RINGS OF SETS

By Garrett Birkhoff

1. **Definitions.** Following Hausdorff,[1] a family $\mathfrak{F}$ of subsets of a class I is said to form a "ring" if and only if it contains, with any two sets[2] S and T, their *sum* (or union) $S \cup T$ and their *product* (or intersection) $S \cap T$. Clearly a ring contains, with any finite number of subsets $S_1, \cdots, S_n$, their sum $S_1 \cup \cdots \cup S_n$ and their product $S_1 \cap \cdots \cap S_n$.

The family $\mathfrak{F}$ is said to constitute a "complete ring" if and only if it contains, with any subfamily $\mathfrak{S}$ of sets S_α, their sum $\underset{\alpha \in \mathfrak{S}}{V} S_\alpha$ and their product $\underset{\alpha \in \mathfrak{S}}{\Lambda} S_\alpha$. The family $\mathfrak{F}$ is also said to be a "σ-ring" if and only if it contains, with any *countable* subfamily $\mathfrak{S}$ of sets S_α, their sum $\underset{\alpha \in \mathfrak{S}}{V} S_\alpha$ and their product $\underset{\alpha \in \mathfrak{S}}{\Lambda} S_\alpha$.

It is obvious that rings containing only a finite number of sets, and σ-rings containing only a countable number of sets, are necessarily complete rings. These theorems can be improved by using chain conditions; however, the family $\mathfrak{C}$ of all finite sets of integers is a countable ring which is not a σ-ring (and a fortiori not complete), while the family $\mathfrak{D}$ of all countable subsets of the continuum is a σ-ring which is not complete.

2. **The importance of the subject.** Rings of sets are mathematically important for a number of reasons. They are conceptually important because one can define them so simply in terms of two fundamental operations. They are also important because the sets of any class I carried within themselves by any one-valued transformation of I into itself are a complete ring. (The proof of this will be left to the reader.) Also, as is well known, the open and closed subsets of any topological space constitute rings, and the measurable subsets of any Cartesian n-space constitute a σ-ring.

Again, the reader will immediately see that

(2α) The sets common to all the rings (resp. σ-rings or complete rings) of any aggregate of rings of subsets of any class I themselves form a ring (resp. σ-ring or complete ring).

It follows that the closed subsets of any topological space Σ invariant under any group of transformations constitute a ring. The study of these rings is important in dynamics,[3] where, however, the existence of minimal closed and connected constituents introduces special considerations. It follows also that

Received January 16, 1937.

[1] *Mengenlehre*, 1927 (2d ed.), p. 77.

[2] We shall systematically use small Latin letters to denote elements, Latin capitals to denote sets of elements, and German capitals to denote families of sets.

[3] Especially in the theory of so-called "central motions". Cf. G. D. Birkhoff, *Dynamical Systems*, 1927, Chap. VII, §6 ff.

the subsets of any class I carried within themselves under any aggregate A of one-valued transformations τ_α of I into itself form a complete ring.

Moreover, all complete rings of sets belong to at least one aggregate A of transformations in this way. More precisely, any complete ring $\mathfrak{R}$ of sets belongs to the "groupoid"[4] of all one-valued transformations carrying every $S \in \mathfrak{R}$ into itself. This shows that rings of sets play the same rôle in the theory of groupoids of one-valued transformations as is played by transitivity and intransitivity in the theory of groups of permutations (one-one transformations).[5]

3. **Equivalent notions.** If we add the empty set O and the all-set I to any complete ring of subsets of a class I, we still have a complete ring. Hence the theory of rings of sets is contained in that of rings containing O and I.

THEOREM 1. *The complete rings of subsets of I which contain O and I can be identified with the different quasi-orderings of I or with the different completely distributive topologies on I.*

Explanation 1. By a "quasi-ordering" of I is meant a binary relation $x \geqq y$ satisfying

P1: $x \geqq x$ (reflexiveness),

P2: $x \geqq y$ and $y \geqq z$ imply $x \geqq z$ (transitivity).

By a "completely distributive topology" is meant a unary operation $S \to \bar{S}$ (called closure) on the subsets of I which satisfies

C1: $\bar{S} \geqq S$, C2: $\bar{O} = O$, C3: $\bar{\bar{S}} = \bar{S}$;

C4: if $S = \underset{\alpha}{V} S_\alpha$, then $\bar{S} = \underset{\alpha}{V} \bar{S}_\alpha$.

(These are related to well-known axioms of Hausdorff on "partial ordering", and of Riesz-Kuratowski on closure.)

Explanation 2. By an "identification" we mean a one-one correspondence preserved under all permutations of the elements of I. It follows that if we call two families of sets of I resp. two relations on I resp. two operations in I "equivalent" if and only if there exists a permutation of the elements of I carrying one into the other, then the numbers of non-equivalent rings of sets, of non-equivalent quasi-orderings, and of non-equivalent completely distributive

[4] A family G of one-valued transformations of I into itself is termed a "groupoid" if and only if it contains the identity $\iota: x \to x$ and the product $\sigma\tau: x \to \tau[\sigma(x)]$ of any two of its members σ and τ. The author is preparing an article on groupoids in collaboration with S. Ulam.

[5] The sets invariant (i.e., the sets identical with, and not merely supersets of, their transforms) under any permutation or set of permutations constitute a "complete field"—i.e., a complete ring which contains, with any set, its complement. Moreover, any complete field belongs to the group of all transformations leaving its subsets invariant ("intransitive" on its subsets)—this leads to the usual partial descriptions of groups of permutations through their "transitive systems".

Actually, in the case of *groups* of permutations of I, any subset carried within itself under all their permutations is necessarily invariant.

topologies on I are the same—as well as the numbers of distinct complete rings of sets, of distinct quasi-orderings, and of distinct completely distributive topologies.

Proof of theorem. Let $\mathfrak{R}$ be any complete ring of sets containing O and I. Make the definitions: (1) $x \geqq y$ $(\mathfrak{R})$ means that every $S \in \mathfrak{R}$ containing x contains y, and (2) $\bar{S}$ is the product of all sets $T_\alpha \in \mathfrak{R}$ containing S. That the relation and operation so introduced satisfy P1–P2 and C1–C2 is obvious; it is also obvious that the correspondence between them and $\mathfrak{R}$ is preserved under all permutations of the elements of I.

To prove C3–C4, recall that, since $\mathfrak{R}$ is a complete ring, $\bar{S}$ is the least set in $\mathfrak{R}$ containing S. This proves C3 and

(3α) $S \in \mathfrak{R}$ if and only if $S = \bar{S}$.

Now suppose $S = \underset{\alpha}{V} S_\alpha$. Clearly $S \geqq S_\alpha$ irrespective of α; hence $\bar{S} \geqq \underset{\alpha}{V} \bar{S}_\alpha$. But conversely $\underset{\alpha}{V} \bar{S}_\alpha \in \mathfrak{R}$, since $\mathfrak{R}$ is a complete ring, and $\underset{\alpha}{V} \bar{S}_\alpha \geqq \underset{\alpha}{V} S_\alpha = S$; hence $\underset{\alpha}{V} \bar{S}_\alpha \geqq \bar{S}$. This proves C4.

It remains to prove that *every* quasi-ordering and *every* completely distributive topology belong to such an $\mathfrak{R}$, and that distinct $\mathfrak{R}$ determine distinct quasi-orderings and distinct topologies—four assertions in all.

By (3α), if $\mathfrak{R} \neq \mathfrak{R}'$, then certainly $\mathfrak{R}$ and $\mathfrak{R}'$ yield distinct topologies. This proves one assertion. We next wish to prove that

(3β) *Every* completely distributive topology is determined by a suitable $\mathfrak{R}$.

Under any such topology, consider the family $\mathfrak{F}$ of "closed" sets $S = \bar{S}$. Clearly $\mathfrak{F}$ contains O, I, and (by C4) $\underset{\alpha}{V} S_\alpha$ if it contains every S_α. But it also contains $\underset{\alpha}{\Lambda} S_\alpha$ under the same hypotheses.

Proof. If $\bar{S}_\alpha = S_\alpha$ for every α, then $\underset{\alpha}{\Lambda} \bar{S}_\alpha = \underset{\alpha}{\Lambda} S_\alpha$, and so $\overline{(\underset{\alpha}{\Lambda} S_\alpha)} \leqq S_\alpha$ for all S_α, whence $\overline{(\underset{\alpha}{\Lambda} S_\alpha)} \leqq \underset{\alpha}{\Lambda} \bar{S}_\alpha = \underset{\alpha}{\Lambda} S_\alpha$, and so by C1 $\underset{\alpha}{\Lambda} S_\alpha$ is closed. Hence $\mathfrak{F}$ is a complete ring of sets with O and I. Moreover, if S is any set, then $\bar{S}$ is the product of the $T_\alpha \in \mathfrak{F}$ containing S—by Cl, $\underset{\alpha}{\Lambda} T_\alpha = \underset{\alpha}{\Lambda} \bar{T}_\alpha \geqq \bar{S}$, and, by C1–C3, $\bar{S}$ is a closed set $T_\alpha \geqq S$. Thus $\mathfrak{F}$ "determines" the given topology. This proves (3β).

Again, if $\mathfrak{R}$ is given, then

(3γ) $S \in \mathfrak{R}$ if and only if $x \in S$ and $x \geqq y$ $(\mathfrak{R})$ imply $y \in S$.

Proof. If $S \in \mathfrak{R}$, by definition the second statement holds. Conversely if the second statement holds, then S contains, with every x, the set $S(x)$ of all $y \leqq x$ $(\mathfrak{R})$—i.e., the product of the $S_\alpha \in \mathfrak{R}$ with $x \in S_\alpha$; obviously $S(x) \in \mathfrak{R}$—and so S is the sum $VS(x)$ of the $S(x)$ of the $x \in S$, and is in $\mathfrak{R}$. By (3γ), if $\mathfrak{R} \neq \mathfrak{R}'$, then $\mathfrak{R}$ and $\mathfrak{R}'$ determine different quasi-orderings.

Finally, every quasi-ordering ρ is determined by some $\mathfrak{R}$. For, given ρ, let $\mathfrak{R}(\rho)$ consist of all S such that $x \in S$ and $x \geqq y$ imply $y \in S$. Clearly $O \in \mathfrak{R}(\rho)$ and $I \in \mathfrak{R}(\rho)$. Also, if a family $\mathfrak{S}$ of S_α is in $\mathfrak{R}(\rho)$, then $(VS_\alpha) \in \mathfrak{R}(\rho)$ and

$(\Lambda S_\alpha) \in \mathfrak{R}(\rho)$. Thus $\mathfrak{R}(\rho)$ is a complete ring of sets containing O and I. Further, if $x \geqq y$, then obviously $x \geqq y$ $(\mathfrak{R}(\rho))$ in the sense that $x \in S \in \mathfrak{R}(\rho)$ and $x \geqq y$ imply $y \in S$. Conversely if $x \geqq y$ $(\mathfrak{R}(\rho))$, then the set $S(x)$ of all $z \leqq x$ (which is in $\mathfrak{R}(\rho)$ by P2 and contains x by P1) contains y—by definition of $x \geqq y$ $(\mathfrak{R}(\rho))$—and so $x \geqq y$. This proves the fourth assertion.

4. **The case of fields of sets.** Which quasi-orderings and which completely distributive topologies correspond to complete fields[6] of sets? And what does this make Theorem 1 reduce to for fields of sets?

THEOREM 2. *In Theorem* 1, *a quasi-ordering corresponds to a (complete) field of sets if and only if it is an equivalence relation; a topology does, if and only if the closures of its points are the subsets of a partition of* I.

Explanation. By an "equivalence relation" is meant a quasi-ordering which satisfies

P3′: $x \geqq y$ implies $y \geqq x$.

By a "partition" of a class I is meant a division of its elements into disjoint subsets, whose sum is I.

Proof. Let $\mathfrak{R}$ be a complete ring of sets, and let $S(x)$ be the product of the sets $S_\alpha \in \mathfrak{R}$ containing x. Then $x \geqq y$ $(\mathfrak{R})$ means $y \in S(x)$. If $\mathfrak{R}$ is a field, and $y \in S(x)$, then the complement $S'(y)$ of $S(y)$ cannot contain x—otherwise $x \in S'(y) \cap S(x) \leqq S(x) - y < S(x)$—and so $y \in S(x)$ implies $x \in S(y)$. This proves P3′. Again, topologically, $S(x)$ is the closure of x. Hence if $\mathfrak{R}$ is a field, unless $S(x)$ and $S(y)$ are disjoint, $S(x) \cap S(y)$ contains some point z, and $x \geqq z$ and $y \geqq z$, whence by P2 and P3′ $x \geqq y$ and $y \geqq x$, and therefore $S(x) = S(y)$.

Conversely, if P3′ holds, and $\mathfrak{R}$ is the family of sets S such that $x \in S$ and $y \leqq x$ imply $y \in S$, then $S \in \mathfrak{R}$ implies that x not in S and $y \leqq x$ imply y not in S (otherwise $y \in S$ and $x \leqq y$ by P3′), whence $S' \in \mathfrak{R}$ and $\mathfrak{R}$ is a field. The fact that the sums of the parts of any partition of I are a complete field of sets is obvious.

COROLLARY.[7] *The complete fields of subsets of* I *which contain* O *and* I *can be identified with the different equivalences on* I *or with the different partitions of* I.

5. **Rings of sets and distributive lattices.** We shall deal below with rings of sets without assuming completeness.

Suppose we consider rings of sets simply as collections of symbols (forgetting that the symbols denote sets of points) related by inclusion, addition and multiplication. Then any ring of sets appears as a "distributive lattice", or system $\mathfrak{R}$ of elements S, T, U satisfying[8]

[6] A (complete) ring of sets is called a (complete) field if and only if it contains the complement of every one of its members.

[7] Part of this result is proved by H. Hasse, *Höhere Algebra*, vol. I, 1933, p. 15, and B. L. van der Waerden, *Moderne Algebra*, p. 14.

[8] Cf. the author's *On the structure of abstract algebras*, Proc. Camb. Phil. Soc., vol. 31

L1: $S \cap S = S$ and $S \cup S = S$.

L2: $S \cap T = T \cap S$ and $S \cup T = T \cup S$.

L3: $(S \cap T) \cap U = S \cap (T \cap U)$ and $(S \cup T) \cup U = S \cup (T \cup U)$.

L4: $S \cap (S \cup T) = S \cup (S \cap T) = S$.

L6: $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$ and

$$S \cap (T \cup U) = (S \cap T) \cup (S \cap U).$$

Moreover, two rings of sets seem indistinguishable when and only when they are "isomorphic"—i.e., admit a one-one correspondence preserving inclusion, sums and products.[9]

Conversely, every abstractly given distributive lattice is known to be obtainable from at least one ring of sets.[10]

6. **Representation theory for distributive lattices.** It is generally true in representation theories for abstract algebras that one gets the simplest results by considering homomorphic (many-one) as well as isomorphic (one-one or "true") representations.

A full representation theory for Boolean algebras by fields of sets has been developed by Stone,[11] and it is interesting to see the complications which arise in the more general case of distributive lattices. These show that the assumption that complements exist cannot be eliminated in Stone's theory.

First, let $\mathfrak{R}$ be any distributive lattice, and let θ be any congruence relation[12] on $\mathfrak{R}$. Then the elements congruent to O form an "ideal" $\mathfrak{O}$ in the sense that

I1: $X \in \mathfrak{O}$ and $A \in \mathfrak{R}$ imply $A \cap X \in \mathfrak{O}$.

I2: $X \in \mathfrak{O}$ and $Y \in \mathfrak{O}$ imply $X \cup Y \in \mathfrak{O}$.

In case $\mathfrak{R}$ is a Boolean algebra, $\mathfrak{O}$ determines θ, but this is not generally true in distributive lattices.

Proof. With Boolean algebras, S and T are congruent mod θ if and only if $(S \cap T') \cup (S' \cap T) \in \mathfrak{O}$, whereas O is an ideal in the chain of three elements $I > X > O$, determined by two distinct congruence relations.

(1935), pp. 433–454. O. Ore calls distributive lattices "arithmetic structures". Considerable work has been done by Fritz Klein on the decomposition of distributive lattices important in number theory; M. Ward has also given categorical definitions of such systems.

[9] Actually, any one-one correspondence preserving any one of these three preserves all; this is not true of many-one correspondences.

[10] Cf. the author's *On the combination of subalgebras*, Proc. Camb. Phil. Soc., vol. 29 (1933), pp. 441–464, Theorem 25.2.

[11] M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc., vol. 40 (1936), pp. 37–111. By a "representation" of a distributive lattice L, we mean a homomorphism between L and a ring of sets.

[12] I.e., any partition of the elements of $\mathfrak{R}$ determining an abstract homomorphism. This is a basic notion of general abstract algebra, whose detailed definition we shall omit.

Again, let $\mathfrak{R}$ be any distributive lattice, and A any element of $\mathfrak{R}$. The relation $X \cong Y \bmod A$ meaning $X \cup A = Y \cup A$ is a congruence relation.

Proof. That it is an equivalence relation is obvious. Moreover, by L1–L6,

$$(X \cup Y) \cap A = (X \cup A) \cup (Y \cup A),$$
$$(X \cap Y) \cup A = (X \cup A) \cap (Y \cup A);$$

hence the correspondence $X \to X \cup A$ defines a homomorphism of $\mathfrak{R}$ onto a subring of itself.

If $\mathfrak{R}$ is a finite Boolean algebra, there are no other congruence relations on $\mathfrak{R}$; this is not true for finite distributive lattices which are not Boolean algebras (proof omitted).

7. **Prime ideals.** Let us now suppose that R is any distributive lattice, and let us attempt to give a full representation theory for R.

Let θ: $R \to \mathfrak{R}$ be any homomorphism from R to a ring of subsets of a class I. We may classify the points of I into three categories: those contained in every set $X \in \mathfrak{R}$, those contained in no set $X \in \mathfrak{R}$, and the others. The first two categories of points are trivial, and so we can assume that $O \in \mathfrak{R}$ and $I \in \mathfrak{R}$.

Under these circumstances, every $p \in I$ divides the elements of R into two categories: those corresponding to sets including p, and those corresponding to sets excluding p. The second set of elements is an "ideal", while the first is a "dual ideal" D in the sense that

D1: $x \in D$ and $a \in R$ imply $a \cup x \in D$.

D2: $x \in D$ and $y \in D$ imply $x \cap y \in D$.

Hence the representation of R through $\mathfrak{R}$ is characterized to within equivalence[13] by which divisions of R into an ideal and complementary dual ideal occur, and how many times each occurs.

But conversely, by I1–I2 and D1–D2, if one is given any correspondence associating each division π of R into an ideal J and complementary dual ideal D with a cardinal number $n(\pi)$, then this belongs to a representation of R by a ring of sets, and so if we define (with Stone, op. cit.) an ideal to be "prime" if and only if its complement is a dual ideal, we have

THEOREM 3. *The inequivalent representations of a given distributive lattice R as a ring of sets are the different functions whose arguments are the "prime ideals" of R, and whose values are cardinal numbers.*

Remark 1. With Boolean algebras, the number of elements in any prime ideal and its dual are the same. Also, no prime ideal contains any other prime ideal. Neither of these properties is true in distributive lattices not Boolean algebras (e.g., the chain $I > X > O$).

[13] I.e., to within differences between the various points $p \in I$. This is standard terminology.

Remark 2. It is natural to call a representation "irredundant" if and only if no prime ideal appears as a point more than once.

8. **The finite case.** Only exceptionally are the prime ideals of infinite Boolean algebras known. But in each finite Boolean algebra of order 2^n they are known to be n sublattices of order 2^{n-1}.

We shall go further and determine the prime ideals of all finite distributive lattices.

Accordingly, let R be any finite distributive lattice, P any prime ideal in R, and $D = R - P$ the dual of P. Form any connected chain[14] $O < x_1 < x_2 < \cdots < x_r = I$ in R; it is clear that in such a chain there will be exactly one "link" $x_i < x_{i+1}$ such that $x_i \in P$ and $x_{i+1} \in D$, and that $x_k \in P$ for $k \leqq i$, while $x_k \in D$ for $k > i$.

(8α) We have $y \in P$ or $y \in D$ according as $v \equiv x_i \cup (y \cap x_{i+1}) = (x_i \cup y) \cap x_{i+1}$ is x_i or x_{i+1}.

Proof. Since $x_i \leqq x_{i+1}$, $x_i \cup (y \cap x_{i+1}) = (x_i \cup y) \cap x_{i+1}$ (by L6 and contraction). Again, for any y, obviously $x_i \leqq v \leqq x_{i+1}$; hence either $v = x_i$ or $v = x_{i+1}$ (no further interpolation being possible). But if $[x_i \cup (y \cap x_{i+1})] = x_i \in P$, then by I1 $(y \cap x_{i+1}) \in P$, and so by D2 (since $x_{i+1} \in D$), $y \in P$. Similarly, if $x_i \cup (y \cap x_{i+1}) = x_{i+1} \in D$, then by I2 (since $x_i \in P$), $y \cap x_{i+1} \in D$, and so by D1, $y \in D$.

Definition. By a "prime factor" of a distributive lattice is meant any symbol x/y, where $y < x$ and no element can be interpolated between y and x. A prime factor x/y will be called a "cleavage" for a given prime ideal P if and only if $y \in P$ and $x \in (R - P)$.

(8β) Any prime factor a/b is a cleavage for some prime ideal.

Proof. Let $x \in P$ if and only if $(b \cup x) \cap a = b$; this makes $x \in (R - P)$ if and only if $(b \cup x) \cap a = a$, since for all x, $b \leqq (b \cup x) \cap a = b \cup (x \cap a) \leqq a$, and a/b is prime. Clearly $a \in (R - P)$ and $b \in P$ (by L4). It remains to prove I1–I2 and D1–D2. But I1 and D1 are obvious, since $(b \cup x) \cap a$ is decreased resp. increased by substituting $x \cap y$ resp. $x \cup y$ for x. Moreover, under the hypotheses of I2,

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

This proves I2. The proof of D2 is dual.

THEOREM 4. *Let R be any finite distributive lattice, and let its prime ideals be $P_1, \cdots, P_r$. Then in every connected chain $O < x_1 < \cdots < x_r = I$, each x_{i+1}/x_i is a cleavage for just one P_i—whence $r = n$.*

Proof. By (8α), if $P_i \neq P_j$, they can have no cleavage in common, and by (8β), every prime factor is a cleavage for some P_i.

We have the Jordan-Dedekind theorem[15] on the constancy of the number of

[14] A chain is called "connected" (or dense by Ore) if no further terms can be interpolated in it.

[15] R. Dedekind, *Werke*, vol. II, p. 254.

links in connected chains as one corollary, and using Theorem 3, we have the further

COROLLARY. *A finite distributive lattice has (to within equivalence) exactly one irredundant isomorphic representation as a ring of sets—and the number of points involved is the number of links in its connected chains.*[16]

9. **The finite case** (continued). Let R denote again any finite distributive lattice, let its prime ideals be $P_1, \cdots, P_n$, and let their duals be $D_1, \cdots, D_n$.

Let further $s_i = s(P_i)$ and $p_i = p(D_i)$ be the sum of the $x \in P_i$ resp. the product of the $x \in D_i$. By I2, $s_i \in P_i$, and by D2, $p_i \in D_i$; hence (cf. I1–D1) $x \in P_i$ means $x \leqq s_i$ and $x \in D_i$ means $x \geqq p_i$.

Now let I denote the partially ordered set[17] of the s_i. Call a subset S of I "closed" if and only if $s_i \in S$ and $s_j \leqq s_i$ imply $s_j \in S$.

(9α) R is isomorphic with the ring of "closed" subsets of I under the correspondence $S \rightleftarrows \underset{s_i \in S}{\Lambda} s_i$.

Proof. Let S be a "closed" subset of I. Then by I1–I2 and D1–D2, $\underset{s_i \in S}{\Lambda} s_i$ is in the P_i corresponding to these s_i, and no others. But given $x \in R$, the subset of $s_i \geqq x$ is closed, $y = \underset{s_i \geqq x}{\Lambda} s_i$ is in the same P_i as x, and hence $y \cup x$ and $y \cap x$ are, and so by (8β) no prime factor can be inserted between them, and $x = y = \underset{s_i \geqq x}{\Lambda} s_i$. Thus the correspondence $x \rightleftarrows \underset{s_i \geqq x}{\Lambda} s$ is one-one. But it clearly preserves inclusion, while by Theorem 1 the closed subsets of I are a ring of sets. This completes the proof.

Consequently two finite distributive lattices having isomorphic partially ordered sets of s_i are isomorphic. But the converse is obvious, since the s_i are intrinsically defined. Since, finally, if X is any (abstractly given) partially ordered set, the ring of its closed subsets is a distributive lattice having the "closures" of points of X for s_i, we obtain

THEOREM 5.[18] *There is a one-one correspondence between the partially ordered sets of n elements and the distributive lattices whose connected chains are of length n.*

In the notation of a previous article (this volume of this Journal, p. 311), by (9α) this is the correspondence $X \rightleftarrows B^X$.

Remark 1. The connected components $X_1, \cdots, X_s$ of X correspond to the indecomposable direct factors of

$$B^X = (B^{X_1}) \times \cdots \times (B^{X_s})$$

in the direct decompositions of B^X.

[16] Cf. *On the combination of subalgebras*, Theorem 17.2.

[17] A set is "partially ordered" (the terminology is Hausdorff's, *Grundzüge der Mengenlehre*, 1914, Chap. VI) by a quasi-ordering satisfying P3: $x \geqq y$ and $y \geqq x$ imply $x = y$. Any subset of a partially ordered set (such as a distributive lattice) is partially ordered by the same relation.

[18] Theorem 5 was announced without proof by the author in a note *Sur les espaces discrets*, Comptes Rendus, vol. 201 (1935), p. 19.

Remark 2. The "Hasse[19] diagram" for X gives an infinitely more compact and intelligible way of writing down a general distributive lattice B^X than the multiplication table used by Dedekind, or than the "Hasse diagram" for B^X itself used by recent authors.

Remark 3. Let $\mathfrak{R}$ be any finite ring of sets, and $L = B^X$ the distributive lattice isomorphic with $\mathfrak{R}$. To find X, take the quasi-ordering determined by $\mathfrak{R}$; identify points x and y satisfying both $x \geqq y$ $(\mathfrak{R})$ and $y \geqq x$ $(\mathfrak{R})$; the partial ordering induced by the quasi-ordering on the sets of "identified" points will yield X.

10. **The indecomposable elements.** Let us again suppose that R is a finite distributive lattice with prime ideals $P_1, \cdots, P_n$ having duals $D_1, \cdots, D_n$.

(10α) Each $s(P_i) = s_i$ is product-indecomposable. Dually, each $p(D_i) = p_i$ is sum-indecomposable.

Explanation. An element a of a lattice R is called "product-indecomposable" when no two elements $x > a$ and $y > a$ exist with $x \cap y = a$; it is called sum-indecomposable when (dually) no two elements $x < a$ and $y < a$ exist with $x \cup y = a$.

Proof. If $x > s_i$ and $y > s_i$, then $x \in D_i$ and $y \in D_i$, whence $(x \cap y) \in D_i$ and $x \cap y \neq s_i$.

(10β) If $x \in R$ is product-indecomposable, it is an s_i. If it is sum-indecomposable, it is a p_i, dually.

Proof. If x is product-indecomposable, then it yields a unique prime factor a/x; let P_i be the corresponding prime ideal. Clearly $x = s(P_i)$, since if $x < s(P_i)$, we would have $y = s(P_i)$, whence $y \in P_i$.

COROLLARY. *The number of sum-indecomposable resp. product-indecomposable elements of a finite distributive lattice is the length of its connected chains.*

10a. **The free distributive lattices.** Consider the "free" distributive lattice generated by n symbols $x_1, \cdots, x_n$; Theorem 1 inclines one to adjoin to it elements O and I such that $O < x_i < I$ for all x_i.

If this is done, then the product-indecomposable elements form a Boolean algebra B^n of 2^n elements. More precisely, they are the elements, O, x_k, $x_i \cup x_j$, $x_i \cup x_j \cup x_k$, $x_h \cup x_i \cup x_j \cup x_k$, $\cdots$, $x_1 \cup \cdots \cup x_{k-1} \cup x_{k+1} \cup \cdots \cup x_n$, $x_1 \cup \cdots \cup x_n$. The corresponding prime factors are

$$x_1 \cap \cdots \cap x_n/0,$$

$$x_k \cup (x_1 \cap \cdots \cap x_{k-1} \cap x_{k+1} \cap \cdots \cap x_n)/x_k,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(x_1 \cup \cdots \cup x_{k-1} \cup x_{k+1} \cup \cdots \cup x_n) \cup x_k \,/(x_1 \cup \cdots \cup x_{k-1} \cup x_{k+1} \cup \cdots \cup x_n),$$

$$I/(x_1 \cup \cdots \cup x_n).$$

[19] Cf. H. Hasse, *Höhere Algebra*, vol. II, 1927, p. 103, p. 123.

It is a corollary that the free distributive lattices with O and I adjoined are the B^{B^n}.

The proofs of the above statements are tedious; they depend on the knowledge of canonical expressions for the elements of the free distributive lattice.[20]

11. **A general decomposition theorem.** Let R be any (finite or infinite) distributive lattice, and let

$$x = x_1 \cap \cdots \cap x_r = y_1 \cap \cdots \cap y_s$$

be any two representations of an element $x \in R$ as a product. Then irrespective of i, $x_i = x_i \cup x = x_i \cup (\underset{j}{\Lambda} y_j) = \underset{j}{\Lambda}(x_i \cup y_j)$. Hence if x_i is product-indecomposable, some $x_i \cup y_j = x_i$. This means some $y_j \leqq x_i$. Symmetrically, some $x_k \leqq y_j$. Hence either $x_k = y_j = x_i$, or x_i is *redundant* in the strong sense that some $x_k < x_i$, whence

$$x = x_1 \cap \cdots \cap x_{i-1} \cap x_{i+1} \cap \cdots \cap x_r .$$

Thus if the decompositions are irredundant, the x_i and y_j are equal in pairs, $r = s$, and so

(11α) *In a distributive lattice, no element has more than one irredundant product-decomposition (sum-decomposition) into elements not themselves further decomposable.*

But conversely, any modular lattice which is not distributive is known[21] to contain a sublattice of five elements a, b, x_1, x_2, x_3 satisfying $a < x_i < b$, $x_i \cap x_j \equiv a$, and $x_i \cup x_j \equiv b$ $[i \neq j]$. Now starting with the two product-decompositions $a = x_1 \cap x_2$ and $a = x_2 \cap x_3$ of a, making further decompositions as long as possible, and eliminating redundant components, we see that any factor for the second decomposition which contains x_1 must contain x_2 or x_3 and hence b—whereas the first decomposition and those derived from it must possess at least one factor containing x_1 but *not* b. Hence if the above process is terminating, we will surely get two distinct product-decompositions of a. But in the presence of the chain-condition, the process *is* terminating. This completes the proof of

THEOREM 6.[22] *A modular lattice satisfying the ascending chain condition is distributive if and only if each of its elements has a unique irredundant product-decomposition.*

[20] The latter are given by Th. Skolem, *Über gewisse "Verbände" oder "Lattices"*, Avh. Norske Videnskaps Akademi i Oslo, Mat.-Naturv. Klasse, 1936, no. 7, pp. 7, 8. From them it is immediately obvious that the elements specified above are the *only* product-indecomposable elements—but there are just enough such elements to give the lattice 2^n dimensions; hence they are *all* product-indecomposable.

[21] Cf. Theorem 4 of the author's *On the lattice theory of ideals*, Bull. Amer. Math. Soc., vol. 40 (1934), p. 617.

[22] This result was announced by the author in Abstract 41-1-75 of the Bull. Amer. Math Soc., vol. 41 (1935), p. 32.

This result is especially interesting in the light of recent proofs by Kurosch and Ore that, in any modular lattice, the number of factors in any two irredundant product-decompositions of the same element into indecomposable factors is the same.[23]

12. **Some enumeration problems.** One very impartial test of one's ability to classify finite systems is one's ability to enumerate them. This suggests the problem of determining the following combinatorial functions.

(12.1) The number $F_1(n)$ of different rings of subsets of n elements. (This is the number of sublattices of the Boolean algebra B^n of 2^n elements.)

(12.2) The number $F_2(n)$ of non-equivalent rings of such subsets. (This is the number of such sublattices non-conjugate under the group of automorphisms of B^n.)

(12.3) The number $F_3(n)$ of non-isomorphic rings of such subsets. (This is the number of non-isomorphic distributive lattices of "dimensions" n.)

(12.4) The number $F_4(n)$ of non-isomorphic partial orderings of n elements.

Remark 1. If we replace "ring" by "field" in the above, $F_1(n)$ becomes a known combinatorial function defined by the recurrence

$$H^*(n+1) = \sum_{h=0}^{n} \binom{n}{h} H^*(n-h).$$

This has been studied by Aitken (Edin. Math. Notes, vol. 28 (1933), pp. xviii–xxiii). Again, $F_2(n)$ becomes the partition function—a celebrated asymptotic formula for which has been given by Hardy and Ramanujan. And lastly, $F_3(n)$ becomes n.

Remark 2. In virtue of Theorems 3 and 5, $F_3(n) = \sum_{k=1}^{n} F_4(n)$. Also, $F_2(n)$ is by Theorem 1 the number of non-equivalent quasi-orderings of n elements, and $F_1(n)$ is the number of *different* quasi-orderings of n elements.

A table for these functions for small n follows.

	1	2	3	4	5	6
$F_1(n)$	1	3	29			
$F_2(n)$	1	3	9	30		
$F_4(n)$	1	2	5	15	51	250

[23] A. Kurosch, *Durchschnittsdarstellungen mit irreduziblen Komponenten in Ringen und in sog. Dualgruppen*, Rec. Math. (Moscow), vol. 42 (1935), pp. 613–16. O. Ore, *On the foundations of abstract algebra.* II, Annals of Math., vol. 37 (1936), p. 270, Theorem 11. The result of Kurosch-Ore contains a decomposition theorem of E. Noether for ideals, and a less well-known result of Remak's on finite groups, as special corollaries.

In calculating these values, assume that $F_2(n)$ is the number of functions from the different partially ordered sets of $k \leqq n$ elements to cardinal numbers whose sum is n. Also $F_1(n)$ can be calculated combinatorially from $F_2(n)$ by summing the occurrences of each type of ring of subsets, over the types existing. To find $F_4(n)$, separate each partially ordered set into its connected components.

It would be very interesting to know more about the $F_k(n)$, numerically or asymptotically. $F_4(n)$ resembles the function describing the number of groups of order 2^n—whose first values are 1, 2, 5, 14, 51, 266, $\cdots$. It appears to increase more rapidly than the function describing the number of non-isomorphic symmetric relations between n objects (or alternatively, the number of non-homomorphic graphs with n vertices), whose first values are 1, 2, 4, 11, 27. But as almost nothing is known about the rate of growth of these functions, these comparisons are not very reliable.

13. **Homomorphic images and sublattices.** Let us try to determine the homomorphisms and sublattices of a given finite distributive lattice, guided by the previous results.

Some authors,[24] inspired by the numerous analogies between lattices and rings, have correlated the congruence relations on lattices with "ideals" and "normal sublattices". But except in the "complemented" case in which each element x possesses a complement x' with $x \cap x' = 0$ and $x \cup x' = I$, this correlation is incomplete.

Actually, in the case of finite distributive lattices, and more generally with arbitrary modular lattices of finite dimensions (the author will publish proofs elsewhere, in an article on modular lattices), congruence relations correspond one-one to subsets of the set of prime factors.

It follows that, if $L = B^X$ is any finite distributive lattice, the congruence relations on it are obtained by setting $x \equiv y(\theta)$ if and only if x and y contain the same P_i. Hence, to obtain the homomorphic images B^Y of B^X, set Y equal to any subset of X having on that subset the same inclusion relation as X.

The determination of the sublattices of B^X is even easier. First, recall that B^X is isomorphic with the ring of subsets of X which are "closed" with respect to the partial ordering of X, by (9α). But a sublattice is clearly just a subring —and by Theorem 1 these subrings are the families of sets "closed" under quasi-orderings ρ of X such that $x \geqq y(\rho)$ whenever $x \geqq y$ in X. Hence, to obtain the sublattices of B^X, strengthen the inclusion relation in X to any quasi-ordering and consider the partially ordered set Y obtained from this after elements x and y such that $x \geqq y$ and $y \geqq x$ have been identified; B^Y will be the general sublattice of B^X.

HARVARD UNIVERSITY.

[24] Cf. for instance Gr. C. Moisil, *Recherches sur l'algèbre de la logique*, Annales Sci. de l'Univ. de Jassy, vol. 22 (1936), pp. 1–118.