Phi]$ or (Θ, Φ).

The assumption that Σ is a closed structure (Ore [1] page 409) may then be formulated by saying that we have two operators u and k defined on Σ^* to Σ such that

$$u\Theta = U; U \supset \Theta; \ X \supset \Theta \text{ implies } X \supset U.$$

$$k\Theta = K; \Theta \supset K; \Theta \supset Y \text{ implies } K \supset Y.$$

6. Let Σ be any closed structure. Then Σ will be said to be *distributively closed* (*relative to cross-cut*) if

$$u[\Theta, \Phi] = [u\Theta, u\Phi]$$

and *distributively closed relative to union if*

$$k(\Theta, \Phi) = (k\Theta, k\Phi)$$

Here Θ, Φ denote any two sub-sets of Σ.

A distributively closed structure of either type is obviously distributive ("arithmetic" is Ore's terminology) in the ordinary sense. A distributively closed structure relative to both union and cross-cut is a $\bar{C}$ lattice in Garrett Birkhoff's terminology (Birkhoff [2]); conversely, it is easily shown that any $\bar{C}$ lattice is a distributively closed structure relative to both union and cross-cut.[6]

The assumption that Σ is distributively closed relative to cross-cut is equivalent to postulate B of Ward [1] on identifying the multiplication $X \cdot Y$ with $[X, Y]$. We accordingly obtain by the argument given in Ward [1] section 4

THEOREM 6.1. *Every structure distributively closed relative to cross-cut is residually closed relative to cross-cut.*

THEOREM 6.2. *Let Σ be a distributive structure containing an all element O_0 in which the ascending chain condition holds. Then Σ is distributively closed relative to cross-cut.*

PROOF. The hypotheses of the theorem imply that Σ is closed relative to union in the ordinary sense. (Ore [1] §2.) Let Θ and Φ be any two sub-sets of Σ with elements $\cdots T_r \cdots ; \cdots F_s \cdots$ and let $\Gamma = [\Theta, \Phi]$. Then $T = u\Theta$, $F = u\Phi$ and $G = u\Gamma$ all exist. We are to prove that $G = [T, F]$. Now (Ore [1]§2) Θ contains k elments $T_1, \cdots, T_k$ such that $T = (T_1, \cdots, T_k)$. Similarly $F = (F_1, \cdots F_l)$ where the F_i are in Φ. Hence since Σ is distributive, $[T, F] = ([T_1, F_1], \cdots [T_k, F_l])$,

Also $G = ([T_{r_1}, F_{s_1}], \cdots, [T_{r_m}, F_{s_m}])$ for Γ is made up of all distinct elements $[T_r, F_s]$. Hence since $T \supset \Theta$, $F \supset \Phi$, $[T, F] \supset [T_{r_i}, F_{s_i}]$ or $[T, F] \supset G$. Also since $G \supset [T_r, F_s]$, $G \supset ([T_1, F_1], \cdots [T_k, F_l])$ or $G \supset [T, F]$. Thus $G = [T, F]$.

COROLLARY. *Every distributive structure of finite order is residually closed.*

IV. Arithmetical Properties of Residually Closed Structure

7. Let Σ be any structure. An element $Q \neq O_0$ of Σ is said to be: (i) *irreducible* if $X \supset Q$ implies $X = O_0$ or $X = Q$; (ii) *prime* if $Q \supset [X, Y]$ implies $Q \supset X$ or $Q \supset Y$; (iii) *indecomposable* if $Q = [X, Y]$ implies $Q = X$ or $Q = Y$; (iv) a *power* if it has precisely one irreducible divisor. Every irreducible is

---

[6] MacNeille [1] calls such a structure a "completely distributive lattice," and proves the independence of distributive closure with respect to union and distributive closure with respect to cross-cut.

indecomposable, and in a distributive structure every irreducible is a prime. (Köthe [1].)

For the remainder of the paper we assume postulate III a and a chain condition:

POSTULATE IV. *The ascending chain condition holds in* Σ

Then as is well known every element A of $\Sigma \neq O_0$ admits of at least one decomposition:

$$(7.1) \qquad A = [Q'_1, Q'_2, \cdots, Q'_l]$$

into a cross-cut of a finite number of indecomposable elements Q' of Σ.

By theorem 3.1, Σ is distributive and hence Dedekindian. Now Σ contains O_0 and hence by the ascending chain condition at least one irreducible P. If P' is any power of the irreducible P, we define the "multiplicity" of P' as the length of any principal chain (Ore [1] page 411) $P > \cdots > P'$ joining P and P' increased by unity. Then every power of P has a unique finite multiplicity, and P itself is of multiplicity unity. It is convenient to consider the all element O_0 as the unique power of P of multiplicity zero. The following lemmas are obvious from this definition:

LEMMA 7.1. *If R and S are both powers of P and $R \supset S$, $R \neq S$ then the multiplicity of R is less than the multiplicity of S.*

LEMMA 7.2. *The powers of any irreducible form a dense sub-structure of* Σ.

Now let A be any element of $\Sigma \neq O_0$. Then by the chain condition, A has at most a finite number of irreducible divisors $P_1, P_2, \cdots P_k$ and for each irreducible P_i there is a power P'_i of the highest positive multiplicity which divides A. Then the element $[P'_1, P'_2, \cdots, P'_k]$ is a divisor of A which we call a *kernel* of A.

THEOREM 7.1. *Every element of Σ has exactly one kernel.*

PROOF. Assign to O_0 the kernel O_0. If $A \neq O_0$, A has at least one kernel by the argument above. Let P' and P'' be powers of the irreducible divisor P of A of maximum multiplicity m dividing A. It suffices to show that $P' = P''$. Let $P^* = [P', P'']$. Then $P^* \supset A$ and P^* is a power of P by lemma 7.2. If $P^* \neq P'$ then since $P' \supset P^*$, the multiplicity of P^* is greater than m by lemma 8.1. Hence $P^* = P'$. Similarly, $P^* = P''$, $P' = P''$.

We denote the kernel of any element A of Σ by θA. If $A = \theta A$, A will be said to be *regular*. Thus all powers are regular. Operations on kernels are governed by the following simple rules:

$$(7.1) \qquad A \supset B \text{ implies that } \theta A \supset \theta B.$$

$$(7.2) \qquad \theta A = O_0 \text{ if and only if } A = O_0.$$

$$(7.3) \qquad \theta(A, B) = (\theta A, \theta B),\ \theta[A, B] = [\theta A, \theta B].$$

$$(7.4) \qquad \theta\theta A = \theta A.$$

The converse of rule (7.1) is generally false. It is obvious from (7.3) that we have:

THEOREM 7.2. *The set of all regular elements of Σ forms a sub-structure of Σ.*

THEOREM 7.3. *The set of all elements of Σ with the same kernel forms a sub-structure of Σ.*

THEOREM 7.4. *If A is regular and $B \supset A$, then B is regular.*

PROOF. We observe that if P' is any power of P and M any element of Σ, then it follows from lemma 7.2 that $P'' = (M, P')$ is also a power of P. Assume that $B \supset A$, A regular. Then

$$B = (B, A) = (B, \theta A) = (B, [P'_1, \cdots, P'_k])$$
$$= [(B, P'_1), \cdots (B, P'_k)] = [P''_1, \cdots P''_k].$$

Hence by rule (7.3) $\theta B = \theta[P''_1, \cdots P''_k] = [\theta P''_1, \cdots \theta P''_k] = [P''_1, \cdots, P''_k] = B$.

Thus the sub-structure of all kernels of Σ is dense over Σ. (Ore [1], page 429).

8. So far no direct use has been made of postulate III a. It is obvious that the sub-structure of all regular elements and the sub-structure of all powers of any irreducible element are residually closed since the structures are dense over Σ and $A : B \supset A$ by rule (i) for residuation. Let A be any indecomposable element of Σ, B any other element of Σ. Then if $A \supset B$, $A : B = O_0$ by rule (iv) and conversely. If $A \not\supset B$, $A : B = A : D$ where $D = (A, B)$ by rule (xv). Then by rule (xvii), $A = [A : D, D]$ Hence $A : D = A$. We therefore have

THEOREM 8.1. *If A is indecomposable, then $A : X = A$ or O_0 for every element X of Σ.*

THEOREM 8.2. *An element of Σ is a prime if and only if it is indecomposable.*

PROOF. Assume that A is indecomposable, $A \supset [B, C]$, $A \not\supset B$. We are to show that $A \supset C$. Since $A \not\supset B$, $A : B = A$ by theorem 8.1. But $A \supset [B, C]$ implies $A : B \supset C$ by (1.2) Hence $A \supset C$. The converse is trivial.

The following two theorems are immediate corollaries.

THEOREM 8.3. *Let A and B be any two elements of Σ with decompositions as in (7.1) $A = [Q'_1, \cdots Q'_l]$, $B = [Q''_1, \cdots, Q''_k]$ into cross-cuts of indecomposable elements. Then a necessary and sufficient condition that $B \supset A$ is that every Q'' should divide at least one Q'.*

THEOREM 8.4 "DECOMPOSITION THEOREM". *Let A be any element of $\Sigma \neq O_0$. Then A admits of a decomposition*

$$A = [Q_1, Q_2, \cdots, Q_l]$$

into a cross-cut of a finite number of indecomposable elements Q such that no Q_i divides a Q_j unless $i = j$. This decomposition is unique save for the order in which the factors Q are written.

Theorem 8.1 was recently proved in a different manner by Birkhoff (Birkhoff [3], page 452).

The following theorem will be useful subsequently.

THEOREM 3.5. *If A and B are any two primes of Σ, then one and only one of the following conditions hold:*

$$\text{(i) } (A, B) = A, \qquad \text{(ii) } (A, B) = B, \qquad \text{(iii) } (A, B) = (A : B, B : A).$$

V. Semi-Arithmetical Structures

9. We shall now develop the consequences of assuming

Postulate V. *If M and N are any two elements of Σ, then*

$$(M : N, N : M) = O_0 .$$

A system satisfying postulates I, II, III a, IV and V will be called a "semi-arithmetical" structure.

Theorem 9.1. *In a residually closed structure, either the third or the fourth distributive law for residuation implies postulate V.*

Proof. We may take the third and fourth laws in the abbreviated forms

L III $$(A, B) : M = (A : M, B : M),$$

L IV $$M : [A, B] = (M : A, M : B),$$

the general forms in section 4 following by an easy induction. Assume L III. Then by rules (v) and (xv), $O_0 = (M, N) : (M, N) = (M : (M, N), N : (M, N) = (M : N, N : M)$. Assume L IV. Then by rules (v) and (x),

$$O_0 = [M, N] : [M, N] = ([M, N] : M, [M, N] : N) = (N : M, M : N).$$

Theorem 9.2. *In a semi-arithmetical structure, the powers of any irreducible form an ordered structure.*

Proof. If P' and P'' are powers of P, $P' : P''$ and $P'' : P'$ are both powers of P But $(P' : P'', P'' : P') = O_0$. Hence either $P' : P'' = O_0$ or $P'' : P' = O_0$, so that by rule (iv), either $P' \supset P''$ or $P'' \supset P'$.

Theorem 9.3. *In a semi-arithmetical structure, all primes with the same kernel form an ordered structure.*

Proof. Let A and B be primes, $\theta A = \theta B = Q \neq O_0$. Then $Q \supset A$, $Q \supset B$ so that $Q \supset (A, B)$. Hence $(A, B) \neq O_0$. But by theorem 8.5 and postulate V, either $(A, B) = A$ or $(A, B) = B$ or $(A, B) = O_0$. Hence either $A \supset B$ or $B \supset A$.

Theorem 9.4. *In a semi-arithmetical structure, if A and B are primes and $\theta A \neq \theta B$, $A \supset B$ if and only if $\theta A \supset \theta B$.*

Proof. Assume that $\theta A \neq \theta B$ and $\theta A \supset \theta B$. Then $\theta(A, B) = (\theta A, \theta B) = \theta A \neq O_0$. But $\theta(A, B) \supset (A, B)$. Hence $(A, B) \neq O_0$. Therefore as in theorem 9.3 either $A \supset B$ or $B \supset A$. If $B \supset A$, $\theta B \supset \theta A$, $\theta B = \theta A$ contrary to hypothesis. Hence $A \supset B$. The converse is trivial.

Theorem 9.5. *Let T be any regular element of Σ. Then the structure Θ of all primes with the kernel T is dense over Σ.*

Proof. By theorem 9.3, Θ is ordered. Suppose that $A \supset X \supset B$, A, B in Θ, X in Σ. Then $\theta X = T$ by rule 7.1. By the decomposition theorem, $X = [C_1, C_2, \cdots C_t]$, $t \geqq 1$, where each C_i is a prime and divides no other C_j, $i \neq j$. Since $A \supset X$, A divides some C_i. Assume that $A \supset C_1$. Then since $C_1 \supset X$, $\theta C_1 = T$. But since $C_t \supset X$, $\theta C_t \supset \theta X$ or $\theta C_t \supset \theta C_1$ by rule (7.1). Thus by theorem 9.4 either $C_t \supset C_1$ or $\theta C_t = T$. In the latter case, either $C_t \supset C_1$ or $C_1 \supset C_t$ by theorem 9.3. Thus in either case, $t = 1$ and X is a prime.

It follows that any set of prime elements with the same kernel form a principal chain.

We say that two elements R and S of Σ are relatively prime if $(R, S) = O_0$. The following theorem is now obvious:

THEOREM 9.6. *Every element $A \neq O_0$ of a semi-arithmetical structure may be uniquely represented save for order as the cross-cut of a finite number of prime elements which are relatively prime in pairs.*

THEOREM 9.7. *In a semi-arithmetical structure the third distributive law for residuation always holds; that is for any three elements A, B of Σ*

L III $$(A, B) : C = (A : C, B : C)$$

PROOF. The law is obviously true if either A or B is O_0. We next show it is true if A and B are primes Q and R. For then either (i) $(Q, R) = O_0$, or (ii) $(Q, R) = Q$ or (iii) $(Q, R) = R$. (i). If $(Q, R) = O_0$, $(Q, R) : C = O_0$. But then $(Q : C, R : C) = O_0$. For either $Q : C = O_0$, or $R : C = O_0$, or $Q : C = Q$ and $R : C = R$. Hence $(Q, R) : C = (Q : C, R : C)$ in this case. (ii). If $(Q, R) = Q$, then $(Q, R) : C = Q : C$. Hence if $Q : C = O_0$, $(Q, R) : C = (Q : C, R : C)$. If $Q : C = Q$, then $R : C = R$. For if $R : C = O_0$, $R \supset C$ But since $(Q, R) = Q$, $Q \supset R$, $Q \supset C$ and $Q : C = O_0$. Thus if $Q : C = Q$, $(Q : C, R : C) = (Q, R) = Q = (Q, R) : C$. In (iii) the proof is similar.

If A and B are not primes, let their canonical decompositions be

$$A = [\cdots, Q, \cdots], B = [\cdots, R, \cdots].$$

Then by the second distributive law for residuation

$$\begin{aligned}
(A : C, B : C) &= ([\cdots, Q, \cdots] : C, [\cdots, R, \cdots] : C) \\
&= ([\cdots, Q : C, \cdots], [\cdots, R : C, \cdots]) \\
&= [\cdots, (Q : C, R : C), \cdots] \\
&= [\cdots, (Q, R) : C, \cdots] \\
&= [\cdots, (Q, R), \cdots] : C \\
&= ([\cdots, Q, \cdots], [\cdots, R, \cdots]) : C \\
&= (A, B) : C.
\end{aligned}$$

In like manner we may prove

THEOREM 9.8. *In a semi-arithmetical structure, the fourth distributive law for residuation always holds.*

On combining theorems 9.1, 9.7 and 9.8, 6.1 and 6.2 we obtain

COROLLARY. *Either the third distributive law for residuation, the fourth distributive law for residuation or postulate V is a necessary and sufficient condition* *that a distributive structure containing an all element in which the ascending chain condition holds may be a semi-arithmetical structure.*

Let us call a structure "arithmetical" if the only prime elements in it are powers of irreducibles. (Arithmetical structures have been exhaustively investigated by F. Klein who calls them "Sternverbande" (Klein [2])). We see then that an arithmetical structure is simply a semi-arithmetical structure in which all elements are regular, or in which the only primes are powers of irreducible elements.

REFERENCES

G. Birkhoff:

1. Bulletin Am. Math. Soc. vol 40 (1934), pp. 613–619.
2. Proc. Cambr. Phil. Soc. vol. 29 (1933), pp. 441–464.
3. Duke Math. Journal, vol. 3, Sept. (1937), pp. 443–454.

R. Dedekind: 1. Collected Works (1931), vol. II, paper 30, pp. 236–271.

R. P. Dilworth: 1. Bulletin Am. Math. Soc., vol. 44 (1938), pp. 262–268.

F. Klein:

1. Deutsche Math., vol. 2 (1937), pp. 216–241.
2. Math. Annalen., vol. 106 (1932), pp. 114–134.

G. Köthe: Deutsche Math. Verein, '37, pp. 125–144.

H. M. MacNeille: 1. Trans. Am. Math. Soc., vol. 42, November 1937, pp. 416–460.

O. Ore: 1. These Annals (2), vol. 36 (1935), pp. 406–432.

M. Ward: 1. Duke Math. Journal, vol. 3, December (1937), 627–636.

California Institute of Technology.