AMERICAN
MATHEMATICAL SOCIETY
COLLOQUIUM PUBLICATIONS

Volume XXV

AMERICAN MATHEMATICAL SOCIETY
COLLOQUIM PUBLICATIONS
VOLUME XXV

LATTICE THEORY

BY
GARRETT BIRKHOFF
PROFESSOR OF MATHEMATICS
HARVARD UNIVERSITY

Revised Edition

PUBLISHED BY THE
AMERICAN MATHEMATICAL SOCIETY
531 West 116th Street, New York City
1948

PREFACE TO THE SECOND EDITION

The development of lattice theory may be divided into three stages. First, following the publication in 1847 of Boole's "Mathematical Analysis of Logic," various mathematical logicians made postulational analyses of Boolean algebra and the algebra of relations. Their main results may be found in Schröder's monumental "Algebra der Logik" (1890–95), and scattered through Whitehead and Russell's "Principia Mathematica."

The second stage began two years after the publication of van der Waerden's "Moderne Algebra." A series of articles published in 1933–7 by myself, von Neumann, Ore, Stone, and Kantorovitch showed that generalizations of Boolean algebra to suitable "lattices" had fundamental applications to modern algebra, projective geometry, point-set theory, and functional analysis, as well as to logic and probability. Some of this work had been anticipated in two little-noticed papers by Dedekind, and in the writings of Menger, Tarski, and Fritz Klein. The first edition of "Lattice Theory," written in 1937–9, attempted to unify and extend the results of these articles.

As a result of all this pioneer work, lattice theory became recognized as a substantial branch of modern algebra, and a steady flow of contributions to it, by numerous mathematicians, has appeared in the last decade. Dilworth, Frink, Tarski, and Whitman have especially enriched and clarified the subject. These contributions constitute the third phase of development of lattice theory; it is continuing.

A minor revision of the first edition would have left the book quite out-of-date for the research worker. Thus of the seventeen "unsolved" problems listed in the first edition, eight have been essentially solved. It is to be hoped that the 111 unsolved problems described in the second edition will meet with the same fate.

The size of the first edition has been nearly doubled, in order to give an adequate account of the discoveries of the last decade, including unpublished results of my own. Even so, many interesting results have been stated without proof as "exercises," while for others, only bibliographical references have been possible. On the other hand, I have been able to include more complete and self-contained accounts of various topics inadequately treated in the first edition, though already known then.

I wish to thank the University of Washington for the opportunity of presenting much of the material as Walker Ames Lectures, during the summer of 1947.

I also wish to thank Andrew Gleason, Orrin Frink, Marshall Hall, and Irving Kaplansky, for improving various parts of the manuscript.

Like its elder sister group theory, lattice theory is a fruitful source of abstract concepts, common to traditionally unrelated branches of mathematics. Both subjects are based on postulates of an extremely simple and general nature. It was this which convinced me from the first that lattice theory was destined to play—indeed, already did play implicitly—a fundamental role in mathematics. Though its importance will probably never equal that of group theory, I do believe that it will achieve a comparable status.

For this to be true, continued creative work will be needed in the future, building on that of the past. It is to the creative efforts of both past and future, and to the memory of my father's faith in the value of such efforts, that the present volume is affectionately dedicated.

TABLE OF CONTENTS

FOREWORD ON ALGEBRA

It will be assumed that the reader is acquainted with some, at least, of the following kinds of algebra: group, ring, field, vector space, linear algebra; they will not be defined here.[1] On the other hand, in order to state many theorems below with the appropriate degree of generality, we shall want some extremely general definitions applying to *all* such algebras, in a way which we shall now make precise.[2]

By an *algebra* A, we shall mean below a set of elements, together with a number of operations f_α. Each f_α shall be a *single-valued* (univalent) function assigning for some *finite* $n = n(\alpha)$ to every sequence $(x_1, \cdots, x_n)$ of n elements of A, a *value* $f_\alpha(x_1, \cdots, x_n)$ in A. It is to be emphasized that though the number of different operations f_α may be infinite, each individual f_α is *finitary*, i.e., applies to only finite sequences of a fixed length depending on α.

By a "subalgebra" of an abstract algebra, we mean a subset which includes every algebraic combination of its own elements—this definition includes the usual definitions of subgroup, subring, subfield, subspace, subalgebra, etc., as special cases. By an "isomorphism" between two algebras admitting the same operations (e.g., two groups or two rings), we mean a one–one element-to-element correspondence which preserves all combinations. By a "homomorphism," is meant a many–one correspondence with the same property. An isomorphism of an algebra with itself is called an "automorphism"; a homomorphism of an algebra with itself (or a subalgebra of itself) is called an "endomorphism."

By a "congruence relation" on an algebra A, is meant an equivalence relation[3] $x \equiv y\ (\theta)$ with the Substitution Property for each f_α:

$$\text{If } x_i \equiv y_i\ (\theta) \text{ for } i = 1, \cdots, n, \text{ then} \\ f_\alpha(x_1, \cdots, x_n) \equiv f_\alpha(y_1, \cdots, y_n)\ (\theta). \tag{1}$$

This means in effect that if we divide A into subclasses of elements "equivalent" mod θ, then for any sequence $X_1, \cdots, X_n$ of such subclasses, with $n = n(\alpha)$,

---

[1] For the basic concepts of modern algebra, see van der Waerden [1]; Birkhoff-MacLane [1]; Albert [1]; or C. C. MacDuffee, *Introduction to abstract algebra.*

[2] The study of such general concepts, implicit in van der Waerden [1], was first made explicitly in G. Birkhoff [3]. For a survey and further references, see *Universal algebra,* by G. Birkhoff, Proc. First Canadian Congress (1945); also K. Shoda, *Über die allgemeinen algebraischen Systeme,* eight notes in Proc. Imp. Acad. Tokyo, vols. 17–19 (1941–1944); A. Church, *The calculus of λ-conversion,* Princeton, 1941.

[3] An "equivalence relation" is simply a binary relation satisfying identically $x \equiv x$, that $x \equiv y$ implies $y \equiv x$, and that $x \equiv y$ and $y \equiv z$ imply $x \equiv z$. An elementary exposition of congruence relations and homomorphisms may be found in Birkhoff-MacLane, Ch. VI, §14.

the set of $f_\alpha(x_1, \cdots, x_n)$ with $x_k \in X_k$ lies in a single subclass Y, which we may define to be $f_\alpha(X_1, \cdots, X_n)$. This defines a homomorphic image A_θ of A, with the same single-valued operations as A. Conversely, if ϕ maps A homomorphically onto an algebra B, and we define $x \equiv y(\phi)$ in A to mean that $\phi(x) = \phi(y)$ in B, we get a congruence relation. This establishes a many-one correspondence between the congruence relations on A and its homomorphic images.

Again, by the "direct union" $X \times Y$ of two algebras X and Y having the same operations f_α is meant the algebra whose elements are the couples $[x, y]$, with $x \in X$ and $y \in Y$, in which algebraic combination is performed component-by-component—i.e.,

$$(2) \qquad f_\alpha([x_1, y_1], \cdots, [x_n, y_n]) = [f_\alpha(x_1, \cdots, x_n), f_\alpha(y_1, \cdots, y_n)].$$

The direct union of n algebras is defined similarly.

With any class $\mathfrak{A}$ of algebras having the same operations f_α, and any cardinal number n (finite or infinite), is associated the *free $\mathfrak{A}$-algebra with n generators* a_k, such that every single-valued transformation ϕ of the a_k into elements of an $A \in \mathfrak{A}$ can be extended to a *homomorphism* of F into A. (A subset G of an algebra Q is said to "generate" Q, if the smallest subalgebra of Q containing G is Q itself.)

Clearly $F_n(\mathfrak{A})$ is unique to within isomorphism. For if F and F', with generators a_k and a_k', both satisfy the definition, then the correspondence $a_k \leftrightarrow a_k'$ can be extended to a two-way homomorphism, which is an isomorphism. Again, if $\mathfrak{A}$ is defined as the set of all algebras satisfying a set $\mathfrak{S}$ of identities or identical implications, we may describe $F_n(\mathfrak{A})$ loosely as the algebra with n generators satisfying $\mathfrak{S}$, of which every other algebra with n generators satisfying $\mathfrak{S}$ is a homomorphic image.

In the applications below, we shall exhibit certain free lattices explicitly, and prove that they satisfy our descriptive definition. Nevertheless, it may be of interest to give a *constructive* definition of $F_n(\mathfrak{A})$ which proves the existence of $F_n(\mathfrak{A})$ in all cases. To do this, we first take n symbols a_k, and call each single-valued transformation ϕ of the a_k into elements of an $A \in \mathfrak{A}$, a "valuation" of the a_k. Again, we call the f_α "functions of order one," and define a "function order m" recursively as an operation of the form

$$(3) \qquad f_\alpha(g_1(x_1', \cdots, x_{r(1)}'), \cdots, g_n(x_1^n, \cdots, x_{r(n)}^n)),$$

where the g_k are functions of order $m - 1$ or less. Clearly any function of order m determines, for each valuation of the a_k and each substitution of a_k for the x_j^i of (3), an element $g(x_1^1, \cdots, x_{r(n)}^n)$ of the A containing the a_k. Thus, if we regard a group as an algebra with the operations x^{-1} and xy, then $(x^{-1}y)x$ is a function of order three.

We are now ready to define $F_n(\mathfrak{A})$. The elements of $F_n(\mathfrak{A})$ consist precisely of the symbols $g(x_1^1, \cdots, x_{r(n)}^n)$, with one a_k substituted for each x_j^i. Two such symbols are considered equal if and only if they give the same result for every valuation ϕ. By definition, these equalities are precisely the *identities* valid in every $A \in \mathfrak{A}$.

It follows that $F_n(\mathfrak{A})$ is a subalgebra of a direct product of replicas (i.e., isomorphs) of the $A \in \mathfrak{A}$, one factor for each valuation ϕ. Moreover any algebra B with n generators satisfying all identities true in any A is a homomorphic image of $F_n(\mathfrak{A})$; hence $F_n(\mathfrak{A})$ is the free algebra with n generators determined by $\mathfrak{A}$, in the sense of our descriptive definition.

Ex. 1. Let A be any algebra, S any subalgebra of A, and θ any congruence relation on A. Show that the set of all elements of A congruent mod θ to at least one $x \in S$ forms a subalgebra.

Ex. 2. (a) Show that if A is any abstract algebra, and A_θ is the "quotient-algebra" of A modulo any congruence relation θ on A, then the congruence relations on A_θ correspond one–one in a "natural" way to the congruence relations ϕ on A which "include" θ, in the sense that $x \equiv y\ (\theta)$ implies $x \equiv y\ (\phi)$.

(b) In what sense does this generalize the so-called Second Isomorphism Theorem? (Cf. van der Waerden [1, vol. 1, p. 136].)

Ex. 3. (a) Show that if a linear algebra is treated as a group with left and right-multiplications by fixed elements as unary operators, then the concept of "subalgebra" defined above is equivalent to the usual concept of "two-sided ideal." How can left-ideals be regarded as subalgebras?

(b) Show that if multiplication by any scalar is also regarded as an operation, the concept of "subalgebra" coincides with the usual definition.

Ex. 4. Let S be a set, and G any group of one–one transformations of S.

(a) Show that (G, S) can be regarded as an algebra with elements from S and (unary) operations from G.

(b) Show that the "congruence relations" on (G, S) correspond one–one with what are usually called partitions into "imprimitive subsets".

Ex. 5. Show that any equation $f(x_1, \cdots, x_r) = h(x_1, \cdots, x_r)$ identically true in a set $\mathfrak{A}$ of algebras is true in any subalgebra, homomorphic image, or direct union of the algebras of $\mathfrak{A}$.

Ex. 6. Show that if an algebra has ν operations and n generators, and if n is infinite, then it has at most $\mathrm{Max}(\nu, n)$ elements.

Ex. 7. Show that if A contains r elements, then the free algebra $F_n(A)$ is a subalgebra of A^{r^n}, and contains at most r^{r^n} elements.

Ex. 8. Show that an algebra A is the "free algebra with n generators" for some set of algebras (or postulates) if and only if it contains elements $a_1, \cdots, a_n$ such that any correspondence $a_i \to a_i'$ $[a_i' \in A]$ can be extended to an endomorphism of A.

Ex. 9. A set G of generators of an algebra A is called "independent" when no proper subset of G generates A. The intersection of the maximal subalgebras of A may be called the "ϕ-subalgebra" of A. Show that, if A is finite, its ϕ-subalgebra consists precisely of those elements occurring in *no* set of independent generators of A.

Ex. 10.[4] (a) Show that any abstract group G is isomorphic with the group of all automorphisms of a suitable abstract algebra, A.

(b) What is the smallest $f(n)$ such that if G contains $n \leqq N$ elements, then A can be found containing at most $f(N)$ elements (Unsolved Problem).

---

[4] References G. Birkhoff [3, p. 445]; R. Frucht, Compositio Math. 6 (1938), 239–250; G. Birkhoff, Revista de la Union Math. Argentina 11 (1946), No. 4; R. Frucht, ibid., vol. 13 (1948), No. 1. For an analogous problem on Galois groups, see E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. 78 (1918), p. 221.

FOREWORD ON TOPOLOGY

The fundamental ideas of point-set theory (i.e., general topology) can be most simply introduced through the concept of a metric space.

A *metric space* is a collection M of elements (points), together with a definition of *distance* $\delta(x, y)$ between any two points $x, y \in M$, satisfying identically:

(i) $\delta(x, x) = 0$, while $\delta(x, y) > 0$ if $x \neq y$,
(ii) $\delta(x, y) = \delta(y, x)$,
(iii) $\delta(x, y) + \delta(y, z) \geqq \delta(x, z)$ (triangle inequality).

A subset S of a metric space is called *open* if and only if, for any $a \in S$, a constant $\epsilon > 0$ can be found, so small that $| x - a | < \epsilon$ implies $x \in S$. A subset S of M is called *closed* if and only if its complement[1] S' is open. One easily sees that

(1) the sum of any number of open sets is open, and
(2) the intersection of any two open sets is open.

Dually, since complementation interchanges sums and products of sets,

(1') the intersection of any number of closed sets is closed, and
(2') the sum of any two closed sets is closed.

Also one verifies trivially

(3) "Space" M is closed, and any point is closed.

Various more general classes of abstract spaces can be defined as follows. Any space with a family of "closed sets" satisfying (1')–(2')–(3) is called a T_1-*space*. The intersection of all closed sets containing a given set X is called the *closure* of X, and denoted $\bar{X}$; one easily verifies

C1. $X \leqq \bar{X}$, C2. $\bar{\bar{X}} = \bar{X}$,
C3*. $\overline{X + Y} = \bar{X} + \bar{Y}$, C4. If p is a point, then $p = \bar{p}$.

Conversely, C1–C4 imply (1')–(2')–(3), X being closed if and only if $X = \bar{X}$. In fact, C1 follows from C3*–C4. If C4 is replaced by the weaker condition that $\bar{p} = \bar{q}$ implies $p = q$, we have defined a T_0-space.[2]

A family Γ of closed sets in a T_0-space T, with the property that every closed subset of T is an intersection of members of Γ, is called a *basis* of closed sets. Dually, a family Δ of open sets, such that every open subset of T is a sum of sets of Δ, is called a basis of open sets. A *sub-basis* of closed sets is a family Σ of closed sets, such that every set of some basis is the sum of a finite set of

[1] The reader is assumed to know what is meant by the set-union or sum, intersection or product, and complement of sets (cf. Birkhoff-MacLane, Ch. XI). Below, $Y + Z$ means the sum of Y and Z.

[2] Cf. F. Riesz, Atti del IV Congr. Int. dei Mat., Vol. II (1909) where conditions C1–C4 were first discussed; the concept of a metric space is due to M. Fréchet, *Sur quelques points du calcul fonctionnel*, Rendic. di Palermo 22 (1906), 1–74. See also Ch. IV, §1.

sets of Σ—hence such that every closed set is an intersection of finite unions of sets of Σ. It may be shown (Ch. IX, §11) that the intersections of finite unions of the sets of *any* family Σ satisfy (1′)–(2′). The concept of a sub-basis of open sets is defined dually. Again, a *neighborhood* $U(x)$ of a point x is an open set which contains x.

The *Cartesian product* (or topological product) $X = X^1 \times X^2 \times X^3 \times \cdots$ of topological spaces $X^1, X^2, X^3, \cdots$ is defined as the space whose points are the $x = (x^1, x^2, x^3, \cdots)$, with $x^i \in X^i$, and having as a sub-basis of closed sets, for each closed set C of a sub-basis of each X^i, the set of all x with $x^i \in C$. Thus closed intervals form a sub-basis of closed sets for a line segment, and rectangles for the square. By (1′), a sub-basis is also constituted by the set of all x with $x^i \in C^i$, for the different choices of a closed set C^i from a sub-basis of each X^i.

An infinite sequence $x_1, x_2, x_3, \cdots$ of points of a metric space is said to *converge* to the limit a, if and only if $\delta(x_n, a) \to 0$ as $n \to \infty$. If a sequence $\{x_n\}$ converges, then it satisfies the Cauchy condition: $\mathrm{Lim}_{m,n\to\infty}\, \delta(x_m, x_n) = 0$; such sequences are called *Cauchy sequences*. A metric space in which every Cauchy sequence is convergent is called *complete*. Each metric space M determines a unique *complete* metric space, defined as the set of all Cauchy sequences $\{x_n\}, \{y_n\}, \cdots; \delta(\{x_n\}, \{y_n\}) = \mathrm{Lim}_{n\to\infty}\, \delta(x_n, y_n)$, and points whose distance apart is zero are identified.

In more general topological spaces, one must discuss also the convergence of general directed sets.[3]

Readers unfamiliar with the subject will find it suggestive to apply the results below to the case of sequences. Convergence as defined below then has its usual meaning, while a "cofinal subset" is simply a subsequence.

A *directed set* of indices is a class A of indices α, with a transitive relation $\alpha \geqq \beta$ (read, α is a successor of β) having the so-called Moore-Smith Property:

(4) Given $\alpha, \beta \in A$, some $\gamma \in A$ satisfies $\gamma \geqq \alpha$ and $\gamma \geqq \beta$;

in words, any two elements of A have a common successor. A directed set $\{x_\alpha\}$ of points is a function assigning, to each index α of a directed set A, a point x_α.

If M is any space with a family Δ of "open" sets, the *convergence* of a directed set $\{x_\alpha\}$ of points of M is defined by the rule

(5) $x_\alpha \to a$ means that for every open set U containing a, $\beta(U)$ exists such that $x_\alpha \in U$ for all $\alpha \geqq \beta(U)$.

The following law of convergence is easily proved,

(6) If $x_\alpha = a$ for all α, then $x_\alpha \to a$.

---

[3] The concept of a directed set is due to E. H. Moore, Proc. Nat. Acad. Sci. (1915), 628–632; its application to general topology to the author, *Moore-Smith convergence in general topology*, Annals of Math. 38 (1937), 39–56; cf. also H. Cartan, C. R., Paris 205 (1937), 595–598 and 777–779 and J. W. Tukey, *Convergence and uniformity in topology*, Princeton, 1940, esp. Ch. III.

One also shows without much difficulty that if a space X is the Cartesian product of spaces $X^1, X^2, X^3, \cdots$, then $x_\alpha \to a$ in X, where $x_\alpha = (x_\alpha^1, x_\alpha^2, x_\alpha^3, \cdots)$ and $a = (a^1, a^2, a^3, \cdots)$, is equivalent to $x_\alpha^i \to a^i$ in every X^i.

Again, we define a *cofinal subset* of a directed set $\{x_\alpha\}$, as a subset $\{x_\sigma\}$ of $\{x_\alpha\}$ such that every term of $\{x_\alpha\}$ has a successor in $\{x_\sigma\}$. There follows directly

(7) If $x_\alpha \to a$, and $\{x_\sigma\}$ is a cofinal subset of $\{x_\alpha\}$, then $x_\sigma \to a$.

If a subset $\{x_\sigma\}$ of $\{x_\alpha\}$ is *not* cofinal, then some $\{x_\alpha\}$ has no successor in $\{x_\sigma\}$. Hence if $x_\beta \in \{x_\sigma\}$, any common successor of x_α and x_β will be in the complement of $\{x_\sigma\}$. But such a successor exists, by (4), and we infer

(8) If a subset of a directed set is not cofinal, its complement is.

If the family Δ of open sets satisfies (1)–(2), then

(9) A subset X of M is closed if and only if X contains the limit of any convergent directed set of its points.

Proof. If the complement X' of X is open, then $x_\alpha \to a$, $a \in X'$ imply that every x_α has a successor in X'; hence $\{x_\alpha\}$ cannot lie in X. Therefore if $\{x_\alpha\}$ is in X, and $x_\alpha \to a$, then $a \in X$. Conversely, if X is not closed, then there exists a point a not in X, yet in every closed set containing X (since by (1) the intersection $\bar{X}$ of all the closed sets containing X is closed, and so is not X). Hence every open set U which contains a has a closed complement U' which does not contain X, and so we can choose[4] x_U in X and U. But now if we define the successors of U to be the neighborhoods contained in it, by (2) the Moore-Smith Property holds, and so $\{x_U\}$ is a directed set of points of X, which clearly converges to a in the sense of (5).

Again, let M be any "space," and let a rule be given which decides, for every directed set $\{x_\alpha\}$ and point a, whether or not $x_\alpha \to a$. If we define "closed" sets by (9), then obviously (1)–(1′) hold. Moreover, if (7) is assumed, then one can show, using (8), that (2)–(2′) hold; if $x_\alpha \to a$, where x_α is in $Y + Z$, Y and Z being closed, then either the subset of x_α in Y or that in Z is cofinal by (8); hence a is in Y or Z (i.e., $a \in Y + Z$) by (7). Finally, if $x_\alpha \to a$, and U is any open set containing a, then the complement U' of U is closed, and $a \notin U'$. Hence the subset of $\{x_\alpha\}$ in U' is not cofinal, and $\beta(U)$ exists, such that no x_α $[\alpha \geqq \beta]$ is in U'; that is, $x_\alpha \in U$ for all $\alpha \geqq \beta(U)$.

This shows that if we reapply (5), we get at least as many "convergent" directed sets as we had originally. The exact conditions under which convergence retains its original meaning—i.e., an abstract characterization of the properties of convergence—is however more complicated.[5]

---

[4] This requires the Axiom of Choice discussed in Ch. III, §6.

[5] What we have shown is that, for any aggregate M, definitions (5) and (9) define a "Galois correspondence" in the sense of Ch. IV, §6. The condition is stated in G. Birkhoff, op. cit., Thm. 6. For the most recent work, see M. M. Day, Duke Jour. 11 (1944), 181–229 (two articles); also L. Alaoglu and G. Birkhoff, Annals of Math. 41 (1940), pp. 294–295.

Ex. 1. (a) Show that a point a is in the *closure* $\bar{X}$ of a set X, if and only if every open set U containing a contains a point of X.

(b) Show that this result requires only (1). (O. Ore)

Ex. 2. (a) Show that any *countable* directed set $\{x_\alpha\}$ either has a last element, or a cofinal subset which is an ordinary sequence $x_{\alpha_1}, x_{\alpha_2}, x_{\alpha_3}, \cdots$.

(b) Let Σ be a T_0-space in which a subset is closed when it contains all limits of countable directed sets. Show that the *closure* $\bar{X}$ of any subset X consists of X and the limits of ordinary convergent sequences.

(c**) Obtain analogous results for uncountable directed sets. (cf. J. Tukey)

Ex. 3. Show that, in a T_1-space, $x_\alpha \to a$ and $x_\alpha \to b$ imply $a = b$ if and only if some pair of open sets U containing a and V containing b are disjoint. (Such a T_1-space is called a Hausdorff space; also a T_2-space.)

Ex. 4. (a) Show that if we define, for any set X, $\bar{X}$ as the set of limits of directed sets of points of X, then C1 follows from (5), C4 from (6) and the assumption of Ex. 3, and C3* from (7) (as in the proof of (9)).

(b) Find a necessary and sufficient condition for C2. (Hint: Try the condition of G. Birkhoff, op. cit., Thm. 5.)

(c) Show that for sequences, it is necessary and sufficient that if $x_j^i \to x_i$ for all j, and $x_i \to x$, then $x_{j(i)}^i \to x$ for some $j(i)$.

CHAPTER I

PARTLY ORDERED SETS

1. Fundamental definition. It is characteristic of mathematics as a deductive science, that it uses very few undefined terms. This is especially true of lattice theory, all of whose concepts can be defined in terms of one undefined relation "x includes y" meaning "y is a part of x." There are innumerable examples of such relations, in a sense which we shall now make precise.

DEFINITION. *By a "partially ordered set," or "partly ordered set,"*[1] *is meant a system X in which a binary relation $x \geqq y$ is defined, which satisfies*

P1: *For all x, $x \geqq x$.* (*Reflexive*)
P2: *If $x \geqq y$ and $y \geqq x$, then $x = y$.* (*Antisymmetric*)
P3: *If $x \geqq y$ and $y \geqq z$, then $x \geqq z$.* (*Transitive*)

The symbol $\geqq$ is read "contains," "includes," or "is greater than or equal to." If $x \geqq y$ but $x \neq y$, one writes $x > y$, and says x "is greater than" or "properly includes" y. The relation $x \geqq y$ is also written $y \leqq x$, and read x is contained in y (or is included in, or is a part of, y). Similarly, $x > y$ is also written $y < x$.

This notation and terminology are generally accepted. Some simple laws governing the inclusion relation, which follow from P1–P3, are stated in Exs. 1–2 below.

If $a \geqq b$ in a partly ordered set P, the set of x satisfying $a \geqq x \geqq b$ is called the closed *interval*[2] $[b, a]$. The elements x satisfying $a \geqq x \geqq b$ are said to be *between* a and b; see Ex. 4 below, and Ch. III, §5.

Finally, by the *order* $n(P)$ of a partly ordered set P, we mean the number of its elements. This may be finite or infinite.

Ex. 1. (a) Show that $x > x$ for no x, and that $x > y$ and $y > z$ imply $x > z$.
(b) Show that if S is a system with an inequality relation $x > y$ satisfying the preceding conditions, then S is a partly ordered system if $x \geqq y$ is defined to mean $x > y$ or $x = y$.

Ex. 2. Show that if $x_1 \geqq x_2 \geqq \cdots \geqq x_n \geqq x_1$, then $x_1 = x_2 = \cdots = x_n$.

[1] From the German "teilweise geordnete Menge," Hausdorff [1], first ed., Ch. VI, §2. The assumptions go back to C. S. Peirce [1], and were also studied by Schröder [1]. They occur in a fragmentary way in Leibniz' works (circa 1690); see C. I. Lewis, *A survey of symbolic logic*, Berkeley, U. S. A., 1918, pp. 373–87; for a fuller account, see L. Couturat, *La logique de Leibniz d'après des documents inédits*, Paris, 1901, Ch. VIII. Thus P1 is Leibniz' Property 7 (p. 380), P2 his Property 17 (p. 382), and P3 his Property 15 (p. 382).
The author also suggests the convenient abbreviation "poset," for partly ordered set.

[2] The related concept of quotient is discussed in Ch. V; the term interval is more descriptive here; cf. also Ch. II.

Ex. 3. Show that there are just three possible ways of partly ordering a set of two elements.

Ex. 4. (a) In a partly ordered set, define the ternary relation $(axb)\beta$ to mean $a \leqq x \leqq b$ or $a \geqq x \geqq b$. Prove that $(axb)\beta$ implies $(bxa)\beta$; that $(axb)\beta$ and $(abx)\beta$ imply $x = b$; that $(axb)\beta$ and $(ayx)\beta$ imply $(ayb)\beta$; that $(axb)\beta$, $(xby)\beta$, and $x \neq b$ imply $(aby)\beta$; that $(abc)\beta$ and $(acd)\beta$ imply $(bcd)\beta$.

(b) Prove corresponding results for the ternary relation $(axb)\gamma$, defined to mean $a < x < b$ or $a > x > b$.

Problem 1. Discuss the independence of the preceding conditions. Discuss their completeness (a) if there exist O, I such that $(OxI)\beta$ for all x, (b*) if no such "extreme" elements exist. (Cf. E. Pitcher and M. F. Smiley, *Transitivities of betweenness*, Trans. Am. Math. Soc. 52 (1942), 95–114; M. F. Smiley, Bull. Am. Math. Soc. 49 (1943), 246–52 and 280–87; also §5 below.)

2. Elementary examples. The world around us abounds with examples of partly ordered sets. Any hierarchy essentially forms a partly ordered set; so do the different parts of any whole. We shall now give some simple mathematical examples of partly ordered sets.

Example 1. P consists of all the subsets of any class I (including I itself and the void class O), $x \geqq y$ means that x includes y as a subset.

Example 2. P consists of the positive integers, and $x \geqq y$ means that x divides y.

Example 3. P consists of the ideals $H, J, K, \cdots$ of any ring R, and $H \geqq K$ means that K is a subset of H.

An ideal is of course a subset H of a ring R distinguished from other subsets of R by the properties (i) $a \in H$ and $b \in H$ imply $a \pm b \in H$, and (ii) $a \in H$ and $b \in R$ imply $ab \in H$ and $ba \in H$. More generally, the subsets of a class "distinguished" by *any* special property form a partly ordered set under set-inclusion. Thus this is true of the subgroups of any group, the subspaces of any vector space, the "measurable" subsets of the line, the topologically closed subsets of any T_0-space, etc.; cf. Chs. III, IV. These examples should make it evident that a partly ordered set will in general contain pairs of elements H, K which are *incomparable*, in the sense that neither $H \geqq K$ nor $K \geqq H$ holds.

More generally still, let A be any partly ordered system, and X any subset of A. Then a relation $x \geqq y$ may be defined in X to mean $x \geqq y$ in A—i.e., by "relativization." If P1–P3 are satisfied by $\geqq$ in A, then they are satisfied *a fortiori* by $\geqq$ in X. We thus obtain the following result.

THEOREM 1. *Any subset of a partly ordered set is itself partly ordered by the same inclusion relation.*

Example 4. Let R be the real numbers, and let $x \geqq y$ have its usual meaning for real numbers.

Example 5. Let F consist of all real single-valued functions $f(x)$ defined on $-1 \leqq x \leqq 1$; and let $f \geqq g$ mean that $f(x) \geqq g(x)$ for all x.

Example 6. Let P consist of the partitions of a set S, or divisions $\pi, \pi', \pi'', \cdots$ of S into non-overlapping subclasses, and let $\pi \leqq \pi'$ mean that π is a *sub-partition* (or "refinement") of π'.

Example 7. Let P consist of those partitions $\theta, \theta', \theta'', \cdots$ of an abstract algebra A which are "congruence relations"—i.e., have the Substitution Property described in the Foreword on Algebra. Define $\theta \leqq \theta'$ as in Example 6.

Ex. 1. Show that Examples 2, 3, 5 can be considered as special cases of Example 1, if isomorphic partly ordered sets are identified, and Theorem 1 is used.

Ex. 2. Define an example of partly ordered set by adding $-\infty$ and $+\infty$ to Example 4.

Ex. 3. Show that special relativity partly orders space-time by a relation according to which $(x, y, z; t) \geqq (x_1, y_1, z_1, t_1)$ if and only if $[(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2]^{1/2} \leqq t - t_1$. Describe the physical meaning of this relation.

3. Isomorphism and duality. By an *isomorphism* between two partly ordered sets S and S^*, is meant a one–one correspondence θ between S and S^* such that

$$x \geqq y \text{ implies } \theta(x) \geqq \theta(y), \text{ and} \tag{1}$$

$$\theta(x) \geqq \theta(y) \text{ implies } x \geqq y. \tag{1'}$$

Two partly ordered sets are called *isomorphic* if and only if there exists an isomorphism between them; an isomorphism of a partly ordered set with itself is called an automorphism. A many–one correspondence satisfying (1) is called *isotone*, or *order-preserving*.

By the *converse* of a relation ρ is meant the relation $\breve{\rho}$ such that $x \breve{\rho} y$ (read, "x is in the relation $\breve{\rho}$ to y") if and only if $y \rho x$. Thus the converse of the relation "includes," is the relation "is included in"; the converse of "greater" is "less." It is obvious from inspection of conditions P1–P3 that

THEOREM 2 (DUALITY PRINCIPLE). *The converse of any partial ordering is itself a partial ordering.*

DEFINITION. *By the "dual" $\breve{X}$ of a partly ordered system X is meant that partly ordered system defined by the converse relation on the same elements.*

Since $\breve{\breve{X}} = X$, this terminology is legitimate; we shall also speak often of systems isomorphic with $\breve{X}$ as dual to X—though it might be better to speak of them as "anti-isomorphic" to X. Obviously partly ordered sets are dual (or anti-isomorphic) in pairs, whenever they are not *self-dual*. Similarly, the definitions and theorems involving partly ordered sets are dual in pairs, when they are not self-dual; if any theorem is true for all partly ordered sets, so is its dual.[3]

This "Duality Principle" extends to algebra, to projective geometry, and to logic, as we shall see later.

Clearly if θ is an anti-isomorphism, then

$$x \geqq y \text{ implies } \theta(x) \leqq \theta(y), \text{ and} \tag{2}$$

$$\theta(x) \leqq \theta(y) \text{ implies } x \geqq y. \tag{2'}$$

More generally, a many–one correspondence is called *antitone* if it satisfies (2).

[3] This was Schröder's formulation of the duality principle [1, vol. 1, p. 315, Thm. 35].

Many important partly ordered sets are self-dual (i.e., anti-isomorphic with themselves). Thus Example 1, §2, is self-dual; the correspondence which carries each subset into its complement is one–one and inverts inclusion. Similarly, the set of all linear subspaces of n-dimensional Euclidean space which contain the origin is self-dual; the correspondence carrying each subspace into its orthogonal complement is one–one and inverts inclusion.

In these cases, the self-duality is of period two: the transform $(x')'$ of the transform x' of any element x is x. We shall call self-dualities (or anti-automorphisms) of period two, "involutions".

Ex. 1. (a) Show that there are just 2 non-isomorphic partly ordered sets of two elements, both of which are self-dual.

(b) Show that there are 5 non-isomorphic partly ordered sets of three elements, 3 of which are self-dual.

Ex. 2*. (a) Let $G(n)$ denote the number of non-isomorphic partly ordered sets of n elements. Show $G_1(4) = 16$, $G_1(5) = 63$. (I. Rose)

(b) Let $G_1^*(n)$ denote the number of different partial orderings of n elements. Show $G_1^*(2) = 3$, $G_1^*(3) = 19$, $G_1^*(4) = 219$. Does $G_1^*(5) = 4231$?

(c) How many of the preceding give self-dual partly ordered sets?

Ex. 3. Show that the partly ordered sets of three elements have isotone mappings onto partly ordered sets of two elements, in 7 cases out of a conceivable 10.

Ex. 4. (a) Show that the system of all closed linear subspaces of Hilbert space, partly ordered by set-inclusion, has an involution.

(b*) Show that the system of all linear subspaces of Hilbert space does not have an anti-automorphism. (Hint: The dual of the property of Ex. 3 (b), Ch. IV, §9, is not satisfied.)

Ex. 5. Show that any isotone correspondence θ of one partly ordered set onto another can be uniquely represented as a product of a strengthening of the order and a "contraction" (§4, footnote).

4. Quasi-ordering. Many mathematical systems possess relations ρ which satisfy P1 and P3, but not P2. We shall call such relations *quasi-orderings*.

For example, let R be any ring of integrity with unity, and let $a \rho b$ mean $ax = b$ for some x in R. Or let Γ be a class of topological spaces, and let $S \rho T$ mean that T is homeomorphic with a subset of S. Again, let Φ consist of the real functions defined on the unit square $0 \leqq x, y \leqq 1$, and let $f \rho g$ mean that $f(x, y) \geqq g(x, y)$ except on a set of measure zero ("almost everywhere"). Other examples are given as exercises.

Each such quasi-ordering is associated in a natural way with an equivalence relation (i.e., a reflexive, symmetric, and transitive relation) and a partial ordering.

THEOREM 3.[4] *Let ρ be any quasi-ordering of a set X. The relation $x \sim y$, meaning that $x \rho y$ and $y \rho x$, is an equivalence relation. If "equivalent" elements are identified, ρ becomes a partial ordering.*

[4] The result is due to Schröder [1, p. 184]. Cf. also H. MacNeille [1] and [2, §2]. The partly ordered set obtained from X by the construction of Thm. 1.3 has been called the "contraction" of X by M. M. Day. Generalizations of partly ordered sets are also discussed by E. Foradori, *Grundgedanken der Teiltheorie*, Leipzig, 1937, 77 pp.

Proof. By P1, $x \sim x$. It is obvious that $x \sim y$ implies $y \sim x$. Finally, if $x \sim y$ and $y \sim z$, then $x \rho z$ since $x \rho y$ and $y \rho z$, while $z \rho x$ since $z \rho y$ and $y \rho x$ (by P3 also); hence $x \sim z$. This shows that $\sim$ is an equivalence relation, or (Birkhoff-MacLane, Ch. VI, Thm. 27) that there is a partition of X into non-overlapping subclasses, such that $x \sim y$ if and only if x and y are in the same subclass. Moreover if $x \rho y$, $x \sim x^*$, and $y \sim y^*$, then $x^* \rho x \rho y \rho y^*$, whence $x^* \rho y^*$—that is, the relation ρ is defined consistently over entire subclasses. It follows immediately from this that ρ satisfies P1 and P3 in the system formed by these subclasses, and that $x \rho y$ and $y \rho x$ imply $x \sim y$ (i.e., $x = y$ in the system formed by the subclasses).

The preceding construction has numerous applications. Thus it specializes to the usual definition of associate numbers in the first example, to Fréchet's definition of topological dimension in the second example, and to the usual definition of equivalent functions in the third example listed above.[5] Other examples are given as exercises.

Ex. 1. Let Λ be the class of topological linear spaces, and let $S \rho T$ mean that T is topologically isomorphic with a subset of S. Define a partly ordered set of "linear dimensions", as in Thm. 3. Cf. S. Banach [1, Ch. XII].

Ex. 2. (a) Let Φ be the class of groups, and let $G \rho H$ mean that H is isomorphic with a subgroup of G. Show that ρ is a quasi-ordering of groups.

(b) Generalize to other classes of algebraic systems.

Ex. 3. (a) Show that in the case of finite groups, $G \sim H$ means that G is isomorphic with H in Ex. 2. Generalize.

(b) State analogous results for finite-dimensional vector spaces and for infinite cardinal numbers.

Ex. 4. For real-valued continuous functions with domain $0 \leqq x < \infty$, define $f = O(g)$ to mean that for some constants $K, N, f(x) \leqq Kg(x)$ for all $x > N$. Show that this is a quasi-ordering, and define the associated equivalence relation $f \sim g$.

Ex. 5. Show that from *any* relation ρ, a transitive relation σ can be obtained by letting $x \sigma y$ mean that for some finite set $a_0, \cdots, a_n$, $a_0 = x$, $a_n = y$, and $a_{i-1} \rho a_i$ $[i = 1, \cdots, n]$.

5. Diagrams. In any hierarchy, it is important to know when one man is another's immediate superior. The notion of an immediate superior can be defined abstractly in any partly ordered set, as follows.[6]

DEFINITION. *By "a covers b," it is meant that $a > b$ and that $a > x > b$ is not satisfied by any x.*

This leads to a graphical representation of any finite partly ordered set X. Small circles are drawn to represent the elements of X, so that a is higher than b whenever $a > b$. A segment is then drawn from a to b whenever a covers b.

---

[5] Cf. Birkhoff-MacLane, Ch. IV, §5; M. Fréchet, *Les dimensions d'un ensemble abstrait*, Math. Annalen 68 (1910), 145–68; S. Saks, *Théorie de l'intégrale*, Warsaw, 1933, p. 36. Fréchet dimension has been generalized by M. Kondo, Proc. Imp. Acad. Tokyo 19 (1943), 215–23.

[6] This definition is due to Dedekind [2, p. 252], who calls a a "next multiple" of b. See also G. Birkhoff [1, p. 445]. Fr. Klein and O. Ore say "a is prime over b."

Any figure so obtained is called a *diagram*[7] of X; examples are drawn in Fig. 1a–1e below.

It is easily shown that any finite partly ordered set is defined up to isomorphism by its diagram; $a > b$ if and only if a sequence $x_0, x_1, \cdots, x_n$ exists such that $a = x_0$, $b = x_n$, and x_{i-1} covers x_i for $i = 1, \cdots, n$. Graphically, this means that one can move from a to b downward along a broken line. This principle makes it easy to construct abstractly examples of partly ordered sets.

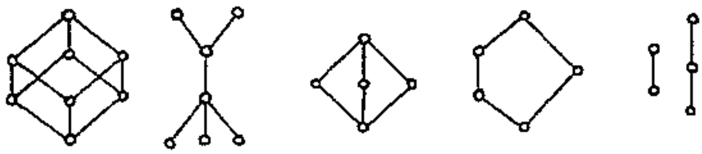

FIG. 1a FIG. 1b FIG. 1c FIG. 1d FIG. 1e

The isomorphism or non-isomorphism of partly ordered sets having few elements can be tested most simply by inspecting their diagrams. Any isomorphism must be one–one between lowest elements, between elements just above lowest elements, and so on. Corresponding elements must be covered by equal numbers of different elements, etc.; with a little imagination, it does not take long to complete the test.

The dual $\breve{X}$ of a partly ordered set X is obtained simply by turning the diagram of X upside down.

Finally, by the *graph* of a partly ordered set is meant the graph (one-dimensional complex, cf. §10) defined by its diagram; this is however less important.

Ex. 1. Which of the diagrams of Fig. 1 represent self-dual partly ordered sets? Define two new self-dual partly ordered sets by means of diagrams.

Ex. 2. Make a square table with 64 entries, showing which pairs of the eight elements 0, x, y, z, u, v, w, I of Fig. 1a satisfy the relation $a > b$.

Ex. 3. (a) Show that the diagram of a partly ordered set is an oriented graph,[8] if we draw an arrow from x to y if and only if x covers y.

(b) Show that a finite oriented graph is associated with a partly ordered set if and only if $\overrightarrow{a_0a_1}, \overrightarrow{a_1a_2}, \cdots, \overrightarrow{a_{n-1}a_n}$ is incompatible with $\overrightarrow{a_0a_n}$.

(c) Show that any oriented graph defines a quasi-ordered set, if $a \geq b$ is defined to mean $a = b$, $\overrightarrow{ab}$, or $\overrightarrow{aa_1}, \overrightarrow{a_1a_2}, \cdots, \overrightarrow{a_nb}$.

Ex. 4. Show that the "covering relations" of any partly ordered set form a new partly ordered set if ("x covers y") > ("u covers v") means that $y \geqq u$. Apply to the examples of Fig. 1.

Ex. 5. Show that any isotone transformation $P \to P_1$ of one partly ordered set P onto another P_1 carries connected components of the graph of P into connected components of the graph of P_1.

Ex. 6.[8] Show that no finite partly ordered set of more than two elements is defined to within isomorphism by its graph.

---

[7] Often, "Hasse diagrams," because of their effective use by H. Hasse. The scheme goes back at least to H. Vogt, *Résolution algébrique des équations*, Paris, 1895, p. 91, and has been used for many years in genealogy.

[8] For the concepts of graph and oriented graph, see D. Koenig, *Theorie der endlichen und unendlichen Graphen*, Leipzig, 1936, esp. Chs. VII–VIII.

6. Greatest and least elements; atoms. It is easily shown that a partly ordered set X can contain at most one element a which satisfies $a \leqq x$ for all $x \in X$. For if a, b are two such elements then $a \leqq b$ and $b \leqq a$ by hypothesis, whence $a = b$ by P2. Such an element, if it exists, is denoted O, and called the least element (or null element) of P.

More generally, by a *least* element of any subset X of P, we mean an element $a \in X$ such that $a \leqq x$ for all $x \in X$. Dually, by a *greatest* element of X, we mean an element $b \in X$ such that $b \geqq x$ for all $x \in X$. The greatest element of P, if it exists, is denoted I; it has also been called the all element of P.

The preceding concepts are not to be confused with the concepts of *minimal* and *maximal* elements. A minimal element of a subset X of a partly ordered set P is an element a such that $a > x$ for no $x \in X$; maximal elements are defined dually. Clearly a least element must be minimal and a greatest element maximal, but the converse is not true (see Fig. 1b).

THEOREM 4. *Any finite subset X of a partly ordered set has minimal and maximal members.*

Proof. Let the elements of X be $x_1, \cdots, x_n$; define $m_1 = x_1$, and m_k as x_k if $x_k < m_{k-1}$ and m_{k-1} otherwise. Then m_n will be minimal. Dually, X will have a maximal element.

An element which covers 0 in a partly ordered set P (i.e., a minimal element in the subset of P obtained by excluding 0) is called an *atom* or *point* (Euclid: "A point is that which has no parts").

Ex. 1. Which of postulates P1–P3 is needed to prove that every least element is minimal?
Ex. 2. In the system P of all subsets of a "space" S, partly ordered by the inclusion relation, what are O, I? What sets do the "points" of P represent?

7. Cardinal arithmetic operations. Many important partly ordered sets can be most conveniently represented as arithmetic combinations of smaller ones, using six generalizations of the ordinary arithmetic operations of addition, multiplication, and exponentiation. The first two of these operations can be defined for arbitrary relations, as we shall now see[9]; we shall however conserve the $\geqq$ notation.

DEFINITION. *Let X and Y be sets, each with a relation $\geqq$. By the cardinal sum $X + Y$ of X and Y, we mean the set of all elements in X or Y, where $\geqq$ keeps its meaning within X and Y, $x \geqq y$ $[x \in X, y \in Y]$ never holds, and X and Y are considered as disjoint. By the cardinal product XY, we mean the set of all couples $(x, y)[x \in X, y \in Y]$, where $(x, y) \geqq (x_1, y_1)$ means $x \geqq x_1$ in X and $y \geqq y_1$ in Y.*

[9] Definitions may be found in Whitehead and Russell [1, §162 and §172], which contain those of addition and multiplication given below. Useful applications to partly ordered sets were given by F. Hausdorff, *Grundzuge der Mengenlehre*, 1st edition, Leipzig, 1914. The definition of cardinal exponentiation given below and its properties were first given by G. Birkhoff, *An extended arithmetic*, Duke Jour. 3 (1937), 311–16; see also G. Birkhoff [5]. The most complete study is by M. M. Day [1]. See also J. M. H. Olmsted, Bull. Am. Math. Soc. 51 (1945), 776–80. J. Riguet, Comptes Rendus Acad. Sci. 226 (1948), 40–1 and 143–6.

Graphically, the addition of two partly ordered sets amounts simply to laying their diagrams side-by-side. Multiplication amounts to forming their combinatorial product (cf. §10 below). It is easily shown that the cardinal sum and product of any two partly ordered sets is partly ordered.

It is also easily seen that if $m, n, \cdots$ denote the finite or infinite unordered sets of $m, n, \cdots$ elements, in which $\geqq$ means $=$, then $m + n$ and mn have their usual meaning (cf. Birkhoff-MacLane [1, Ch. XIII]). Further, $1A = A$, $2A = A + A$, etc., for all A. In addition, one easily proves the following generalizations of the usual arithmetic identities

$$(3) \qquad X + Y = Y + X, \qquad X + (Y + Z) = (X + Y) + Z,$$

$$(4) \qquad XY = YX, \qquad X(YZ) = (XY)Z,$$

$$(5) \qquad X(Y + Z) = XY + XZ, \qquad (X + Y)Z = XZ + YZ.$$

Here the equality sign means "is isomorphic with."

Definition. *Let X and Y be any partly ordered sets. The cardinal power Y^X with base Y and exponent X is the set of all isotone functions $y = f(x)$ from X to Y, partly ordered by letting $f \geqq g$ mean that $f(x) \geqq g(x)$ for all $x \in X$.*

We omit the proof that Y^X is always a partly ordered set, as well as the proofs of the identities

$$(6) \qquad X^{Y+Z} = X^Y X^Z, \quad (XY)^Z = X^Z Y^Z, \quad (X^Y)^Z = X^{YZ}.$$

We also omit the proofs of the duality relations

$$(7) \qquad \overbrace{A + B} = \breve{A} + \breve{B}, \quad \overbrace{AB} = \breve{A}\breve{B}, \quad \overbrace{B^A} = \breve{B}^{\breve{A}}.$$

These proofs, together with the proofs of many other relations, may be found in G. Birkhoff [5] and M. M. Day [1].

Ex. 1. Show that the partly ordered set of Fig. 1a is 2^3, where 2 is defined in §8.

Ex. 2. Show that if X and Y are partly ordered sets, then so are $X + Y$, XY, and Y^X.

Ex. 3. (a) Prove (3)–(5).

(b) Prove (6).

(c) Prove (7).

Ex. 4. Prove that if $n(X)$ is defined as the order of X, then $n(X + Y) = n(X) + n(Y)$ and $n(XY) = n(X)n(Y)$, but that $n(Y^X) < n(Y)^{n(X)}$ is possible.

Ex. 5. Prove that $X^1 = X$, while $X^m X^n = X^{m+n}$ for any cardinal numbers (unordered sets) m and n.

Ex. 6. (a) Show that the set of intervals of a partly ordered set P, partly ordered by set-inclusion, is isomorphic to a subset of $P\breve{P}$.

(b) Show that it is in one-one correspondence with P^2, where 2 represents the ordered set of two elements.

(c) Show that if (with Ore [1, p. 425]) we define $[x, y] \geqq [x_1, y_1]$ to mean $x \geqq x_1$ and $y \geqq y_1$, we get P^2.

Ex. 7. Show that, in the notation of §8, the order $f(m, n)$ of m^n is defined by the special values $f(1, n) = 1$, $f(m, 1) = m$, and the recurrence relation $f(m, n) = f(m - 1, n) + f(m, n - 1)$.

Ex. 8. Show that $X^0 = 1$ for all X, but $0^X = 0$ for all X, if 0 is the void set. Infer that 0^0 is meaningless.

8. Ordinal arithmetic. By the finite *ordinal* number $\mathbf{n}$, written in bold-face type, we shall mean throughout the set of integers $1, 2, \cdots, n$ in their natural order—or any isomorphic set. We shall now define three operations on partly ordered sets which reduce in the case of ordinal numbers to ordinary addition, multiplication, and exponentiation—except that powers of ordinals with infinite exponents need not be ordinals,[10] and powers of infinite partly ordered sets need not be partly ordered.

DEFINITION. *The ordinal sum $X \oplus Y$ of two (non-overlapping) partly ordered sets X and Y is the set of all $x \in X$ and $y \in Y$, where $x \leqq x_1$ in X and $y \leqq y_1$ in Y preserve their original meaning, and $x \leqq y$ for all $x \in X, y \in Y$. The ordinal product $X \circ Y$ is the set of all couples (x, y), where $(x, y) \leqq (x_1, y_1)$ is defined to mean that either $x < x_1$, or $x = x_1$ and $y \leqq y_1$. The ordinal power ${}^XY$ consists of all functions $y = f(x)$ from X to Y, where $f \leqq g$ means that for every x such that $f(x) > g(x)$, there exists an $x_1 < x$ such that $f(x_1) < g(x_1)$.*

Though ordinal addition and multiplication are commutative when applied to finite ordinals, they are not for infinite ordinals. However, they are associative,

$$(8) \qquad X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z \text{ and } X \circ (Y \circ Z) = (X \circ Y) \circ Z.$$

Multiplication is also semi-distributive on sums, and exponentiation on sums. In formulas, we have for any partly ordered sets X, Y, Z,

$$(9) \qquad (X \oplus Y) \circ Z = (X \circ Z) \oplus (Y \circ Z), \text{ and } {}^{X \oplus Y}Z = {}^XZ \circ {}^YZ.$$

It should also be observed that there are many identities relating ordinal operations and cardinal operations.[11] Finally, it should be remarked that the three ordinal and two of the three cardinal operations are all special cases of two generalized operations.[12] We define the lexicographic sum $\sum_X Y_x$ of a family of (non-overlapping) partly ordered sets Y_x, one for each index x in a basic partly ordered set X, as the set of all elements y_x in some Y_x, partly ordered by letting $y_x \leqq y^*_{x^*}$ mean that $x < x^*$ or $x = x^*$ and $y \leqq y^*$. Similarly, we define the lexicographic product $\prod_X Y_x$ as the set of all functions $f(x)$ which select, for each $x \in X$, a $y = f(x) \in Y_x$, partly ordered by letting $f \leqq g$ mean that if $f(x) > g(x)$ for some x, then $f(x_1) > g(x_1)$ for some $x_1 < x$.

If X is the unordered set 2 of two elements, $\sum_2 Y_x = Y_1 + Y_2$; if X is the ordered set $\mathbf{2}$ of two elements, $\sum_{\mathbf{2}} Y_x = Y_1 \oplus Y_2$; if all the Y_x are isomorphic to a fixed Y, $\sum_X Y_x = X \circ Y$. Graphically, $\sum_X Y_x$ may be constructed by replacing each element x in the diagram of X by the diagram of Y_x.

---

[10] An infinite ordinal means a well-ordered set; the difficulty of exponentiating infinite ordinals and partly ordered sets is related to the problem of well-ordering an uncountable set (see Ch. III).

[11] The interested reader will find many in the references given above, esp. in the articles by M. M. Day and the author.

[12] This is implicitly shown in Whitehead and Russell, loc. cit.; see also G. Birkhoff, *An extended arithmetic*, Duke Jour. 3 (1937), pp. 315–16, and M. M. Day, loc. cit., who have modified (for infinite exponents) the definition of lexicographic multiplication.

Similarly, if $X = 2$, then $\prod_2 Y_x = Y_1 Y_2$; if $X = \mathbf{2}$, then $\prod_{\mathbf{2}} Y_x = Y_1 \circ Y_2$; if all the Y_x are isomorphic to a fixed Y, then $\prod_X Y_x = {}^X Y$.

We omit the proofs of the preceding results, as we shall not require them in the sequel.

Ex. 1. Let ω denote the ordered set of the positive integers. Prove that $\omega \oplus 1 \neq 1 \oplus \omega$ and that

$$2 \circ \omega = (1 \oplus 1) \circ \omega = (\omega \circ 1) \oplus (\omega \circ 1) \neq \omega \circ (1 \oplus 1) = \omega \circ 2.$$

Ex. 2. Show that the ordinal sum $X \oplus Y$ and the ordinal product $X \circ Y$ of any two partly ordered sets are always partly ordered.

Ex. 3. Show that if J denotes the set of all integers $0, \pm 1, \pm 2, \cdots$ in their usual ordering, then ${}^J B$ is not transitively ordered. Infer that ordinal powers of partly ordered sets need not be partly ordered. (This corrects an error in G. Birkhoff [5, p. 251].)

Ex. 4. Show that ${}^\omega B$ is not well-ordered, being in fact isomorphic to the Cantor discontinuum.

Ex. 5. Prove the identities of formula (8).

Ex. 6. Prove the identities of formula (9).

Ex. 7. Prove that

$$\breve{X \oplus Y} = \breve{Y} \oplus \breve{X}, \breve{X \circ Y} = \breve{X} \circ \breve{Y}, \text{ and } \breve{({}^Y X)} = {}^Y \breve{X}.$$

Ex. 8. (a) Let $r[A]$ denote the number of ordered pairs (x, y) of elements of a partly ordered set A satisfying $X \leqq Y$. Prove that: $n[A] \leqq r[A] = (n[A])^2$, $r[A + B] = r[A] + r[B]$, $r[AB] = r[A]r[B]$, $r[A \oplus B] = r[A] + r[B] + n[A]n[B]$, $r[A \circ B] = (r[A] - 1)(n[B])^2$.

(b) What about $r[A^B]$ and $r[{}^B A]$?

Problem 2. Decide whether or not there exists a "natural" simple ordering of the class of all real functions. What about ${}^J J$, ${}^R R$? (R denotes the rational numbers.)

9. Chains; Jordan-Dedekind condition. The relation of inclusion in many partly ordered sets satisfies

P4. Given x and y, either $x \geqq y$ or $y \geqq x$.

In other words, of any two elements, one is less and the other greater.

DEFINITION 6. *A partly ordered set satisfying* P4 *is said to be "simply ordered," and called a "chain".*

The positive integers, ordered with respect to magnitude, form a chain; so do the real numbers. Clearly any subset of a chain is a chain; so is the dual of any chain. Moreover

THEOREM 5. *With chains, the notions minimal and least (maximal and greatest) are effectively equivalent. Hence any finite chain has a least (first) and greatest (last) element.*

Proof. If $x < a$ for no $x \in X$, then, by P4, $x \geqq a$ for all $x \in X$.

Now writing down in order the first (smallest) element of a finite chain, then the first of the remaining elements, etc., we see that each element is contained in all later elements and (by P2) no others. We conclude

THEOREM 6. *Every finite chain of n elements is isomorphic with the chain of integers* $1, \cdots, n$.

By the *dimension* or *height* $d[x]$ of an element x of a partly ordered set P, we mean the maximum "length" d of chains $x_0 < x_1 < \cdots < x_d = x$ in P having x for greatest element—in case d is finite. Similarly, by the dimension or *length* $d[P]$ of P, we mean the maximum length of a chain in P.

It is clear that $d[P]$ is the maximum of the $d[x]$; it is also clear that in determining dimensions one need only consider chains $x_0 < x_1 < \cdots < x_d = d$ which are "maximal" or "connected" in the sense that x_i covers x_{i-1} for all i. The notion of dimension is especially important if P has a 0 and satisfies the

Jordan-Dedekind chain condition. *All finite connected chains between fixed end points have the same length.*

This condition is satisfied by Examples 1–3 of §2, by the irreducible algebraic varieties in n-space, and by many other important examples (cf. §11). If it is satisfied by P, it is convenient to represent each $x \in P$ by a small circle (vertex) $d[x]$ units above 0. If x covers y, then there is a connected chain $x > y > y_1 > \cdots > 0$ of length $d[y] + 1$ from x to 0, and conversely. Hence x covers y if and only if $x > y$ and $d[x] = d[y] + 1$—and segments in the diagram of P connect elements on adjacent levels only.

Lemma. *Let P be any partly ordered set which has a 0 and I and in which all chains are finite. Then P satisfies the Jordan-Dedekind chain condition if and only if there exists an integer-valued function $d[x]$ such that*

(*) *x covers y if and only if $x > y$ and $d[x] = d[y] + 1$.*

We leave the proof to the reader; the result may be extended to the case that the Moore-Smith condition is satisfied and all bounded chains are finite.

Ex. 1. (a) Show that in Example 1 of §2, $d[P]$ is the number of distinct points in I, and the Jordan-Dedekind chain condition is satisfied.

(b) Show that in Example 2 of §2, the Jordan-Dedekind chain condition is satisfied, but that no element covers 0.

(c) Show that the condition is satisfied in Figs. 1a–1c, but not in Fig. 1d.

Ex. 2. Show that the elements of dimension one, in a partly ordered set with 0, are its "points".

Ex. 3. (a) Show that if X and Y are (finite or infinite) chains, then so are $X \oplus Y$ and $X \circ Y$.

(b) When is XY a chain?

Ex. 4* (a) Show that if X and Y are partly ordered sets of finite length, then $d[XY] = d[X \oplus Y] = d[X] + d[Y]$, while $d[X \circ Y] = d[X]d[Y] + d[XY]$.

(b) Show that $d[X + Y] = \mathrm{Max}\{d[X], d[Y]\}$, $d[{}^XY] + 1 = (d[Y] + 1)^{(d[X]+1)}$, and $d[Y^X] + 1 = (d[Y] + 1)n[X]$, where $n[X]$ is the order of X.

(c) What can you say about individual elements in the preceding cases?

Ex. 5. Construct a partly ordered set of five elements which satisfies the Jordan-Dedekind chain condition, but does not possess a dimension function $d[x]$, such that $d[x] = d[y] + 1$ if x covers y.

Ex. 6. (a) Prove (or disprove) that the cardinal product of any two partly ordered sets of finite length which satisfy the Jordan-Dedekind chain condition also satisfies it.

(b) Show that 2^ω does not satisfy the infinite Jordan-Dedekind chain condition of [LT] (that all maximal chains between the same end points be isomorphic).

Ex. 7*. Show that a finite partly ordered set P is a set-union of n chains if and only if every $(n+1)$-element subset of P contains a comparable pair.[13] (R. P. Dilworth)

10. Abstract configurations and topological complexes. The concept of an abstract configuration is a more or less vague one, which has been defined in different ways by various authors.[14] It is however generally agreed that the concept should include the concepts of combinatorial complex (in the topological sense) and of a projective geometry, and be included in that of a partly ordered set. We shall therefore introduce our own definition.

FIG. 2a

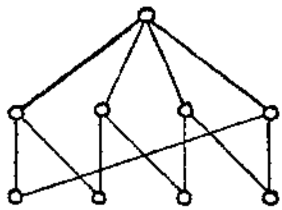

FIG. 2b

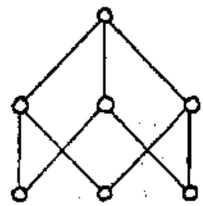

FIG. 2c

DEFINITION. *A configuration is a partly ordered set of finite length with I which satisfies the Jordan-Dedekind chain condition. Two elements* $x, y \in P$ *are called incident if* $x \geqq y$ *or* $y \geqq x$.

In all practical applications, it is also true that $x > y$ implies that x contains a "point" not in y.

We shall see in Ch. VII that the points, lines and planes of Euclidean, projective and hyperbolic geometry form (with or without the void set) are "configurations" in this sense. "Points" have dimension one (zero if the void set is excluded); "lines" have dimension two in this abstract configuration. This is obvious to anyone with the relevant geometrical background; also that similar examples can be found in n dimensions and (except in the hyperbolic case) over arbitrary fields.

Our concern here is rather with topological complexes as abstract configurations. Again, any topological complex[15] is a configuration, and topological "p-cells" (or p-dimensional elements) are the elements with $d[x] = p$. The incidence number $[x:y]$ differs from zero if and only if x "covers" y. Further, "products" in the sense of §7 correspond to Cartesian products in the usual sense;[16] this is illustrated in Figs. 2a–2c where the diagrams of the abstract config-

[13] For a related analysis of P as a product of chains, see B. Dushnik and E. W. Miller, Am. Jour. 63 (1941), 600–10. See also Ch. II, §4, Ex. 6.

[14] Cf. E. H. Moore, *Tactical memoranda*, I–III, Am. Jour. 18 (1896), p. 264; A. B. Kempe, Proc. Lond. Math. Soc. 21 (1890), 147–82; F. Levi, *Geometrische Konfigurationen*, Berlin, 1927; S. Gorn, *On incidence geometry*, Bull. Am. Math. Soc. 46 (1940), p. 158–67.

[15] In the sense of S. Lefschetz, *Algebraic topology*, p. 89; cf. also [LT, §18]. Simplicial and polyhedral complexes are special cases.

[16] Cf. E. R. van Kampen, *Die kombinatorische Topologie*, Hague, 1929, p. 17; also Alexandroff-Hopf [1, p. 299]. We must omit the void set to make this happen.

urations representing a segment S_1 (1-simplex), square $S_1 \times S_1$, and triangle (2-simplex) S_2 are drawn. The topological "sum" of two manifolds also corresponds to the cardinal sum (cf. §7) of the corresponding configurations. Finally, if we include the void set, the configuration determined by the topological "dual"[17] of a complex C is the dual (in the sense of §3) of the configuration determined by C.

Moreover the configuration determined by an n-simplex is simply $\mathbf{2}^{n+1}$ ($\mathbf{2}$ denotes as always the ordered set of two elements) with 0 deleted. Hence *one can easily characterize those configurations which represent simplicial complexes.* However no abstract characterization of polyhedra (subdivisions of the n-sphere) is known; hence it is not clear how to characterize configurations which represent polyhedral complexes.

Lefschetz (loc. cit.) has proposed in effect calling an abstract configuration a "complex" if and only if it satisfies the following self-dual Orientability Condition: values ± 1 can be so assigned to the covering relations (alias incidence relations) that, for any x and x'' with $d[x] = d[x''] + 2$, $\sum_{x'} [x : x'][x' : x''] = 0$. He has shown, following earlier ideas of M. H. A. Newman,[18] A. W. Tucker,[19] and W. Mayer, that many of the most important concepts of topology apply to such "complexes." More research should further clarify the situation.

Ex. 1. (a) Draw the diagram representing a triangular prism (product of simplex and segment; cf. Figs. 2a, 2c).

(b) Draw the diagram representing a cube.

Ex. 2. Draw the dual of the diagram with 0 representing a cube, and show that it represents an octahedron.

Ex. 3. (a) Characterize the abstract configurations which represent polygonal subdivisions of a 1-sphere (circle).

(b) Same for polyhedral subdivisions of the 2-sphere. (Hint: Each edge has two vertices, and the faces meeting at a point are cyclically ordered.)

Ex. 4. We shall call a configuration P of finite length "symmetric" if its automorphisms are transitive on elements of each dimension. Show that a symmetric configuration satisfies the condition of E. H. Moore, that the number (n, k) of n-cells incident with a k-cell is a single-valued function (n, k) of n and k.

Problem 3. Characterize combinatorially all the abstract configurations which represent polyhedral subdivisions of the n-sphere.[19]

Problem 4. Obtain an easily applied test which will show whether a given configuration satisfies the Orientability Condition.

Problem 5. Determine all symmetric configurations having small length and few elements. (Cf. E. H. Moore, loc. cit.; also R. D. Carmichael, *Groups of finite order*, Boston (1937), Ch. XIV; also Problem 53 below.)

11. Partly ordered sets and T_0-spaces. There is another important simple

[17] For "dual complexes," cf. Alexandroff-Hopf [1, p. 427], Lefschetz, p. 9, or O. Veblen, *Analysis situs*, p. 88.

[18] See M. H. A. Newman, Proc. Akad. Wet. Amsterdam 29 (1926), 611–41; ibid. 30 (1927), 670–73; E. R. van Kampen, op. cit.

[19] A. W. Tucker, *An abstract approach to manifolds*, Annals of Math. 34 (1933), 191–243, and *Cell spaces*, ibid., 37 (1936), 92–100. See also J. W. Alexander, *Gratings and homology theory*, Bull. Am. Math. Soc. 53 (1947), 201–33, and Ch. XI, §2 below.

connection of partly ordered sets with topology, through the concept of T_0-space[20] as defined in the Foreword. We define the *M-closure* of any subset S of a partly ordered set X, as the set $\bar{S}$ of all t such that $t \leqq s$ for one or more $s \in S$.

By P1, $\bar{S} \geqq S$, and by P3, $\bar{\bar{S}} = \bar{S}$. Again, clearly $\overline{S + T} = \bar{S} + \bar{T}$. And finally, by P2, $\bar{p} = \bar{q}$ implies $p = q$. Hence X is a T_0-space. Moreover in this space, $q \in \bar{p}$ if and only if $q \leqq p$. But conversely, the definition of $q \leqq p$ as meaning $q \in \bar{p}$ partly orders the points of any T_0-space. (Proof: $p \in \bar{p}$; again $p \in \bar{q}$ and $q \in \bar{p}$ imply $\bar{p} = \bar{q}$, and so $p = q$; finally, $p \in \bar{q}$ and $q \in \bar{r}$ imply $p \in \bar{\bar{r}} = \bar{r}$).

Now if we consider only finite sets $S = \sum_{i=1}^{n} P_i$, then $\bar{S} = \sum_{i=1}^{n} \bar{P}_i$ is the set of $q \leqq p_i$ for one or more $p_i \in S$, and so the correspondences are reciprocal. We conclude

THEOREM 7. *There is a one-one correspondence between finite partly ordered sets X and finite T_0-spaces $\mathfrak{X}$; $q \leqq p$ in X means $q \in \bar{p}$ in $\mathfrak{X}$.*

THEOREM 8. *In the preceding theorem, 2^X is isomorphic with the "ring" of all open subsets of $\mathfrak{X}$, and hence anti-isomorphic with the ring of all closed subsets of $\mathfrak{X}$.*

Explanation. A collection of subsets is called a "ring" if it contains with any two subsets S and T, their union $S \smile T$ and their intersection $S \frown T$.

Proof. Associate with each subset S of $\mathfrak{X}$ its "characteristic function" $f_S : f_S(p) = 1$ or 0 according as $p \in S$ or $p \notin S$. Then $S \geqq T$ if and only if $f_S \geqq f_T$, and S is closed if and only if $q \leqq p$ implies $f_S(q) \geqq f_S(p)$—and hence open if and only if f_S is isotone. This establishes the isomorphism asserted.

Ex. 1. Define the *J-closure* of a subset S of a partly ordered set X, so as to be dual to its M-closure.

12. Methods of enumeration. Let P be any partly ordered system with 0, all of whose intervals $[0, a]$ (sets of x satisfying $0 \leqq x \leqq a$) are finite. Various authors[21] have defined the *Möbius function* μ on P recursively by:

---

[20] The analogy between polyhedral complexes and T_0-spaces is pointed out in different language in Alexandroff-Hopf [1, p. 132].

[21] For the Möbius function of number theory, cf. Uspensky and Heaslet, *Elementary number theory*, Ch. V. The computation of the number of ways of coloring a map in λ colors was first done by G. D. Birkhoff (*A determinant formula for the number of ways of coloring a map*, Annals of Math. 14 (1913), 42–6; see also Proc. Edin. Math. Soc. ser. 2, 2 (1930), and Annali di Pisa, ser. 2, 3 (1934)); H. Whitney, *The coloring of graphs*, Annals of Math. 33 (1932), 688–718; and the reduction formulas on p. 362 of G. D. Birkhoff and D. C. Lewis, Trans. Am. Math. Soc. 60 (1946), 355–451. The applications of the preceding technique to the enumeration of subgroups of p-groups, and of the number of ways of generating a group, are due to P. Hall (Proc. Lond. Math. Soc. 36 (1933), 26–95, and op. cit. infra).

L. Weisner (Trans. Am. Math. Soc. 38 (1935), 474–84) first, and P. Hall (Quar. Jour. 7 (1936), 134–51) more generally formulated the method; see also H. Whitney, *A logical expansion in mathematics*, Bull. Am. Math. Soc. 38 (1932), 572–9, and M. Ward, *The algebra of lattice functions*, Duke Jour. 5 (1939), 357–71.

There is a connection between the Möbius function of a topological complex and its Euler-Poincaré characteristic.

(10) $$\mu[0] = 1. \quad \text{and} \quad \mu[x] = -\sum_{y<x} \mu[y] \quad \text{if } x > 0.$$

The reason for calling this the Möbius function is that it reduces to the Möbius function of number theory in the case of the positive integers, if $x \leqq y$ means x divides y (dual of Example 2, §2).

Philip Hall (op. cit.) has showed that if $\lambda(x; n)$ denotes the number of chains of length n which can be interpolated between 0 and x, then

(11) $$-\mu[x] = \lambda(x; 1) - \lambda(x; 2) + \cdots.$$

He also showed that if P is a lattice in the sense of Ch. III, then $\mu[x] = 0$ unless x is the join of points.

If P satisfies the Jordan-Dedekind chain condition, and $d[x]$ denotes the dimension of $x \in P$, then we can associate with every $x \in L$ a "characteristic polynomial," defined by

(12) $$p_x[\lambda] = \lambda^{d[x]+1} - \sum_{y<x} p_y[\lambda].$$

This is related to the Möbius function by the fact that if $\mu_y[x]$ denotes the Möbius function for x in the subset P_y of $x \geqq y$, then

(13) $$p_x[\lambda] = \sum_{y \leqq x} \lambda^{d[y]+1} \mu_y[x] = \mu[x]\lambda + \cdots.$$

For example, consider the map-coloring problem. We define a "submap" of a map Ω to be one formed from Ω by obliterating boundaries. The "submaps" of any Ω form a partly ordered set with 0 which satisfies the Jordan-Dedekind chain condition; the dimension of any submap is one less than the number of its regions. Moreover since there are λ^n ways of coloring n regions in λ colors, each of which colors either Ω or a unique submap of Ω so that no two adjacent regions have the same color, we see by (12) and induction that there are exactly $p_\Omega[\lambda]$ ways of coloring Ω in λ colors so that no two adjacent regions have the same color.

Other examples are given as exercises.

Ex. 1. (a) Show that in the example of the original Möbius function $\mu[n] = 0$ unless n is square-free, while $\mu[n] = (-1)^s$ if n is square-free, with s distinct prime factors.
(b) Show that if $n = p_1 \cdots p_r$, where the p_i are primes, then $p_n[\lambda] = \lambda(\lambda - 1)^r$.

Ex. 2. What is the number of ways of coloring the map of n triangles, whose sides are the edges of a regular n-gon and radii to its center?

Ex. 3. Any selection of λ elements of a group G of finite order g generates either G or a subgroup S of G. Infer that the number of ways of generating G by λ elements is $P_G[\lambda]$, determined recursively by $P_G(\lambda) = \lambda^g - \sum_{S<G} p_S[\lambda]$.

Problem 6. Which finite partly ordered sets with I satisfying the Jordan-Dedekind condition are characterized to within isomorphism by $p_I[\lambda]$? By the set of all $p_x[\lambda]$?

CHAPTER II

LATTICES

1. Definition. The general theory of partly ordered sets is based on a single undefined relation. That of lattices is also based indirectly on this relation, but directly on two dual binary operations which are analogous in many ways to ordinary addition and multiplication. It is this analogy which makes lattice theory a branch of algebra.

By an *upper bound* to a subset X of a partly ordered set P is meant an element $a \in P$ which contains every $x \in X$. A *least* upper bound is an upper bound contained in every other upper bound (see Ch. I, §6). The notions of a lower bound and a greatest lower bound are defined dually. It is clear from P2 that a subset of a partly ordered set can have at most one l.u.b. (least upper bound) and g.l.b. (greatest lower bound).

DEFINITION.[1] *A lattice is a partly ordered set P any two of whose elements have a g.l.b. or "meet" $x \frown y$, and l.u.b. or "join" $x \smile y$.*

Evidently the dual $\check{L}$ of any lattice L is again a lattice, with meets and joins interchanged. Also it is easy to show by induction that any finite subset has a g.l.b. and a l.u.b. Partly ordered sets in which *every* subset has a g.l.b. and l.u.b. are called *complete* lattices, and are discussed in Ch. IV.

Let X be any subset of a lattice L. Choose $a_0 \in X$. Either a_0 is an upper bound to X, or there exists $a_1 \in X$ such that $a_1 \nleqq a_0$; in this event, define $b_1 = a_0 \smile a_1$. Again, either b_1 is an upper bound of X, or there exists $a_2 \nleqq b_1$; in this case, define $b_2 = b_1 \smile a_2 = (a_0 \smile a_1) \smile a_2$. Either the chain $a_0 < b_1 < b_2 < \cdots$ so constructed terminates after a finite number of steps in an upper bound b_n of X—which is certainly a *least* upper bound (cf. §3)—or L contains an infinite ascending chain $a_0 < b_1 < b_2 < \cdots < b_n < \cdots$. In summary, *$X$ has a least upper bound or L has an infinite ascending chain.*

It is a corollary that if all chains are finite in a lattice L, then every subset of L has a l.u.b. and g.l.b. (L is a complete lattice). In particular, L itself has an upper bound I and a lower bound O.

We shall find it convenient to use the terms "supremum" and "sup" synonymously with l.u.b., and "infimum" and "inf" synonymously with g.l.b. The terms "superior" and "majorant" are also suggestive synonyms for upper bound, but we shall not ordinarily use them.

Ex. 1. Show that if sup X exists, then the upper bounds of X are precisely the elements which contain sup X.

---

[1] The definition of sums and products in terms of inclusion is due to C. S. Peirce [1, p. 33]; see also E. Schröder [1, p. 197], Th. Skolem [1]. H. Whitney has suggested the names "cap" and "cup" for the symbols $\frown$ and $\smile$.

2. Examples. A large fraction of the most important partly ordered systems considered in mathematics are lattices. Moreover in these systems, the operations $\frown$ and $\smile$ usually correspond to familiar and significant constructions.[2]

Example 1. Let Σ consist of all the subsets of any aggregate I, and let inclusion mean set-inclusion. Then "joins" are sums of sets and "meets" are set-products.

Example 2. Let J be the set of positive integers, and let $m \leqq n$ mean "m divides n." Then $m \frown n =$ g.c.d. (m, n) and $m \smile n =$ l.c.m. (m, n).

Example 3. Let Σ consist of the subgroups of any group, and let inclusion mean set-inclusion. Then the terms "join" and "meet" have their usual meaning (also called union and intersection).

Other simple examples are given in each later chapter. We shall find the following more technical example useful now.

Example 4. Let H consist of the congruence relations[3] on an abstract algebra A; let $\theta \leqq \theta'$ mean that θ is a subpartition of θ'—i.e., that $x \equiv y \pmod{\theta}$ implies $x \equiv y \pmod{\theta'}$. Then H is a lattice. Moreover $\theta \frown \theta'$ defines the product of the partitions θ and θ', in the usual sense that $x \equiv y \pmod{\theta \frown \theta'}$ means $x \equiv y \pmod{\theta}$ and $x \equiv y \pmod{\theta'}$. In the degenerate case that A has no operations, H is the lattice of all partitions of A.

Ex. 1. (a) Obtain diagrams (Ch. I, §5) of 5 non-isomorphic lattices of five elements; 3 are self-dual.

(b) Show that every lattice of five elements is isomorphic to one of these.

(c) Show that there are just 4 non-isomorphic lattices of less than five elements.

(d) Show that there are just fifteen lattices of six elements, of which exactly seven are self-dual. (Hint: Add O, I to partly ordered sets of four elements.)

(e) How many are there of seven elements? (Hint: Add O, I to posets of 5 elements. How many are lattices? Make table.)

Ex. 2. Show that the "cells" (i.e., vertices, edges, faces, etc.) of a polyhedron in Euclidean space form a lattice, provided all the cells are convex and the void set is called a cell (cf. Ch. I, §10).

Ex. 3. Show that the "submaps" of a finite map (Ch. I, §12) are a lattice.

Ex. 4. Show that the convex subsets of space form a lattice.

Ex. 5. (a) Show that if $H^*(n)$ denotes the number of partitions of an aggregate of n elements, then

$$H^*(n+1) = \sum_{h=0}^{n} \binom{n}{h} H^*(h), \quad \text{where} \quad \binom{n}{h} = n!/h!(n-h)!.$$

(b) Show that $e^{e^x - 1} = \sum H^*(n)x^n/n!$ (cf. G. Williams, Am. Math. Monthly 52 (1945), 323–7).

3. Lattices as abstract algebras. There is a profound analogy between the

[2] The abundance of lattices in mathematics was apparently not realized before Dedekind [1, pp. 113–4]. Following Dedekind, Emmy Noether stressed their importance in algebra. Their importance in other domains seems to have been discovered independently by Fr. Klein [1], K. Menger [1], and the author; cf. also A. A. Bennett, *Semi-serial order*, Am. Math. Monthly 37 (1930), 418–23.

[3] In the general sense of the Foreword; cf. also Birkhoff-MacLane, Ch. VI, §14.

expressions $x \smile y$, $x \frown (y \smile z)$, $\cdots$ met with in lattice theory, and expressions like $x + y$, $x(y + z)$, $\cdots$ familiar from ordinary algebra.[4] For instance, one readily verifies as immediate consequences of our basic definition, the identities

L1. $x \frown x = x$ and $x \smile x = x$,
L2. $x \frown y = y \frown x$ and $x \smile y = y \smile x$,
L3. $x \frown (y \frown z) = (x \frown y) \frown z$ and $x \smile (y \smile z) = (x \smile y) \smile z$,
L4. $x \frown (x \smile y) = x$ and $x \smile (x \frown y) = x$.

These are called respectively the idempotent, commutative, associative, and absorption laws (the names are mostly Boole's).

Theorem 1. *Identities* L1–L4 *completely characterize lattices.*

Proof. In any system satisfying L1–L4, $x \frown y = y$ if and only if $x \smile y = x \smile (x \frown y) = x$; moreover if one defines $x \geqq y$ to mean $x \frown y = y$, then one gets a *lattice* in which $x \frown y$ and $x \smile y$ are the greatest lower and least upper bounds of x and y, respectively.[5] For example, $x \frown x = x$ implies P1. Again, if $x \geqq y$ and $y \geqq x$, then $y = x \frown y = y \frown x = x$ by L2 and hypothesis, proving P2. While if $x \geqq y$ and $y \geqq z$, by L3, $x \frown z = x \frown (y \frown z) = (x \frown y) \frown z = y \frown z = z$, whence $x \geqq z$. Finally, since by L1–L3 $x \frown (x \frown y) = (x \frown x) \frown y = x \frown y$, $x \frown y$ is a lower bound to x; by L2, it is therefore a lower bound to y also. But it is a *greatest* lower bound since $x \geqq z$ and $y \geqq z$ imply $(x \frown y) \frown z = x \frown (y \frown z) = x \frown z = z$ by L3. Dually, $x \smile y$ is the least upper bound of x and y, completing the proof.

We note that the elements O and I satisfy

$$(1) \qquad O \frown x = O, \quad O \smile x = x, \quad x \frown I = x, \quad x \smile I = I \quad \text{for all } x.$$

The first three of these identities are analogous to the laws $0x = 0$, $0 + x = x$, and $x1 = x$ of ordinary arithmetic.

Ex. 1. Let S be any algebraic system with an idempotent, commutative, and associative binary operation $x \circ y$. Show that S is a partly ordered set in which $x \frown y = x \circ y$ if $x \geqq y$ is defined[6] to mean $x \circ y = y$.

Ex. 2. Show that a system with finite chains which satisfies the conditions of Ex. 1 is really a lattice if it has an I.

Ex. 3*. Are the six identities of L2, L3, L4 for a lattice independent postulates, or is it possible to prove half of one of these conditions from the other five?

Problem 7. What are the consequences of weakening L1 to $x \frown x = x \smile x$ and L4 to $x \frown (x \smile y) = x \smile (x \frown y)$?

---

[4] This was first pointed out a century ago by Boole [1], before the technique of postulate theory existed. L1 and L2 on addition occur in Leibniz, who also in a sense anticipated Thm. 2 (cf. C. I. Lewis, *A survey of symbolic logic*, Berkeley, 1918, p. 376, Thm. 6, and p. 383, Prop. 21).

[5] As Dedekind noted [1, p. 109], L1 can be proved from L4, since $x = x \frown [x \smile (x \frown y)] = x \frown x$ and dually. The separation of L1–L4 from the other identities of Boolean algebra was first accomplished by E. Schröder [1].

[6] See Huntington [1, p. 294]; G. Birkhoff [5, Thm. 2]; J. C. C. McKinsey, Jour. Symbolic Logic, 8 (1943), p. 72, Lemma I. Such systems may be called *semilattices* (Halbverbände by Fr. Klein, Math. Zeits. 48 (1943), 275–88 and 715–34).

4. Sublattices and polynomials. The analogy between the characterization of lattices by L1–L4 and the usual definitions of groups, rings, etc., suggest applying the general terminology of abstract algebra to lattices.

Thus they lead us to define a *sublattice* of a lattice L as a subset which contains with any two elements their join and their meet. The reader should be cautioned that, as in the case of Examples 1, 3 of §2, a subset of a lattice L may be a lattice with respect to the inclusion relation of L, without being a sublattice of L.

We also define a *lattice polynomial* as a function of variables $x_1, \cdots, x_n$ which is either one of the x_i, or (recursively) a join or meet of other lattice polynomials. Thus lattice polynomials are composite functions obtained from the primitive operations of join and meet, and the sublattice generated by any subset X of a lattice L consists of the lattice polynomial functions of the elements of X.

Since the lattice operations are associative, we can define recursively, by analogy with the usual $\prod$-$\sum$ notation,

$$\text{(2)} \qquad \bigwedge_{i=1}^{n} x_i = x_1 \frown \cdots \frown x_n \quad \text{and} \quad \bigvee_{i=1}^{n} x_i = x_1 \smile \cdots \smile x_n .$$

This notation is due to C. S. Peirce [2].

A number of formal laws satisfied by lattice polynomials are useful. Thus we have

THEOREM 2. *Lattice polynomials are isotone functions of their variables: if $f(x_1, \cdots, x_n)$ is any lattice polynomial, and $a_i \leqq b_i$ for all i, then $f(a_1, \cdots, a_n) \leqq f(b_1, \cdots, b_n)$.*

Proof. By induction, it suffices to show that $x \leqq x'$ implies $x \frown y \leqq x' \frown y$ and $x \smile y \leqq x' \smile y$. But if $x \leqq x'$, then

$$x \frown y = (x \frown x') \frown y = x \frown (x' \frown y) \leqq x' \frown y,$$

and dually

$$x' \smile y = (x' \smile x) \smile y = x' \smile (x \smile y) \geqq x \smile y.$$

We have as a special case the one-sided distributive laws

$$\text{(3)} \quad x \frown (y \smile z) \geqq (x \frown y) \smile (x \frown z) \text{ and } x \smile (y \frown z) \leqq (x \smile y) \frown (x \smile z).$$

For by Theorem 2, $x \frown (y \smile z)$ is an upper bound to both $x \frown y$ and $x \frown z$; hence it contains their join. The second law follows by duality. Assuming $x \geqq z$ in (2), we get the one-sided modular law

$$\text{(4)} \quad \text{If } x \geqq z, \text{ then } x \frown (y \smile z) \geqq (x \frown y) \smile z.$$

A more general consequence is the following Minimax Inequality[7]

$$\text{(5)} \qquad \bigwedge_{i=1}^{m} \left(\bigvee_{j=1}^{n} a_{i,j} \right) \geqq \bigvee_{j=1}^{n} \left(\bigwedge_{i=1}^{m} a_{i,j} \right).$$

[7] This is discussed at length in the case of real numbers by J. von Neumann and O. Morgenstern [1, pp. 89–91]. The present generalization is immediate.

Stated at length, let $a_{i,j}$ be defined for $i = 1, \cdots, m$ and $j = 1, \cdots, n$. Then the greatest lower bound (as i varies) of the least upper bounds $\bigvee_j a_{i,j}$ of the $a_{i,j}$ (as i is fixed and j is varied) contains the least upper bound (as j varies) of the greatest lower bounds $\bigwedge_i a_{i,j}$ of the $a_{i,j}$ (as j is fixed and i varies). The proof is immediate since, for all i, j

$$b_i = \bigvee_j a_{i,j} \geqq a_{i,j} \geqq \bigwedge_i a_{i,j} = c_j,$$

whence $\bigwedge_i b_i$ is an upper bound to the c_j, and hence to $\bigvee_j c_j$.

Ex. 1. Prove that $(a \smile b) \frown (c \smile d) \geqq (a \frown c) \smile (b \frown d)$ identically.

Ex. 2. Prove (4) directly from L1–L4.

Ex. 3. Prove that any interval of a lattice is a sublattice, and that so is any intersection of intervals.

Ex. 4. An element a of a lattice is called *join-irreducible* if $x \smile y = a$ implies $x = a$ or $y = a$. Show that if all chains in a lattice L are finite, then every $a \in L$ can be represented as a join $a = x_1 \smile \cdots \smile x_n$ of a finite number of join-irreducible elements.

Ex. 5. Let J be the set of join-irreducible elements of a finite lattice L. Associate with each $a \in L$ the set $S(a)$ of $x \leqq a$ in J. Show that this represents L order-isomorphically by subsets of J, and that meets in L correspond to intersections in the representation.[5]

Ex. 6. We define the (meet) *breadth* of a finite lattice L, as the smallest integer b such that any meet $x_1 \frown \cdots \frown x_n$ $[n > b]$ is always a meet of a subset of b of the x_i.

(a) Show that $b = 1$ if and only if L is a chain.

(b) Show that if the diagram of L can be drawn in the plane without having lines cross, as in Ex. 7, then $b \leqq 2$.

(c)* Show that if $b(L) = n$, and S is a sublattice or lattice-homomorphic image of L, then $b(S) \leqq n$.

(d) Show that $b(LM) = b(L) + b(M)$.

(e) Show that the smallest lattice with $b(L) = n$ is 2^n.

(f) Show that $b(L) = b(\breve{L})$. (I. Rose)

(Hint: Form joins of $(n-1)$-element subsets of n meet-irredundant elements.)

Ex. 7. (a) Show that a finite partly ordered set P whose Hasse diagram can be embedded in the plane is a lattice, if and only if P has an O and an I.

(b) Show that any lattice L whose graph is planar contains a join-irreducible element not O or I.

(c)* Show that a finite lattice L has a plane diagram if and only if there exists a "complementary" partial ordering $<$ among its elements such that $a, b \in L$ are $<$-comparable if and only if they are incomparable under $<$. (J. Zilber)

Ex. 8. (a) Show that any lattice L is a sublattice of a complemented lattice, containing only three additional elements.

(b) Show that if L is finite, only one additional element is needed.

Ex. 9*. The ϕ-sublattice $\phi(L)$ of a lattice L is defined as the intersection of its maximal sublattices. Find necessary and sufficient conditions on L for $\phi(L)$ to be void.

Problem 8. Find a necessary and sufficient condition on a lattice L, in order that every lattice M whose (unoriented) graph is isomorphic with the graph of L be lattice-isomorphic with L. (See Ch. I, §5, Ex. 6*.)

5. Homomorphisms and ideals. An *isomorphism* between two partly ordered sets P and P^* was defined in §3 of Ch. I as a one–one correspondence which

---

[5] Cf. A. D. Campbell, *Set-coordinates for lattices*, Bull. Am. Math. Soc. 49 (1943), 395–8. For any finite lattice L, it is interesting to find the "representation" in the above sense which minimizes the number of points needed.

preserved order, so that

(6) $x \geqq y$ in P if and only if $\theta(x) \geqq \theta(y)$ in P^*.

Such a correspondence must preserve joins and meets, whenever they exist, so that if P, P^* are lattices

(6′) $\theta(x \frown y) = \theta(x) \frown \theta(y)$, (6″) $\theta(x \smile y) = \theta(x) \smile \theta(y)$.

An automorphism of P is an isomorphism of P with itself.

Now consider many–one correspondences $\theta: L \rightarrow L^*$ between lattices. As first observed by Ore [1, p. 416], they may satisfy

(7) $x \geqq y$ implies $\theta(x) \geqq \theta(y)$,

but neither (6′) nor (6″); they may satisfy (6′) but not (6″); or (6″) but not (6′); or they may satisfy both. We shall term such correspondences isotone, meet-homomorphisms, join-homomorphisms, and lattice-homomorphisms, respectively.

It is easily shown that (6′) or (6″) implies (7). Thus since $x \geqq y$ means $x \frown y = y$, using (6′) it implies $\theta(x) \frown \theta(y) = \theta(x \frown y) = \theta(y)$, whence (7) follows. It is also easily shown that the set J of antecedents of 0 under any lattice-homomorphism or join-homomorphism is an ideal, in the following sense.[9]

Definition. *A subset J of elements of a lattice L is an ideal if and only if*
(8) *$x \in J$ and $y \in J$ imply $x \smile y \in J$, and*
(8′) *$x \in J$ and $t \leqq x$ imply $t \in J$.*
The dual of an ideal is a dual ideal.

Proof. If $\theta(x) = \theta(y) = 0$, then $\theta(x \smile y) = \theta(x) \smile \theta(y) = 0 \smile 0 = 0$, and, if $t \leqq x$, $\theta(t) \leqq \theta(x) = 0$.

It is also easily shown that (8′) is equivalent to

(8″) $x \in J$ and $a \in L$ imply $a \frown x = x \frown a \in J$.

For $x \frown a \leqq x$ for all a, whence (8′) implies (8″); conversely, if $t \leqq x$, then $t = x \frown t$, whence (8″) implies (8′).

If we continue to regard $x \frown y$ as the analog of xy, and $x \smile y$ as that of $x + y$, conditions (8), (8″) are the exact analogs of the usual definition of an ideal of a ring. But whereas in a ring, every homomorphic image is determined to within isomorphism by the ideal of elements mapped on zero, this is not true in many lattices. Thus the chain of three elements can be mapped lattice-homomorphically both onto itself and onto the chain of two elements, so that the only element mapped onto 0 is 0. Cf. however Thm. 3 below.

To make the general situation clear, we define (just as in the Foreword on Algebra) a *congruence relation* on a lattice L as an equivalence relation θ with the Substitution Property–

[9] This definition is due to Stone [1]; cf. also Tarski [1] and Moisil [1, p. 17].

(S) If $x \equiv x^*(\theta)$ and $y \equiv y^*(\theta)$, then $x \frown y \equiv x^* \frown y^*(\theta)$ and $x \smile y \equiv x^* \smile y^*(\theta)$.

We observe that, as usual,[10] identification of congruent elements yields a lattice-homomorphic image of L, and all lattice-homomorphic images of L can be obtained in this way.

We note the following result for future reference.

LEMMA. *If $u \equiv v \pmod{\theta}$ in a lattice L, then $x \equiv y \pmod{\theta}$ for all x, y in the interval $u \frown v \leqq x, y \leqq u \smile v$.*

Proof. Under the assumptions, $x = x \smile (u \frown v) \equiv x \smile (u \frown u) \equiv x \smile u \pmod{\theta}$, and dually $x = x \frown (u \smile v) \equiv x \frown (u \smile u) = x \frown u \pmod{\theta}$. Hence

$$u = u \frown (u \smile x) \equiv u \frown x \equiv x \pmod{\theta}.$$

Similarly $u \equiv y \pmod{\theta}$, whence $x \equiv y \pmod{\theta}$.

That is, the antecedents of any element under any lattice-homomorphism form a *convex sublattice*, or sublattice which contains with any a, b, all elements between a and b.

COROLLARY. *A congruence relation θ on a lattice L of finite length is determined if, whenever x covers y, we know whether $x \equiv y \pmod{\theta}$.*

Proof. For any $u, v \in L$, form a chain $u \frown v = a_0 < a_1 < \cdots < a_n = u \smile v$, such that a_i covers a_{i-1}. If $u \equiv v \pmod{\theta}$, then every $a_i \equiv a_{i-1} \pmod{\theta}$ by the lemma; conversely, if every $a_i \equiv a_{i-1} \pmod{\theta}$, then $u \frown v \equiv u \smile v \pmod{\theta}$, whence $u \equiv v \pmod{\theta}$ by the lemma.

Ex. 1. Show that the ideals of any lattice themselves form a lattice.

Ex. 2. (a) Show that if L is any lattice, and a is any element of L, then the set of all $x \leqq a$ is an ideal (such an ideal is called a *principal* ideal).

(b) Show that if L has finite length, every ideal is principal.

(c) Show that in any case, the principal ideals form a sublattice of the lattice of all ideals.

Ex. 3. (a) Show that the congruence relations on a finite chain correspond one-one to its subdivisions into intervals.

(b) Show that every isotone transformation of a chain is a lattice-homomorphism.

Ex. 4. Show that in the case of a lattice of finite length, the antecedents of any element under any lattice-homomorphism form an interval $[a, b]$.

Ex. 5. Show that if, in a lattice, we define $(axb)\beta$ (with Glivenko) whenever $a \frown b \leqq x \leqq a \smile b$, many of the formal properties of betweenness are valid, but that $(axb)\beta$ and $(abx)\beta$ need no longer imply $x = b$. (Cf. Ex. 4, §1, Ch. I.)

Ex. 6*. Find a lattice of length 5 and 18 elements which has a dual automorphism, but no involutory dual automorphisms.

Ex. 7. (a) Show that a meet-homomorphism of a lattice L onto a lattice M is necessarily an isomorphism if $x < x'$ implies $\theta(x) < \theta(x')$.

(b) Show that this is not true of all isotone transformations.

Ex. 8. (a) Show that the correspondence from each subset S of a group G to the subgroup $\bar{S}$ which it generates is a join-homomorphism of the lattice of all subsets of G onto the lattice of all subgroups of G.

[10] Cf. Birkhoff-MacLane, Ch. VI, §14. In the present case, by commutativity, (S) can be replaced by the weaker condition that $x \equiv x^*$ (θ) implies $x \frown a \equiv x^* \frown a$ (θ) and $x \smile a \equiv x^* \smile a$ (θ). A useful notation is $x \theta x^*$ instead of $x \equiv x^*$ (θ).

(b) Obtain an isotone map of 2^2 onto the ordinal 4 which is neither join- nor meet-homomorphic.

Ex. 9. Show that not every congruence relation on the complemented lattice of Fig. 1d, Ch. I, §5, is determined by the ideal of elements congruent to 0.

Ex. 10. (a) Show that a subset X of a lattice L is an ideal if and only if it is the inverse image of 0 under some join-homomorphism of L (cf. §6, Ex. 3b).

(b) Show that X is an ideal if and only if $a, b \in J$ implies $a \smile b \in J$ and conversely $a \smile b \in J$ implies $a, b \in J$.

Ex. 11. (a) Show that, for any a, b of a lattice L, the correspondence $x \to [(a \frown b) \smile x] \frown [a \smile b]$ is an isotone and idempotent map of L onto the interval $[a \frown b, a \smile b]$ consisting of fixpoints.

(b)* Show that if θ and ϕ are both isotone transformations of a partly ordered set P, then the set of fixpoints of $\theta\phi$ is isomorphic with the set of fixpoints of $\phi\theta$. (W. Schwan)

Ex. 12. (a)* Show that any lattice of $n > 6$ elements contains a sublattice of exactly six elements. (I. Kaplansky)

(b) Show that the analogous assertion for 7 elements is false. (Hint: try 2^3.)

Problem 9. Given N, what is the smallest integer $\psi(N)$ such that every lattice with $n > \psi(N)$ elements contains a sublattice of exactly N elements.

6. Further results; complemented lattices. In certain lattices, every congruence relation is determined by the ideal of elements congruent to 0.

DEFINITION. *By a complement of an element x of a lattice L with O and I is meant an element $y \in L$ such that $x \frown y = O$ and $x \smile y = I$; L is called complemented if all its elements have complements. A lattice L is called relatively complemented if all its closed intervals are complemented.*

That is, L is relatively complemented if and only if, given $a \leqq x \leqq b$, an element y exists such that $x \frown y = a$ and $x \smile y = b$. This element is a "relative complement" of x in the closed interval $[a, b]$.

THEOREM 3. *In a relatively complemented lattice with O, or even in a lattice with O where all closed intervals $[O, a]$ are complemented, every congruence relation is determined by the ideal of $x \equiv O$ (mod θ).*

Proof. It is easily shown that the $t \equiv 0$ (θ) form an ideal J_θ. By the lemma of §5, $x \equiv y$ (θ) if and only if $x \frown y \equiv x \smile y$ (θ). Let $x \frown y = v$, $x \smile y = u$; by hypothesis, w exists such that $v \frown w = 0$, $v \smile w = u$. Moreover $u \equiv v$ (θ) implies $w = u \frown w \equiv v \frown w = 0(\theta)$, and $w \equiv 0(\theta)$ implies $u = v \smile w \equiv v \smile 0 = v$ (θ). In summary, $x \equiv y$ (θ) if and only if $w \in J_\theta$ exists such that $x \frown y \frown w = 0$ and $(x \frown y) \smile w = x \smile y$; thus J_θ determines θ.

The following result holds not only in every lattice, but more generally in every algebra in the sense of the Foreword on Algebra.

THEOREM 4. *Let A be any algebra, and let C be any set of congruence relations θ on A. We define new relations ξ and η by*

(i) $a \equiv b$ (ξ) *means* $a \equiv b$ (θ) *for all* $\theta \in C$,

(ii) $a \equiv b$ (η) *means that for some finite sequence*

$$a = x_0, x_1, \cdots, x_m = b, \quad x_{i-1} \equiv x_i \ (\theta_i) \text{ for some } \theta_i \in C.$$

Then ξ, η *are congruence relations; moreover* ξ *is the* g.l.b. *and* η *the* l.u.b. *of the* $\theta \in C$.

Remark. The congruence relations on A are understood to be partly ordered as in Example 7 of Ch. I, §2.

Proof. It is obvious that $\xi \leqq \theta \leqq \eta$ for all $\theta \in C$; further, it is obvious that if $\xi' \leqq \theta \leqq \eta'$ for all $\theta \in C$ and ξ', η' are equivalence relations, then $\xi' \leqq \xi$ and $\eta' \geqq \eta$. Moreover it is easily checked that ξ and η are equivalence relations: reflexivity and symmetry are immediate; so is transitivity for ξ, assuming it for all $\theta \in C$; transitivity of η follows from the definition, since if $a \equiv b\ (\eta)$ and $b \equiv c\ (\eta)$, then there exists a finite sequence $a = x_0, x_1, \cdots, x_m = b = y_0, y_1, \cdots, y_n = c$ such that $x_{i-1} \equiv x_i\ (\theta_i)$ for some $\theta_i \in C$ and $y_{j-1} \equiv y_j\ (\theta_j')$ for some $\theta_j' \in C$ $[i = 1, \cdots, m; j = 1, \cdots, n]$. It remains to prove the Substitution Property for ξ and η.

Again, it is obvious that ξ has the Substitution Property: if $x_i \equiv y_i(\xi)$ for all i and f is any n-ary operation of ξ, then $f(x_1, \cdots, x_n) \equiv f(y_1, \cdots, y_n)(\xi)$ since, for all i, $x_i \equiv y_i\ (\theta)$ and so $f(x_1, \cdots, x_n) \equiv f(y_1, \cdots, y_n)$ for all $\theta \in C$. This is true even if the operations of A are not finitary. Finally, to show that η has the Substitution Property for f, we observe that if $a_i \equiv b_i(\eta)$ for $i = 1, \cdots, n$, we can form chains $a_i = x_{i0}, x_{i1}, \cdots, x_{im} = b_i$ so that $x_{i-1,j} \equiv x_{i,j}(\theta_{i,j})$ as in (ii). Then we can replace each $x_{i-1,j}$ by $x_{i,j}$ without changing $f(a_1, \cdots, a_n)$ mod η; after mn steps, we get[11] $f(b_1, \cdots, b_n)$.

THEOREM 5. *The congruence relations on any lattice* L *satisfy the infinite distributive law,*

$$\theta \frown \bigvee_c \theta_\gamma = \bigvee_c (\theta \frown \theta_\gamma). \tag{9}$$

Proof. By (5) and P2, it suffices to prove that

$$a \equiv b\ (\text{mod } \theta \frown \bigvee_c \theta_\gamma) \quad \text{implies} \quad a \equiv b\ (\text{mod} \bigvee_c\ (\theta \frown \theta_\gamma)). \tag{9'}$$

In the notation $\eta = \bigvee \theta_\gamma$ of Theorem 4, this is the statement that $a \equiv b\ (\theta)$ and $a \equiv b\ (\eta)$ imply that there exists a sequence $a = y_0, y_1, \cdots, y_m = b$ with $y_{i-1} \equiv y_i\ (\theta)$ and $y_{i-1} \equiv y_i\ (\theta_i)$ for some $\theta_i \in C$. But $a \equiv b\ (\eta)$ implies that $a = x_0, x_1, \cdots, x_m$ exist with $x_{i-1} \equiv x_i\ (\theta_i)$. We now set $y_i = [(a \frown b) \smile x_i] \frown (a \smile b)$; clearly $y_0 = a$, $y_m = b$, $y_{i-1} \equiv y_i\ (\theta)$—by the lemma of §5—and $y_{i-1} \equiv y_i\ (\theta_i)$, since θ_i enjoys the Substitution Property.

Ex. 1. Let L be the lattice of congruence relations on an algebra A with finitary operations. Show that if B is obtained from A by introducing further finitary operations, then the lattice of congruence relations of B is a sublattice of L. (A complete sublattice; cf. Ch. IV.)

Ex. 2. Simplify the proof of Thm. 4, in case L is a lattice.

---

[11] Theorem 4 is due to G. Birkhoff [3, Theorem 24], and V. S. Krishnan, *Binary relations, congruences and homomorphisms*, Jour. Madras Univ., B, vol. 16, p. 16. Theorem 5 is due to N. Funayama and T. Nakayama, *On the distributivity of a lattice of lattice-congruences*, Proc. Imp. Acad. Tokyo 18 (1942), 553–4. Cf. N. Funayama, *On the congruence relations on lattices*, ibid., pp. 530–1; also Ch. VI below.

Ex. 3. (a) Show that the ideals $H, K, \cdots$ of any lattice L themselves form a lattice under inclusion, in which $x \in H \smile K$ means $x \leqq a \smile b$ for some $a \in H$ and $b \in K$.

(b) Show that the join-homomorphisms of a lattice L into the two-element chain 2 form a lattice M dually isomorphic with the lattice of ideals of L. (A. Komatu, Proc. Imp. Acad. Tokyo 19 (1943), p. 119.)

Ex. 4. Let A, B be systems with one idempotent, commutative, associative "join" operation $+$ (i.e., semi-lattices; cf. Ex. 1, §3) and an identity 0.

(a) Show that each suitably defined "ideal" H of A determines a least congruence relation θ_H, and that $x \equiv y\ (\theta_H)$ means $x + a = y + a$ for some $a \in H$.

(b) Show that every homomorphism $A \to B$ can be uniquely represented as the product $\alpha\beta$ of a "regular" homomorphism of the type described in (a), and an "irreducible" homomorphism under which[13] the inverse image of 0 is 0.

Problem 9. Try to generalize Thms. 4–5 to "centerless algebras" in the sense of Jónsson and Tarski [1]—i.e., to algebras with a unit e, such that $a + (x + y) = (a + x) + y = x + (a + y)$ for all x, y, and $a + a' = e$ for some a', imply $a = e$.

7. Products and powers. In the terminology of Ch. I, §§7–8, the "cardinal sum" of two lattices is never a lattice, for if x and y come from different summands, they have no upper bound. On the other hand, the "ordinal sum" $L \oplus M$ of two lattices is always a lattice.

THEOREM 6. *The cardinal "product" LM of two lattices L and M is the direct union of the lattices, considered as abstract algebras; hence it is always a lattice. So is M^X, if M is a lattice and X is any partly ordered set.*

Proof. Let $[x, y]$ and $[x', y']$ be any two elements of LM. Then $[x \smile x', y \smile y']$, where $x \smile x' \in L$ and $y \smile y' \in M$, is easily shown to be an upper bound to $[x, y]$ and $[x', y']$, which is contained in every other upper bound. The proof that LM is a lattice is completed by duality. As regards M^X, let $y = f(x)$ and $y = g(x)$ be any two isotone, single-valued functions from X to M. Then if for all x, we define $h(x) = f(x) \smile g(x) \in M$, we get a function h which is isotone, single-valued, and a least upper bound of f and g in M^X. Dually, $h^*(x) = f(x) \frown g(x)$ is a greatest lower bound, completing the proof.

Ex. 1. Show that the conditions of Theorem 6 are necessary, as well as sufficient, for LM resp. M^X to be a lattice.

Ex. 2. Show that the ordinal product $L \circ M$ is a lattice if and only if L, M are lattices and, in addition, L is a chain or M has an O and an I.

Ex. 3. Show that the ordinal power ${}^X M$ is a lattice if and only if one of the following three conditions holds: (i) M is a lattice and X is unordered, (ii) M is a lattice with O and I, (iii) M is a chain while the elements above each fixed $a \in X$ form a chain.[14]

Problem 10. How generally is it true that, if an operation $x \circ y$ is defined in terms of a relation ρ, the cardinal product XY of two sets with a relation ρ, under the definition $[x, y]\rho[x^*, y^*]$ means $x\rho x^*$, and $y\rho y^*$ makes $[x, y] \circ [x^*, y^*] = [x \circ x^*, y \circ y^*]$?

8. Unique factorization theorem. Let P be any product of partly ordered sets X_i; we assume in §§8–9 that P has a 0 and I. Clearly each component of $I \in P$ is a I for X_i, and dually for 0; hence the X_i all have a 0 and a I.

---

[13] V. S. Krishnan, *The theory of homomorphisms and congruence relations for partially ordered sets*, Proc. Ind. Acad. Sci. 22 (1945), 1–19.

[14] The result of Ex. 2 is due to M. M. Day [1, Thm. 7.10]; that of Ex. 3 to the author [5, Thm. 12].

We define e_i as the element of P whose X_i-component is I and whose other components are 0. Then the $t \leqq e_i$ of P will form a subset X_i^* of P isomorphic with X_i. Moreover for any $a = [a_1, a_2, a_3, \cdots] \in P$, the X_i-component of a is $a_i = a \frown e_i$, which thus exists, and is the X_i-component of a_i. The other components of a_i are 0. Hence $a_i \in X_i^*$ and $a_i = \sup_i a_i$. Again, the $t \leqq a$ in P are the elements each of whose components t_i is contained in the corresponding component of a. Hence

Lemma. *The set A of $t \leqq a$ in P is the product of factors isomorphic with the sets A_i of $t \leqq a_i$.*

Now suppose P can be factored into X_i and also into Y_j. Define elements e_i as above, and analogously elements e'_j such that the $x \leqq e_j$ form a set Y_j^* isomorphic with Y_j. Finally, denote by Z_j^i the set of $t \leqq e_i \frown e'_j$ in P. Then by the lemma, each X_i^* is the product of the Z_j^i with superscript i, and each Y_j^* that of the Z_j^i with subscript j. We infer

Theorem 7. *Associated with any two factorizations of a partly ordered set P with O and I, into factors X_i and Y_j respectively, is a factorization into Z_j^i, such that the product of the Z_j^i with fixed i is X_i, and the product of the Z_j^i with fixed j is Y_j.*

Corollary. *If P can be factored into indecomposable factors, this factorization is unique, in the strict sense that any factorization of P is obtainable by grouping these indecomposable factors into subfamilies.*[14]

Theorem 8 (Dilworth). *Any relatively complemented lattice L of finite length is a cardinal product of "simple" relatively complemented lattices.*

Proof. Let θ be any congruence relation; J the ideal of $x \equiv O \pmod{\theta}$, and J the dual ideal of $x \equiv I \pmod{\theta}$. Since L has finite length, J is a principal idea with greatest element a, and J' is a principal dual ideal with least element a'.

Consider the correspondence $x \to x \smile a$. If $x \equiv y \pmod{\theta}$, then $x \frown y \frown w = O$ and $(x \frown y) \smile w = x \smile y$ for some $w \leqq a$, by Thm. 3. Hence $(x \frown y) \smile a = (x \smile y) \smile w \smile a = x \smile y \smile a$, whence $x \smile a = y \smile a$. Conversely, if $x \smile a = y \smile a$, then $x \equiv x \smile a = y \smile a \equiv y \pmod{\theta}$. Therefore $x \to x \smile a$ maps x on the largest element of the residue class containing x, and is an idempotent *lattice-endomorphism*. Dually, $x \to x \frown a'$ is an idempotent lattice-endomorphism mapping each x on the smallest element of the residue class containing x. From these, we get in particular $a' \smile a = I$ and $a \frown a' = O$; thus a and a' are complements.

[14] These results were proved by the author for distributive lattices in [1, p. 457], and later for general lattices [3, p. 616]. A similar theorem which applies to other algebraic systems has recently been proved by B. Jónsson and A. Tarski [1]. Throughout, we ignore one-element factors; otherwise there would be no indecomposable factors. A trivial inductive argument shows that if P has finite length n, then it can be represented as a product of at most n indecomposable factors. T. Nakayama [1] has shown that the unique factorization theorem is valid in any directed set whose dual is also directed.—but not in all partly ordered sets, since $(1 + 2^2)(1 + 2 + 2^2) = (1 + 2^3 + 2^4)$.

Again, if $x \frown a' = 0$, then

$$a = 0 \smile a = (x \frown a') \smile a = (x \smile a) \frown (a' \smile a) = x \smile a$$

and so $x \leqq a$. (In this sense, a is a *strong* complement of a'). But now, for *any* x, $a \frown x$ has a relative complement t in a, such that $(a \frown x) \frown t = 0$ and $(a \frown x) \smile t = x$. Clearly $a \frown (x \frown t) = 0$, whence $t = x \frown t \leqq a'$, as well as $t \leqq x$. Hence

$$(a \frown x) \smile (a' \frown x) \geqq (a \frown x) \smile t = x.$$

It follows that the correspondence $x \to (a \frown x, a' \frown x)$ is an isomorphism of L with a cardinal product of J and the ideal of $x \leqq a'$. Hence unless L is simple, it is a cardinal product, q.e.d.

Ex. 1. (a) Show by direct calculation that if $e \frown e' = 0$ and $e \smile e' = I$ in a lattice L, and if $x = (x \frown e) \smile (x \frown e')$ and dually for all $x \in L$, then L is the direct union of the sublattices of $s \leqq e$ and the $t \leqq e'$.

(b) Show that if the modular law holds, the dual of $x = (x \frown e) \smile (x \frown e')$ need not be assumed.

Problem 11. Is Theorem 7 still valid for lattices? For partly ordered systems with an O but no I?[14]

9. Center of a lattice. The preceding proof suggests defining the *center* of a partly ordered set P with O and I as the set[15] of elements $e \in P$ which have one X_i-component I and the others O, under some direct factorization of P.

Since cardinal multiplication of lattices is commutative and associative, we see that for this it is necessary and sufficient that $e = [I, O]$ under some representation $P = X_i Z$ of P as a product of two factors. Using this, we prove easily the

LEMMA. *Each element of the center has a unique complement, also in the center. The center of any partly ordered set is preserved under dual automorphisms.*

Proof. Clearly $[I, O] \frown [x, y] = [x, O]$ and $[I, O] \smile [x, y] = [I, y]$; hence $[x, y]$ is a complement of $[I, O]$ if and only if $[x, y] = [O, I]$, which is unique. Again, P is the product of the $x \leqq [I, O]$ and $y \leqq [O, I]$ if and only if it is the product of the $s \geqq [I, O]$ and the $t \geqq [O, I]$; hence if $[I, O]$ is in the center of L, it is also in the center of the dual of L.

Now note that the proof of Theorem 7 shows incidentally that if e_i and e_j' are in the center of L, then $e_i \frown e_j'$ exists and is also in the center. By duality (i.e., the preceding lemma), so does $e_i \smile e_j'$, whence we conclude,

THEOREM 9. *The center of any lattice with O and I is a sublattice invariant under dual isomorphisms.*

10. Neutral elements. A lattice L is called *distributive* if and only if, for every $x, y, z \in L$,

(10) $x \frown (y \smile z) = (x \frown y) \smile (x \frown z)$ and $x \smile (y \frown z) = (x \smile y) \frown (x \smile z)$.

[15] This definition is generalized from the notion of "center" of a complemented modular lattice as defined by J. von Neumann [2, Part I, pp. 38–40, and Part III, p. 1].

Distributive lattices are discussed in Ch. IX.

Definition. *An element a of a lattice L is neutral if and only if every triple $\{a, x, y\}$ generates a distributive sublattice of L.*

Lemma 1. *If a is neutral, then* (i) *the dual correspondences $x \to x \frown a$ and $x \to x \smile a$ are endomorphisms of L, and* (ii) *$x \frown a = y \frown a$ and $x \smile a = y \smile a$ imply $x = y$.*

Proof. Ad (i), observe that $(x \frown y) \frown a = (x \frown a) \frown (y \frown a)$ by L1–L3 and $(x \smile y) \frown a = (x \frown a) \smile (y \frown a)$ by (10)—and dually. Ad (ii), observe that by direct computation, using (10) twice,

$$x = x \frown (x \smile a) = x \frown (y \smile a) = (x \frown y) \smile (x \frown a) = (x \frown y) \smile (y \frown a)$$

$$= y \frown (x \smile a) = y \frown (y \smile a) = y.$$

It follows from Lemma 1 that the correspondence $x \to [x \frown a, x \smile a]$ from L is an isomorphism between L and a sublattice of the cardinal product AB of the lattice (ideal) A of $x \leqq a$ and the lattice (dual ideal) B of $x \geqq a$. Moreover under this correspondence $a \to [a, a] = [I, O]$, since $a = I$ in A and $a = O$ in B. Conversely, $[I, O]$ is obviously neutral in AB or in any sublattice of AB, since $\{I, x, y\}$ and $\{O, x, y\}$ always satisfy (10); we leave the twelve calculations to the reader; they reduce by duality and symmetry to four. Consequently

Theorem 10. *An element of a lattice L is neutral if and only if it is carried into $[I, O]$ under an isomorphism of L with a sublattice of a (cardinal) product AB.*[16]

Corollary. *An element is in the center of L if and only if it is neutral and complemented.*

Proof. By the lemma of §9, any element of the center of L is complemented; by Thm. 10, it is neutral. Conversely, by Thm. 9, if a neutral element $[I, O] = a$ has a complement $a' = [x, y]$, then $[O, O] = [I, O] \frown [x, y] = [x, O]$, whence $x = O$; dually, $y = I$. Hence $[x, y] = [O, I]$, and (by Thm. 9) is itself neutral. It is now clear that the correspondence $z \to (z \frown a, z \frown a')$ represents L as the cardinal product of the ideal A of $t \leqq a$ and the ideal A' of $t \leqq a'$, and that hence $a = [I, O]$ and $a' = [O, I]$ are in the center of L.

Theorem 11. *The set of neutral elements of a lattice L is the intersection of its maximal distributive sublattices.*

Proof. First, if a is not neutral, then some triple $\{a, x, y\}$ is not distributive. Hence *no* maximal distributive sublattice[17] obtained by enlarging the distributive sublattice generated by $\{x, y\}$ can contain a. We conclude that the intersection of the maximal distributive sublattices of L contains no non-neutral elements.

---

[16] The results of §10 are due to the author, *Neutral elements in general lattices*, Bull. Am. Math. Soc. 46 (1940), 702–5; in modular lattices, the concept is due to O. Ore [1, pp. 419–21].

[17] In assuming that any distributive sublattice can be extended to a maximal distributive sublattice, we anticipate Ch. III, §6—being a distributive sublattice is a property of finite character.

Conversely, let S be any maximal distributive sublattice of L; let a be neutral. Using Thm. 10, it is easily shown that the sublattice $\{a, S\}$ of $L \leqq AB$ generated by $a = [I, O]$ and S is distributive—whence, S being maximal, $a \in S$. (Detailed proof: It is sufficient to prove that the A-components of $\{a, S\}$ and the B-components of $\{a, S\}$ form distributive lattices—and for these, we only adjoin I resp. O.)

COROLLARY. *The neutral elements of any lattice form a distributive sublattice.*

Ex. 1.(a) Show that conditions (i)–(ii) of Lemma 1 are sufficient as well as necessary for neutrality.

(b) Using Fig. 1d of Ch. I, §5, show that neither condition alone is sufficient.

Ex. 2. Show that the sublattice of neutral elements of a lattice L is invariant under all automorphisms and dual automorphisms of L.

Ex. 3. Prove the Corollary of Theorem 11 using only Theorem 10.

Ex. 4. Show that no neutral element of a lattice can have more than one complement.

11. Free lattices. The "free" lattice FL($\aleph$) with $\aleph$ generators has been explicitly determined by Whitman,[18] for any cardinal number $\aleph$. We construct it as follows.

First, FL($\aleph$) includes "generators" x_α, where the subscripts α run through a class of $\aleph$ elements; thus if $\aleph$ is finite, they may be written $x_1, \cdots, x_n$. These generators will also be called "expressions of weight zero." We then define inductively an "expression of weight w," as any expression $p \frown q$ or $p \smile q$, where the sum of the weights of p and q is $w - 1$. Thus the "weight" of any expression, is the total number of connectives $\frown$ and $\smile$ occurring in it. The elements of FL($\aleph$) consist of all "expressions," it not being however supposed that distinct expressions represent distinct elements.

We now quasi-order (Ch. I, §4) FL($\aleph$), by systematic iteration of the following four basic rules,

(11) $$p \smile q \leqq a \text{ if } p \leqq a \text{ and } q \leqq a,$$

(11′) $$b \leqq p \frown q \text{ if } b \leqq p \text{ and } b \leqq q,$$

(12) $$p \frown q \leqq a \text{ if } p \leqq a \text{ or } q \leqq a,$$

(12′) $$b \leqq p \smile q \text{ if } b \leqq p \text{ or } b \leqq q.$$

Clearly (11) and (11′) are dual, and so are (12) and (12′). For instance, if we wish to find out whether $p \smile q \leqq r \smile s$, we first apply test (11) to $p \smile q$, treating $r \smile s$ as a, and then (12′) to $r \smile s$, treating $p \smile q$ as b. Hence $p \smile q \leqq r \smile s$ if and only if (i) $p \leqq r \smile s$ and $q \leqq r \smile s$, or (ii) $p \smile q \leqq r$, or (iii) $p \smile q \leqq s$. In this way the verification of $p \smile q \leqq r \smile s$ is reduced to combinations of four or fewer questions, in each of which the total weight of the expressions involved is reduced by one. Hence, repeating this process of reduction, *if the sum of the weights of a and b is $w + w'$, we can test for $a \leqq b$ by $4^{w+w'}$ or fewer elementary tests*, of the form $x_i \leqq x_j$ (which is true if and only if $i = j$).

[18] P. Whitman, *Free lattices*, Annals of Math. 42 (1941), 325–30, and *Free lattices*. II, ibid. 43 (1942), 104–15. Further results may be found in Dilworth [2].

LEMMA 1. *$FL(\aleph)$ is a quasi-ordered set.*

Proof. Inductively, $p \leqq p$ and $q \leqq q$ imply $p \leqq p \smile q$ and $q \leqq p \smile q$ by (12′), whence $p \smile q \leqq p \smile q$ by (11). Hence, by duality and induction, the relation is reflexive. We now prove transitivity: that $a \leqq b$ and $b \leqq c$ imply $a \leqq c$. We first consider the case that one of the extreme terms a, c is involved in reducing one or both of the two inequalities.

If $p \smile q \leqq b$ by (11) and $b \leqq c$, then $p \leqq b \leqq c$ and $q \leqq b \leqq c$, whence by induction $p \leqq c$ and $q \leqq c$, and so by (11) $p \smile q \leqq c$. Again, if $p \frown q \leqq b$ by (12) and $b \leqq c$, then $p \leqq b \leqq c$ or $q \leqq b \leqq c$, whence by induction $p \leqq c$ or $q \leqq c$, and so by (12) $p \frown q \leqq c$. Dually, if $a \leqq b \leqq p \frown q$ or $a \leqq b \leqq p \smile q$ follows by a decomposition of $p \frown q$ resp. $p \smile q$, we can prove $a \leqq p \frown q$ resp. $a \leqq p \smile q$.

There remains the case that both $a \leqq b$ and $b \leqq c$ are first reduced by writing $b = p \smile q$ (or $b = p \frown q$). If $a \leqq p \smile q$ by (12′) and $p \smile q \leqq c$ by (11), then $a \leqq p$ or $a \leqq q$, *and* $p \leqq c$ and $q \leqq c$. Hence $a \leqq p \leqq c$ or $a \leqq q \leqq c$; in either case, by induction, $a \leqq c$. The case $a \leqq p \frown q \leqq c$ is dual, completing the proof. Now using Thm. 3. of Ch. I, we infer the following

COROLLARY. *If we define $a = b$ in $FL(\aleph)$ to mean that $a \leqq b$ and $b \leqq a$, then $FL(\aleph)$ is a partly ordered set.*

LEMMA 2. *$FL(\aleph)$ is a lattice, in which the expression $a \frown b$ is* g.l.b. (a, b) *and $a \smile b$ is* l.u.b. (a, b).

Proof. By (12) and Lemma 1, $a \frown b \leqq a$ and $a \frown b \leqq b$. By (11′), $x \leqq a$ and $x \leqq b$ imply $x \leqq a \frown b$. Hence $a \frown b$ is g.l.b. (a, b). Dually, $a \smile b$ is l.u.b. (a, b).

THEOREM 12. *$FL(\aleph)$ is the free lattice generated by the symbols x_α.*

Proof. Choose elements g_α in any lattice L, one corresponding to each x_α. By direct substitution, each $a \in \mathrm{FL}(\aleph)$ determines a unique element $a^* \in L$. By Lemma 2, this correspondence is homomorphic, from $\mathrm{FL}(\aleph)$ onto the sublattice of L generated by the g_α.

Ex. 1. Show that FL(2) has four elements.

Ex. 2*. (a) Show that FL(3) is infinite.
(b) Show that FL(3) contains an infinite chain.

Ex. 3. (a) Show that the x_i are the only set of generators of FL(n) which is not redundant.[19]
(b) Show that the group of automorphisms of $FL(n)$ is the symmetric group on the x_i.

Ex. 4*. Show that of all the elements equal to a given element in FL($\aleph$), there is only one of shortest length, apart from those equivalent to it under the commutative and associative laws.

Ex. 5*. (a) Show that FL(3) contains FL(n) as a sublattice, for any finite or countable n.
(b) Show that FL(3) does not contain 2^3 (the Boolean algebra of order eight) as a sublattice.

Ex. 6*. Show that in $FL(n)$, $\bigvee_{i=1}^{n} x_i$ covers $\bigvee_{i=2}^{n} x_i$, and that $\bigvee_{i=3}^{n} x_i$ covers $\bigvee_{i=2}^{n} x_i \frown \bigvee_{i=1}^{n-1} x_i$.

[19] Exs. 3–6 state results proved in the papers of Whitman listed earlier; Ex. 2 is due to

CHAPTER III

CHAINS AND CHAIN CONDITIONS

1. Chains of real numbers. In Ch. I, §9, a *chain* was defined as a partly ordered set satisfying

P4. Given x and y, either $x \leqq y$ or $y \leqq x$.

Other equivalent definitions are possible (see Exs. 1–2 below).

Every finite chain of n elements is, by Thm. 6 of Ch. I, isomorphic with the chain of positive integers $1, \cdots, n$. We shall denote this chain by boldface $\boldsymbol{n}$. We shall also let ω denote the chain of all positive integers, J the chain of all integers, R the chain of all rational numbers, and $R^{\#}$ the chain of all real numbers. Many chains can be represented as subchains of the latter, and hence pictured as sets of points on a line. This graphical picture is very suggestive. For example, it makes it easy to visualize the meaning of the following

DEFINITION. *A chain C is called dense-in-itself if and only if, given $a < b$ in C, there exists $c \in C$ satisfying $a < c < b$. A subset S of a chain C is called order-dense in C if and only if, for every $a < b$ in C, not in S, an element s of S can be found satisfying $a < s < b$.*

THEOREM 1. *Any countable[1] chain is isomorphic with a subchain of the chain R of rational numbers. Any countable chain which is dense-in-itself is isomorphic with either R, $R \oplus \mathbf{1}$, $\mathbf{1} \oplus R$, or $\mathbf{1} \oplus R \oplus \mathbf{1}$.*

Proof. The rational numbers may be enumerated, as $r_1, r_2, r_3, \cdots$; similarly, the elements of the given chain can be enumerated as $a_1, a_2, a_3, \cdots$. Set $f(a_1) = 0$. By induction, we know that either (i) a_n exceeds $a_1, \cdots, a_{n-1}$, or (ii) a_n is less than $a_1, \cdots, a_{n-1}$, or (iii) a_n is between a_i and a_j for some greatest $a_i < a_n$ and least $a_j > a_n$ $[i, j < n]$. In case (i), set $f(a_n) = n$; in case (ii), set $f(a_n) = -n$; in case (iii), define $f(a_n)$ as the first r_i in the same order-relation to $f(a_1), \cdots, f(a_{n-1})$ as a_n is to $a_1, \cdots, a_{n-1}$. Since R is "dense-in-itself," such an $f(a_n)$ will always exist. The correspondence is evidently isotone, and makes $f(a_n)$ distinct from $f(a_1), \cdots, f(a_{n-1})$. Furthermore, if C is dense-in-itself, the image of C includes all rational numbers between some $-m$ and n: it cannot omit any (first) r_i between two rational numbers of the form $f(a_n)$. Here either $-m$ or n may be infinite, and there are four cases accordingly.

[1] We assume that the reader is acquainted with the definitions of countable and uncountable sets; cf., for example, Birkhoff-MacLane, Ch. XII. An excellent introductory account of simply ordered sets is E. V. Huntington's *The continuum and other types of serial order*, Harvard University Press, 2d ed., 1917. For more advanced treatments, see Hausdorff [1]; W. Sierpinski [1]; A. Denjoy, *L'énumération transfinie*; Livre I, Paris 1946.

Again, we note that R is order-dense in R^*. This is typical, in the following sense.

THEOREM 2. *A chain C is isomorphic with a subchain of R^*, if and only if C contains a countable order-dense subset.*

Proof. Suppose C contains a countable order-dense subset $A = \{a_1, a_2, a_3, \cdots\}$; without losing generality, we may suppose that A contains the greatest and least elements of C, if they exist. By Thm. 1, we can map A onto a subchain of the chain of rational numbers. By hypothesis and Definition 1, every c in $C - A$ (every c in C but not in A) is uniquely determined by the *cut* which it defines in A, i.e., by the partition of A into the set of $a_i < c$ and the set of $a_i > c$. Let $r_1 = \text{l.u.b. } f(a_i)$ with $a_i < c$, and $r_2 = \text{g.l.b. } f(a_i)$ with $a_i > c$; we define $2f(c) = r_1 + r_2$. This defines an isomorphism between C and a subset of R^*. We omit details, because Theorem 2 plays no rôle in advanced theory, and because the reader should be able to supply them.

Conversely, if C is isomorphic with a subset of R^*, we can find a countable dense subset of C by enumerating the intervals $I_i : m_i/n_i \leqq x \leqq m_i'/n_i'$ of R^* having rational end points and choosing one c_i from each I_i except when no element of C corresponds to an element of I_i.

Ex. 1. Show that a chain can be defined as a set of elements in which a transitive relation $x > y$ is defined, such that for any elements u, v, one and only one of the relations $u > v$, $u = v$, $v > u$ holds. (You may assume that equality is a reflexive, symmetric and transitive relation.)

Ex. 2. (a) Show that chains are those partly ordered sets, all of whose subsets are lattices.

(b) Show that an isotone transformation of a chain is always a lattice homomorphism.

(c*) Show that if every isotone transformation of a lattice L is a lattice-homomorphism, then L is a chain.

Ex. 3. Characterize the relation of betweenness in a chain, by its abstract properties. (See D. Hilbert, *Grundlagen der Geometrie*, 7th ed., p. 5 ff.; E. V. Huntington, *Interrelations among the four principal types of order*, Trans. Am. Math. Soc. 38 (1935), 1–9; also Ex. 4, Ch. I, §1).

Ex. 4. Show that $\boldsymbol{R} \oplus \boldsymbol{R}$ and $\boldsymbol{R} \circ \boldsymbol{R}$ are both isomorphic with $\boldsymbol{R}$, first by giving an explicit construction; and then by using Thm. 1.

Ex. 5. (a) Show that $R^* \oplus R^*$ is isomorphic to a subset of R^*, obtained by deleting 0, but not to R^* itself.

(b) Show that if X and Y are both isomorphic with subchains of R^*, then so is $X \oplus Y$.

Ex. 6*. (a) Show that $R^* \circ R^*$ is *not* isomorphic with a subchain of R^*.

(b) Show that if X and Y are isomorphic with subchains of R^*, and Y contains two or more elements, then $X \circ Y$ is isomorphic with a subchain of R^* if and only if X is countable.

2. Well-ordering. A fundamental concept in the higher theory of infinite chains is that of a well-ordered set.

DEFINITION. *A partly ordered set W is called well-ordered, or an ordinal, if and only if every non-void subset of W has a first (i.e., least) element.*

Applied to subsets of two elements, this implies that W must be a chain (given $a \neq b$, either $a < b$ or $b < a$). Moreover by Thm. 6 of Ch. I, in the case of finite sets, the concepts of being well-ordered and of being a chain are equivalent. It follows immediately that any subset of a well-ordered set is well-ordered.

The property of being well-ordered is not self-dual in the infinite case; in fact, W and its dual $\breve{W}$ are both well-ordered if and only if W is a finite chain.

The simplest infinite ordinal (i.e., well-ordered set) is given by the sequence ω of positive integers $1, 2, 3, \cdots$. The statement that this is well-ordered is one form of the Principle of Finite Induction.[2] This principle can be extended (cf. §4) to the following

PRINCIPLE OF TRANSFINITE INDUCTION. *Let $\{P_\alpha\}$ be any well-ordered set of propositions. If we can prove, for every α, that the truth of P_α is implied by the truth of all P_β with $\beta < \alpha$, then every P_α is true.*

Proof. There can be no first false P_α; hence the set of all false P_α is void.

We can restate this in another form. By a *limit-number* in a well-ordered sequence, we mean a term α such that, given $\beta < \alpha$, there exists γ satisfying $\beta < \gamma < \alpha$. Then, by definition, we get as a corollary the

SECOND PRINCIPAL OF TRANSFINITE INDUCTION. *Let $\{P_\alpha\}$ be any well-ordered set of propositions. In order to prove the truth of all P_α, it suffices to prove that:* (i) *P_1 is true,* (ii) *if P_α is true, then $P_{\alpha+1}$ is true,* (iii) *if α is a limit-number, and all P_β with $\beta < \alpha$ are true, then P_α is true.*

Other ordinals can easily be constructed by performing ordinal operations.

THEOREM 3. *The ordinal sum and product of any two ordinals V, W are themselves ordinals.*

Proof. If S is any non-empty subset of $V \oplus W$, then either $S \leqq W$ contains a first element, or the intersection $S \frown V$ of S and V is non-empty and contains a first element, which is (since $v < w$ for any $v \in V$, $w \in W$) a first element of S. Again, if S is any non-empty subset $V \circ W$, then the set T of $v \in V$ such that $(v, w) \in S$ for some w is non-empty, and must have a first element v_1. The set of $w \in W$ such that $(v_1, w) \in S$ is not empty by construction; let w_1 be its first element. Then (v_1, w_1) is the first element of $V \circ W$.

It follows that we can construct many ordinals: $\omega \oplus \mathbf{1}, \omega \oplus \mathbf{2}, \cdots, \omega \oplus \omega = \mathbf{2} \circ \omega, (\mathbf{2} \circ \omega) \oplus \mathbf{1}$, etc. It is usual to write these using the ordinary (i.e., cardinal) symbols for addition and multiplication, thus, $\omega + \mathbf{1}, \omega + \mathbf{2}, \cdots, \mathbf{2}\omega, \mathbf{2}\omega + \mathbf{1}, \cdots$, but for consistency we shall adhere to our general notation.

Let W be any well-ordered set. Then W must contain a first element, w_1; $W - w_1$ must contain a first element w_2; $\cdots$. Hence, *if W is infinite, it must contain an initial interval isomorphic with ω,* consisting of $w_1, w_2, w_3, \cdots$. Hence we can write $W = \omega \oplus R$, where R is the residual final interval. Repeating the process, we either have $W = \omega \oplus \boldsymbol{n}$ for some finite ordinal $\boldsymbol{n}$, or $W = \omega \oplus \omega \oplus S = (\mathbf{2} \circ \omega) + S$, where S is a residual final interval.

[2] See Birkhoff-MacLane, Ch. I, §§4, 5; esp. p. 13, Ex. 8.

We can continue this process, to show that W either is of the form $(m \circ \omega) + n$, or contains an initial segment isomorphic with ${}^2\omega$ (i.e. the ordinal ω raised to the ordinal power with exponent ordinal two). Continuing further, we get the *ordinal polynomials* in ω

(1) $W = a_n \circ {}^n\omega \oplus a_{n-1} \circ {}^{n-1}\omega \oplus \cdots \oplus a_0$, where $a_0, \cdots, a_n$ are finite ordinals.

Our construction shows that every ordinal which is not isomorphic to an ordinal polynomial in ω contains initial segments isomorphic with every such polynomial, and in this sense is "bigger" than all of them. Our construction further indicates the possibility that the ordinals themselves form a well-ordered set $1, 2, 3, \cdots; \omega, \omega \oplus 1, \omega \oplus 2, \cdots; 2 \circ \omega, (2 \circ \omega) \oplus 1, \cdots; 3 \circ \omega, (3 \circ \omega) \oplus 1, \cdots$. We shall prove this formally in §3.

Let us first take stock of what we have achieved so far. We have exhibited in fairly concrete form a large number of countable well-ordered sets. However, we have failed to construct any uncountable well-ordered set. *The problem of "constructing" an uncountable well-ordered set is probably the most important unsolved problem of set theory.*

Ex. 1. Represent $(3 \circ \omega) \oplus 4$ and ${}^3\omega$ as subsets of R^*.

Ex. 2. Prove in detail that every ordinal polynomial is countable.

Ex. 3. (a) Show that ${}^\omega 2$ is a chain, but not a well-ordered set.

(b) Represent it as a subset of R^* ("Cantor discontinuum").

(c) Represent R^* with $-\infty$ and $+\infty$ adjoined as an image of ${}^\omega 2$ under an isotone transformation.

Ex. 4. Show that for ${}^YX$ to be a chain, it is sufficient for Y to be well-ordered and X a chain. What conditions are necessary and sufficient?

Ex. 5*. We define a *selection operator* on a set S, as a single-valued function which assigns, to each non-empty subset T of S, an element $\phi(T)$ of T. Show that S can be regarded as a well-ordered set, and ϕ as the operator of selecting the first element of T, if and only if it has the *absorption property* $\phi(VT_\sigma) = \phi(V\phi(T_\sigma))$. (Here V denotes the set-union for all values of σ.) If we denote $\phi(a, b)$ as $a \frown b$, what formal properties can you show that ϕ possesses? (Cf. L1–L3 infra.)

Ex. 6. Show that every ascending well-ordered set $x_1 < x_2 < x_3 < \cdots < x_\omega < \cdots$ of real numbers is countable.

Ex. 7. (a) Show that a chain is either well-ordered or contains the dual $\breve{\omega}$ of ω.

(b) Show that if a chain and its dual are both well-ordered, then it is finite.

(c) Let C be a conditionally complete chain in which every element has an immediate predecessor and an imediate successor. Show that C is J.

Ex. 8. Show that if a well-ordered set S can be mapped onto a set T by an isotone transformation, then T is well-ordered.

Problem 12*. Well-order by a specific construction some uncountable set. Well-order by a specific construction the real numbers.

3. Fundamental theorem about ordinals. We shall now obtain some important properties of ordinals, based on constructions involving *ideals*. We note that an ideal of a chain C is a subset of C which contains, with any $c \in C$, all $x < c$; i.e., it is an initial interval. The void set is not excluded.

LEMMA 1. *The ideals of a well-ordered set W consist of W itself, and for each $a \in W$, the set of $x < a$.*

Proof. For each $a \in W$, the set of $x < a$ is an ideal. Conversely, if J is an ideal of W other than W, then there must be a first element a of W not in J; clearly J contains all $x < a$, but not a or any $c > a$.

LEMMA 2. *There is at most one isomorphism between ideals J and K of well-ordered sets V, W.*

Proof. Suppose there are two, say θ and θ^*. Since J is well-ordered, there must be a first $a \in J$ such that $\theta(a) \neq \theta^*(a)$, say $\theta(a) > \theta^*(a)$. Then the image $\theta(J)$ of J cannot contain $\theta^*(a)$, since $\theta(b) > \theta^*(a)$ if $b \geqq a$, and $\theta(b) = \theta(b^*) < \theta^*(a)$ if $b < a$. Yet $\theta(a) > \theta^*(a)$; hence $\theta(V)$ is not an ideal, contrary to hypothesis.

We now observe that if θ_α is, for each α, a single-valued correspondence of a subset S_α of a set X into a set Y, and if $\theta_\alpha(x) = \theta_\beta(x)$ for all α, β whenever both are defined, then the θ_α have a greatest *common extension* θ, which is single-valued, defined by making $\theta(x) = \theta_\alpha(x)$ if $\theta_\alpha(x)$ is defined for one or more α. It follows from Lemma 2 that there is a most extensive isomorphism between ideals of well-ordered sets V and W. By Lemma 1, this involves either all of V or all of W, or is between the set of $x < a$ and $y < b$ for some $a \in V$ and $b < W$. But in the last case it could be further extended, by letting $\theta(a) = b$. Hence we include

LEMMA 3. *Of any two well-ordered sets V, W, one is isomorphic with an ideal of the other.*

It follows that if we let $V \leqq W$ mean that V is isomorphic with an ideal of W, then P4 holds. But P1, P3 are obvious, and P2 (with $=$ meaning isomorphism) is a corollary of Lemma 2. Finally, if Ω is any non-void set of ordinals (well-ordered sets), take some $W \in \Omega$. The set of $V \not> W$ consists by Lemma 3 of ordinals isomorphic with ideals of W, and these form a well-ordered set by Lemma 1. We conclude

THEOREM 4. *Any set of ordinals is well-ordered, if we define $V \leqq W$ to mean that V is isomorphic with an ideal of W; here $V = W$ means that V and W are isomorphic.*[3]

By Lemma 1, each ordinal W is isomorphic with the well-ordered set of ordinals $V < W$.

LEMMA 4. *Let W be a well-ordered set, and let ψ be any rule which determines, for each $a \in W$ and choice of $\psi(b)$ for all $b < a$, a unique $\psi(a)$. Then $\psi(a)$ is uniquely and consistently defined for all $a \in W$.*

[3] For Theorem 3 see Hausdorff [1, §13], who attributes the result to G. Hessenberg *Grundbegriffe der Mengbenlehre*, 1906). The ideas go back to Cantor and Dedekind. Cf. also G. Hessenberg, *Kettentheorie und Wohlordnung*, Jour. f. Math. 135 (1910), 81–133; J. von Neumann, *Axiomatisierung der Mengenlehre*, Math. Zeits. 27 (1928), 670–752.

Proof. For each initial interval A of W, let $P(A)$ be the proposition that $\psi(a)$ is uniquely and consistently defined for all $a \in A$. Since the A are well-ordered, it is enough to show that there is no first A for which $P(A)$ is false. But this is obviously impossible if A has a last element a; since ψ is uniquely and consistently defined for all $B < A$, we can also make a common extension (uniquely and consistently defined) to A, if A is the union of the initial segments $B < A$. (Cf. van der Waerden [1], 1st ed., vol. 1, p. 197.)

Ex. 1. Show that in a well-ordered set, every element α not the last has a unique successor, denoted $\alpha + 1$.

Ex. 2. (a) Show that $V \leqq W$ if and only if V is isomorphic with a subset of W.

(b) Show that there is no isotone transformation of $\omega \oplus 1$ onto all of ω.

Ex. 3. (a) Show that $V \leqq W$ is equivalent to $W = V \oplus X$ for some X, and that this X is uniquely defined.

(b) Infer that we have one-sided subtraction and cancellation.[4]

(c) Show that, however, $X \oplus V = Y \oplus V$ does not imply $X = Y$.

Ex. 4. Show that $X \circ V = Y \circ V$ implies $X = Y$, unless $V = 0$, whereas $\omega \circ 2 = \omega \circ 1$.

Ex. 5. (a) Which polynomials $p(\omega) = W$ are isomorphic with all their dual ideals[5]— i.e., satisfy $W = X \oplus W$ for all $X < W$?

(b) Which polynomials $p(\omega) = W$ are isomorphic with all their "cofinal" subsets —i.e., with all subsets S such that every $w \in W$ satisfies $w < s$ for some $s \in S$? Cf. Ex. 6(b).

(c) An ordinal which is isomorphic with all its dual ideals is called by Sierpinski "indecomposable." Show that any ordinal has a unique representation as a sum of non-increasing indecomposables.

Ex. 6. (a) Which polynomials $p(\omega) = W$ have the property that, for all $X \leqq \omega$, $W = T \circ X$ for some T?

(b) Which have the property that $W = W \circ X$ for all $X < W$?

(c) Show that 2 and ω have no common right-multiple.

(d) Show that the set of all left-divisors of any ordinal number is finite.

Ex. 7. (a) Let θ be any isomorphism of a well-ordered set ω with a part of itself. Show that $\theta(x) \geqq x$ for all x (Hausdorff).

(b) Show that $\alpha < \beta$ implies ${}^{\alpha}2 < {}^{\beta}2$, for well-ordered sets.

Ex. 8. (a) Let A, B be any ordinal numbers, with $A < B$. Show that unique ordinals X, R exist such that $B = (X \circ A) \oplus R$ $[0 \leqq R < B]$. (Left-division algorithm.)

(b) Show that any ordinal number can be represented as an ordinal product of a finite number of factors, not further factorable into smaller factors.

(c) Show that $\omega \circ (\omega \oplus 1) = \omega \circ \omega$; hence no unique factorization theorem is true.

Ex. 9*. (a) Using Transfinite Induction, show that we can define an ordinal arithmetic by the rules (cf. formulas (8)–(9) of Ch. I, §8) suggested by Cantor.

(i) $X \oplus (Y \oplus 1) = (X \oplus Y) \oplus 1$,

(ii) $X \circ (Y \oplus 1) = (X \circ Y) \oplus X$,

(iii) ${}^{Y \oplus 1}X = {}^{Y}X \circ X$,

and (for limit-ordinals)

(i′) $X \oplus (\mathrm{Lim}\, Y_\alpha) = \mathrm{Lim}\, (X \oplus Y_\alpha)$,

(ii′) $(\mathrm{Lim}\, Y_\alpha) \circ X = \mathrm{Lim}\, (Y_\alpha \circ X)$,

(iii′) ${}^{(\mathrm{Lim} Y_\alpha)}X = \mathrm{Lim}\, ({}^{Y_\alpha} X)$.

---

[4] The possibility of one-sided cancellation suggests trying to define transfinite rational numbers; see J. W. Olmsted, Bull. Am. Math. Soc. 51 (1945), 776–80.

[5] See Sierpinski [1, p. 176 ff.], who calls such terminal segments "residues"; they may also be called dual ideals. For Ex. 5(c), see Sierpinski [1, p. 182]; for Ex. 6(d), see ibid., p. 196; for Ex. 9, see pp. 196–99.

(b) Show that the resulting operations of addition and multipication are identical with those of Ch. I, §8; but that $^{\omega}2$ and $^{\omega}\omega$ have different meanings in the two systems.

(c) Show that $X \circ (\text{Lim } Y_\alpha) \geqq \text{Lim } (X \circ Y_\alpha)$, but that equality need not hold.

Ex. 10. (a) Let $\aleph_1$ denote the first uncountable ordinal. Show that $\aleph_1$ is isomorphic with all its cofinal subsets.

(b) Let $f(x)$ be any isotone function assigning to each $x \in \aleph_1$ an $f(x) \leqq x$ in $\aleph_1$, and suppose the set of $f(x)$ has no upper bound in $\aleph_1$. Show that $x = f(x)$ for uncountable many x. (Hint: Otherwise, the set of y greater than every $x = f(x)$ would be uncountable, hence isomorphic with $\aleph_1$. Define $g(y)$ as the least x with $f(x) \geqq y$. Form any sequence with $y_{n+1} = g(y_n)$; take $y_n \uparrow b$, and show $f(b) = b$, contrary to hypothesis.)

(c) Show that the set of $f(x) = x$ contains a limit ordinal.[6]

Problem 13. Develop a canonical form for the representation of an ordinal product. (See Ex. 8 above; consider the possible extreme right-hand factors.)

Problem 14. Simply order "intrinsically" (i.e., naturally) the sets (i) of all real functions of a real variable, (ii) of all rational-valued functions of a rational argument, (iii) of all functions from J to J. Try to preserve as many "natural" laws as you can.

4. Chain conditions; atomicity. Hilbert showed that classical invariant theory depended fundamentally on the fact that the ideals in many polynomial rings formed a lattice satisfying the following ascending chain condition.[7]

Definition. *A partly ordered set P satisfies the ascending chain condition (resp. descending chain condition) if and only if every non-void subset of P has a maximal (minimal) element.*

If P satisfies the ascending chain condition, then so (obviously) does every subset of P; if P and Q both do, then so do $P + Q$, $P \oplus Q$, PQ, and $P \circ Q$. Again, since being minimal and least are equivalent for chains, we see that a chain satisfies the *descending* chain condition if and only if it is well-ordered. More generally, we have

Theorem 5. *The following statements about a partly ordered set P are equivalent:* (i) *P satisfies the ascending chain condition*, (ii) *in the dual $\check{P}$ of P, every chain is well ordered*, (iii) *all ascending chains in P are finite.*

Proof. If P fails to satisfy the ascending chain condition, then it contains a non-void subset X without maximal element. Choose $a_1 \in X$; since a_1 is not maximal, we can find $a_2 > a_1$ in X; then $a_3 > a_2$ in X for the same reason, and so on. We thus get an infinite ascending chain $a_1 < a_2 < a_3 < \cdots$ isomorphic to the ordinal ω, and (iii) fails. If (iii) fails, since the dual of ω is not well-ordered, (ii) fails. Finally, if (ii) fails, since in chains minimal elements are least elements, (i) fails, and the circle of proof is completed.

If P satisfies the ascending chain condition, then we can also argue by induction as follows. If a property Φ is not true of every element of P, then there must

[6] Ex. 10 summarizes unpublished work of R. Vazquez Garcia.

[7] Cf. the discussion of Hilbert's Basis Theorem in van der Waerden [1, §80], from which much of this section is taken. Other applications were pointed out by E. Artin, Hamb. Abh. 5 (1927), 245–289.

be some maximal element m which fails to have it. All $x > m$ will then have the property. We conclude the

GENERALIZED INDUCTION PRINCIPLE. *Let a partly ordered set P satisfy the ascending chain condition, and let Φ be any property. In proving that every $a \in P$ has property Φ, we can assume, for each a, that all $x > a$ have property Φ.*

It may be that not all chains of a partly ordered set P are well ordered, and yet that any $a < b$ can be joined by at least one well-ordered maximal chain. For example, this is true of the system of all subsets of any class—using the Axiom of Choice (§8 infra), we can add to any set single points one at a time until we exhaust any prescribed overset. It is also true of the system of all closed subsets of any topological space, and of the algebraically closed subfields of any field (since we can adjoin points resp. transcendental elements one at a time).

When this is true, P will be called $\uparrow$-atomic,[8] and if the dual of P is $\uparrow$-atomic, P will be called $\downarrow$-atomic. The system of all subsets of the continuum is both $\uparrow$-atomic and $\downarrow$-atomic (being self-dual).

Among systems which are neither $\uparrow$-atomic nor $\downarrow$-atomic, we mention: The real numbers; measurable sets modulo sets of measure zero (see Ch. X, §12; all maximal chains are isomorphic with line segments); and the system of all sets of positive integers modulo finite subsets.

Ex. 1. (a) Show that any finite partly ordered set satisfies both chain conditions.

(b) Show that P satisfies both chain conditions if and only if all its chains are finite.

(c) Show that ${}^{P}Y$ is partly ordered if and only if P satisfies the ascending chain condition.

Ex. 2. (a) Let L be any lattice which satisfies the ascending chain condition. Show that *every* subset of L has a least upper bound.

(b) Show that if a lattice L satisfies the ascending chain condition, then every ideal in L is principal.

Ex. 3. (a) Let P be the set of all finite sequences $\xi = (x_1, \cdots, x_m)$, $\eta = (y_1, \cdots, y_n)$, $\cdots$ of positive integers. Define $\xi \leqq \eta$ if ξ can be obtained from η by a finite sequence of "reductions," each of which either deletes a component or replaces it by a smaller integer. Prove that P satisfies the descending chain condition. (R. P. Dilworth)

(b) In a lattice which satisfies the ascending chain condition, show that the irredundant representations of any element as meet also satisfy the ascending chain condition.

Ex. 4. Show that any join-homomorphic image of a lattice which satisfies the ascending chain condition also satisfies it.

Ex. 5.* Show that if the lattice of congruence relations of an abstract algebra A satisfies the ascending *or* the descending chain condition, then any representation of A as a cardinal product can be refined to a representation of A as a cardinal product of indecomposable factors.

Ex. 6. Let L be the lattice of all subgroups of the group G of all sequences $(x_1, x_2, x_3, \cdots)$ of integers under addition mod n, where $x_i = 0$ except for a finite set of i. Show that L is $\uparrow$-atomic but satisfies neither chain condition.

---

[8] This use of the word "atomic" goes back in the case of complete Boolean algebras to A. Tarski [2]. Our definition is different in appearance from Tarski's, but effectively equivalent for Boolean algebras (see Ch. X, Thm. 16).

Ex. 7. Let P be a partly ordered set, in which (i) every chain is finite, and (ii) every totally unordered subset is finite. Show that P is finite. (D. Kőnig)

Ex. 8. Show that the conditions (i) P satisfies the descending chain condition and (ii) P contains no infinite totally unordered subset are together equivalent to (iii) any infinite subset of P contains an infinite ascending chain. (I. Kaplansky)

Ex. 9.* Let L be the lattice of all subalgebras of an algebra A. Show that if $a > b$ in L, then c, d exist in L such that $a \geqq c > d \geqq b$ and c covers d.

Ex. 10. Show that the lattice of all subalgebras of an algebra A satisfies the ascending chain condition if and only if every subalgebra S of A is generated by a finite set of elements. (Bruce Crabtree)

Ex. 11.* Let L be the lattice of all subsets of a countable set, modulo finite subsets. Show that any maximal chain of L has a well-ordered uncountable subchain. (A. Gleason—E. E. Mőise)

5. Topology of chains. It is well known that the topology of the real continuum can be defined in terms of order; this can be generalized to arbitrary partly ordered sets. The generalization to chains came first historically;[9] we shall now discuss it.

DEFINITION. *Let C be any chain. The open intervals of C are* (i) *C itself, denoted $(-\infty, +\infty)$,* (ii) *for any $a \in C$, the set $(a, +\infty)$ of all $x > a$,* (iii) *for any $a \in C$, the set $(-\infty, a)$ of all $x < a$, and* (iv) *for any $a < b$ in C, the set (a, b) of all x satisfying $a < x < b$. The closed intervals $[-\infty, +\infty]$, $[a, +\infty]$, etc. of C are obtained from the open intervals by writing $\leqq$ in place of $<$. By a neighborhood of an element $p \in C$ is meant any open interval containing x.*

THEOREM 6. *Any chain is a normal Hausdorff space under its intrinsic topology—and the latter is invariant under automorphisms and dual automorphisms.*

Proof. This means first that any $p \in C$ has a neighborhood (i.e., C); that the intersection of any two neighborhoods of p is a neighborhood of p; that any neighborhood of p is also a neighborhood of all its points, i.e., that our "open intervals" can be taken as a basis of neighborhoods. Again if $p \neq q$ in C, either p covers q or $p > a > q$ for some a, or dually. In the first case, $(-\infty, p)$ and $(q, +\infty)$ form a pair of disjoint neighborhoods; in the second, $(-\infty, a)$ and $(a, +\infty)$ do; dually for the last two cases. Hence, C is a Hausdorff space and, in particular, a T_1-space. We postpone the proof of normality, until after Thm. 7.

In any Hausdorff space, a non-void *open* set is defined as a union of neighborhoods (hence, in our case, of open intervals) and a *closed* set as a set whose complement is open. It is easily shown that any union of open sets is open, and that any intersection of closed sets is closed. The *closure* $\bar{S}$ of a set S is defined as the intersection of all closed sets containing S; the *interior* of S as the union of all open sets contained in S.

The most general closed set in a chain is thus an intersection of complements

---

[9] Prof. E. W. Chittenden kindly furnished me with the following references: Hahn, Wiener Ber. 122 (14), 945–67; Haar and Kőnig, Crelle's Jour. 139 (1910), 16–28; Mahlo, Leipz. Ber. 63 (1906), p. 319; F. Riesz, Math. Annalen 61 (1905), 406–21; F. Hausdorff, Math. Annalen 65 (1908), 435–505, and Leipz. Ber. vol. 58, p. 128, and vol. 59. The present formulation was first given in [LT, §35]; see also O. Frink [1].

of open intervals. But the complement of any open interval is the sum of one or two closed intervals. Hence the most general closed set is an intersection of finite sums of closed intervals. This proves

THEOREM 7. *In any chain C, the closed intervals form a sub-base for the family of closed sets.*

Now let S and T be any disjoint closed sets in C; then $S \smile T$ will be closed, and so its complement will be a union of open intervals I_α. In each I_α, choose an x_α (this requires the Axiom of Choice). Each point of S not interior to S must be separated from T on each side by some I_α, since T is closed and $S \frown T = 0$. We adjoin to p the open interval (p, x_α) or (x_α, p), as the case may be. After augmenting T similarly, we have embedded S and T in disjoint open sets; this is the definition of normality, and we have finished the proof of Thm. 6.

Now suppose that C is a *complete chain*—i.e. (Ch. II, §1), that every non-empty subset of L has a l.u.b. and a g.l.b. Every finite chain is complete; so is the real number system $R^\#$ if $-\infty$ and $+\infty$ (i.e., O and I) are adjoined. More generally, if X and Y are any two complete chains, then so are $X \oplus Y$ and $X \circ Y$. In this way, a large variety of non-isomorphic complete chains can be constructed.

DEFINITION. *Let $\{x_\alpha\}$ be any directed set of elements of a complete chain. We define*

$$(2) \qquad \text{Lim inf } \{x_\alpha\} = \text{Sup}_\beta \{\text{Inf}_{\alpha \geqq \beta} x_\alpha\}, \qquad \text{Lim sup } \{x_\alpha\} = \{\text{Inf}_\beta \text{Sup}_{\alpha \geqq \beta} x_\alpha\}.$$

It follows by the minimax inequality (5) of Ch. II, that

$$(3) \qquad \text{Lim inf } \{x_\alpha\} \leqq \text{Lim sup } \{x_\alpha\}.$$

THEOREM 8. *In a complete chain, $x_\alpha \to a$ if and only if*

$$(4) \qquad \text{Lim inf } \{x_\alpha\} = \text{Lim sup } \{x_\alpha\} = a.$$

Proof. To say $x_\alpha \to a$ means, as in the Foreword on Topology, that every open interval (b, c) containing a contains, for some β, all x_α with $\alpha \geqq \beta$. But if this is true, $\text{Inf}_{\alpha \geqq \beta} x_\alpha \geqq b$—and, since this is true for all $b < a$, Lim inf $\{x_\alpha\} \geqq a$. Dually, $x_\alpha \to a$ implies Lim sup $\{x_\alpha\} \leqq a$, whence, by (3), $a =$ Lim inf $\{x_\alpha\} =$ Lim sup $\{x_\alpha\}$. Conversely, if Lim inf $\{x_\alpha\} = a =$ Lim sup $\{x_\alpha\}$, and $a \in (b, c)$, then $\text{Inf}_{\alpha \geqq \beta} x_\alpha > b$ and $\text{Sup}_{\alpha \geqq \gamma} x_\gamma < c$ for some β, γ; hence if $\delta \geqq \beta, \gamma$ then $x_\alpha \in (b, c)$ for all $\alpha \geqq \delta$, and so $x_\alpha \to a$.

COROLLARY. *In a complete chain, if $x_\alpha \to a$, then there exist directed sets $t_\alpha \uparrow a$ and $u_\alpha \downarrow a$ with $t_\alpha \leqq x_\alpha \leqq u_\alpha$.*

(The notation $t_\alpha \uparrow$ means that $\alpha \leqq \alpha'$ implies $t_\alpha \leqq t_{\alpha'}$, and $Vt_\alpha = a$.)—Exs. 9–10 below show that this result is not valid for arbitrary chains. The result is however valid for sequences in any lattice; cf. Ex. 8 below.

THEOREM 9. *A chain C is complete if and only if it is topologically compact.*[10]

Proof. Let $\{W_\alpha\}$ be any family of open sets covering C, a complete chain. Since each W_α is a union of open intervals, C is covered also by a family of open intervals $V_{\alpha,\beta} \leqq W_\alpha$. To show that C is compact, it is clearly sufficient to show that C can be covered by a finite subfamily of $V_{\alpha,\beta}$. But let A be the set of all a such that $[0, a]$ can be covered by a finite subsystem of $V_{\alpha,\beta}$. We first note that $\sup A = b \in A$, since some $V_{\alpha,\beta}$ contains b and hence some $a \in A$ giving a finite covering of the interval $[O, b] \leqq [O, a] \cup V_{\alpha,\beta}$. We shall now show that $b = I$, whence $C = [O, I]$ can be covered as desired. Indeed, let c be the g.l.b. of the $x > b$; adding any neighborhood of c to any finite covering of $[O, b]$, we would get a finite covering of a larger interval unless the set of $x > b$ is void—i.e., unless $b = I$. This would contradict the definition $b = \sup A$.

Conversely, let X be any subset of a compact chain C. For each finite subset F of X, we define Y_F as the least of the $x \in F$; clearly none of the finite intersections $[-\infty, Y_F]$ of the closed intervals $[-\infty, x]$ is void; hence $\bigwedge_x[-\infty, x]$ is non-void, and X has a lower bound a. Now consider the set of all closed intervals $[a, x]$ where $x \in X$ and a is a variable lower bound to X. No finite intersection is void; hence $\bigwedge[a, x]$ contains an element b. But any such b clearly is a lower bound of X which contains every lower bound of X; hence $b = \operatorname{Inf} X$, which exists. Dually, $\operatorname{Sup} X$ exists, completing the proof.

Ex. 1. (a) Show that a subset S of a chain C which is "dense-in-itself," is order-dense (§1) if and only if $\bar{S} = C$.

(b) Show that the intrinsic topology of any dense subset of C may be obtained from that of C by relativization, but that this is not true of all subsets of C.

Ex. 2. (a) Show that if $x_\alpha \to a$ in a well-ordered set, then for some α, $x_\beta \leqq a$ for all $\beta \geqq \alpha$.

(b) Show that $x_\gamma \uparrow a$ for some cofinal subset $\{x_\gamma\}$ of $\{x_\alpha\}$.

Ex. 3. A transfinite ordinal is called a *limit*-ordinal if and only if $\alpha = \beta \oplus 1$ for no β. Show that "limit-ordinals" are those which are topological limits of other numbers.

Ex. 4. Show that if $a \in \bar{X}$ on a chain, then a is the limit of a monotone well-ordered subset of X.

Ex. 5. Show that any isotone image of a complete chain is complete.

Ex. 6. Show that any isotone function from a complete chain to itself has a fixpoint.[11]

Ex. 7. (a) Show that, in a complete chain, every open set can be expressed uniquely as the union of disjoint open intervals.

(b) Show that any chain C with a countable order-dense subset has a countable neighborhood basis.

Ex. 8. Show that in $C = R^* \circ 2$, the countable subset S of all pairs $(r, 1)$ and $(r, 2)$, with r rational, satisfies $\bar{S} = C$ but is not order-dense in the sense of §1. (Cf. Exs. 1(a), 7(b).)

Ex. 9. (a) Prove directly that, in a chain, $x_n \to a$ if and only if sequences $t_n \uparrow a$ and $u_n \downarrow a$ exist, with $t_n \leqq x_n \leqq u_n$. (Hint: Define t_n as the least element of the set $a, x_n, x_{n+1}, \cdots$, and show that it exists. Cf. [LT, Thm. 2.15].)

(b) Show that if we define x_α for $\alpha < 2 \circ \omega$ as $1/n$ for $\alpha = n$, and $1 - 1/(n + 2)$ for $\alpha = \omega \oplus n$, then $x_\alpha \to 1$. Yet, on $(0, 1)$ we cannot find $y_\alpha \leqq x_\alpha$ with $y_\alpha \uparrow 1$.

[10] This result is due to Haar and König, op. cit. supra.

[11] This result is due to B. Knaster, Annales de la Soc. Polonaise de Math. 6 (1927), p. 133. It is generalized in Thm. 8 of Ch. IV.

Ex. 10*. Replace each $x < \aleph_1$ in Ex. 10 of §3 by a replica $(x, 1) > (x, 2) > (x, 3) > \cdots$ of the dual $\breve{\omega}$ of ω, obtaining $\aleph_1 \circ \breve{\omega}$. Show that the well-ordered set (x, n), well-ordered as in $\aleph_1 \circ \omega$, converges to $\aleph_1$. Show that we cannot find $y_{x,n} \uparrow a$ with $y_{x,n} \leqq (x, n)$ in $\aleph_1 \circ \breve{\omega}$ even cofinally. (Hint: We would have to have $y_{x,n} \leqq (x, n)$ in $\aleph_1 \circ \omega$ as well as in $\aleph_1 \circ \breve{\omega}$, this would imply by Ex. 10 of §3 that $y_{x,n} = (x, n)$ for some cases, and hence $y_{x,n+1} \geqq y_{x,n} = (x, n) > (x, n + 1)$, contrary to hypothesis.)

Ex. 11*. Show that, if A, B, C are complete chains, then $A \circ B = A \circ C$ implies $B = C$. (A. Gleason)

Problem 15. Prove that every chain is a normal Hausdorff space without using the Axiom of Choice, or show that this cannot be proved. (Notes: A. Gleason says it can be proved for complete chains. A related unsolved problem is stated in Tukey [1, p. 15].)

6. Axiom of choice. We shall now discuss an assumption which appears to be independent of, and yet consistent with,[12] the usual logical assumptions regarding classes and correspondences—but whose absolute validity has been seriously questioned by many authors. This is the so-called Axiom of Choice.[13]

It may be stated in many forms, and it implies that every set can be well-ordered. An especially simple formulation is the following

(AC1) Every chain C in a partly ordered set P is contained in a *maximal* chain M in P.

That is, there exists a set $M \leqq P$ which is a chain, and which is contained in no larger chain N, $N \leqq P$. It is easy to show that (AC1) implies the following condition, whose importance was first pointed out by M. Zorn.[14]

(AC2) If every chain C of a partly ordered set P has an upper bound $U(C)$ in P, then P contains a maximal element.

Indeed, any upper bound U of any maximal chain M of P will obviously be a maximal element of P, and such maximal chains exist, if (AC1) holds.

Tukey has significantly generalized (AC2). He calls a property Φ of sets S "a property of finite character," if $S \in \Phi$ is equivalent to $F \in \Phi$ for all finite subsets of S. Clearly, in this case, $S \in \Phi$ implies $T \in \Phi$ for every $T \leqq S$; hence properties of finite character are what are often called "independence properties." Tukey's condition is

(AC3) Let Φ be a property of finite character defined for the subsets of a set S. Then there is a maximal subset M of S having the property Φ (i.e., a maximal $M \in \Phi$).

We now show that (AC2) implies (AC3). Let C be a maximal chain of

[12] See K. Gödel, *The consistency of the continuum hypothesis*, Princeton 1940.

[13] First formulated by E. Zermelo, Math. Annalen 59 (1904), p. 514, and 65 (1908), p. 261. Condition (AC1) is due to Hausdorff, *Grundzüge der Mengenlehre*, 1st ed. p. 140.

[14] M. Zorn, Bull. Am. Math. Soc. 41 (1935), p. 667. Further applications were made by J. W. Tukey [1, Ch. I, §6]; see also G. Birkhoff and O. Frink, *Representation of lattices by sets*, Trans. Am. Math. Soc. 64 (1948), 299-316. The condition itself was noted earlier by R. L. Moore (*Foundations of point set theory*, New York 1932, p. 84), and Kuratowski.

sets $X_\sigma \in \Phi\ [X_\sigma \leqq S]$. Then if F is any finite subset of the union U of the $X_\sigma \in C$, since each $a_i \in F$ is contained in some $X_i \in C$, the largest of these X_i will contain F; hence $F \in \Phi$. It follows that $U \in \Phi$, whence Φ satisfies the hypotheses of (AC2) and so (assuming (AC2)) has a maximal member.

It is evident that the condition that a set T satisfy all properties Φ_α of a collection $\hat{f}$ of properties of finite character is itself a property of finite character. Hence we also have

(AC3′) Let $\hat{f}$ be any collection of properties Φ_α of finite character on a set S. Then there is a maximal subset M of S satisfying every $\Phi_\alpha \in \hat{f}$.

We shall apply this useful condition in §4. For the present we merely note that the property of being a chain is of finite character. (It is of character two: it requires that, given $x, y \in T$, either $x \geqq y$ or $y \geqq x$!). Hence (AC3′) implies (AC1), and completing the circle of implications (AC1) $\rightarrow$ (AC2) $\rightarrow$ (AC3) $\rightarrow$ (AC3′) $\rightarrow$ (AC1). *Each of these conditions is thus equivalent to all the others.*

We shall now show that they are also equivalent to the original Axiom of Choice (Auswahlsaxiom) of Zermelo:

(AC) Let I be any set. There exists a single-valued function which selects from each non-void subset T of I a well-defined element $g_M(T)$ of T.

Consider the class Γ of all single-valued functions $g{:}g(T) \in T$ defined on some (but not necessarily all) subsets of I. We shall write $g \leqq h$ if $h(S)$ exists and equals $g(S)$ whenever $g(S)$ is defined; this makes Γ a partly ordered set. We now choose a *maximal chain* M in Γ, assuming (AC1), and form the *common extension* g_M of the $g \in M$. Then g_M must be defined for all non-void T; otherwise there would exist a non-void T_0 with some element t_0, with $g_M(T_0)$ undefined. We could define

$$g^*\begin{cases} g^*(T) = g_M(T) \in T \text{ if } g_M(T) \text{ is defined,} \\ g^*(T_0) = t_0 \in T_0 . \end{cases}$$

By adding g^* to M, we would get a larger chain than M, giving a contradiction. Hence (AC1) implies (AC).

Zermelo's Theorem states that (AC) is equivalent to

(AC4) Every set I can be well-ordered.

Proof. Consider the relations ρ which well-order *subsets* $S(\rho)$ of I. Write $\rho \leqq \rho^*$ if $S(\rho)$ is an initial interval of $S(\rho^*)$. Consider only well-ordering relations "compatible" with the g_M of (AC), in the sense that g_M selects from the complement $I - A$ of each initial interval of $S(\rho)$ defined by ρ the first element after A. It may be shown as in Lemma 3, §3 that these ρ form a *chain*. Hence, their common extension $\bar{\rho}$ is single-valued, a well-ordering (any subset of the union V of the $S(\rho)$ contains a first element for some ρ—hence for all ρ), and compatible with g_M. Now $\bar{\rho}$ is clearly maximal; I say it well orders I. Otherwise we could define $\rho_1 > \bar{\rho}$ by making ρ_1 have V for an initial segment, and defining $g_M(I - V) = v$ as the last element of V increased by v. We omit the details.[15]

Since we have already proved (AC1) $\rightarrow$ (AC2) $\rightarrow$ (AC3) $\rightarrow$ (AC3′) $\rightarrow$ (AC1) and (AC1) $\rightarrow$ (AC) $\rightarrow$ (AC4), if we can prove (AC4) $\rightarrow$ (AC1) we shall have proved

THEOREM 10. *Statements* (AC), (AC1), (AC2), (AC3), (AC3′), *and* (AC4) *are equivalent formulations of the same hypothesis.*

We shall now prove (AC4) $\rightarrow$ (AC1). Given P and C as in (AC1), we first well-order the elements in P but not in C in a transfinite sequence, W. We define a function which assigns to each $a \in W$ the value $\psi(a) = M$ if, for all $b < a$ such that $\psi(b) = M$ and all $b \in C$, either $a \geqq b$ or $a \leqq b$, and the value $\psi(a) = M'$ otherwise. By Lemma 4 of §3, this function is uniquely and consistently defined; the set of all a with $\psi(a) = M$ is clearly a chain and a maximal chain, completing the proof.

Ex. 1. Strengthen the formulation of (AC3), by showing that every $T \in \Phi$ can be extended to a maximal M containing T in Φ.

Ex. 2. (a) Show that every partial ordering can be strengthened to a simple ordering. (E. Szpilrajn, Fund. Math. 16 (1930), 386–9).

(b) Show that a partial ordering can be strengthened to a well-ordering if and only if it satisfies the descending chain condition.

Ex. 3. Show that every chain has a well-ordered cofinal subset.

Ex. 4*. Let P be any partly ordered set in which every well-ordered chain has a l.u.b. Let f be any function on P to P such that $f(x) \geqq x$ for all $x \in P$. Without assuming any form of the Axiom of Choice, show that $f(m) = m$ for some $m \in P$. (See Bourbaki, *Théorie des ensembles*, p. 36.)

Problem 16. Discuss the proofs of §6 from the point of view of the "hierarchy of types," of Whitehead and Russell [1].

7. Applications; continuum hypothesis. Using the Axiom of Choice, we can prove many simple results of extreme generality, which it is apparently impossible to prove otherwise.

THEOREM 11. *Any set of cardinal numbers is well-ordered, if we define $S \leqq T$ to mean that there is a one–one correspondence between S and a subset of T.*

Proof. Each ordinal number W is a well-ordered set, which determines a cardinal number $n(W)$; moreover, the correspondence $W \rightarrow n(W)$ is isotone. Moreover, by (AC4), every cardinal number is an $n(W)$ for some W. But any set of ordinal numbers is well-ordered; hence (Ex. 7, §2) the same is true for cardinal numbers.

Using the Axiom of Choice, we can also prove that

$$\alpha + \beta = \alpha\beta = \mathrm{Max}\,(\alpha, \beta) \tag{2}$$

if α or β is infinite, for cardinal numbers. This means that a large part of trans-

[15] Cf. B. L. van der Waerden [1, 1st ed., vol. 1, pp. 194–6].

finite cardinal arithmetic is strictly uninteresting. As corollaries, we get the laws

$$\alpha + \alpha = \alpha^2 = \alpha \tag{3}$$

if α is infinite.

THEOREM 12. *A T_1-space C is compact if it contains a sub-basis B of closed sets U_β, satisfying the condition:*

(HB) *if no finite set of the U_β has a void intersection, then the U_β have a point in common.*[16]

Proof. Let K be any collection of basic closed subsets T_α with the "finite intersection property" that no finite subset F of $S_\phi \in K$ has a void intersection. Let M be a *maximal* extension of K; since the finite intersection property is a property of finite character, by (AC3) M exists. Since B is a sub-basis, any $S_\mu \in M$ is the union of a finite collection F_μ of $U_{\mu,i}$ of B. Since $U_{\mu,i} \frown (S_i \frown \cdots \frown S_{i,r(i)}) = 0$ for all $U_{\mu,i} \in F_\mu$ and suitable $S_{i,j}$ would imply

$$S_\mu \frown (\wedge S_{i,j}) = \vee(U_{\mu,i}) \frown (\wedge S_{i,j}) = \vee[U_{\mu,i} \frown \wedge S_{i,j}] \leqq \vee 0 = 0,$$

it must be possible for each S_μ to add some $U_{\mu,i}$ to M without destroying the finite intersection property. But M is maximal; hence for every $S_\mu \in M$ some $U_\mu \leqq S_\mu$ of B is also in M; in particular, this is true for the T_α. But since the U_μ satisfy (HB) and have the finite intersection property, $\wedge U_\mu > 0$. A fortiori, $\wedge T_\alpha \geqq \wedge S_\mu \geqq \wedge U_\mu > 0$.

COROLLARY 1. *Any Cartesian product of compact T_1-spaces is itself compact.*

We have already seen in §2 that the smallest infinite cardinal number is countable infinity, $\aleph_0$. But it is known that the real numbers have a larger cardinal number c (cf. Birkhoff-MacLane, Ch. XII). Since no uncountable set has been constructively well-ordered, no uncountable set has a known position in the well-ordered sequence $\aleph_0, \aleph_1, \aleph_2, \cdots$ of infinite cardinal numbers. A celebrated conjecture is the so-called

Continuum Hypothesis. *The power of the continuum c is the second infinite cardinal number*: Sierpinski has shown that this conjecture is equivalent to a large number of other unproved (and undisproved) propositions of set theory.[17]

Ex. 1. Using the Axiom of Choice, prove directly that the cardinal numbers satisfy P2 (Schröder-Bernstein Theorem).

Ex. 2. Show that the "first" ordinal having a given infinite cardinal number is always a limit-ordinal.

Ex. 3*. Show that in the lattice of all congruence relations on any algebra, the ends of any

[16] Theorem 12 is due to J. W. Alexander, *Ordered sets, complexes, and the problem of bicompactification*, Proc. Nat. Acad. Sci. 25 (1939), 296–8; the present proof to O. Frink, *Topology in lattices*, Trans. Am. Math. Soc. 51 (1942), p. 574. Corollary 1 is due to Tychonoff, Math. Annalen 111 (1935), 762–6.

[17] W. Sierpinski, *L'hypothèse du continu*, Paris, 1927; see also K. Gödel, op. cit. in §6 and Am. Math. Monthly 54 (1947), 515-24; H. Eyraud, Comptes Rendus Acad. Sci. 224 (1947), 85-7.

interval $\theta_1 \leqq \theta \leqq \theta_2$ can be connected by a chain in which covering relations are *dense* (Cf. Problem in Ch. VII, §5.)

Ex. 4*. Show that the Axiom of Choice is implied by the following weak form of Thm. 11: given two cardinal numbers α and β, either $\alpha \leqq \beta$ or $\beta \leqq \alpha$ (Law of Trichotomy P4).[18]

Ex. 5*. Show that the laws $\alpha + \alpha = \alpha$ and $\alpha^2 = \alpha$ cannot be proved without using the Axiom of Choice.

Problem 17. (Sierpinski) A cardinal number $\aleph$ is called *inaccessible* from below if there are $\aleph$ distinct cardinal numbers less than $\aleph$. Does there exist an uncountable inaccessible cardinal number?

Problem 18. Prove or disprove that every proper sublattice S of a lattice L can be extended to a maximal proper sublattice. (Suggestion: the answer may be yes for distributive lattices.)

8. Homogeneous continua; Souslin's problem. The real number system $R^\#$ is so fundamental in mathematics that much effort has been spent on giving abstract characterizations of its order relation.

THEOREM 13. *The real number system $R^\#$ and the set J of all integers are the only two chains which* (i) *give every bounded subset a* l.u.b. *and a* g.l.b., (ii) *have a countable dense subset,* (iii) *are "homogeneous," in the sense that they have a transitive group of automorphisms.*

Proof. By Thm. 2, condition (ii) states that the chain C is isomorphic with a subset of $R^\#$; we so represent it. The complement of $\bar{C}$ is then open, and consists of a countable family of non-overlapping open intervals. Condition (i) implies that at least one end point of each finite such open interval must belong to C. If in one case, both end points a, b belong to C, then some element $a \in C$ is covered by another element $b \in C$; it follows by (iii) that *every* $X \in C$ must be covered by some $y \in C$, and similarly that every x *covers* some $z \in C$. We can hence find a subinterval of C isomorphic with J; we omit the details. Finally, if some $a \in C$ were not in J, we could by (i) form sup J or inf J; but such elements could not both cover and be covered by other elements; hence $J = C$.

Otherwise, just one end point of each open interval belongs to C. In this case, if we move each point p of C towards the origin by an amount exactly equal to the sum of the lengths of the intervals between p and the origin, we get an isomorphic map of C on $R^\#$ or an interval of $R^\#$. Since if one $x \in C$ were greatest or least, every element would be (by (iii)), we see that either C consists of 0 alone (exceptional case), or C is isomorphic to an open interval of $R^\#$—and hence to $R^\#$ itself.

Various modifications of the preceding conditions are possible. Thus we can replace (iii) by a hypothesis (iii′) that *no* covering relation holds (i.e., that the chain is dense-in-itself), and get $R^\#$; or we can replace it by the hypothesis (iii″) that every $a \in C$ covers and is covered by other elements, and get J.

A very interesting modification of (ii) is Souslin's Condition: (ii′) Every

[18] This result is due to F. Hartogs, Math. Annalen 76 (1915), p. 443; Ex. 5 is due to Tarski, Fund. Math. 5 (1924), 147–54; see also Sierpinski [1, p. 282].

set of disjoint open intervals of C is countable. It is easily shown, using Thm. 2, that (ii) implies (ii′). For every positive integer n, there are at most $n + 1$ disjoint intervals of length $1/n$ or greater whose midpoint satisfies $m \leqq x \leqq m + 1$—hence only countably many disjoint intervals of positive length in R^* are possible.

Souslin's Problem[19] is to determine whether or not, conversely, (ii′) implies (ii) in any chain. This seems to be extremely difficult. The most natural approach involves constructing a maximal transfinite sequence of closed sets $S_1, S_2, S_3, \cdots, S_\omega, S_{\omega+1}, S_{\omega+2}, \cdots$ of points of subdivisions of C, by the following procedure. Without loss of generality, we can assume that C is complete (compact). Let S_1 be the void set. Form S_{n+1} from S_n by adding one point $\phi(J)$ from each open interval J between successive points of S_n; since the complement of S_n consists of a countable family of disjoint open intervals, this is possible. If α is a limit-number, S_α is the closure of the set-union of all S_β with $\beta < \alpha$. The open intervals defined in this way form a partly ordered set P which determines C to within isomorphism (homeomorphism), and Souslin's problem can be reduced to the study of P.

Condition (ii′) implies that the partly ordered set P of intervals so defined satisfies the ascending chain condition, (S1) for any $a \in P$, the set of all $x \geqq a$ in P form a chain, (S2) every chain is countable,[20] and (S3) every set of incomparable elements is countable. To say that a subset of C is dense is to say that it has a representative in every interval. This leads to the following intriguing form of Souslin's Problem.

Let P be any *tree* (i.e., partly ordered set which satisfies condition (S1)). If every chain and every set of incomparable elements of P is countable, then P is countable.

Another interesting set of conditions on chains has been proposed by G. D. Birkhoff.[21] These are equivalent to: (i**) the union $\bigvee_{i=1}^{\infty} I_n$ of any expanding sequence $I_1 < I_2 < I_3 < \cdots$ of open intervals is an open interval, Souslin's Condition (ii′), and (iii**) all intervals are isomorphic.

Chains satisfying (i**) and (iii**) are called *homogeneous linear continua*, and they yield natural generalizations of the real number system R^*. Examples of homogeneous linear continua not isomorphic to R^* have been found by Vaz-

---

[19] Proposed by M. Souslin, Fund. Math. 1 (1920), p. 223. Much work on this problem has been done by G. Kurepa (Thesis, Publ. Math. Univ. Belgrade 4 (1935), 1–138, cf. also Revista Ci. Lima 42 (1940), 827–46, 43 (1941), 483–500, and 47 (1945), 457–89; Studia Math. 9 (1940), 23–42; Acta. Math. 75 (1943), 139–50. See also W. Sierpinski, Ann. Scuo. Norm. Sup. Pisa 2 (1933), 285–7; E. W. Miller, Am. Jour. 65 (1943), 673–8; N. Cuesta, Revista Mat. Hisp. Am. 4 (1944), 175–87, 215–33; and Ex. 9, §3, and Exs. 7–8, §4, above.

[20] Since an uncountable nested sequence of intervals $I_1 > I_2 > I_3 > \cdots$ would yield an uncountable set of disjoint intervals, $I_\xi - I_{\xi+1}$.

[21] See *Los continuos lineales homogeneos de George D. Birkhoff*, and *Nota sobre el continuo*, by R. Vazquez and F. Zubieta, Bol. Soc. Mat. Mex. 1 (1944), 1–18 and 2 (1945), 91–94. There is a lacuna on p. 6, which leaves the problem mentioned below unsolved. The other reference is to R. Arens, ibid., vol. 2 (1946), p. 33.

quez and Zubieta, and by R. Arens. It might be more feasible to solve Souslin's Problem for homogeneous linear continua, than in the general case.

Ex. 1. Show that any dense subset T of a dense subset S of a chain C is dense in C.

Ex. 2. (a) Show that in any non-void chain C satisfying (iii**), given $a < b$, there exists x such that $a < x < b$.

(b) Infer that, for any a, $x < a$ and $x > a$ have solutions. (Hint: Use the isomorphism between $(-\infty, +\infty)$ and $(a, +\infty)$.)

Ex. 3. (a) Show that any linear homogeneous continuum C is "sequentially compact," in the usual topological sense that every sequence of elements of C contains a convergent subsequence.

(b) Show that any non-void C has at least the power of the continuum. (Zubieta-Vasquez)

Ex. 4. (a) In any chain C, compare the following three numbers: (i) the smallest cardinal number of a dense set (Cantor), (ii) the least upper bound of the cardinal numbers of sets of disjoint open intervals (Souslin), (iii) the least upper bound of the cardinal numbers of nested (transfinite) sequences $(a_1, b_1) > (a_2, b_2) > (a_3, b_3) > \cdots > (a_\omega, b_\omega) > (a_{\omega+1}, b_{\omega+1}) > \cdots$ of open intervals.

(b) Observe that (ii) gives a greater number than (iii), in the case of $R^{\#} \circ R^{\#}$.

Ex. 5*. Show that a chain is isomorphic with a subset of $R^{\#}$ if and only if every more than countable class of intervals contains a more than countable subclass, of which any two have a common element.[22]

Problem 19. Solve one of the forms of Souslin's Problem, either in the general case, or in the case of linear homogeneous continua.

---

[22] B. Knaster, Mat. Sbornik 16 (58), 281–90 (1945).

CHAPTER IV

COMPLETE LATTICES

1. Definition; closure operations. In Ch. II, §1, we defined a *complete lattice* as a partly ordered set in which every subset had a least upper bound and a greatest lower bound.[1] Clearly any finite lattice is complete and so is any lattice whose chains are finite. So is any complete chain such as the real number system with $-\infty$, $+\infty$; so is any cardinal product or power of complete lattices, and so are the ordinal sum and product of any two complete lattices.

However, the most typical complete lattices are obtained not in these ways, but through *closure operations*, in the following sense.

Definition. *By a "closure operation" on the subsets X of an aggregate I, we mean an operation $X \to \bar{X}$ such that*

C1. $\bar{X} \geqq X$ (*Extensive*),

C2. $\bar{\bar{X}} = \bar{X}$ (*Idempotent*),

C3. $X \geqq Y$ *implies* $\bar{X} \geqq \bar{Y}$ (*Isotone*).

By a "closed" set, we mean one X equal to its "closure" $\bar{X}$.

Theorem 1. *The subsets "closed" with respect to any closure operation form a complete lattice, in which* g.l.b. *means intersection.* (*E. H. Moore*)

Proof. The set-product P of any family Φ of closed subsets X_ϕ is closed, since by C3, $\bar{P} \leqq \bar{X}_\phi = X_\phi$ for all $X_\phi \in \Phi$, whence $\bar{P} \leqq P$. Hence P is a g.l.b. to the X_ϕ. Again, the closure $\bar{S}$ of the set-union S of the X_ϕ contains every X_ϕ by C1, and is contained in every closed set T containing every X_ϕ, since $T \geqq S$ and so $T = \bar{T} \geqq \bar{S}$ by C3 for every such T. Hence $\bar{S}$ is a l.u.b. to the X_ϕ.

There is a generalization of Moore's argument which yields a strong presumption that if g.l.b. or l.u.b. always exist, then both always exist. More precisely,

Theorem 2. *If P is a partly ordered set with I, and every non-void subset of P has a* g.l.b.—*or dually—then P is a complete lattice.*

Proof. Let X be any subset of elements x_ϕ of P, and let U be the set of upper bounds to the x_ϕ. Since U contains I, it is non-void; let $a = \text{Inf } U$. Since every x_ϕ is a lower bound of U, a contains every x_ϕ; since a is a lower bound of U, it is contained in every element containing every x_ϕ; hence $a = \sup X$, which thus exists.

E. H. Moore considered *in abstracto* properties of sets which, like the property

[1] The distinction between lattices and complete lattices was made by the author [1, p. 442]. The definition of a "closure operation" given below is due to E. H. Moore, *Introduction to a form of general analysis*, New Haven, 1910, pp. 53–80.

of being "closed" under a closure operator, (i) are satisfied by I, (ii) are satisfied by any intersection $\wedge X_\phi$ of sets X_ϕ which satisfy them. He called such properties of sets "extensionally attainable," and showed that every extensionally attainable property was associated with a closure property (Ex. 2).

More generally, if S is any subset of a complete lattice L which contains I, and contains with any subset X of L also Inf X, then S is also a complete lattice. We leave the proof to the reader.[2] If S always contains Inf X and Sup X, then S is called a *closed sublattice*.

Ex. 1. Show that the "join" of any two sets, in the lattice of all sets closed under any closure operation, is the closure of their set-union.

Ex. 2. (a) Show that if $X \to \bar{X}$ is any closure operator, then $\bar{X}$ is the intersection of the "closed" sets containing X.

(b) Show that if Φ is any property of sets satisfying (i)–(ii) above (i.e., "extensionally attainable"), and we define $\bar{X}$ as the intersection of those sets which have the property and contain X, then C1–C3 hold.

Ex. 3. Show that the g.l.b. of the void set of elements of a lattice is I, if it exists. Infer a modification of Thm. 2. (J. von Neumann)

Ex. 4. (a) Show that the ordinal sum and product of any two complete lattices are complete.

(b) Obtain necessary and sufficient conditions that the ordinal sum of two partly ordered sets be complete.

(c) Show that L^X is a complete lattice if L is, and X is any partly ordered set.

Ex. 5. Show that if $x \to \bar{x}$ is any operation in a complete lattice which satisfies C1–C3, then the "closed" elements a (such that $a = \bar{a}$) form a complete lattice.

Ex. 6*. (a) Show that if we define $^- \geqq {}^{-*}$, within the set of all closure operators on a complete lattice L, to mean $\bar{X} \geqq \bar{X}^*$ for all X, we get a complete lattice.

(b) Show that this is not necessarily true if L is an incomplete lattice. (I. Rose)

Ex. 7. Show that reflexiveness, symmetry and transitivity are "extensionally attainable" properties of relations. (Cf. Ex. 5, §4, Ch. I.)

Ex. 8. (a) Let $X \to \bar{X}$ be any operation which satisfies C1 and C3, but not C2. Show that if, for every ordinal α, we define $X_{\alpha+1}$ as $\bar{X}_\alpha$, if $X_1 = X$, and if, for every limit-ordinal τ, $X_\tau = \bigvee_{\beta<\tau} X_\beta$, then the sequence $\{X_\alpha\}$ is monotone and ultimately constant.

(b) Show that if we define $\overline{X}$ as this value, then $X \to \overline{X}$ is the least closure operation "containing" $X \to \bar{X}$ (cf. Ex. 5).

Ex. 9*. Show that C1–C3 are equivalent to the single condition $Y \cup Y \cup \bar{\bar{X}} \leqq \overline{X \cup Y}$. (A. Monteiro, Portug. Math. 4 (1945), 158–60.)

Ex. 10. (a) Show that a lattice-homomorphic image of a complete lattice need not preserve l.u.b. or g.l.b. of infinite sets. (Hint: Map $\omega \oplus 1$ onto $1 \oplus 1$.)

(b**) Show that a lattice-homomorphic image of a complete lattice L need not be complete. (Hint: Let L consist of O, I, and all infinite matrices $X = (x_{ij})$, where $S \geqq Y$ means $x_{ij} \geqq y_{ij}$ for all $i, j = 1, 2, 3, \cdots$. Let $x \equiv y \pmod \theta$ mean that the set of differences $|x_{ij} - y_{ij}|$ is bounded. Define X^k by $x^k_{kj} = j$ and $x^k_{ij} = 0$, if $k \neq i$, and Y by $y_{ij} = j$ and $y_{ij} = 0$ if $i \neq j$. Show that $\bigvee X^k$ does not exist, by showing that if T contains every $X^k \pmod \theta$ then so does $T - Y$).

Ex. 11. A lattice-homomorphism is called "complete" if and only if it preserves g.l.b. and l.u.b. of arbitrary sets. Show that the inverse image of any element under any complete homomorphism between complete lattices is a closed interval.

[2] For this result, and Exs. 5–6 below, see Morgan Ward, *The closure operators of a lattice*, Annals of Math. 43 (1942), 191–6. See also N. Nakamura, Proc. Imp. Acad. Tokyo 17 (1941), 5–6.

2. Examples. Evidently topological closure in any T^0-space is a "closure operation"; C1–C2 are postulated, and C3 follows since $X \geqq Y$ means $X \smile Y = X$, whence $\bar{X} = \overline{X \smile Y} = \bar{X} \smile \bar{Y} \geqq \bar{Y}$. Hence

THEOREM 3. *The closed (and dually, the open) subsets of any topological* (T_0)-*space form a complete lattice.*[3]

We note also, as a corollary of Thm. 4, Ch. II, that the congruence relations on any algebra with finitary operations form a complete lattice. In fact, since the part of the proof involving ξ does not require the operations to be finitary, we obtain from Thm. 2 above the stronger result that *the congruence relations on any abstract algebra form a complete lattice.* In particular, the set of all partitions of any aggregate forms a lattice; this lattice is discussed further in Ch. VII, §5.

THEOREM 4. *The subalgebras of any abstract algebra A form a complete lattice.*

Proof. Trivially, A is a subalgebra of itself; also (cf. the Foreword for definitions), the intersection of any family of subalgebras is a subalgebra. It is a corollary that the subgroups of any group, the subrings of any ring, the subspaces of any vector space, etc. form complete lattices.

The preceding observations pave the way for the study of the structure of abstract algebras, a topic taken up in more detail in Ch. VI. The convex bodies in space also form a complete lattice; the "convex hull" of any set X can be defined as the set of all $\lambda_1 x_1 + \cdots + \lambda_n x_n$, with $x_i \in X$, and $\lambda_i \geqq 0$ for $i = 1, \cdots, n$, and $\sum \lambda_i = 1$. Many other examples are studied in later chapters.

Ex. 1. Show that the following form complete lattices: (a) The normal subgroups of any group, (b) the characteristic subgroups of any group, (c) the right-ideals of any ring, (d) the ideals of any lattice, (e) the invariant subalgebras of any linear algebra.

Ex. 2. Let Φ be any class of single-valued transformations of a set I. Show that the subsets X of I with the property that $X\phi \leqq X$ for all $\phi \in \Phi$ form a complete lattice.

Ex. 3. A subset S of a vector space V with scalars in an ordered field F is called *convex* if $x, y \in S, \lambda, \mu \geqq 0$ and $\lambda + \mu = 1$ imply $\lambda x + \mu y \in S$. Prove that the convex subsets of V form a complete lattice.

3. Conditional completeness; σ-lattices. Many important lattices, though not complete, have the property that *every non-void bounded subset has a* g.l.b. *and a* l.u.b. Such lattices are called *conditionally complete.* Thus the real number system $R^{\#}$ is conditionally complete; so is the set of all functions subharmonic in a given region and assuming given boundary values.

We can prove the following partial analog of Theorem 2.

THEOREM 5. *For a lattice L to be conditionally complete, it is sufficient that*

[3] This result has been generalized by O. Ore, *Some studies of closure relations,* Duke Jour. 10 (1943), 761–85. Ore considers analogs of topological constructions for complete lattices with closure operations. See also *Mappings of closure relations,* Annals of Math. 47 (1946), 56–72.

every bounded non-void subset have a g.l.b. *In L, every non-void subset which has a lower bound has a* g.l.b.

Proof. Suppose every bounded subset X of L has a g.l.b.; consider the set U of upper bounds of X. Since X is bounded, U is non-void; select $a \in U$, and let V be the set of the $a \frown u$ [$u \in U$]. Then V is bounded above by a and below by X; hence it has a g.l.b. b. Clearly $b \geqq x$ for all $x \in X$, since the $x \in X$ are all lower bounds of V; clearly also $b \leqq a \frown u \leqq u$ for all $u \in U$; hence $b = \text{Sup } X$.

Again, if Y is a non-void subset of L which has a lower bound, form similarly for some fixed $c \in Y$, the $c \frown y$ [$y \in Y$]. These will be a bounded set, whose g.l.b. will similarly be Inf Y.

Actually, as noted by B. C. Rennie, it is sufficient that every well-ordered subset have a l.u.b. and dually; but the proof of this requires the Axiom of Choice.

The duals of the two statements of Thm. 5 follow similarly.

We shall now show that the only difference between conditionally complete lattices and complete lattices is the absence of a O and a I. This generalizes the fact that we can make $R^{\#}$ into a complete lattice by adjoining $-\infty$ and $+\infty$.

Theorem 6. *Let P be any partly ordered set in which every non-void subset having a lower bound has a* g.l.b. *Then if elements O, I are added to P, we get a complete lattice, $\overline{P}$.*

Proof. Let X be any non-void subset of $\overline{P}$; we easily reduce to the case of a subset of P. If X has a lower bound in P, the g.l.b. of X in P will still be a g.l.b. in $\overline{P}$; otherwise, $I = \text{Inf } X$, being the only lower bound of X. Now apply Theorem 2 of §1.

The example graphed in Fig. 1e, p. 12, shows that it is not sufficient to assume merely that every bounded set has a g.l.b. and l.u.b.

In set theory, much use is made of "σ-rings" of sets, or families Φ which contain the union $\bigvee_{i=1}^{\infty} X_i$ and intersection $\bigwedge_{i=1}^{\infty} X_i$ of any countable subfamily of sets $X_1, X_2, X_3, \cdots$ of Φ. For example, the measurable subsets and the Borel subsets of the line, plane, and space, all are σ-rings of sets. Evidently every σ-ring of sets is a σ-lattice, in the following sense.

Definition. A lattice L in which every countable subset has a g.l.b. and l.u.b. is called a *σ-lattice.*

Another interesting family of properties of partly ordered sets are the (m, n) Interpolation Properties.

Definition. *A partly ordered set P will be said to have the (m, n) Interpolation Property if and only if, whenever $a_1, \cdots, a_m \in P$ and $b_1, \cdots, b_n \in P$ satisfy $a_i \leqq b_j$ for all i, j, there exists an element $c \in P$ such that $a_i \leqq c \leqq b_j$ for all i, j.*

See Ex. 4 below; also F. Riesz [2] and G. Birkhoff [6, §28].

Ex. 1. Show that any σ-lattice L in which all chains are countable (as in $R^{\#}$) is complete.
Ex. 2. Show that a lattice which satisfies the ascending chain condition is conditionally

complete and has a I, but need not have an O. Illustrate by the lattice of positive integers under divisibility.

Ex. 3. For any infinite cardinal number $\aleph$, we can define a $\aleph$-lattice as a partly ordered set in which every non-void subset of $\aleph$ or fewer elements has a g.l.b. and l.u.b.

(a) Formulate and prove analogs of Exs. 1–2.

(b*) Define Lim Inf and Lim Sup for suitably restricted directed sets.

Ex. 4. (a) Show that the (2, 0)-Interpolation Property is the Moore-Smith property.

(b) Show that the $(1, n)$- and $(m, 1)$-Interpolation Properties always hold.

(c) Show that the (2, 2)-Interpolation Property implies the (m, n)-Interpolation Property for all finite m, n.

(d) Show that if the (m, n)-Interpolation Property is satisfied for all finite and infinite $m > 0, n > 0$, then P satisfies the hypotheses of Thm. 6.

(e) Show that if $m = 0, n = 0$ are included, we get a complete lattice.

Ex. 5. (a) Show that the upper semi-continuous real-valued functions (cf. §9) on any topological space form a conditionally complete lattice.

(b) Prove that the subharmonic functions assuming given values on the boundary of a region R form a conditionally complete lattice. (Hint: Show the infimum exists if there is a lower bound, and is subharmonic).

Ex. 6*. (a) Show that the different closure operators topologizing an aggregate S, so as to make it a T_1-space, form a conditionally complete lattice, if $^- \leqq {}^{-*}$ is defined to mean $\bar{X} \leqq \bar{X}^*$ for all $X \leqq S$.

(b) Show that the different distance functions $\rho, \rho^*, \cdots$ definable on S making S a metric space are a conditionally complete lattice if $\rho \leqq \rho^*$ means $\rho(x, y) \leqq \rho^*(x, y)$ for all $x, y \in S$.

(c) State the sense in which the ordering of (b) is dual to that of (a). (Cf. G. Birkhoff, *On the combination of topologies*, Fund. Math. 26 (1936), 156–66.)

Ex. 7*. Show that the summability procedures using Toeplitz matrices A form a semi-lattice, if we define $A \geqq B$ to mean that any series $x_1, x_2, x_3, \cdots$ summable (B) is summable (A), and to the same limit. What more can you say?

4. Generalized laws; fixpoint theorem. The idempotent, commutative, and associative laws can all be combined into a single law L* which, with L4, characterizes complete lattices.

THEOREM 7. *In any complete lattice, every subset S of elements X_α has a* g.l.b. $\bigwedge_S x_\alpha$ *and a* l.u.b. $\bigvee_S x_\alpha$; *moreover*

L*. *If Φ is any family of sets S_ϕ, and S denotes the set-union of the S_ϕ, then* $\bigwedge_\Phi\{\bigwedge_{S_\phi} x_\alpha\} = \bigwedge_S x_\alpha$, *and dually* $\bigvee_\Phi\{\bigvee_{S_\phi} x_\alpha\} = \bigvee_S x_\alpha$.

Conversely, any system with operations determining from any subset S elements $\bigvee_S x_\alpha$ and $\bigvee_S x_\alpha$ so that L* *and* L4 *holds is a complete lattice.*[4]

Proof. To be a lower bound of S_ϕ is the same as being a lower bound to $\bigwedge S_\phi$; hence to be a lower bound of S is to be a lower bound of every S_ϕ, hence of every $\bigwedge S_\phi$—whence $\bigwedge_\Phi\{\bigwedge_{S_\phi} x_\alpha\} = \bigwedge_S x_\alpha$. The rest of L* follows by duality. Conversely, L1–L3 are easily shown to be special cases of L*. While $\bigwedge_S x_\alpha \leqq x_\alpha$ for all $x_\alpha \in S$ (since the union of x_α and S is S, $x_\alpha \frown \bigwedge_S x_\alpha = \bigwedge_S x_\alpha$), and if $t \frown x_\alpha = t$ for all $x_\alpha \in S$, then $t \frown \bigwedge_S x_\alpha = \bigwedge(x_\alpha \frown t) = \bigwedge t = t$; hence $\bigwedge_S x = \operatorname{Inf} S$; cf. Ch. II, Thm. 1.

[4] This result is due to G. Birkhoff [1, p. 442] and [LT, p. 20]. Cf. the discussions of the generalized distributive laws in Ch. IX, §11, and Ch. X, §10.

We can also prove an interesting fixpoint theorem.

THEOREM 8. *Let $y = f(x)$ be any isotone function from a complete lattice L to itself. Then $a = f(a)$ for some $a \in L$.*

Proof. Define a as the least upper bound of the set S of elements $x \in L$ such that $x \leqq f(x)$. Since $0 \leqq f(0)$, S is non-void. Since $f(x)$ is isotone, and $a \geqq x$ for all $x \in S$, $f(a) \geqq f(x) \geqq x$ for all $x \in S$; hence $f(a) \geqq \sup S = a$. It follows, since $f(x)$ is isotone, that $f(f(a)) \geqq f(a)$, whence $f(a) \in S$. But this implies $f(a) \leqq a$, since $a = \sup S$. We conclude[5] $a = f(a)$.

Ex. 1. In any semi-lattice, define $x_1 \circ \cdots \circ x_n$ by induction as $x_1 \circ (x_2 \circ \cdots \circ x_n)$.

(a) Prove from L3 by induction the *generalized associative* law: If $y_i = x_{s_{i-1}} \circ \cdots \circ x_{s_i}$ $[0 = s_0 < s_1 < \cdots < s_m = n]$, then $y_1 \circ \cdots \circ y_m = x_1 \circ \cdots \circ x_n$.

(b) Prove that $x_1 \circ \cdots \circ x_n$ is invariant under every permutation of the x_i, using only L2 and L3.

(c) Prove (L*) by induction, using L1–L3, provided Φ and all s_ϕ are finite.

Ex. 2. Show how L1, L2, L3 are special cases of (L*).

Ex. 3. State a weakened form of (L*) valid for σ-lattices.

Ex. 4. Show that if $f(x)$ is an isotone operator in a conditionally complete lattice, and if $a \leqq f(a) \leqq f(b) \leqq b$, then $c = f(c)$ for some c between a and b.

Ex. 5. Show that in Thm. 8, there is a *least* fixpoint. Do the fixpoints form a lattice? Show that they need not form a sublattice.

5. Polarity. Let ρ be any binary relation defined between the members of two aggregates I and I^*. As usual, if $x \in I$, $x^* \in I^*$, we write $x\rho x^*$ when x is in the relation ρ to x^* and $x\rho' x^*$ when it is not—thus ρ' is the complement of ρ. We do not require I and I^* to be different.

If X is any subset of I, denote by X^* the set of x^* such that $x\rho x^*$ for all $x \in X$; conversely, if Y is any subset of I^*, denote by Y^+ the set of $x \in I$ such that $x\rho y$ for all $y \in Y$. Clearly,

LEMMA 1. *For any relation ρ, we have the inequalities*

(1) *If $X \geqq X_1$ in I, then $X^* \leqq X_1^*$ in I^*,*

(1*) *If $Y \geqq Y_1$ in I^*, then $Y^+ \leqq Y_1^+$ in I,*

(2) *$X \leqq (X^*)^+$ and $Y \leqq (Y^+)^*$ for all X in I, Y in I^*.*

Thus since $x\rho x^*$ for all $x \in X$, $x^* \in X^*$, $X \leqq (X^*)^+$; we leave the details to the reader.

COROLLARY. *For any subsets X of I and Y of I^*,*

(3) *$((X^*)^+)^* = X^*$ and $((Y^+)^*)^+ = Y^+$.*

Proof. By (2), $X^* \leqq ((X^*)^+)^*$; also by (2), $X \leqq (X^*)^+$, whence by (1) $X^* \geqq ((X^*)^+)^*$; hence $((X^*)^+)^* = X^*$ by P2.

THEOREM 9. *The operations $X \to (X^*)^+$ and $Y \to (Y^+)^*$ are closure opera-*

[5] This result is closely related to Thm. 1, of L. Kantorovitch, *On a class of functional equations*, Doklady URSS 4 (1946), 219–24; see also B. Knaster, ref. in Ch. III, §5, Ex. 6. A remotely related result is due to A. D. Wallace, Bull. Am. Math. Soc. 51 (1945), 413–16, with bibliography.

tions; moreover, the correspondences $X \to X^*$ and $Y \to Y^+$ define a dual isomorphism between the complete lattices of "closed" subsets of I and I^*.

Proof. By (2), $X \to (X^*)^+$ satisfies C1; using (1) and (1*), $X \geqq X_1$ implies $(X^*)^+ \geqq (X_1^*)^+$, proving C2; by (3), $(((X^*)^+)^*)^+ = (X^*)^+$, which proves C3. Hence $X \to (X^*)^+$ is a closure operation; similarly for $Y \to (Y^+)^*$. By (3), the correspondences $X^* \to (X^*)^+$ and $Y^+ \to (Y^+)^*$ are inverse, in the sense that their product in either order is the identity; hence they are both one-one. Finally, by (1), they invert inclusion, which completes the proof.

Example 1. Let $I = I^*$ be any ring, and let $x\rho y$ mean that $xy = 0$. Then every X^* is a right-ideal, every X^+ a left-ideal. In the case of "regular" rings (including semi-simple linear associative algebras), the converse is also true, and so the lattices of right- and of left-ideals are dually isomorphic.

Example 2. Let I be any field or division ring (sfield), and let I^* be any finite group of automorphisms α of I. If we define $x\rho\alpha$ to mean $\alpha(x) = x$, we get the well-known dual isomorphism[6] between subgroups of I^* and certain subfields of I.

There are other important examples where $I = I^*$ and ρ is symmetric. The following case is typical.

Example 3. Let $A = \| a_{ij} \|$ be any symmetric $n \times n$ matrix; then $x_i a_{ij} x_j = 0$ will define a conic, quadric, or hyperquadric Q according as $n = 2$, $n = 3$, or $n > 3$. For two vectors $\xi = (x_0, \cdots, x_n)$ and $\eta = (y_0, \cdots, y_n)$ of projective n-space I, we define $\xi\rho\eta$ to mean that the sum $x_i a_{ij} y_j = 0$. The "closed" subsets of I are then its points, lines, planes and other subspaces; if X is any such subspace, X^* is its *polar*[7] with respect to Q.

The preceding example suggests calling, in general, X^* the *polar* of X with respect to the relation ρ; it also suggests the following result.

COROLLARY. *If $I = I^*$ and the relation ρ is symmetric, then $X^+ = X^*$, and in the complete lattice of closed sets $X = (X^*)^*$, the correspondence $X \to X^*$ is an involution. In symbols,*

(4) $$(X^*)^* = X,$$

(5) $$(X \frown Y)^* = X^* \smile Y^*, \quad (X \smile Y)^* = X^* \frown Y^*.$$

If ρ is also anti-reflexive (if $x\rho x$ for no x, or if $x\rho x$ implies $x\rho y$ for all y), then

(6) $$X \frown X^* = 0 \text{ and } X \smile X^* = I.$$

Example 4. Let I be any group, and let $x\rho y$ mean that $xy = yx$. Then (4)–(5) hold; the closed sets are certain subgroups; and the correspondence $X \to X^*$ carries each subgroup into its "centralizer."

Example 5. Let I be any class, and let $x\rho y$ mean $x \neq y$. Then (4)–(6)

[6] Cf. M. Krasner Jour. de Math. 17 (1938), 266–86; N. Jacobson, *The fundamental theorem of Galois theory for quasi-fields*, Annals of Math. 41 (1940), 1–7.

[7] W. C. Graustein, *Introduction to higher geometry*, New York, 1940, Ch. XIV, §§1–3.

holds; every set is closed; and the involution $X \to X^*$ carries each set into its set-complement.

Example 6. Let I be Cartesian n-space, and let $x\rho y$ mean $x \perp y$ (x is orthogonal to y). Then (4)–(6) hold; the "closed" subsets are the linear subspaces; and the involution carries each subspace into its orthogonal complement. (This is a special case of Example 3.)

Proof. Since $X^* = X^+$, (4) is implied by (3), and (5) by Theorem 9—a dual isomorphism interchanges joins and meets. Again in (6), $X \frown X^*$ contains only elements x such that $x\rho x$—i.e., only elements of O (which is the void set in Example 5 and the origin in Example 6).

6. Galois connections. The preceding results can be generalized[8] by abstraction in the following way, to partly ordered sets.

Definition. *Let P, Q be any partly ordered sets, and let $x \to x^*$, $y \to y^+$ be any correspondences defined for all $x \in P$, $y \in Q$, such that*

(1) *If $x \geqq x_1$ in P, then $x^* \leqq x_1{}^*$ in Q,*

(1*) *If $y \geqq y_1$ in Q, then $y^+ \leqq y_1$ in P,*

(2) *$x \leqq (x^*)^+$ and $y \leqq (y^+)^*$ for all $x \in P$, $y \in Q$.*

The correspondences $x \to x^*$, $y \to y^+$ are said to define a Galois connection between P and Q.

The formal proofs of (3) given in §5, and of the fact that the correspondences $x \to (x^*)^+$ and $y \to (y^+)^*$ are closure operations, then go through without change. Applying Theorem 1, we get

Theorem 10. *Let $x \to x^*$, $y \to y^+$ define a Galois connection between any two complete lattices L and M. Then the Galois connection gives a dual isomorphism between the complete lattices S and T of "closed" subsets of L and M.*

We also get paraphrases of the other results stated above; thus formulas (4)–(6) hold for symmetric and anti-reflexive relations.

Though the majority of Galois connections are between sets, as suggested by Examples 1–6 above and Exs. 1–4 below, there are some important Galois connections between elements of abstract lattices. The following illustration is suggestive;[9] cf. also Exs. 6–7 below.

Example 7. Let L be any finite distributive lattice, and let $x^* = x^+$ be the join of the elements y_α such that $x \frown y_\alpha = 0$. Then rules (1)–(5) and $x \frown x^* = 0$ hold; moreover, the elements $x = x^*$ form a self-dual lattice.

Many of the following exercises require assumptions from outside of lattice theory; others may be based on F. W. Levi, *Rearrangement of convergent series*,

[8] The results of §5 are due to the author [LT, §32]; the observation that it is sufficient to assume (1)–(1*)–(2) is due to O. Ore, *Galois connexions*, Trans. Am. Math. Soc. 55 (1944), 493–513. Cf. also C. Carathéodory, *Gepaarte Mengen, Verbände, Somenringe*, Math. Annalen 48 (1942), 4–26; C. J. Everett, *Closure operators and Galois theory in lattices*, Trans. Am. Math. Soc. 55 (1944), 514–25; M. Krasner, op. cit. supra.

[9] See Ch. IX, §12, where it is generalized to completely meet-distributive lattices, and Ch. XIV, §11, where it is generalized to l-groups.

Duke Jour. 13 (1946), 579–85; see also D. W. Hall and J. W. T. Youngs, Annals of Math. 3 (1947), 710–16.

Ex. 1. Let I be any finite Abelian group; let I^* be the group if its characters, and let $x\rho X$ $[x \in I, X \in I^*]$ mean $X(x) = 0$.

(a) Show that the "closed" subsets of I and I^* are their subgroups.

(b) Infer that the subgroup-lattice of I is dual to that of I^*.

(c) Prove that the subgroup-lattice of I is self-dual.

Ex. 2. (a) Let $x\rho y$ mean that $x \perp y$ in Hilbert space. Show that the complete lattice of closed subspaces of Hilbert space is self-dual.

(b) Let I be any Banach space, and let I^* be the space of its functionals; define $x\rho\lambda$ $[x \in I, \lambda\rho I^*]$ to mean $\lambda(x) = 0$. Show that the lattices of "regularly closed" subspaces of I and I^*, in the sense of Banach (i.e., those closed in the weak topology—see L. Alaoglu, Annals of Math. 41 (1940), 252–67, Thm. 1.4), are dual.

Ex. 3. Let ρ be any binary relation. Amplify the notation of §5 by letting $X \wedge X_1$ and $X \vee X_1$ denote set-product and set-union. Show that, for any closed sets $X = (X^*)^+$, $X_1 = (X_1^*)^+$, we have $X \frown X_1 = X \wedge X_1$ but $X \smile X_1 = ((X \wedge X_1)^*)^+ = (X^* \wedge X_1^*)^+ > X \vee X_1$ in general. (F. W. Levi)

Ex. 4. Let M_n be the class of all $n \times n$ matrices: let $A\rho B$ $[A, B \in M_n]$ mean $AB = BA$. Apply the Frobenius-Burnside-Schur Thm. to ascertain how Thm. 8 applies to this case.

Ex. 5. Let L be any complete lattice, and let Ω be any groupoid of isotone maps $x \to w(x)$ of L into itself. Define $x\rho w$ to mean $w(x) \leqq x$.

(a) Show that if $X \leqq L$, then X^* is a subgroupoid of Ω; and if $\Sigma \leqq \Omega$, then Σ^+ is a complete lattice in L.

(b) Show that if $w(\vee X_\alpha) = \vee[w(X_\alpha)]$—as in the case L consists of all subsets of I, and $w(x)$ is the set of all values of $w(p)$ $[p \in x]$—then Σ^+ is a closed sublattice of L.

(c) What can you say if w is not isotone?

Ex. 6. (a) Obtain analogs of the results of §5 if (2) is replaced by its dual: $X \geqq (X^*)^+$ and $Y \geqq (Y^+)^*$ for all $X \leqq I, Y \leqq I^*$.

(b) Let $X \to X'$ be the correspondence carrying each subset of a topological space I into the interior of its complement (i.e., the complement of its closure). Show that this satisfies the conditions of (a).

(c) Infer that the "regular open sets" of I (sets which are the interiors of their closures) form a complete lattice.

Ex. 7. Let P be the lattice of all subsets of the group G of all permutations of the elements of a class I, and let Q be the lattice of partitions of I. For each $X \in P$, let X^* be the partition defined by letting $a \equiv b(X^*)$ mean $\phi(a) = b$ for some $\phi \in X$; for each $\pi \in Q$, let π^+ be the subgroup of G leaving invariant the classes into which π divides I.

(a) Show that this is a Galois correspondence. (C. J. Everett)

(b) Show that it can also be obtained concretely, by letting $\phi\rho S$ $[\phi \in G, S \leqq I]$ mean that $\phi(S) \leqq S$.

(c*) Relate the two approaches, by noting that Q is isomorphic to the lattice of the subalgebras of the "Boolean algebra" of all subsets of I.

Ex. 8*. Let I be the class of all algebraic systems with a single binary operation; let I^* be the class of all identities on a binary operation. Define $A\rho L$ $[A \in I, L \in I^*]$ to mean that L is identically true in A. Describe the resulting dual isomorphism. (Cf. G. Birkhoff [3, Thms. 7–10.])

Ex. 9*. Let A be any algebra, and Ω any set of endomorphisms of A. Show that the subalgebras S of A satisfying $\omega(S) \leqq S$ for all $\omega \in \Omega$ form a complete sublattice of the lattice $L(A)$ of all subalgebras of A. Describe a dual isomorphism between this sublattice and a suitable lattice of subsets of Ω.

Problem 20. Let I be any set of "points"; let Γ be the class of all subsets X, Y, Z of I; let Σ be the class of all pairs $(\{x_\alpha\} \to a)$ of a directed set $\{x_\alpha\}$ of points of I and a single point $a \in I$. Define $X\rho(\{x_\alpha\} \to a)$ to mean that if every sufficiently large $x_\alpha \in X$, then $a \in X$. Show that the resulting polarity gives the correspondence between closed sets and convergence described in the Foreword on Topology. To what abstract conditions do $\Delta = (\Delta^*)^+$ and $T = (T^+)^*$ correspond (Δ a subset of Γ and T of Σ)?

7. Representation theorem; completion by cuts. Let P be any partly ordered set and let $x\rho y$ in §5 mean that $x \leqq y$ in P. Then by definition, X^* is the set of upper bounds, and X^+ the set of lower bounds to X; hence $(X^*)^+$ is the set of all lower bounds of the set of all upper bounds of X.

In particular, if x is any element of P, then x^* is the set of $u \geqq x$ and $(x^*)^+$ is the set (principal ideal) of $t \leqq x$. Hence if $x > y$, $(x^*)^+ > (y^*)^+$. Moreover if $a = \operatorname{Inf} X$ then $t \leqq a$ if and only if $t \leqq x_\alpha$ for all $x_\alpha \in X$; hence $(a^*)^+$ is the intersection of the $(x_\alpha^*)^+$. We conclude the following representation theorem.[10]

THEOREM 11. *Any partly ordered set P is isomorphic to a family $\Phi(P)$ of subsets of P in such a way that* g.l.b. *in P go into intersections.*

COROLLARY 1. *The inclusion relation is completely characterized by postulates* P1–P3.

It is however not true that the operations of set-union and intersection are characterized by L1–L4; these operations satisfy the distributive law L6 (cf. Ch. IX) which is not true in general lattices. We must content ourselves with the following converse of Thm. 4.

COROLLARY 2. *Any finite lattice L is isomorphic with the lattice of all subalgebras of a suitable abstract algebra A.*

Proof. Let A consist of the elements of L, with the zero-ary operation with constant value 0, unary operators α, one for each $a \in L$, defined by $\alpha(x) = x \frown a$, and the binary operation $x \smile y$. The "subalgebras" of A are then simply the non-void ideals of L, which, being principal, are isomorphic with L itself.

A modification of the preceding construction, due to MacNeille[11] shows that Dedekind's celebrated construction of irrational numbers by "cuts" will really work in arbitrary partly ordered sets.

THEOREM 12. *Any partly ordered set P can be embedded in a complete lattice L, so that inclusion is preserved, together with all* g.l.b. *and* l.u.b *existing in P.*

Proof. We first adjoin a O to P, unless P has a least element already. Then let L consist of all non-void "closed" subsets $X = (X^*)^+$ of P (cf. paragraph one); L is a complete lattice, by Thm. 9. By Thm. 11, the correspondence $x \to (x^*)^+$ embeds P in L with preservation of inclusion and g.l.b. Now suppose

[10] Thm. 10 and its corollaries are due to the author [1], the original statement of Cor. 2 being however inexact. For an extension of Cor. 2 to infinite lattices, see G. Birkhoff and O. Frink, *Representations of lattices by sets*, Trans. Am. Math. Soc. 64 (1948), p. 299–316.

[11] Cf. H. M. MacNeille, [1] and [2, §11]; R. Dedekind, *Stetigkeit und irrationale Zahlen*, Braunschweig, 1892, p. 11.

$a = \sup X_\alpha$ in P. Then $(T^*)^+ \geqq (X^*)^+$ in L, by (3), if and only if $T^* \leqq X^*$; but $X^* = a^*$ by definition of l.u.b. Hence $(T^*)^+ \geqq (X^*)^+$ if and only if $T^* \leqq a^*$, or, by (1*), $(T^*)^+ \geqq (a^*)^+$. Hence $(a^*)^+$ is a l.u.b. of $(X^*)^+$, whence l.u.b. are preserved, q.e.d.

Caution. The preceding construction is not the only logical way of embedding partly ordered sets in complete lattices; see Ch. V, §9.

We note that if L is a lattice, and X is any subset of L, then $(X^*)^+$ is an *ideal*. For if $a, b \in (X^*)^+$, then a, b are lower bounds to X^*; hence X^* is an upper bound to a and b, and so to $a \smile b$, whence $a \smile b \in (X^*)^+$. Again, if $a \in (X^*)^+$ and $t \leqq a$, then trivially $t \in (X^*)^+$. This makes the following terminology legitimate.[12]

DEFINITION. *A closed ideal of a partly ordered set P is a subset of P which contains (in fact, consists of) all lower bounds to the set of its upper bounds.*

Ex. 1. A "segment" of a partly ordered set has been defined[13] as an intersection of closed intervals.

(a) Show that if a subset S of a lattice is a segment, then $a, b \in S$ and $a \frown b \leqq x \leqq a \smile b$ imply $x \in S$.

(b) Show that an ideal of a lattice is a segment if and only if it is a closed ideal.

Ex. 2. (a) Show that a lattice is complete if and only if all its closed ideals are principal ideals.

(b) Show that the closed ideals of a lattice L do not necessarily form a sublattice of the lattice of all ideals of L.

Ex. 3. (a) Determine the completion by cuts of the cardinal number 3 and of the partly ordered sets of Figs. 1b and 1e of p. 4.

(b) Show that the lattice of all (closed) ideals of n is $n \oplus 1$.

Ex. 4. (a) Show that the completion by cuts of a direct union $C \times D$ of two chains is not in general isomorphic to the direct union $\bar{C} \times \bar{D}$ of the completions by cuts of the factors.

(b) Find necessary and sufficient conditions for $\overline{C \times D} \cong \bar{C} \times \bar{D}$. Is the isomorphism always "natural"?

Ex. 5. (a) Show that if $=$ and $\leqq$ are interpreted in the sense of isomorphism, then the operation $P \to L(P)$ of "completion by cuts" has the following characteristic[14] properties: $P \leqq L(P)$; $P \leqq Q$ implies $L(P) \leqq L(Q)$; $L(L(P)) = L$.

(b) Show that it is effectively self-dual, in the sense that $L(\breve{P})$ is dually isomorphic to $L(P)$.

(c) Show that the "metric completion" of Ch. V, §9, has these properties also.

8. Intrinsic topologies. Let $\{x_\alpha\}$ be any directed set of elements of a complete lattice L. We define[15] $x_\alpha \to a$ (in words, x_α order-converges to a) to mean

---

[12] The concept, in the case of Boolean algebras, is due to M. H. Stone [3]; cf. also A. Tarski, *Ideale in Mengenkörpern*, Ann. Soc. Pol. Math. 15 (1937), 186–9. The adjective "closed" seems more descriptive than the term "normal" used hitherto.

[13] J. W. Duthie, *Segments of ordered sets*, Trans. Am. Math. Soc. 51 (1942), 1–14.

[14] G. Birkhoff, *The meaning of completeness*, Annals of Math. 38 (1937), 57–60.

[15] This definition was first introduced for sequences by the author [3] (esp. Thm. 20), and independently by L. Kantorovitch, Doklady URSS 4 (1935), 70–71. Cf. also Hausdorff [1, p. 19] and [LT, p. 32]. Also, see Ky Fan, *Le prolongement des functionelles continues sur un espace semi-ordonné*, Revue Sci. (Rev. Rose.) 82 (1944), 131–9.

(7) $$a = \bigwedge_{\alpha} \{ \bigvee_{\beta \geqq \alpha} x_\alpha \} = \bigvee_{\alpha} \{ \bigwedge_{\beta \geqq \alpha} x_\beta \};$$

that is, it means Lim sup$\{x_\alpha\}$ = Lim inf $\{x_\alpha\} = a$. Setting $u_\alpha = \bigvee_{\beta \geqq \alpha} x_\beta$ and $v_\alpha = \bigwedge_{\beta \geqq \alpha} x_\beta$, we see that $x_\alpha \to a$ if and only if there exist monotone directed sets $u_\alpha \downarrow a$ and $v_\alpha \uparrow a$, such that $u_\alpha \geqq x_\alpha \geqq v_\alpha$ for all α. Of course, one can prove the corresponding relations for ordinary countable sequences in any σ-lattice.

If P is any partly ordered set, we can define $x_\alpha \to a$ in P to mean that $x_\alpha \to a$ in the completion of P by cuts; this "relative topology" would repay further study. We know by Ch. III, §5, Ex. 9b, that even in a chain, $x_\alpha \to a$ need not imply that $u_\alpha \downarrow a$ and $v_\alpha \uparrow a$ exist, with $u_\alpha \geqq x_\alpha \geqq v_\alpha$ for all α, though the converse is of course true.

One verifies easily the first two formulas below,

(8) If $x_\alpha = a$ for all a, then $x_\alpha \to a$,

(9) If $x_\alpha \to a$ and $x_\alpha \to b$, then $a = b$,

(10) If $x_\alpha \to a$, and $\{x_\sigma\}$ is a cofinal subset of $\{x_\alpha\}$, then $x_\sigma \to a$.

To prove (10), we note that for any α, there exists $\sigma \geqq \alpha$; then $\bigvee_{\tau \geqq \sigma} x_\tau$ in $\{x_\sigma\}$ is contained in $\bigvee_{\beta \geqq \alpha} x_\beta$ in $\{x_\sigma\}$, since every x_τ is an x_β. Hence, using duality

$$a = \text{Lim sup } \{x_\alpha\} \geqq \text{Lim sup } \{x_\sigma\} \geqq \text{Lim inf } \{x_\sigma\} \geqq \text{Lim inf}\{x_\alpha\} = a,$$

from which (10) follows directly.

Example 1. Let L be the complete lattice of all subsets of an infinite aggregate I. Let the indices F be the different finite subsets of I, and let $F \geqq G$ mean that F contains G. Let x_F be the set F; then $\{x_F\}$ is a monotone directed set. One shows easily that $x_F \uparrow I$, though if I is uncountable, no well-ordered[16] directed set (i.e., transfinite sequence) of the x_F can converge to I.

As usual, we define a subset X of a partly ordered set P to be *closed* in the order topology, if and only if $\{x_\alpha\} \leqq X$ and $x_\alpha \to a$ imply $a \in X$; in words, if and only if the limit of any order-convergent directed set of elements of X is itself in X. We conclude from (8)–(10), as in the Foreword on Topology, Ex. 3,

THEOREM 13. *Every partly ordered set P is a Hausdorff space in its order topology.*

Another useful result is the following

LEMMA 1. *Any closed interval* $[a, b]$, $[-\infty, b]$, $[a, +\infty]$, *or* $[-\infty, +\infty]$ *is closed in the order topology.*

Proof. If $x_\alpha \to c$, where $a \leqq x_\alpha \leqq b$ for all α, then every $\bigvee_{\beta \geqq \alpha} x_\beta \geqq a$; hence $c = \bigwedge_\alpha \{\bigvee_{\beta \geqq \alpha} x_\beta\} \geqq a$. Dually, $c \leqq b$, completing the proof. Since the meaning of a "closed interval" is unchanged, Lemma 1 is true in any partly ordered set.

DEFINITION. *By the interval topology of a partly ordered set P, we mean that defined by taking the closed intervals of P as a sub-base of closed sets.*

---

[16] Indeed, for all τ, the infimum of the x_σ ($\alpha \geqq \tau$) would be finite; but the union of any increasing well-ordered series of finite sets is at most countable.

We note that, since any finite interval is the intersection of two semi-infinite intervals, we can take the closed semi-infinite intervals as a sub-base of closed sets. We also note that it does not work at all to take "open intervals" as a basis of open sets. Thus consider the Cartesian plane, letting $(x, y) \leqq (x', y')$ mean that $x \leqq x'$ and $y \leqq y'$. Then $(-1, 0) < (x, y) < (1, 0)$ is not an open set in any natural sense.

Since every point is a closed interval, we see directly

THEOREM 14. *Every partly ordered set P is a T_1-space in its interval topology.*[17]

By Lemma 1, the interval topology is "weaker" than or homeomorphic to the order topology. We shall now give a case where it is actually weaker.

Example 2. Let L be the complete lattice consisting of O, I, and countably many elements $x_1, x_2, x_3, \cdots$ satisfying $O < x_i < I$ for all i but $x_i < x_j$ for no $i \neq j$. Consider the sequence $\{x_n\}$. In the interval topology, $x_n \to O$ and $x_n \to I$; in the order-topology, L is a discrete space.

This is illustrative in two ways: L is a Hausdorff space in its order topology, but not in its interval topology; L is compact in its interval topology, but not in its order topology.

THEOREM 15. *Every complete lattice is compact in its interval topology.*[17]

Proof. By Thm. 12, Ch. III, it is sufficient to show that the closed intervals have the "finite intersection property." But let C be any class of closed intervals $[a_\gamma, b_\gamma]$, such that the intersection $[a_\gamma \cup a_{\gamma'}, b_\gamma \cap b_{\gamma'}]$ of any *two* intervals of C is non-void. Then $a_\gamma \leqq b_{\gamma'}$ identically; hence $a = \bigwedge a_\gamma \leqq \bigwedge b_\gamma = b$, and so *all* the $[a_\gamma, b_\gamma]$ of C contain $[a, b]$ and have a non-void intersection.

Ex. 1. Prove formulas (8)–(9) of the text.

Ex. 2. Let P be the direct union $P = Q \times R$ of partly ordered sets Q and R.

(a) Show that in its order topology, P is the Cartesian product of Q and R.

(b) Show that *if* P has an O and an I, P is also the topological product of Q and R in interval topology.

(c) Infer that if P is a direct union of chains with O and I, the order and interval topologies are equivalent.

(d) Generalize to the case of infinitely many factors.

Ex. 3. Let L be the conditionally complete lattice of all couples (x, y) of real numbers, where $(x, y) \geqq (x', y')$ means $x \geqq x'$ and $y \geqq y'$ (i.e., $L = R^{*2}$). Show that the directed set $(x, -x)$, ordered according to increasing x, approaches every element of L in the interval topology.

Ex. 4. (a) Show that any lattice is topologically dense in its completion by cuts under the order topology. Show this is not true for most partly ordered sets.

(b) Show that a lattice which is not complete is not compact in its interval or order topology. Infer that an ideal is a closed ideal, and that a sublattice is a closed sublattice if and only if it is topologically closed.

Ex. 5. Using Ex. 1 of §7, show that the interval topology in any partly ordered set may be obtained by relativization from that of its completion by cuts.

Ex. 6. Prove that the complete lattice of Example 2 is non-compact and discrete under any Hausdorff topology invariant under all lattice-automorphisms and dual automorphisms.

---

[17] This important result, like many other ideas of this section, is due to O. Frink, *Topology in lattices*, 51 (1942), 569–82.

Ex. 7. Define a *tower* as a partly ordered set isomorphic with the directed set of all finite subsets of some class. Show that every directed subset contains a cofinal subset $\{x_\alpha\}$, where the α are a tower and $\alpha > \beta$ implies $x_\alpha \geqq x_\beta$. (M. Krasner)

Problem 21. Find a necessary and sufficient condition for an element of a complete lattice to be isolated (a) in the order topology, (b) in the interval topology.

Problem 22. Find necessary and sufficient conditions for a compact Hausdorff space to be homeomorphic with a suitable complete lattice in its interval topology.

Problem 23. Find necessary and sufficient conditions for a lattice to be a Hausdorff space in its interval topology. For it to be a normal space in its order topology.

Problem 24. In what lattices L is every closed ideal an intersection of principal ideals?

9. Star-convergence; semi-continuous functions. We have seen (§6, Problem 20) that there is a Galois connection between the families of convergent directed sets of an aggregate S, and the families of closed (or open) subsets of S. In this correspondence, a family of closed sets is a closed family if and only if it is a T_1-space; we do not know necessary and sufficient conditions for a family of convergent directed sets to be closed. We do however know that (8)–(10) are necessary. So is

(11) If, from the points of every cofinal subset $\{x_\beta\}$ of a directed set $\{x_\alpha\}$, a directed set can be constructed which converges to a, then $x_\alpha \to a$.

Proof. We know that we are dealing with a T_1-space. Unless $x_\alpha \to a$, some open set U contains a and fails to contain *any* successor of some x_α. The set of successors of x_α is however cofinal in $\{x_\alpha\}$. *No* directed subset of points of this cofinal subset, which lies entirely outside U, converges to a.

Definition. *The star-topology of a lattice is the T_1-topology defined by order convergence.*

In particular, for ordinary sequences $\{x_n\}$, we shall write $x_n \to {}^*a$, and say that $\{x_n\}$ star-converges to a, if every subsequence $\{x_{n(k)}\}$ of $\{x_n\}$ contains a subsubsequence $\{x_{n(k(i))}\}$ which order-converges to a as $i \to \infty$. In this case, $\{x_n\}$ certainly converges to a in the star topology; moreover (see Ch. V, §9; Ch. XV, §§9–10) this special case is sufficient for the applications of star-convergence which we have in mind.[18]

Various interesting problems relating to star-convergence are mentioned below in exercises.

In general, a topological algebra may be defined[19] as a topological space with algebraic operations which are continuous in the topology. Guided by this

---

[18] Star-convergence was introduced in spaces with convergent sequences by P. Urysohn, *Sur les classes (L) de M. Fréchet*, Enseignement Math. 25 (1926), 77–83. Star-convergence in lattices was introduced independently by Kantorovitch [1, p. 143], and by von Neumann and the author (Annals of Math. 38 (1937), p. 56).

[19] By analogy with O. Schreier's definition of a topological group (Abh. Hamb. 4 (1926), 15–32; cf. L. Pontrjagin (*Topological groups*, Ch. III). For topological lattices, cf. [LT, p. 37]; also L. Nachbin, Comptes Rendus Acad. Sci. 226 (1948), pp. 381, 547, 778; and M. Koutsky, ibid. 225 (1947), 659–61.

idea, though realizing that we might have used star-convergence or the interval topology instead, we shall define a *topological lattice* as a lattice with a topology under which

(12) $x_\alpha \to x$ and $y_\beta \to y$ imply $x_\alpha \frown y_\beta \to x \frown y$ and $x_\alpha \smile y_\beta \to x \smile y$.

In the case of ordinary sequences, this is equivalent to

(12′) $x_n \to x$ and $y_n \to y$ imply $x_n \frown y_n \to x \frown y$ and $x_n \smile y_n \to x \smile y$.

This condition does not hold in general lattices (see Exs. 3–4 below).

LEMMA. *In order for* (12) *to hold in a complete lattice under its order topology, it is sufficient that*

$$(13) \qquad x_\alpha \uparrow x \textit{ imply } a \frown x_\alpha \uparrow a \frown x \textit{ and dually.}$$

Proof. (The condition is obviously necessary.) In (12), let u_α be the meet of the successors of x_α, and u_β the meet of the successors of y_β; we must prove that $u_\alpha \frown v_\beta \uparrow x \frown y$, and, by duality, it is sufficient to prove this. But clearly $u_\alpha \frown v_\beta$, and $u_\alpha \frown v_\beta$ are isotone; hence it is sufficient to prove that Sup $(u_\alpha \frown v_\beta) = x \frown y$; this we now do. Since $x \geqq u_\alpha$ and $y \geqq v_\beta$, $x \frown y \geqq u_\alpha \frown v_\beta$ for all α, β and so $x \frown y \geqq$ Sup $(u_\alpha \frown v_\beta)$. Conversely, for all α, Sup $(u_\alpha \frown v_\beta) \geqq u_\alpha \frown$ Sup $v_\beta = u_\alpha \frown y$ by (13); hence, Sup $(u_\alpha \frown v_\beta) \geqq$ Sup $(u_\alpha \frown y) = x \frown y$, again by (13).

We now prove a result which is not unlike Theorem 8: to prove it, we need the concept of a semicontinuous function.

DEFINITION. *A function $y = f(x)$ from a T_1-space to a partly ordered set is called lower semicontinuous*[20] *if $x_\alpha \to a$ and $f(x_\alpha) \leqq c$ for all x_α imply $f(a) \leqq c$.*

THEOREM 16. *A lower semicontinuous function from a compact space S to a partly ordered set P assumes a minimal value.*

Proof. Form a maximal chain M of elements $y \in P$ such that $f(x) \leqq y$ for some $x \in S$. Such a chain will exist, since being a chain and having $f(x) \leqq y$ for some $x \in S$ and all $y \in M$ are properties of finite character (of character two and one, respectively). For each $y \in M$, let S_y be the non-void set of $x \in S$ with $f(x) \leqq y$. Since $f(x)$ is lower semicontinuous, each S_y is closed. Since the S_y form a simply ordered set under set-inclusion ("nested chain"), any finite subset of S_y has a non-void intersection. Since S is compact, there is hence a point a contained in every S_y $[y \in M]$. Now $f(x) < f(a)$ $[x \in S]$ would imply that x could be added to M, contrary to the hypothesis that M is maximal. We conclude that $f(a)$ is the desired minimal value.

COROLLARY. *A lower semicontinuous function from a compact space to a chain assumes a least value.*

[20] Lower semicontinuous real-valued functions are not only convenient in analysis generally; they play a central role in the modern existence theorems of the calculus of variations. This was shown by Tonelli, following Fréchet.

The dual results are of course also true.

Ex. 1. Let $f(x)$ be a continuous isotone function on a σ-lattice. Let $a_1 = f(a)$, $a_{n+1} = f(a_n)$, and $b = \text{Sup } \{a_n\}$. Show that if $a \leqq f(a)$, then $f(b) = b$; i.e., b is a fixpoint.

Ex. 2. (a*) Let L be any complete lattice, in which every ascending well-ordered set is countable. Show that if an isotone directed set $\{x_\alpha\}$ converges to a, then a (not necessarily cofinal) sequence $\{x_{\alpha(n)}\}$ can be found, such that $x_{\alpha(n)} \uparrow a$. (Hint: Show that a maximal well-ordered set $x_{\alpha(\gamma)}$ exists, such that $y_{\gamma+1} = x_{\alpha(\gamma)} \smile y_\gamma > y_\gamma$, and is countable).

(b) Carry through the discussion of §§8–9 on the level of sequential convergence in a σ-lattice.

Ex. 3. (a) Let L be the complete lattice of all ideals in the ring J of integers, and let (m) denote the set of multiples of m. Show that $(p^n) \downarrow 0$, yet $(p^n) \smile (q) = (1)$ does not converge to $0 \smile (q)$, if p and q are distinct primes.

(b) Show that in the complete lattice of all subalgebras of any algebra, $S_\alpha \uparrow S$ implies $S_\alpha \frown T \uparrow S \frown T$. (Hint: Observe that l.u.b. is set-union, and use Thm. of Ch. IX). Generalize to the lattice of all subsets "closed" under any closure property of finite character.

(c) Show that (12′) holds in the star topology if and only if it holds in the order topology.

Ex. 4. Show that in the complete lattice of all closed subsets of a line, $x_\alpha \downarrow x$ implies $(a \smile x_\alpha) \downarrow (a \smile x)$, but not dually.

Ex. 5. (a) Show that the lattice $J(L)$ of all ideals of any lattice L satisfies (i) $J(L)$ is complete, (ii) every element of $J(L)$ is a meet of meet-irreducible elements, (iii) $x_\alpha \uparrow x$ implies $a \frown x_\alpha \uparrow a \frown x$, (iv) the elements a such that $a = \text{Inf } X$ implies $a = \text{Inf } F$, for some finite subset F of X, are a lattice L^*.

(b) Conversely, show that (i)–(iv) imply that $J(L)$ is the lattice of all ideals of the dual of L^*. (A. Komatu, Proc. Imp. Acad. Tokyo 19 (1943), 119–24.)

Ex. 6. (a) Show that every complete homomorphism is continuous in the order topology.

(b**) Is it continuous in the star-topology? The interval topology?

Ex. 7*. Show that FL(n) is not complete but is a topological lattice. (P. Whitman)

Problem 25. Find simple sufficient conditions for the star topology and interval topology to be equivalent. (E.g., are they equivalent in metric lattices? Are they always equivalent?)

Problem 26. Discuss the simplifications of §§8–9 which are possible in lattices of breadth two in the sense of Ch. II, §4, Ex. 6. In the case of lattices of finite breadth.

CHAPTER V

MODULAR LATTICES

1. Definition and examples. Just as the elements of many groups satisfy the identity $xy = yx$, so the elements of many important lattices satisfy the following "modular identity."

L5. If $x \leqq z$, then $x \smile (y \frown z) = (x \smile y) \frown z$.

A lattice is called *modular* if and only if its elements satisfy the modular identity L5. Modular lattices are also called Dedekind lattices (Dedekindsche Verbände) and Dedekind structures.

THEOREM 1. *The normal subgroups of any group form a modular lattice.*[1]

Proof. In any lattice, we have the one-sided modular law (Ch. II, §4, (4)); hence we need only show that $x \leqq z$ implies $x \smile (y \frown z) \geqq (x \smile y) \frown z$. Suppose that X, Y, Z are normal subgroups of a group, with $X \leqq Z$. Then $X \smile Y$ is the set XY of all products xy $[x \in X, y \in Y]$, as is easily shown by group theory.[2] Hence $(X \smile Y) \frown Z$ consists of the xy in Z. But in this case, $y = x^{-1}(xy) \in Z$, since $X \leqq Z$; hence xy is in $X \smile (Y \frown Z)$, and $(X \smile Y) \frown Z \leqq X \smile (Y \frown Z)$, as claimed.

It will be shown in Ch. VI that, more generally, the Ω-subgroups of any group with a class Ω of operators which includes all inner automorphisms form a modular lattice. The great significance of this fact for algebra will also be discussed in detail.

In Ch. VIII, it will be shown that the elements of any projective geometry form a modular lattice. In the first sections of Chs. IX, X, XIII, and XIV, other examples of lattices are discussed which satisfy the even stronger *distributive* law $x \frown (y \smile z) = (x \frown y) \smile (x \frown z)$. However, in the present chapter, attention will be confined to abstract modular lattices and their properties.

We do note, however, that the dual of any modular lattice is modular, and that any sublattice, homomorphic image or product of modular lattices is modular.

Ex. 1. (a) Show that L5 is equivalent to: if $x < z$, then $x \smile (y \frown z) \nless (x \smile y) \frown z$.
(b) Show that the distributive law implies the modular law.

Ex. 2. (a) Show that the lattice of Fig. 1d, Ch. I, §5, is not modular.
(b) Show that the lattice of Fig. 1c, ibid., is modular.
(c) Show that the lattice of (a) is the only non-modular five-element lattice.

Ex. 3. Show that the modular law is self-dual.

[1] Theorems 1–4 are essentially due to Dedekind [2] (1900). See also Dirichlet, *Zahlentheorie*, §169, pp. 498–9.

[2] Obviously every such $xy \in X \smile Y$; while since $(xy)(x'y') = (xx')((x'^{-1}yx')y')$ and $(xy)^{-1} = (y^{-1}x^{-1}y)y^{-1}$ are in XY, XY is the entire subgroup $X \smile Y$.

Ex. 4. Prove that $[(x \frown y) \smile (x \frown z)] \frown [(x \frown y) \smile (y \frown z)] = x \frown y$ in any modular lattice. (H. Löwig, Annals of Math. 44 (1943), 573–9, proves a stronger result.)

Ex. 5. Prove that any sublattice, homomorphic image, or product of modular lattices is modular, quoting the relevant theorems from the Foreword on Algebra.

2. Alternative characterizations. Let L be any lattice, and let $z > x$ and y be chosen in L. By the one-sided modular law, we have

$$x \frown y \leqq x \leqq x \smile (y \frown z) \leqq (x \smile y) \frown z \leqq x \smile z \leqq y \smile z,$$

$$x \frown y \leqq y \frown z \leqq y \leqq x \smile z \leqq y \smile z.$$

Using duality, we see that all the inclusion relations of the diagram of Fig. 3a are valid. Furthermore, since $(x \smile y) \frown z \geqq x$, $[(x \smile y) \frown z] \smile y \leqq x \smile y$, which is however an obvious upper bound to $(x \smile y) \frown z$ and y; hence $[(x \smile y) \frown z] \smile y = x \smile y$ and dually. That is, *the sublattice generated by $z > x$ and y in any lattice is a homomorphic image of the lattice of Fig.* 3a.

Theorem 2. *A lattice L is non-modular if and only if it contains a sublattice isomorphic to the five-element lattice of Fig.* 1d, Ch. I, §5.

For this lattice is non-modular, and if $z > x$, y fail to satisfy L5, then the sublattice of Fig. 3a consisting of y, $x \smile y$, $y \frown z$, $(x \smile y) \frown z$, and $x \smile (y \frown z)$ satisfies the conditions.

Corollary 1. *In a modular lattice, $v > u$ is incompatible with $y \smile u = y \smile v$ and $y \frown u = y \frown v$; moreover this condition conversely implies modularity.*

Corollary 2. *In a modular lattice,*

($\xi 1'$) *if y covers a, and $a < x \nleqq y$, then $x \smile y$ covers x, and dually,*

($\xi 1''$) *if a covers y and $a > x \ngeqq y$, then x covers $x \frown y$.*

Proof. Unless $x \smile y$ covered x, the sublattice generated by x, y, and any z between x and $x \smile y$ would be the forbidden non-modular five-element lattice.

In particular, Cor. 2 yields the dual *covering conditions*:

(ξ') If x and y cover a, and $x \neq y$, then $x \smile y$ covers x and y,

(ξ'') If a covers x and y, and $x \neq y$, then x and y cover $x \frown y$.

Again, define "x at most covers a" to mean: "x covers a or $x = a$." Then (ξ') implies

($\xi 2'$) If x and y at most cover a, then $x \smile y$ at most covers x.

For the cases $x = a$, $x = y$, and $y = a$ are trivial. A dual condition ($\xi 2''$) may be inferred dually from (ξ'').

Now let L be any lattice in which all bounded chains are finite. We shall show that (ξ') implies the Jordan-Dedekind chain condition (Ch. I, §9). For each positive integer m, let $P(m)$ be the assertion that if one maximal[3] chain γ: $a = x_0 < x_1 < \cdots < x_m = b$ has length m, then every maximal chain between

[3] By a "maximal" or "connected" chain, we mean as usual that x_i covers x_{i-1} for all $i = 1, \cdots, m$.

a and b has length m. $P(1)$ is trivial in any lattice; we shall show that $P(m-1)$ implies $P(m)$. Indeed, let $\gamma': a = y_0 < y_1 < \cdots < y_n = b$ be any other (finite) maximal chain connecting a and b; set $u = x_1 \smile y_1$ (cf. Fig. 3b).

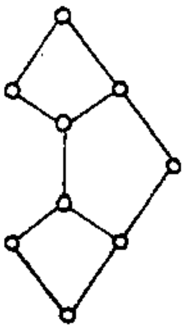

FIG. 3a

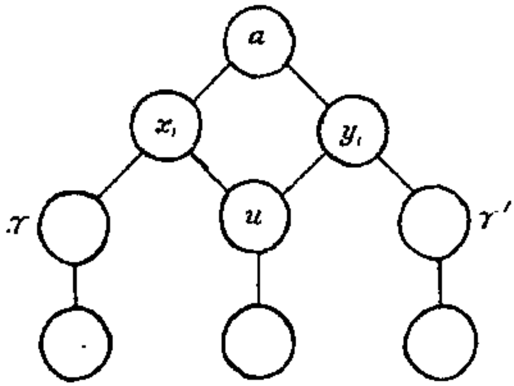

FIG. 3b

The case $x_1 = y_1$ is trivial. Otherwise, by (ξ'), u covers x_1 and y_1; form any maximal chain γ'' connecting u and b. By $P(m-1)$, the chain x_1, γ'' has length $m-1$, like $x_1 < x_2 < \cdots < x_m$; hence γ'' has length $n-2$; hence y_1, γ'' has length $m-1$; hence, by $P(m-1)$ again, $y_1 < y_2 < \cdots < y_n$ has length $m-1$, and so $m = n$.

It follows that we can define a *dimension* function $d[x]$ as in Ch. I, §9, such that x covers y if and only if $x > y$ and $d[x] = d[y] + 1$. Since the Jordan-Dedekind chain condition is self-dual, it is implied equally by the dual (ξ'') of (ξ'). Furthermore, we can prove the following

LEMMA 1. *The inequality* $d[x] + d[y] \geqq d[x \smile y] + d[x \frown y]$ *is implied by* (ξ'); *the reverse inequality is implied by* (ξ'').

Proof. Form any connected chains

$$x \frown y = x_0 < x_1 < \cdots < x_m = x, \qquad x \frown y = y_0 < y_1 < \cdots < y_n = y.$$

Then assuming by induction that $x_{i-1} \smile y_j$ and $x_i \smile y_{j-1}$ at most cover $x_{i-1} \smile y_{j-1}$, we conclude from $(\xi 2')$ that $x_i \smile y_j = (x_{i-1} \smile y_j) \smile (x_i \smile y_{j-1})$ at most covers $x_{i-1} \smile y_j$ and $x_i \smile y_{j-1}$. We infer that $d[x \smile y_j] - d[x \smile y_{j-1}] \leqq 1$, and hence $d[x \smile y] - d[x] \leqq n = d[y] - d[x \frown y]$, which proves the first assertion. The second follows by duality.

It is a corollary that in any lattice L where all bounded chains are finite, and (ξ')–(ξ'') hold, the Jordan-Dedekind chain condition holds, and

$$d[x] + d[y] = d[x \frown y] + d[x \smile y]. \tag{1}$$

Finally, if L is any lattice with a numerical function satisfying (1), then we see that if $x \leqq z$, then

$$d[x \smile (y \frown z)] - d[(x \smile y) \frown z] = d[x] + d[y \frown z] - d[x \frown y] - d[x \smile y] - d[z] + d[y \smile z].$$

This reduces after rearrangement, since $d[x] - d[x \frown y] - d[x \smile y] = -d[y]$ and similarly for the other three terms, to $d[y] - d[y] = 0$. Hence *if* $u > v$ implies $d[u] > d[v]$, as in the present case, we cannot have $x \smile (y \frown z) < (x \smile y) \frown z$. By the one-sided modular law (Ch. II, §4, (4)) we conclude that L5 must hold.

In summary, we have proved

THEOREM 3. *Let L be any lattice in which all bounded chains are finite. The following conditions are equivalent:* (i) *the modular identity*, (ii) *the covering conditions* (ξ')–(ξ''), (iii) *the Jordan-Dedekind chain condition, together with* (1).

The covering conditions give an easily applied graphical test. The various conditions of Theorem 3 will be studied more intensively in §§6, 7, 9 below; for the present, we shall consider some more purely algebraic constructions.

Ex. 1. (a) In a modular lattice L, define $x \equiv y(\theta)$ if there is a finite maximal chain joining $x \frown y$ and $x \smile y$. Show that this defines a congruence relation on L, and that elements are congruent if and only if they are in the same connected component of the diagram of L.

(b) Show that it gives the real number system from the ordinal power ${}^{\omega}2$.

(c) Show that this process can be iterated.[4]

Ex. 2*. Show that the free lattice generated by $x > y > z$ and u contains exactly twenty elements. (I. Kaplansky)

Ex. 3*. Let $\alpha: f(x, y, z) = g(x, y, z)$ be any identity valid in a lattice L whenever $x > z$. Show that either (i) L consists of a single element, or (ii) α is equivalent to L5, or (iii) α holds in every lattice.

3. Free modular lattice with three generators. We shall now determine the free modular lattice with three generators.

THEOREM 4. *The free modular lattice with three generators has twenty-eight elements, and the diagram of Fig.* 4.

Proof. Since the partly ordered set L_{28} of Fig. 4 has twelve-fold symmetry (all permutations of subscripts and duality), it is not hard to prove, by considering a limited number of representative cases, that every pair of elements has a join (and meet). The modular law can then be easily checked, using (ξ') and duality. We leave the details to the reader. Independent proofs that L_{28} is a modular lattice are suggested in Exs. 1–2 below. Further, it is generated by x_1, x_2, x_3. In fact, $u_1 = x_2 \smile x_3$ and cyclically, $v_1 = x_2 \frown x_3$ and cyclically,

[4] Cf. Ore [1, pp. 421–4], for further details.

$I = x_1 \smile x_2 \smile x_3$, $O = x_1 \frown x_2 \frown x_3$, $a_i = x_i \frown u_i$, $b_i = x_i \smile v_i$, $c_1 = u_2 \frown u_3$ and cyclically, $d_1 = v_2 \smile v_3$ and cyclically, $c = u_1 \frown u_2 \frown u_3$, $d = v_1 \smile v_2 \smile v_3$, and $e_i = u_i \frown (x_i \smile v_i) = (u_i \frown x_i) \smile v_i$.

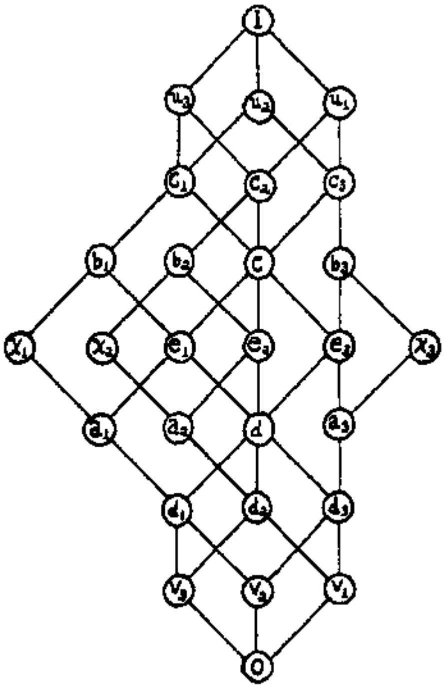

FIG. 4

Conversely, the join- and meet-functions diagrammed in Fig. 4 are all consequences of L1–L5. The calculations involved in proving this can also be greatly reduced by symmetry. We give only two samples,

$$a_1 \smile a_2 = (x_1 \frown u_1) \smile (x_2 \frown u_2) = ((x_1 \frown u_1) \smile x_2) \frown u_2 \qquad \text{(by L5)}$$

$$= (u_1 \frown (x_1 \smile x_2)) \frown u_2 = u_1 \frown u_3 \frown u_2 = c.$$

$$b_2 \smile e_2 = (x_2 \smile v_2) \smile (a_3 \smile v_3) = x_2 \smile a_3 \qquad \text{(by absorption)}$$

$$(\text{since } v_3 \leqq x_2 \text{ and } v_2 = x_3 \frown x_1 \leqq x_3 \frown u_3 = a_3)$$

$$= x_2 \smile (x_3 \frown (x_1 \smile x_2)) = (x_2 \smile x_3) \frown (x_1 \smile x_2) = c_2 .$$

These samples are typical, in that they use L5 as a *mixed associative law.*

On the other hand, the free modular lattice generated by four elements is infinite. Indeed, consider the lattice formed by the points and lines of the projective plane I, together with I and the void set O. It is easy to verify condition (iii) of Theorem 3; hence the lattice is modular. Yet the sublattice generated by the four points (0, 1), (1, 0), (0, 1), and (1, 1) is infinite.[5]

Ex. 1. (a) Construct a table of joins from Fig. 4. (This does not mean that the associative law has been proved yet.)

(b) Prove that all formulas of this table follow from L1–L5.

(c) Infer, without using Thm. 4, that the free modular lattice with three generators has at most 28 elements.

(d) Let A be the commutative group with 256 elements, and generators $e_1, \cdots, e_8$ of order two. Let X_1, X_2, X_3, be the subgroups generated by $\{e_1, e_2, e_4, e_7\}$, $\{e_2, e_3, e_5, e_8\}$, $\{e_1, e_3, e_6, e_7 + e_8\}$. Show that all 28 subgroups of Fig. 4 are distinct.

(e) Infer, without using Thm. 4, that the free modular lattice with three generators is that defined by Ex. 1 (a).

Ex. 2. (a) Represent the partly ordered set of Fig. 4 as a sublattice of $2^6 \times M_5$, where M_5 denotes the five-element modular lattice. (Hint: Let $x_1 = (I, I, O, I, O, O, x)$, $x_2 = (O, I, I, O, I, O, y)$, etc., as suggested by Ex. 1 (d).)

(b) Infer that Fig. 4 represents a modular lattice, without using Thm. 4.

Ex. 3. Show that the modular lattice of Fig. 4 has "breadth" 3, in the sense of Ch. II, §4, Ex. 6.

Ex. 4. Show that in a modular lattice, any congruence relation which identifies two adjacent vertices of a quadrangle of elements linked by covering relation identifies the other two vertices. (Hint: If $x \equiv x \frown y$ (θ), then $x \smile y \equiv y$ (θ).)

Ex. 5. (a) Infer from Ex. 4 that if $x \frown (y \smile z) = (x \frown y) \smile (x \frown z)$ for three particular elements x, y, z of a modular lattice, then all the 12 equations obtained from this by permuting x, y, z and dualizing are also true.

(b) Show that this is not true in any non-modular lattice.

Ex. 6. Let $\alpha: f(x, y, z) = g(x, y, z)$ be any identity valid in a modular lattice L. Show that either (i) L consists of single element, or (ii) α is equivalent to the distributive law, or (iii) α holds in every modular lattice.[6] (Hint: Use Ex. 4.)

Ex. 7.** Show that a lattice is a subdirect union of **2** and M_5, as described in Ex. 2, if and only if it satisfies identically

L51. $a \smile (x \frown b) \smile (y \frown b) \geqq b \frown (a \smile x) \frown (a \smile y) \frown (x \smile y)$, and

L52. $a \smile (x \frown b) \smile (y \frown b) \smile (x \frown y) \geqq b \frown (a \smile x) \frown (a \smile y)$.

Problem 27. (a) Do the subgroups of a commutative group satisfy any identities on 4 elements not implied by L1–L5?

(b) Same question for $n > 4$.

(c) Same questions for the normal subgroups of a non-commutative group.

Problem 28. Solve the Decision Problem for the free modular lattice with four generators—with n generators.

Problem 29. Determine the free modular lattice generated by $\mathbf{2} + \mathbf{1} + \mathbf{1}$. (R. M. Thrall)

---

[5] This example was noted by the author [1, p. 464]. It really amounts to recalling that the harmonic net generated by a complete quadrangle is infinite (Veblen and Young, pp. 80–87). The free modular lattice with four generators even has infinite length. Let I be the Abelian group generated by $x_1, x_2, \cdots, x_n, \cdots$. Let S_1 be the subgroup generated by the x_{2k}, S_2 by the $x_{2k} + x_{2k+1}$, S_3 by the x_{2k+1}, S_4 by the $x_{2k+1} + x_{2k+2}$, where $k = 0, 1, 2, \cdots$. Let $T_1 = S_1$, $T_{4n+1} = T_{4n} \frown S_1$, $T_{4n+2} = T_{4n+1} \smile S_2$, $T_{4n+3} = T_{4n+2} \frown S_3$, $T_{4n+4} = T_{4n+3} \smile S_4$. Then $T_4 > T_8 > T_{12} > \cdots$, as can easily be checked.

[6] See M.-P. Schutzenberger, C. R. Acad. Sci. Paris 221 (1945), 218–20, for a statement of some similar results, also relevant to Problem 27a. The author has lost the proof of Ex. 7; one can reduce to the case that all prime quotients are projective by Thm. 10 of Ch. VI and the Cor. of Thm. 10, Ch. V. Then it is sufficient to exclude the cases of *2* and Fig. 1c.

4. Free modular lattice generated by two chains. Let L be any lattice, and let $O = x_0 < x_1 < \cdots < x_m = I$ and $O = y_0 < y_1 < \cdots < y_n = I$ be any two chains in L between O and I. Clearly the set of $u^i_j = x_i \frown y_j$ includes all x_i and y_j (for $x_i \frown y_n = x_i$ and $x_m \frown y_j = y_j$); dually, the set of $v^i_j = x_i \smile y_j$ includes them. Hence so does the set of *joins* of the u^i_j, and that of the *meets* of the v^i_j.

LEMMA 1. *Any join of the u^i_j can be written in the form $(x_{i(1)} \frown y_{j(1)}) \smile \cdots \smile (x_{1(r)} \frown y_{j(r)})$, where $i(1) > \cdots > i(r)$ and $j(1) < \cdots < j(r)$.*

Proof. If two u^i_j have the same superscript, then since the y_j are a chain, one u^i_j must be contained in, and hence by L4 can be absorbed by, the other. Thus we can make all the $i(k)$, and similarly all the $j(k)$, distinct. Moreover if $i > i'$ and $j \geqq j'$, then $(x_i \frown y_j)$ will absorb $(x_{i'} \frown y_{j'})$, since it includes it. Hence after we have absorbed as many elements as possible, and utilized L2 to arrange the $i(k)$ in descending order, we will have $j(1) < \cdots < j(r)$ also.

LEMMA 2. *If $a_i \geqq a_{i+1}$ and $b_i \leqq b_{i+1}$ for all i in a modular lattice, then*

$$(a_1 \frown b_1) \smile \cdots \smile (a_r \frown b_r) = a_1 \frown (b_1 \smile a_2) \frown \cdots \frown (b_{r-1} \smile a_r) \frown b_r ,$$

$$(b_1 \smile a_1) \frown \cdots \frown (b_r \smile a_r) = b_1 \smile (a_1 \frown b_2) \smile \cdots \smile (a_{r-1} \frown b_r) \smile a_r .$$

Proof. By duality and induction on r, we need only prove the first identity on the assumption that the second holds when there are fewer than r summands. But by L5 applied twice, $(a_1 \frown b_1) \smile \cdots \smile (a_r \frown b_r)$ can be rewritten in the form

$$a_1 \frown [b_1 \smile (a_2 \frown b_2) \smile \cdots \smile (a_{r-1} \frown b_{r-1}) \smile a_r] \frown b_r .$$

And by the second identity for the case $(r - 1)$, the two expressions

$$(b_1 \smile a_2) \frown (b_2 \smile a_3) \frown \cdots \frown (b_{r-1} \smile a_r),$$

$$b_1 \smile (a_2 \frown b_2) \smile (a_3 \frown b_3) \smile \cdots \smile (a_{r-1} \frown b_{r-1}) \smile a_r$$

are equal. And if we substitute the former for the latter in the square brackets above, we get the right-hand side of the first identity, q.e.d.

LEMMA 3. *The joins of the u^i_j are a sublattice.*

Proof. Evidently any join of joins of u^i_j is a join of u^i_j; but any meet of joins of u^i_j is by Lemmas 1–2 a meet of meets of v^i_j, hence a meet of v^i_j, and hence by Lemmas 1–2 a join of u^i_j.

Now observe that if X_i denotes the set of points (x, y) of the rectangle $0 \leqq x \leqq m$, $0 \leqq y \leqq n$ satisfying $x \leqq i$, and if Y_j denotes the set of points satisfying $y \leqq j$, and if joins and meets are interpreted as set-unions and set-products, then all of the expressions admitted in Lemma 1 describe different sets (of saw-tooth shape). For example, Fig. 5c represents $(x_5 \frown y_5) \smile (x_3 \frown y_4) \smile (x_4 \frown y_2) \smile (x_6 \frown y_1)$ $[m = 6, y = 5]$. By Lemma 3, these sets describe a *ring* of sets (i.e., a sublattice of the lattice of all subsets of the square), which thus represents isomorphically the *free* modular lattice generated by the two chains. We infer that this lattice is distributive in the sense of Ch. IX, and is finite. In summary, we have proved

THEOREM 5. *The free modular lattice generated by two finite chains is a finite distributive lattice.*[7]

COROLLARY. *Any two finite chains between the same end points have refinements whose subintervals are projective (see §5) in pairs.*

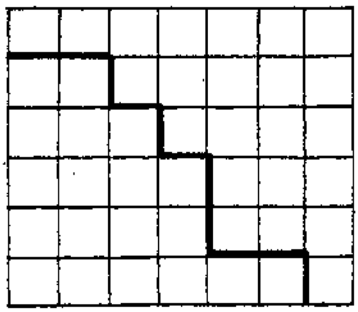

FIG. 5a

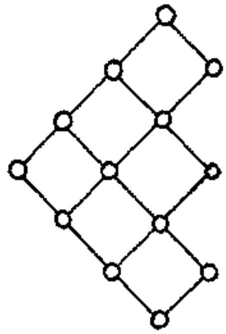

FIG. 5b

Ex. 1. (a) Show that the free modular lattice generated by $a > b$ and $c > d$ has 18 elements. (This is not a special case of Thm. 5, unless O and I are adjoined.)

(b) Show that if $m = 1$, $n = 3$, and O, I are not adjoined, the diagram of the lattice of Thm. 5 is that shown in Fig. 5b.

Ex. 2. (a) Let the two chains in Thm. 5 have $m - 1$ and $n - 1$ elements respectively. Show that if O, I are added to the resulting distributive lattice, it becomes $2^{m,n}$ in the notation of Ch. I, §7.

(b) Show that it has $(m + n)!/m!n!$ elements. (Hint: identify the heavy line in Fig. 5a with a representation $xxyxyyxxy$ of x^5y^5.)

Ex. 3. (a) Show that if $m = 2$, the lattice of Thm. 5 is planar.

(b) What is its breadth in general?

5. Dedekind's transposition principle. The concept of a *projectivity* applies to modular lattices in general, as we shall now see.[8]

DEFINITION. *A (closed) interval $[x, y]$ is called "prime" if and only if y covers x. Intervals which can be written as $[x \frown y, x]$ and $[y, x \smile y]$ are called transposes, while two quotients $[x, y]$ and $[x', y']$ are called projective (in symbols $[x, y] \sim$*

[7] This result is due to the author [LT, p. 51]. The proof is practically that of O. Schreier' *Über den J-H'schen Satz*, Hamb. Abh. 6 (1928), 300–2, and H. Zassenhaus, *Zum Satz von Jordan-Hölder-Schreier*, ibid. 10 (1934), 106–8.

[8] Dedekind [2, p. 245] speaks of a "quotient-symbol" (x, y) where we speak of the "closed interval" $[x, y]$. In [LT], the redundant notation x/y and terminology "quotient" was used; cf. also the author [1, p. 452], and O. Ore [1, 2]. We refer below only to closed intervals, but shall call them intervals for brevity.

$[x', y']$) *if and only if there exists a finite sequence* $[x, y], [x_1, y_1], [x_2, y_2], \cdots,$ $[x', y']$ *in which any two sucessive quotients are transposes.*[9]

THEOREM 6. *Let L be any modular lattice, and let u and v be any two elements of L. Then the correspondences* $x \to u \smile x$ *and* $y \to v \frown y$ *are inverse isomorphisms between* $[u \frown v, v]$ *and* $[u, u \smile v]$. *Moreover they carry quotients in these intervals into transposed quotients.*

Proof. If $u \frown v \leqq x \leqq v$, then $u = u \smile (u \frown v) \leqq u \smile x \leqq u \smile v$, and if $x \leqq x'$, then $u \smile x \leqq u \smile x'$. Hence the first correspondence is isotone from $[u \frown v, v]$ to a subset of $[u, u \smile v]$. Dually, the second correspondence is isotone from $[u, u \smile v]$ to a subset of $[u \frown v, v]$. But $u \frown v \leqq x \leqq v$ implies $v \frown (u \smile x) = (v \frown u) \smile x = x$ by L5; dually, $u \smile (v \frown y) = y$ for all $y \in [u\ u \smile v]$. Thus the two correspondences are inverses, hence both one–one, and so isomorphisms. To see that they yield transpositions, note that if $u \frown v \leqq x \leqq x' \leqq v$, then $[x, x']$ and $[u \smile x, u \smile x']$ are transposes, and dually. For

$$x' \smile (x \smile u) = (x' \smile x) \smile u = x' \smile u, \text{ while}$$

$$x' \frown [u \smile x) = (x' \frown u) \smile x = [(x' \frown v) \frown u] \smile x$$

$$= [x' \frown (v \frown u)] \smile x = (v \frown u) \smile x = x.$$

COROLLARY. *Projective intervals are isomorphic, in any modular lattice.*

THEOREM 7. *The lattice generated by* $[u \frown v, u] = X$ *and* $[u \frown v, v] = Y$ *is the cardinal product* XY.

Proof. We let (x, y) denote $x \smile y$, for any $x \in X, y \in Y$. Then by L2–L3,

$$(x, y) \smile (x', y') = x \smile y \smile x' \smile y' = (x \smile x') \smile (y \smile y') = (x \smile x', y \smile y').$$

Again, by Theorem 6 and L5 respectively, we have

$$(x, y) = x \smile y = [(v \smile x) \frown u] \smile y = (v \smile x) \frown (u \smile y).$$

Hence $(x, y) \frown (x', y') = [(v \smile x) \frown (v \smile x')] \frown [(u \smile y) \frown (u \smile y')]$ by L2–L3. And by Theorem 6, $(v \smile x) \frown (v \smile x') = v \smile (x \frown x')$ and $(u \smile y) \frown (u \smile y') = u \smile (y \frown y')$. Hence

$$(x, y) \frown (x', y') = [v \smile (x \frown x')] \frown [u \smile (y \frown y')] = (x \frown x', y \frown y')$$

as before. This completes the proof. By induction, we get the

COROLLARY. *If* $(x_1 \smile \cdots \smile x_k) \frown x_{k+1} = a$ *for* $k = 1, \cdots, n - 1$, *then the sublattice generated by the intervals* $X_k = [a, x_k]$ *is* $X_1X_2 \cdots X_n$.

But the definition of $X_1X_2 \cdots X_n$ is symmetric in the subscripts. Hence

[9] The term "transposable" is due to Ore; the term "projectivity" is due to von Neumann. The idea of transposition goes back to Dedekind; that of projectivity is due to Ore (who speaks of "similar" quotients). Theorem 6 is due to Dedekind [2, XI, p. 259]; cf. also Ore [1, p. 418].

the condition of the preceding corollary is invariant under all permutations of the subscripts, and we can legitimately state[10] the

Definition. *Under the hypotheses of the preceding corollary, $x_1, \cdots, x_n$ are said to be independent over a.*

The concept of independence over O contains as special cases the usual notions of "disjointness" in set theory, and of linear independence of subspaces of a linear space. "Independence under a" can clearly be defined dually.

Ex. 1. Deduce conditions (ξ')–(ξ'') as corollaries of Theorem 6.

Ex. 2. Assuming the Jordan-Dedekind chain condition, deduce (1) as an immediate corollary of Theorem 6.

Ex. 3. Show that the conditions of Theorem 6 are necessary as well as sufficient for modularity.

Ex. 4. (a) In the diagram of a modular lattice of finite length, show that the opposite sides of a quadrilateral represent transposed prime intervals.

(b*) Show that two prime intervals are projective if and only if one can pass from one to another by a finite sequence of substitutions of one side of a quadrilateral in the diagram for the opposite side.

Ex. 5*. For any elements a, b of any lattice L, let $a/a \wedge b$ denote the set of all $x = (x \smile b) \frown a$, and let $a \vee b/b$ denote the dual set of all $y = (y \frown a) \smile b$. Show that $a/a \wedge b$ and $a \vee b/b$ are always isomorphic lattices, though not in general sublattices of L. Show that L5 is equivalent to the identity $a/a \wedge b = a/a \frown b$. (W. Schwan)

Ex. 6**. Let L be a lattice in which $[a \frown b, a]$ and $[b, a \smile b]$ are isomorphic for all a, b. Show that if L satisfies either the ascending or descending chain condition, it is modular.[11]

6. Valuations. In general, by a *valuation* on a lattice L is meant a real-valued function $v[x]$ defined on L which satisfies

V1. $$v[x] + v[y] = v[x \frown y] + v[x \smile y].$$

A valuation is called *isotone* if and only if

V2. $x \geqq y$ implies $v[x] \geqq v[y]$;

positive, if and only if $x > y$ implies $v[x] > v[y]$. It is called of *bounded variation* if and only if, for some finite K and all chains

γ: $$x_0 < x_1 < \cdots < x_n, \qquad \sum_{i=1}^{n} | v[x_i] - v[x_{i-1}] | < K.$$

Probability and measure functions on sets are valuations (cf. Ch. XI below); so is dimension in projective geometry; any real-valued function on a chain is a valuation. The preceding definition[12] contains as special cases the usual defini-

[10] Following J. von Neumann [2, vol. 1, p. 11]; Theorem 3.4 is nearly the same as von Neumann's Theorem 1.2. See also Fr. Klein, Deutsche Math. 2 (1937), 216–41.

[11] Morgan Ward, Bull. Am. Math. Soc. 45 (1939), 448–51.

[12] Conditions V1–V2 go back to Dedekind [2] implicitly; cf. also the author [1, Cor. 9.2]. The general definition of "bounded variation" is due to the author (Bull. Am. Math. Soc. 44 (1938), p. 186).

tions (Saks [1, pp. 18, 148]) of bounded variation, both for ordinary real functions and for functions of sets. Again, we have

LEMMA 1. *A real-valued functional $v[x]$ on a relatively complemented lattice is a valuation provided*

V1*. $$v[x \smile y] = v[x] + v[y] \quad \text{whenever } x \frown y = 0.$$

Proof. For any x, y, let t be a relative complement of $x \frown y$ in $[0, y]$. By definition, $(x \frown y) \frown t = 0$ and $(x \frown y) \smile t = x$; hence $v[y] = v[x \frown y] + v[t]$. Moreover, since $t \leqq y, x \frown t = x \frown (y \frown t) = (x \frown y) \frown t = 0$, while $x \smile t = [x \smile (x \frown y)] \smile t = x \smile [(x \frown y) \smile t] = x \smile y$; hence $v[x \smile y] = v[x] + v[t]$. Subtracting the two equations, $v[x \smile y] - v[y] = v[x] + v[t] - v[x \frown y] - v[t]$, giving V1.

We shall now determine all valuations $v[x]$ on any modular lattice of finite length.

Clearly if, for an interval $[a, b]$ of L, we define $v[a, b] = v[b] - v[a]$, then by (1) transposed intervals and hence *projective intervals have the same values*. But the relation of projectivity between (prime) intervals is reflexive, symmetric and transitive—i.e., an equivalence relation. Hence each valuation assigns a unique valuation λ_p to each class of projective prime quotients.

Moreover if $\gamma: 0 = x_0 < x_1 < \cdots < x_n = x$ is any chain connecting 0 to x, then $v[x] = v[0] + \sum v[x_{i-1}, x_i]$. Hence if $p[x, \gamma]$ denotes the number of occurrences of a prime interval projective to p in γ, we have

(2) $$v[x] = v[0] + \sum \lambda_p p[x, \gamma].$$

We shall now sharpen the proof based on Fig. 3b in §2, to show that $p[x, \gamma]$ *is the same for all γ joining* 0 *and x*. Indeed, let $P(m)$ be the proposition that if one maximal chain connecting 0 and x contains m prime intervals projective with p, then every such chain contains m such intervals. Assuming $P(m - 1)$, we prove $P(m)$ as in §2. The only difference is the observation that, since $[y_0, y_1]$ and $[y_1, u]$ are transposes of $[x_1, u]$ and $[x_0, x_1]$ respectively, $p[x, \gamma]$ is unaltered when we pass from x_0, x_1, γ'' to y_0, y_1, γ''.

We thus define $p[x]$ to be the common value of the $p[x, \gamma]$. From Theorem 6, we infer immediately

(2′) $$p[x \smile y] - p[x] = p[y] - p[x \frown y];$$

whence $p[x]$ is a valuation. Further, evidently

LEMMA 2. *Any linear combination $\lambda_0 + \sum \lambda_k v_k[x]$ of valuations is itself a valuation.*

It is a corollary that (2) represents a valuation of L for any choice of coefficients λ_p. We summarize.

THEOREM 8. *The different valuations on a modular lattice L of finite length correspond one-one to the choices of $v[0]$ and valuations λ_p assigned to the classes of projective prime intervals of L:*

$$v[x] = v[0] + \sum \lambda_p p[x], \tag{2''}$$

where $p[x]$ is the number of prime intervals projective to p in any maximal chain joining 0 *with x.*

Ex. 1. Prove that every functional on a chain satisfies V1.

Ex. 2. Generalize Theorem 8 to all modular lattices in which all bounded chains are finite.

Ex. 3. Generalize Theorem 8 to the case of functions with values in an Abelian group.

Ex. 4. (a) Let $v[x]$ and $v^*[y]$ be positive valuations on lattices X resp. Y. Show that $v[x] + v^*[y]$ defines a positive valuation of XY.

(b) Construct a positive valuation of X^d [d = countable infinity].

Ex. 5. Let G be an oriented graph such that if $a\mu x$ and $a\mu y$, then b exists such that $x\mu b$ and $y\mu b$. Show that if $a\mu x_1\mu x_2\mu \cdots \mu x_m$ and $a\mu y_1\mu y_2\mu \cdots \mu y_n$, then (i) z exists such that $x_m\mu x_{m+1}\mu \cdots \mu x_{m+n} = z$ and $y_n\mu y_{n+1}\mu \cdots \mu y_{n+m} = z$, and (ii) if $x_m\mu z$ for no z, then $a\mu z_1\mu \cdots \mu z_n$ implies $z_m = x_m$. (Applications of this and analogous results to canonical forms have been made by M. H. A. Newman, Annals of Math. 43 (1942), 223–43.)

Ex. 6*. Let P be any partly ordered set in which every bounded chain is finite. Show that any maximal chain between two elements can be deformed into any other chain between the same elements, by a sequence of substitutions of one side of a "simple cycle" for another.[13] (A "simple cycle" is a pair of chains γ, γ' between x and y such that $x < t < y$ excludes $t \geqq u$, $u' > x$ [$u \in \gamma$, $u' \in \gamma'$] and $t \leqq v$, $v' < y$ [$v \in \gamma$, $v' \in \gamma'$].)

7. Metric lattices. A lattice L with an isotone valuation is called *quasi-metric*; if the valuation is positive, L is called a *metric lattice*. The argument immediately preceding Thm. 3 shows in effect that *any metric lattice is modular*. We repeat it. If $x \leqq z$, V1 implies

$$v[x \smile (y \frown z)] - v[(x \smile y) \frown z] = v[x] + v[y \frown z] - v[x \frown y] - v[x \smile y]$$
$$- v[z] + v[y \smile z] = -v[y] + v[y] = 0 \quad \text{(applying V1 four times).}$$

This makes $x \smile (y \frown z) < (x \smile y) \frown z$ impossible, and so (by the one-sided modular law) implies L5.

More generally, in any quasi-metric lattice, we define

$$\partial(x, y) = v[x \smile y] - v[x \frown y] \tag{3}$$

as the *distance*[14] from x to y. We shall now apply metric concepts due ultimately to Fréchet (cf. Foreword on Topology).

LEMMA. *The transformations $x \to a \smile x$ and $x \to a \frown x$ are contractions; in fact*

$$\partial(a \smile x, a \smile y) + \partial(a \frown x, a \frown y) \leqq \partial(x, y). \tag{4}$$

[13] See S. MacLane, *A conjecture of Ore, etc.*, Bull. Am. Math. Soc. 49 (1943), 567–8; also O. Ore, ibid., 558–66.

[14] V. Glivenko [1] first discussed the distance (3) abstractly. J. von Neumann [2, Ch. XVII], obtained Thm. 9 for general valuations; the author [6, Thm. 30] had already obtained it for Boolean algebras.

Proof. By definition, the left-hand side of (4) is $v[a \smile x \smile y] - v[(a \smile x) \frown (a \smile y)] + v[(a \frown x) \smile (a \frown y)] - v[a \frown x \frown y]$. By the one-sided distributive law, this is at most

$$v[a \smile x \smile y] - v[a \smile (x \frown y)] + v[a \frown (x \smile y)] - v([a \frown x \frown y].$$

Transposing the middle terms, and using V1 twice, we get

$$v[a] + v[x \smile y] - v[a] - v[x \frown y] = \partial[x, y].$$

THEOREM 9. *Any quasi-metric lattice is a quasi-metric space, in which joins and meets are uniformly continuous. The relation $\partial(x, y) = 0$ is a congruence relation, mapping L isometrically and lattice-homomorphically onto a metric lattice.*

Explanation. A quasi-metric space is one in which

(5) $$\partial(x, x) = 0,\ \partial(x, y) \geqq 0,\ \partial(x, y) = \partial(y, x),$$

and

(6) $$\partial(x, y) + \partial(y, z) \geqq \partial(x, z) \qquad \text{(Triangle inequality)}.$$

Cf. the definition of a metric space (Foreword on Topology).

Proof. The conditions of (5) are obvious. Again,

$$\begin{aligned}\partial(x,y) + \partial(y,z) &= \partial(x \smile y, y) + \partial(y, x \frown y) + \partial(y \smile z, y) + \partial(y, y \smile z)\\ &\geqq \partial(x \smile y \smile z, y \smile z) + \partial(y \smile z, y) + \partial(y, x \frown y) + \partial(x \frown y, x \frown y \frown z)\end{aligned}$$

since $\partial((x \smile y \smile z), y \smile z) \leqq \partial(x \smile y, y)$ and $\partial((x \frown y \frown z), y \frown z) \leqq \partial(x \frown y, y)$ by (4). But the last sum is

$$\partial(x \smile y \smile z, x \frown y \frown z) \geqq \partial(x \smile y, x \frown y) = \partial(x, y),$$

proving (6). We shall prove uniform continuity of joins in the sharp form

(7) $$\begin{aligned}\partial(a \smile b, c \smile d) &\leqq \partial(a \smile b, c \smile b) + \partial(c \smile b, c \smile d) && \text{by (5)}\\ &\leqq \partial(a, c) + \partial(b, d) && \text{by (4) and L2.}\end{aligned}$$

That of meets follows dually. In fact, one can show

(7′) $$\partial(a \smile b, c \smile d) + \partial(a \frown b, c \frown d) \leqq \partial(a, c) + \partial(b, d).$$

Finally, (5) shows that $\partial(x, y) = 0$ is reflexive and symmetric, while (6) and $\partial(x, z) \geqq 0$ show it is transitive; hence it is an equivalence relation. It has the substitution property for joins and meets by (7′); hence it is a congruence relation, modulo which L is a lattice-homomorphic image L^*. By (6), congruent pairs of elements are equal distances apart; hence the correspondence $L \to L^*$ is isometric, and (5)–(6) hold in L^*. But in L^*, $x \neq y$ implies $\partial(x, y) > 0$ by definition; hence L is a metric space.

THEOREM 10. *Let L be any modular lattice of finite length. The congruence relations on L correspond one-one to the sets of classes of projective prime quotients, which they annul. Hence they form a Boolean algebra.*

Proof. Let θ be any congruence relation on L. If $x \equiv x \smile y \pmod{\theta}$, then $x \frown y \equiv (x \smile y) \frown y = y \pmod{\theta}$ and dually; hence if θ annuls a (prime) quotient, it annuls all projective (prime) quotients (we use the fact that θ is transitive). Conversely, let $S = S(\theta)$ be any set of classes of projective prime quotients; define $v_S[x]$ as the sum of the $p[x]$ for p *not* in S. By Thm. 8, this is a valuation; it is clearly isotone. By Thm. 9, this valuation defines a congruence relation $\theta(S)$. Moreover $x \equiv y \pmod{\theta(S)}$ if and only if $x \smile y \equiv x \frown y$ (mod $\theta(S)$)—which happens if and only if every prime quotient in any maximal chain joining $x \frown y$ with $x \smile y$ is in S. Hence θ is determined by $S(\theta)$, and the correspondence $\theta \to S(\theta)$ is one–one. It is, however, clearly isotone; hence it is an isomorphism.

COROLLARY 1. *A modular lattice of finite length is "simple" (i.e., without proper congruence relations) if and only if all its prime quotients are projective.*

Again, consider the free modular lattice L with three generators graphed in §3, Fig. 4. Direct computation of the prime quotients shows that L can be mapped homomorphically onto the distributive lattice **2** in six ways, and in one way onto the line M with three points graphed in Fig. 1c, p. 6. Moreover, M is "simple." It follows that if x, y, z are any three elements of a modular lattice, and if any two distinct elements of M are equal in the sublattice generated by x, y, z then x, y, z generate a distributive sublattice. In summary, we have

THEOREM 11. *Elements x, y, z of a modular lattice generate a distributive sublattice if either of the equations $x \frown (y \smile z) = (x \frown y) \smile (x \frown z)$ or $x \smile (y \frown z) = (x \smile y) \frown (x \smile z)$ holds.*

It follows that each of the preceding equations is in effect a self-dual and symmetric condition on the three variables x, y, z; cf. Ex. 5(a) of §3 and Thm. 8 of Ch. VI.

Ex. 1. Show that in a metric lattice, $\partial(x,y) + \partial(y, z) = \partial(x, z)$ if and only if $y \in [x \frown z, x \smile z]$. (Pitcher-Smiley)

Ex. 2. Let $v[x]$ assume values in an ordered group G, so that V1 is satisfied.
(a) Show that if $v[x]$ is positive, L is still modular.
(b*) Show that if G is commutative, we can prove a generalization of Thm. 9.
(c**) What if G is not commutative?

Ex. 3. Show directly that if either of the equations of Thm. 11 holds, then x, y, z generate the lattice of Fig. 6a, or a lattice-homomorphic image thereof. (Hint: Use Ex. 4, §3.)

Ex. 4. (a) Show that in a metric lattice, all intervals projective to a given interval $[a, b]$ have the same length $v[b] - v[a]$.
(b) Infer that no interval can be projective with a proper part of itself.

8. Ideals, neutral elements. The following result, due to Dilworth, is useful.

THEOREM 12. *The ideals of any modular lattice themselves form a modular lattice under set-inclusion.*

Remark. In the case of lattices of finite length, where every ideal is principal, this result is trivial.

Proof. Suppose $X \leqq Z$, Y are ideals; by the one-sided modular law, we need only show that every $t \in (X \smile Y) \frown Z$ is in $X \smile (Y \frown Z)$. But for ideals in general, $t \in (X \smile Y) \frown Z$ means $t \leqq (x \smile y) \frown z$ for some $x \in X, y \in Y$, $z \in Z$; since $X \leqq Z$, $z_1 = x \smile z$ is also in Z, and clearly $t \leqq (x \smile y) \frown z_1$, where $x \leqq z_1$. By L5, this implies $t \leqq x \smile (y \frown z_1)$; hence that $t \in X \smile (Y \frown Z)$.

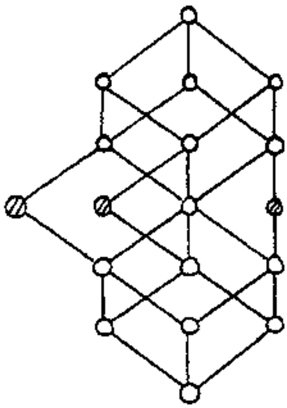

FIG. 6a

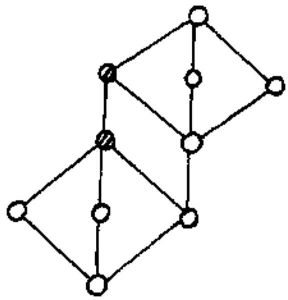

FIG. 6b

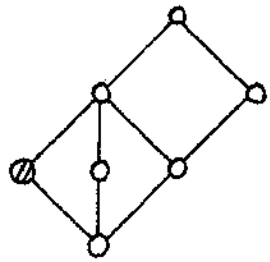

FIG. 6c

We next ask, which ideals of a modular lattice are the set of elements congruent to 0 under a suitable congruence relation?

THEOREM 13. *In a modular lattice, an element a is neutral if and only if $x \to x \frown a$ or $x \to x \smile a$ is an endomorphism of L.*

Proof. If $x \to x \frown a$ is an endomorphism, then $(x \smile y) \frown a = (x \frown a) \smile (y \frown a)$, and so every triple a, x, y generates a distributive sublattice, by Thm. 11. Hence a is neutral, by definition. The proof is completed by the Duality Principle, and reference to Ch. II, §10, Lemma 1.

It is a corollary that if a is neutral, then the ideal $[0, a]$ consists of all elements mapped on 0 under a suitable lattice-homomorphism. However, as in Fig. 6b, there also exist principal ideals $[0, a]$ consisting of all elements mapped on 0 under a lattice-homomorphism, for which a is not neutral.

Further, if a is neutral, then it is easy to show that a has at most one complement. The converse is however false; thus Marshall Hall has noted that the element shaded in black in Fig. 6c has a unique complement, yet is not neutral (cf. Thm. 11, Ch. VIII).

Ex. 1. Let $X_1, \cdots, X_n$ be ideals of a lattice L, and let $p(X_1, \cdots, X_n) = K$ be any polynomial function of the X_i, in the lattice of all ideals of L. Show by induction that if no X_i occurs more than once in p, then K consists of the $t \leqq p(x_1, \cdots, x_n)$, for some choice of $x_1 \in X_1, \cdots, x_n \in X_n$.

Ex. 2. (a) In Ex. 1, let terms X_i occur repeatedly in p. Let q be the polynomial obtained from p by substituting a new letter x_i, x_i', x_i'' for each new occurrence of the variable X_i in p. Show that K still consists of the $t \leqq q(x_1, \cdots, x_n, x_i', \cdots)$, for some choice of x_i, x_i', x_i'' in X_i.

(b**) Does *every* identity or identical implication in L imply the corresponding law in K?

Ex. 3. An ideal J of a modular lattice L is called *neutral* if and only if $t \leqq (x \smile a) \frown (y \smile b)$ $[x, y \in J]$ implies $t \leqq z \smile (a \frown b)$ for some $z \in J$.

(a) Show that the principal ideal generated by a single element $a \in L$ is neutral if and only if a is neutral.

(b) Show that J is neutral if and only if it is neutral as an element in the lattice of all ideals of L.

(c) Show that any neutral ideal is a congruence class under some (lattice) congruence relation.

Ex. 4**. Show by an example that the completion by cuts of a modular lattice need not be modular. (See refs. of Ch. IX, §6.)

9. Metric topology vs. order topology. Let M be any metric lattice; we can complete M as a metric space, as in the Foreword on Topology. Further, by (7), if $\{x_n\}$ and $\{y_n\}$ are Cauchy sequences, then so will $\{x_n \smile y_n\}$ and $\{x_n \frown y_n\}$ be Cauchy sequences, which we define as $\{x_n\} \smile \{y_n\}$ and $\{x_n\} \frown \{y_n\}$, respectively.[15] Then L1–L4 can be proved by passage to the limit; moreover $\{v[x_n]\}$ will converge to a limit, which we can define as $v[\{x_n\}]$—then proving that it is a "positive valuation" in the sense of §6. This defines from M a unique (metrically) *complete metric lattice.* Hence we obtain almost immediately from Thm. 9,

THEOREM 14. *Any metric lattice M has a unique metrically complete hull, in which it is (metrically) dense.*

The reader should be cautioned that, in general, the metric completion of M is not usually isomorphic with the completion of M by cuts (see Ch. XI, §10). However, it is usually a complete lattice.

THEOREM 15. *Any metrically complete metric lattice M is conditionally complete, and satisfies*

$$(8) \qquad x_n \uparrow x \textit{ implies } v[x_n] \uparrow v[x] \textit{ and dually;}$$

conversely, a σ-complete metric lattice satisfying (8) *is metrically complete. In a metrically complete metric lattice, metric convergence and star convergence are equivalent.*[16] *(See Ch.* IV, §9, *for the definition of star-convergence.)*

Proof. Let M be a complete metric lattice, and let S be any bounded subset

[15] We are simply generalizing the well known Cantor-Méray process of metric completion of the rationals to form real numbers; cf. Hausdorff [1, p. 106].

[16] Thm. 15 is due to J. von Neumann and the author (Annals of Math. 38 (1937), p. 56). The equivalence of star convergence and metric convergence was also shown by Kantorovitch [1]. For further work, see M. F. Smiley and L. R. Wilcox, *Metric lattices*, Annals of Math. 40 (1939), 309–27, corrected ibid., vol. 47 (1946), p. 831; F. Maeda, *Lattice functions and lattice structure*, Jour. Sci., Hiroshima Univ. 9 (1939), 85–104; and Ky Fan, Revue Sci. (Revue Rose Ill.) 82 (1944), 131–9.

of M. Consider the joins sup X of the finite subsets X of S; since S is bounded and $v[x]$ isotone, the set of real numbers $v[\sup X]$ will be bounded; hence it will have a least upper bound v_s. Hence we can find $X_1, X_2, X_3, \cdots$ such that $v[X_n] \geqq v_s - 2^{-n}$. Then, letting U denote the (finite) set-union of X_m and X_n, we have by (6),

$$\partial(\sup X_m, \sup X_n) \leqq v[\sup U] - v[\sup X_m] + v[\sup U] - v[\sup X_n]$$
$$\leqq 2^{-m} + 2^{-n} \text{ by construction.}$$

Hence, by metrical completeness, the sup X_n converge metrically to some $s \in M$. Now let $x \in S$ be given; by the lemma of §7,

$$v[x \smile s] - v[s] = \lim_{n\to\infty} \{v[x \smile \sup X_n] - v[\sup X_n]\} \leqq 2^{-n}$$

for all n. Hence $x \smile s = s$, and s is an upper bound to S. While if u is any upper bound to S, then $u \geqq \sup X_n$ for all n, and so $u \frown s = s$ by continuity (see (7)). Hence s is a least upper bound of S. The existence of inf S follows dually; hence M is conditionally complete.

To prove (8), note that if $x_n \uparrow x$, then $v[x_n] \uparrow$ and yet $v[x_n] \leqq v[x]$ for all n; hence $v[x_n] \uparrow c$ for some real number c. It follows that $\partial(x_m, x_n) = |v[x_m] - v[x_n]| \to 0$, as $m, n \to \infty$; hence $\partial(x_m, y) \to 0$ as $m \to \infty$ for some y, by metric completeness; clearly $v[x_m] \uparrow v[y]$; moreover $y \frown x_n = \text{Lim}\, x_m \frown x_n = \text{Lim}\, x_n = x_n$ (using metric limits); hence y is an upper bound to the x_n. But by definition, $x = \sup \{x_n\}$; hence $x \leqq y$ and $v[x] \leqq v[y]$. But we have already shown $v[x_n] \uparrow v[y]$ and $v[x_n] \leqq v[x]$ for all m; hence $v[x_n] \uparrow v[x]$, proving (8).

Conversely, let M be a σ-complete metric lattice assumed only to satisfy (8). From any subsequence of a Cauchy sequence, one can extract a subsubsequence $\{x_n\}$ satisfying $\partial(x_n, x_{n+1}) < 2^{-n}$ for all $k = 1, 2, 3, \cdots$. We shall show that (i) for some y, $\partial(x_n, y) \to 0$, thereby proving metric completeness, and (ii) $\{x_n\}$ order-converges to y, thereby proving that metric convergence implies star-convergence.

Indeed, form $y_{n,r} = x_n \smile x_{n+1} \smile \cdots \smile x_{n+r}$. For fixed n, $y_{n,r} \uparrow$. By σ-completeness, $y_{n,r} \uparrow y$, where, by (8), $\partial(y_{n,r}, y) \to 0$. Hence

$$\partial(x_n, y_n) \leqq \sum_{r=0}^{\infty} \partial(y_{n,r}, y_{n,r+1}) = \sum_{r=0}^{\infty} \partial(y_{n,r} \smile x_{n+r}, y_{n,r} \smile x_{n+r+1})$$
$$< \sum_{r=0}^{\infty} 2^{-n-r} = 2 \cdot 2^{-n} \text{ by (4) of §7.}$$

Dually, define $z_{n,r} = x_n \frown x_{n+1} \frown \cdots \frown x_{n+r}$; then $z_{n,r} \downarrow z_n$, where $\partial(x_n, z_n) \leqq 2 \cdot 2^{-n}$. Moreover $y_n \geqq x_n \geqq z_n$; since $y_n \geqq y_{n,r+1} \geqq y_{n+1,r}$ for all r, $y_n \geqq y_{n+1}$; dually, $z_n \leqq z_{n+1}$. By σ-completeness again, $y_n \downarrow y$ and $z_n \uparrow z$, where

$$\partial(y, z) = \lim_{n\to\infty} \partial(y_n, z_n) \leqq \lim_{n\to\infty} \{\partial(y_n, x_n) + \partial(x_n, z_n)\} = 0,$$

since $\partial(y_n, x_n) + \partial(x_n, z_n) < 4 \cdot 2^{-n}$ for all n. Hence $y = z$, and (ii) $\{x_n\}$ order-converges to y. Further, we have (i) since

$$\partial(x_n, y) = v[x_n \smile y] - v[x_n \frown y] \leqq v[y_n] - v[z_n] < 4 \cdot 2^{-n}.$$

To complete the proof of Thm. 15, we must show that star-convergence implies metric convergence. But since a sequence converges metrically if all its sequences contain metrically convergent subsubsequences, we need only show that order-convergence implies metric convergence. This follows immediately from (8), since if $u_n \downarrow x$ and $w_n \uparrow x$, where $u_n \geqq x_n \geqq w_n$, then $\partial(x_n, x) = v[x_n \smile x] - v[x_n \frown x] \leqq v[u_n] - v[w_n] \downarrow 0$ by (8), completing the proof. Since in any lattice with O and I, conditional completeness implies σ-completeness, we obtain

COROLLARY 1. *In a metric lattice with O and I satisfying* (8), *metric completeness, (order) completeness, and σ-completeness are equivalent.*

See however Cor. 2, Thm. 12, Ch. XI.

THEOREM 16. *Any complete metric lattice is a topological lattice.*

Proof. We appeal to the Lemma of Ch. IV, §9. Suppose $x_\alpha \uparrow x$, and let $s = \sup v[x_\alpha]$. We can select $t_n = x_{\alpha(n)}$ $[n = 1, 2, 3, \cdots]$ with $\alpha(n) \leqq \alpha(n+1)$ and $\partial(t_n, a) < s + 2^{-n}$. Since $\alpha(n) \leqq \alpha(n+1)$, $\partial(t_n, t_{n+1}) < 2^{-n}$; hence $t_n \rightarrow t$ metrically for some t, where $v[t] = s$. We shall now show that $t \geqq x_\alpha$ for all α. Otherwise $v[t \smile x_\alpha] - v[t] > 2^{-n}$ for some n; hence $v[t_m \smile x_\alpha] - s > 2^{-n}$ for some m, n; hence $v[x_\beta] > s + 2^{-n}$ for any common successor of $x_{\alpha(m)} = t_m$ and x_β; this contradicts the definition of s. It follows that $t \geqq x$; but $v[t] = s \leqq v[x]$; hence $t = x$ and $\partial(x_\alpha, x) \downarrow 0$. By (4) of §7, $\partial(a \frown x_\alpha, a \frown x) \downarrow 0$ for all a, from which one easily shows that $a \frown x$, which is evidently an upper bound to the isotone directed set $\{a \frown x_\alpha\}$ is its least upper bound—and hence its limit. Now use duality.

Ex. 1. (a) Show that if (8) holds, then $x_n \uparrow x$ implies $\partial(x_n, x) \downarrow 0$. State the dual proposition.

(b) Show that (8) holds in a metric lattice if and only if order-convergence of sequences implies metric convergence.

Ex. 2. Show that in the proof of Thm. 15, $\partial(y_n, z_n) < 2 \cdot 2^{-n}$.

Ex. 3. (a) Give an example of a metrically complete metric lattice which is not complete.

(b) Show that in a metrically complete metric lattice, a sublattice is metrically bounded if and only if it is order-bounded.

Ex. 4. (a) Show that for isotone directed sets $\{x_\alpha\} \uparrow$, order-convergence and metric convergence are equivalent.

(b*) Is this true for general directed sets?

Problem 30. Decompose any valuation on a metric lattice into "discontinuous" and "continuous" components, and obtain an analog to Thm. 15 for arbitrary metric lattices. Find necessary and sufficient conditions for a metric lattice to be a topological lattice.

10. Jordan's decomposition. Jordan's decomposition of functions of bounded variation into monotone summands was generalized by F. Riesz to additive set-functions.[17] It can be generalized to valuations on lattices.

Consider the valuations $v[x]$ on a lattice L which satisfy $v[a] = 0$ for some fixed a. They evidently form a vector space, since any linear combination of valuations is a valuation. We define

$$v \geqq v_1 \text{ means } v[x] - v_1[x] \text{ is isotone.} \tag{9}$$

Then P1, P3 are obvious, and P2 follows since we require $v[a] - 0$. Further, evidently

$$v \geqq v_1 \text{ implies } v + v_2 \geqq v_1 + v_2 \text{ for all } v_2 . \tag{10}$$

Hence the valuations on L with $v[a] = 0$ form a *partly ordered vector space* in the sense of Ch. XIV.

Next, we identify valuations with *functions of intervals*. If $x \leqq y$, we define $v[x, y] = v[y] - v[x]$. Then V1 simply asserts that perspective and hence *projective intervals have the same values*.

With any chain $\gamma: x = x_0 < x_1 < \cdots < x_n = y$ in $[x, y]$, we associate the *positive variation*

$$v^+[x, y; \gamma] = \sum_{i=1}^{n} \sup \{v[x_{i-1}, x_i], 0\} \tag{11}$$

of $v[x]$ on γ, defined as the sum of the positive increments of $v[x]$ along γ. We define

$$v^+[x, y] = \sup_\gamma v^+[x, y; \gamma] \tag{12}$$

as the positive variation of v on $[x, y]$. Clearly if γ'' is any subdivision of γ, then $v^+[x, y; \gamma''] \geqq v^+[x, y; \gamma]$. Again, if γ' is any chain $x = x_0' < x_1' < \cdots < x_m' = y$ subdividing $[x, y]$, by the Cor. of Thm. 5, γ will have a subdivision γ'' whose subintervals will be projective to corresponding intervals of some subdivision of γ' —hence such that $v^+[x, y; \gamma''] = v^+[x, y; \gamma'] \geqq v^+[x, y; \gamma']$. We infer that

$$v^+[x, y] = \sup_{\gamma''} v^+[x, y; \gamma''] \text{ for refinements } \gamma'' \text{ of } \gamma. \tag{13}$$

By definition (cf. §6), $v[x]$ is of *bounded variation* if and only if every $v^+[x, y]$ and dual $v^-[x, y]$ is finite. We call these the *positive and negative variations* of $v[x]$ on $[x, y]$.

In this case, since projective intervals have corresponding chains and (as remarked above) equal $v^+[x, y; \gamma]$ for corresponding chains, projective intervals have equal $v^+[x, y]$. It follows that

$$v^+[x] = v^+[a, a \smile x] - v^+[a \frown x, a] \tag{14}$$

---

[17] See F. Riesz [1] and Verh. Zurich Congress (1932), vol. I, pp. 258–9. Jordan's construction is given in his *Cours d'Analyse*, vol. 1, p. 54; the phrase Jordan decomposition is due to S. Saks [1, p. 8]. The generalization to valuations was first made in [LT, p. 45].

is a valuation of L. Further, since substitution of x_1 for x expands $[a, a \smile x]$ and contracts $[a \frown x, a]$, $v^+ \geqq 0$; by construction, $v^+ \geqq v$. Conversely, if $v_1 \geqq v, 0$, then for every γ, $v_1[x, y] \geqq v^+[x, y; \gamma]$; hence $v_1[x, y] \geqq v^+[x, y]$, and so $v_1 \geqq v^+$. In summary,

THEOREM 17. *If $v[x]$ is of bounded variation, then $v \smile 0$ exists and is the v^+ defined by* (11)–(13).

It follows that the valuations of bounded variation with $v[a] = 0$ are a *vector lattice* in the sense of Ch. XV. From this many further consequences will be traced.

Ex. 1. Define $v^-[x]$, dual to $v^+[x]$ defined by (10)–(14).

Ex. 2. Show that if $v[x]$ is of bounded variation, then $v^+[x] + v^-[x] = v[x]$ for all x. (Suggestion: Show that $v[x, y; \gamma] = v^+[x, y; \gamma] + v^-[x, y; \gamma]$.)

Ex. 3. Show that if $x[x, y]$ is any function of intervals giving the same value to perspective intervals, then $w[x] = w[a, a \smile x] - w[a \frown x, a]$ is a valuation associated with $w[x, y]$.

Ex. 4*. Generalize Thm. 17 to "valuations" whose values lie in any complete lattice-ordered group.

Ex. 5. Let $f[x]$ be any valuation on a relatively complemented lattice, with $f[0] = 0$. Show that $f[x]$ is of bounded variation if and only if Sup $f[x]$ is finite, and positive if and only if $f[x] \geqq 0$ identically. (See [LT, §86], for details; also Lemma 1, §7, supra.)

CHAPTER VI

APPLICATIONS TO ALGEBRA

1. Normal and permutable congruence relations. A *quasi-group* is a system with a binary multiplication, such that any two of the three terms of $ab = c$ uniquely determine the third. This means that multiplication is single-valued, and that $ax = c$ and $yb = c$ have unique solutions. A *loop* is a quasi-group with a two-sided "identity" 1, satisfying $1x = x1 = x$ for all x. The general theory of quasi-groups and loops may be found elsewhere.[1]

DEFINITION. *A congruence relation θ on a loop G is called normal when*

(1) $$ux \equiv x\ (\theta) \text{ or } xu \equiv x\ (\theta) \textit{ implies } u \equiv 1\ (\theta).$$

THEOREM 1. *All congruence relations on a loop G are normal if either:* (i) *G is a group, or* (ii) $(ux)x^{-1} = u = x^{-1}(xu)$ *for all $u, x \in G$, and some x^{-1}, or* (iii) *G is finite.*

Proof. Case (ii) obviously includes case (i); hence we begin with it.[2] But using (ii), we get $u = (ux)x^{-1} \equiv (1x)x^{-1} = xx^{-1} = 1(\text{mod } \theta)$ and symetrically. Finally, suppose (iii) holds. In any loop, $x \equiv y(\theta)$ implies $xb \equiv yb(\theta)$. Since $x \to xb$ carries distinct elements into distinct elements, the number of elements in the residue class containing xb is at least as great as the number in the residue class containing x. But for any x, y, $xb = y$ has a solution; hence all residue classes have the same cardinal number. If G is finite, this implies (1); otherwise the correspondence $t \to tx$ would introduce new congruence relations.

DEFINITION. *Two congruence relations θ and θ' will be called permutable if and only if*

(2) $$\theta\theta' = \theta'\theta,$$

in the general sense of relation multiplication (Ch. XIII, §5). *In other words, writing $a\theta x$ for $a \equiv x$* (mod θ), *we require that if $a\theta x$ and $x\theta' b$ for some x, then $a\theta' y$ and $y\theta b$ for some y—and conversely.*[3]

[1] Cf. A. Suschkewitch, Trans. Am. Math. Soc. 31 (1929), 204–14; B. A. Hausmann and O. Ore, Am. Jour. 59 (1937), 983–1004; G. N. Garrison, Annals of Math. 41 (1940), 474–87; A. A. Albert, Trans. Am. Math. Soc. 54 (1943), 507–19 and 55 (1944), 401–19; R. H. Bruck, ibid. 55 (1944), 19–52, and 60 (1946), 245–354.

[2] It is also fulfilled by, for example, the elements having inverses in any "alternative ring"; cf. M. Zorn, Abh. Math. Sem. Hamb. 8 (1930), p. 123, and Annals of Math. 42 (1941), 676–86.

[3] The importance of permutable equivalence relations was first stressed by P. Dubreil and M. L. Dubreil-Jacotin in 1939; see P. Dubreil, *Algèbre*, Paris, 1946, p. 21. See also O. Ore, Duke Jour. 9 (1942), 573–627, esp. pp. 590–91; also Ch. VII, §5, below, and O. Boruvka, *On decompositions of sets*, Rozpravy II, Tridy Ceske Akad. 53 (1943), No. 23.

THEOREM 2. *A normal congruence relation on a loop is permutable with any congruence relation.*

Proof. Suppose that $a\theta x$ and $x\theta' b$; set $a = ux$, $b = xv$, and $y = u(xv) = ub$. Since $x\theta' b$, $y = ub \equiv ux = a(\theta')$. Again, since $ux = a \equiv x = 1x(\theta)$, and θ is normal, $u \equiv 1(\theta)$ and so $y = ub \equiv 1b = b(\theta)$. This proves that $\theta\theta' \leqq \theta'\theta$; to prove the converse, we simply reverse the order of multiplication.

An extension of Thm. 2 to quasi-groups has been obtained by F. Kiokemeister, Am. Jour. 70 (1948), 99-106.

COROLLARY. *In any group (with or without operators), or in any loop satisfying* (ii) *or* (iii), *all congruence relations are permutable.*

For if we adjoin new operations to an algebra, then the lattice of congruence relations becomes smaller. (For a stronger result, see Ch. II, Thm. 4.) Hence if (1) holds for a group (or other loop) G, it holds for the same group as a group with operators.

Ex. 1. (a) Show that the ordinal 4 is a lattice whose congruence relations are not permutable.

(b) Give a short proof, from first principles, that the congruence relations on any group are permutable. (Hint: set $y = ax^{-1}b$.)

Ex. 2*. Show that any system with an associative multiplication, in which $xa = b$ and $ay = b$ have solutions x, y for any given a, b, is a group.[4]

Ex. 3*. Prove (or disprove) the conjecture that the congruence relations on any relatively complemented lattice are permutable.

Ex. 4. Show that any two congruence relations on a loop are permutable if $(ux)x^{-1} = u$ for all x, u (i.e., it is not necessary to assume $x^{-1}(xu) = u$).

Ex. 5. Can a quasi-group be defined as an algebra with three binary operations ab, $a * b$, and $a \circ b$, satisfying $a(a * b) = b$ and $(a \circ b)b = b$? What about ternary operations $a(b * c)$ and $(a \circ b)c$?

Ex. 6. Show that there exist homomorphisms of loops on multiplicative systems, in which the latter are not loops or even quasi-groups. (Kiokemeister and Bates)

Problem 31. Is there any quasi-group whose congruence relations are not permutable? Can such a quasi-group be a loop or be finite?

Problem 32. In the proof of (2), is it sufficient to assume that $ux \equiv x\,(\theta)$ implies $u \equiv 1\,(\theta)$?

2. Direct decompositions. We shall now derive two fundamental properties of algebras with permutable congruence relations.

THEOREM 3. *The congruence relations on any algebra with permutable congruence relations form a modular lattice, in which $\theta \smile \theta' = \theta\theta' = \theta'\theta$.*

Proof. Since $a \equiv b\ (\theta \smile \theta')$ means (Ch. II, Thm. 4) that for some finite chain, $a = x_0\theta x_1\theta' x_2\theta x_3\theta' \cdots x_n = b$, it is clear that $\theta \smile \theta'$ is the union of the finite products $\theta\theta'\theta\theta' \cdots$. But by (1) and $\theta^2 = \theta$, $\theta'^2 = \theta'$, this is simply $\theta\theta' = \theta'\theta$; hence $\theta \smile \theta' = \theta\theta' = \theta'\theta$, by induction.

Using the one-sided modular law (Ch. II, formula (4)), it therefore remains to prove that if $\theta_1 \geqq \theta_2$, then $\theta_1 \frown (\theta\theta_2) \leqq (\theta_1 \frown \theta)\theta_2$. But suppose $a \equiv b\ (\theta_1)$ and $a \equiv b\ (\theta\theta_2)$—i.e., $a \equiv b\ (\theta_1 \frown (\theta\theta_2))$. Then for some x, $a \equiv x\ (\theta)$ and

[4] This result is due to E. V. Huntington, Trans. Am. Math. Soc. 6 (1905), 181-197; it shows that any associative quasi-group is a group.

$x \equiv b\,(\theta_2)$. But $\theta_1 \geqq \theta_2$; hence $x \equiv b\,(\theta_1)$. Since also $a \equiv b\,(\theta_1)$ and θ_1 is transitive, we infer $x \equiv a\,(\theta_1)$; hence $x \equiv a\,(\theta \frown \theta_1)$. We now get immediately $a \equiv b\,((\theta_1 \frown \theta)\theta_2)$, since $x \equiv b\,(\theta_2)$.

LEMMA. *Let θ_1, θ_2 be any permutable congruence relations on an algebra A, such that $\theta_1 \frown \theta_2 = O$, $\theta_1 \smile \theta_2 = I$. Then A is isomorphic with the direct union $A_1 \times A_2$, where A_i is the homomorphic image of A mod θ_i ($i = 1, 2$).*

Proof. For elements $x, y, \cdots$ of A, and $i = 1, 2$, let $x_i, y_i, \cdots$ denote the residue class of A mod θ_i containing $x, y, \cdots$, respectively. Then clearly the correspondence $x \to (x_1, x_2)$ is a homomorphism of A onto a subalgebra S of $A_1 \times A_2$. Since $\theta_1 \frown \theta_2 = 0$, $x_1 = y_1$ and $x_2 = y_2$ implies $(x_1, x_2) = (y_1, y_2)$; that is, the homomorphism is an isomorphism. Since $\theta_1\theta_2 = \theta_1 \smile \theta_2 = I$, there exists for any (x_1, x_2) and (y_1, y_2) a (z_1, z_2) such that $(x_1, x_2) \equiv (z_1, z_2)\,(\theta_1)$ and $(z_1, z_2) \equiv (y_1, y_2)\,(\theta_2)$—i.e., such that $x_1 = z_1$ and $z_2 = y_2$. This means that (x_1, y_2) is an element of S for any x_1 and y_2; hence $S = A_1 \times A_2$, completing the proof.

THEOREM 4. *The representations of an algebra A as a direct union $A = A_1 \times \cdots \times A_r$ correspond one-one with the sets of permutable congruence relations $\theta_1, \cdots, \theta_r$ on A satisfying*

$$(3) \qquad \theta_1 \frown \cdots \frown \theta_r = O, \textit{ and } (\theta_1 \frown \cdots \frown \theta_{i-1}) \smile \theta_i = I \qquad [i = 2, \cdots, r].$$

Remark. These are simply dually independent elements whose meet is O.

Proof. Suppose $A = A_1 \times \cdots \times A_r$; let $x \equiv y\,(\theta_i)$ mean that $x = [x_1, \cdots, x_r]$ and $y = [y_1, \cdots, y_r]$ have the same i-component $x_i = y_i$. Then (3) is obvious. Conversely, suppose (3) holds. Then by the lemma, $A = B_r \times A_r$, where B_r is A mod $\theta_1 \frown \cdots \frown \theta_r$. By induction on r, $B_r = A_1 \times \cdots \times A_{r-1}$, completing the proof.

Ex. 1. Show that Thm. 3 is not true of systems with infinitary operations—e.g., that it is not true of all topological Abelian groups, even though they satisfy (1).

Ex. 2. Show that if an algebra satisfies (1), then so do all its homomorphic images.

Ex. 3. Show that if an algebra has only unary operations, then it satisfies (2) if and only if it has three or fewer congruence relations.

3. Jordan-Hölder Theorem. To obtain the Jordan-Hölder Theorem in its various forms, we require not only that the congruence relations on an algebra be permutable but also that the algebra contain a one-element subalgebra.

DEFINITION. *Let A be an algebra with a selected one-element subalgebra 1, all of whose congruence relations $\theta, \theta', \cdots$ are permutable. For any θ, we define $S(\theta)$ as the subalgebra of $x \equiv 1\,(\theta)$ in A. If $\theta \geqq \theta'$, we define the quotient-symbol θ/θ' to denote the homomorphic image of $S(\theta)$ mod θ'.*

THEOREM 5. *Under the preceding hypotheses on A, we have for all θ_1, θ_2,*

$$(4) \qquad (\theta_1 \smile \theta_2)/\theta_2 \textit{ and } \theta_1/(\theta_1 \frown \theta_2) \textit{ are isomorphic.}$$

Remark. This generalizes what is often called the First Isomorphism Theorem (e.g., in van der Waerden [1, p. 136]).

Proof. By the Second Isomorphism Theorem (cf. Ex. 2 of the Foreword on Algebra), we can identify elements congruent mod $\theta_1 \frown \theta_2$; hence we can assume $\theta_1 \frown \theta_2 = O$ without loss of generality. Again, no elements are concerned in (4) except those of $S(\theta_1 \smile \theta_2)$; in this, $\theta \smile \theta' = I$. We thus reduce to the case of the lemma of §2. In this case, $S(\theta_1 \smile \theta_2)$ mod θ_2 is isomorphic with A_2; $S(\theta_1)$ consists of the elements $[1, a_2]$, which is isomorphic with A_2, completing the proof.

Corollary. *Let A be any algebra with a one-element subalgebra* 1 *and permutable congruence relations. Then projective intervals* $[\theta', \theta]$ *in the (modular) lattice of congruence relations on A determine isomorphic quotient-symbols.*

The proof is immediate, if we recall the definition of projectivity and Thm. 3 above.

Now let us refer to the proof of Thm. 3, Ch. V, with especial reference to Fig. 3b. Let us strengthen $P(m)$ to the assertion $Q(m)$: if $a = x_0 < x_1 < \cdots < x_m = b$ and $a = y_0 < y_1 < \cdots < y_m = b$ are any two maximal chains, then there is a one–one correspondence between the $[x_{i-1}, x_i]$ and $[y_{i-1}, y_i]$, such that corresponding intervals are projective. Since $[x_1, u]$ and $[a, y_1]$, and $[a, x_1]$ and $[y_1, u]$ are projective, we can prove $Q(m)$ from $Q(m - 1)$, just as before we proved $P(m)$ from $P(m - 1)$. In the light of the preceding corollary, $Q(m)$ however implies the following generalized[5] Jordan-Hölder Theorem for *principal* series.

Theorem 6. *Let* $O = \theta_0 < \theta_1 < \cdots < \theta_m = I$ *and* $O = \theta_0' < \theta_1' < \cdots < \theta_n' = I$ *be any two finite maximal chains of congruence relations on an algebra A with a one-element subalgebra whose congruence relations are permutable. Then the* $m = n$ *and the* θ_i/θ_{i-1} *are pairwise isomorphic with the* θ_j'/θ_{j-1}'.

The same argument yields the Jordan-Hölder Theorem for *composition* series. In this, θ_{i-1} is supposed to be a maximal congruence relation on the subalgebra $S(\theta_i)$. For the proof to go through, we must require that the congruence relations on the $S(\theta_i)$ be permutable, as well as those on A. Since the classes of

[5] There is an enormous literature on this result. The original result was due to C. Jordan, *Commentaire sur Galois*, Math. Annalen 1 (1869), 141–160 (with numerical interpretation) and O. Hölder, *Zuruckführung einer beliebigen Gleichung* $\cdots$, ibid. 34 (1889), 26–56. The extension to groups with operators was due to E. Noether and W. Krull. The lattice-theoretic proof for groups was indicated by Dedekind [2], and made explicit by the author [1, Thm. 26.1, 27.1]. The generalization to quasi-groups was suggested by B. A. Hausmann and O. Ore, and by Albert (op. cit. in §1); by D. Rees, Proc. Camb. Phil. Soc. 36 (1940), 387–400; and by D. C. Murdoch, Bull. Am. Math. Soc. 47 (1941), 134–38; the lattice-theoretic formulation is due to M. F. Smiley, Bull. Am. Math. Soc. 50 (1944), 782–785. The present formulation is new.

algebras discussed in Theorem 1 are closed under subalgebras and homomorphic image, this is true of them, and we have[6]

COROLLARY 1. *If A is a group (with or without operators), or a loop satisfying one of the conditions of Thm. 1, then the quotient-groups occurring in any two finite composition series are pairwise isomorphic.*

In connection with this specialization to loops, it should be observed that in Thm. 6, no claim is made either that $S(\theta)$ uniquely determines θ (i.e., that a congruence relation is determined by the subalgebra of elements congruent to 1), or that $S(\theta_1 \smile \theta_2)$ is the least upper bound of $S(\theta_1)$ and $S(\theta_2)$ in the lattice of subalgebras of A. These facts are however true in loops, where the $S(\theta)$ are the so-called *normal subloops*; hence they are true in groups.[7]

Two kinds of generalization of the Jordan-Hölder Thm. to algebras without chain conditions have been made. The first is due to Schreier and Zassenhaus,[8] and is a corollary of Thm. 6, Ch. V.

COROLLARY 2. *Let $O = \theta_0 < \theta_1 < \cdots < \theta_m = I$ and $O = \theta_0' < \theta_1' < \cdots < \theta_n' = I$ be any two finite chains of congruence relations on A. Then these chains can be refined by interpolation of terms $\theta_{i,j} = \theta_{i-1} \smile (\theta_j' \frown \theta_i)$ and $\theta_{i,j}' = \theta_{j-1}' \smile (\theta_i \frown \theta_j)$ so that corresponding quotients $\theta_{i,j}/\theta_{i,j-1}$ and $\theta_{i,j}'/\theta_{i-1,j}'$ are isomorphic.*

In fact, without reference to induction, we can show directly that both $\theta_{i,j}/\theta_{i,j-1}$ and $\theta_{i,j}'/\theta_{i-1,j}'$ are perspective to $(\theta_i \smile \theta_{j-1}') \frown (\theta_{i-1} \smile \theta_j')/\theta_{i-1} \smile \theta_{j-1}'$. This proof yields Thm. 6 as a corollary.

Finally, one can use transfinite induction[9] to show that Thm. 6 holds also for *ascending* maximal transfinite sequences of congruence relations on algebras having a one-element subalgebra and permutable congruence relations, but not for descending sequences.

Ex. 1. Show that Thm. 6 and its corollaries apply to loops with operators.

Ex. 2. Show that every loop has a unique one-element subalgebra.

Ex. 3. Show that if 1 is a one-element subalgebra of any algebra A, and θ is any congruence relation on A, then the $x \equiv 1\ (\theta)$ form a subalgebra of A.

---

[6] The Jordan-Hölder Thm. for composition series has been discussed at length. See O. Ore, Trans. Am. Math. Soc. 41 (1937), 266–275; A. J. Uzkow, Mat. Sbornik 46 (1938), 31–43; E. George, Crelle's Jour. 180 (1939), 110–120; A. G. Kurosh, Math. Revs. 2 (1941), p. 343, and Mat. Sbornik 16 (1945), 59–72; O. Ore, Bull. Am. Math. Soc. 49 (1943), 558–566; R. J. Duffin and R. S. Pate, Duke Math. Jour. 10 (1943), 743–50; P. Lorenzen, Math. Zeits. 49 (1944), 647–653; M. Chatelet, Revue Sci. Ill. 85 (1947), 579–96; R. Croisot, Comptes Rendus 226 (1948), 767–8.

[7] For other pitfalls involved in attempts at too extreme generalization, cf. G. N. Garrison, Annals of Math. 47 (1946), 50–55.

[8] O. Schreier, Abh. Hamb. 6 (1928), 300–302; H. Zassenhaus, ibid. 10 (1934), 106–108. The lattice-theoretic formulation was given in [LT, p. 51]; a postulational study has been made by V. Korinek; see also R. Baer, Am. Jour. 67 (1945), 450–460.

[9] This result is due to A. Kurosh, Math. Annalen 111 (1935), 13–18, and the author, Bull. Am. Math. Soc. 40 (1934), 847–850. The non-duality is due to the fact that if $\theta_\alpha \uparrow \tau\theta$, then $\alpha \frown \theta_\alpha \uparrow \alpha \frown \theta$, whereas the dual of this need not hold.

Ex. 4. Formulate Thm. 6 as a theorem (a) on the left-ideals of rings, (b) in representation theory, (c) on the invariant subalgebras of a hypercomplex algebra.

Ex. 5. (a) Show that the additive group of dyadic fractions $m/2^n$ contains no well-ordered increasing maximal chain of normal subgroups.

(b) State a Jordan-Hölder Theorem for this group.

Problem 33. Let A be an algebra with a one-element subalgebra and permutable congruence relations. Can A have distinct congruence relations $\theta \neq \theta'$ such that $S(\theta) = S(\theta')$?

4. Groups with operators. An endomorphism of a group or loop G is usually called an *operator*. A *group with operators* (or loop with operators) is thus the system (G, Ω) consisting of a group (or loop) G, and a set Ω of endomorphisms of (operators on) G, which are regarded as unary operations of the algebra (G, Ω). A Ω-homomorphism of (G, Ω) into (H, Ω) is thus a single-valued correspondence $\alpha: x \to \alpha(x)$ of G into H, such that

$$\alpha(x\omega) = [\alpha(x)]\omega \text{ for all } \omega \in \Omega. \tag{5}$$

If α is one-one, it is an Ω-*isomorphism*.

The results of §3 apply to any group with operators, and to any loop with operators provided the number of elements is finite or $x^{-1}(xu) = (ux)x^{-1} = u$ for all x, u. For under these hypotheses, as remarked in §1, all Ω-congruence relations (being congruence relations) are permutable. Further, since $ax = a$ has 1 for its only solution, and $1\omega = (11)\omega = (1\omega)(1\omega)$ by (5), $1\omega = 1$ for all ω. Hence any group or loop with operators has a one-element subalgebra. It follows that the Jordan-Hölder Theorem applies also to groups with operators, corresponding quotients even being Ω-isomorphic instead of merely isomorphic.

Using the concept of operator, one can sharpen the Jordan-Hölder Theorem and its corollaries for groups *without* operators. Indeed, every congruence relation on a group is also a congruence relation for all "inner automorphism" operators $x \to a^{-1}xa$. Hence the isomorphisms referred to in the Jordan-Hölder Theorem are preserved under all inner automorphisms. Such isomorphisms α are called "central isomorphisms" in group theory. They satisfy

$$a^{-1}\alpha(x)a = \alpha(a^{-1}xa) = \alpha(a)^{-1}\alpha(x)\alpha(a) \quad \text{for all} \quad a, x,$$

whence $\alpha(a)a^{-1}$ is permutable with all $\alpha(x)$, and $\alpha(a) = az$, where z is in the center.

This can be generalized to loops with operators, as follows. By the Substitution Property, any congruence relation on a loop G is also a congruence relation for the unary operations $x \to a(xb)$ and $x \to (ax)b$. If $b = a^{-1}$, then 1 is a one-element subalgebra, though of course $x \to a(xa^{-1})$ need not be an isomorphism. *If* G satisfies the hypotheses of Thm. 1, then all congruence relations are permutable. Hence if we define a "central isomorphism" between two quotient-loops of the same loop with operators to be one preserved under all correspondences $x \to a(xa^{-1})$ and $x \to (a^{-1}x)a$, then

THEOREM 7. *In the Jordan-Hölder Theorem for loops, corresponding quotients are centrally isomorphic, provided inverses exist.*

Ex. 1. An Ω-subgroup of a group with operators is defined as a normal subgroup N such that $N\omega \leqq N$ for all operators ω. Show that the congruence relations on a group with operators correspond to its Ω-subgroups.

Ex. 2. Show that for a group with operators, and suitable Ω-subgroups M, N, $(Mx\omega) \frown N > (Mx \frown N)\omega$ is possible.

Ex. 3. Generalize Ex. 1 to loops with operators, which are finite or satisfy $(ux)x^{-1} = u = x^{-1}(xu)$.

5. Six-way operator-isomorphism. Let x_1, x_2, x_3 be any three congruence relations on an algebra A with a one-element subalgebra and permutable congruence relations. If we refer to Fig. 4, Ch. V, we will find that

$$(6)\qquad e_1 \frown e_2 = e_2 \frown e_3 = e_3 \frown e_1 = d, \qquad e_1 \smile e_2 = e_2 \smile e_3 = e_3 \smile e_1 = c.$$

Hence e_1/d and e_3/d are both perspective to c/e_2, and so, by the Cor. of Thm. 5, they are isomorphic. Similarly, e_1/d and e_2/d are isomorphic, and by Thm. 3, c/d is the direct union of any two of these. We conclude[10]

THEOREM 8. *Let θ_1, θ_2, θ_3 be congruence relations on an algebra A with a one-element subalgebra and permutable congruence relations. Further, let $\alpha_1 = (\theta_2 \smile \theta_3) \frown [\theta_1 \smile (\theta_2 \frown \theta_3)]$ and cyclically, let $\beta = (\theta_1 \frown \theta_2) \smile (\theta_2 \frown \theta_3) \smile (\theta_3 \frown \theta_1)$, and let γ be dual to β. Then the six quotients α_i/β and γ/α_i are isomorphic, and γ/β is the direct union of any two of them.*

We now observe that in the case of groups, or of loops satisfying the second sufficient condition $(ux)x^{-1} = u = x^{-1}(xu)$ of Thm. 1, we have central isomorphism by Thm. 7. But for any $[a, 1]$ of α_1/β and $[1, y]$ of α_3/β in $(\gamma/\beta) = (\alpha_1/\beta) \times (\alpha_3/\beta)$, clearly

$$([a, 1]^{-1}[1, y])[a, 1] = [(a^{-1}x)a, 1^{-1}y1] = [1, y].$$

By central isomorphism $[(a^{-1}x)a, 1^{-1}1] = [x, 1]$ for the element $[x, 1]$ of α_i/β corresponding to $[1, y]$ in α_3/β. But every $[x, 1]$ corresponds to some $[1, y]$; hence $(a^{-1}x)a = x$ for all x, a. Right multiplying by a^{-1}, we get $a^{-1}x = xa^{-1}$. We conclude the

COROLLARY. *If A is a group, or loop in which $(ux)x^{-1} = u = x^{-1}(xu)$ for all x, u, then the α_i/β of Thm. 8 are commutative.*

Ex. 1. Show that if A is a ring or hypercomplex algebra in Thm. 8, then $xy = 0$ for all $x, y \in \gamma/\beta$. Is this true for non-associative rings?

6. Subdirect unions. Let S be any subalgebra of a finite direct union $A_1 \times \cdots \times A_r$ of abstract algebras A_i. Then S is a subalgebra of the direct union $S_1 \times \cdots \times S_r$ of the subalgebras S_i of elements of A_i appearing as i-components of elements of S. We shall say that S is a *subdirect union* of the S_i.

[10] Historical note: For the isomorphism of e_1/d and e_3/d, see C. Jordan, *Traite des substitutions*, p. 42, and O. Bolza, Am. Jour. 11 (1889), 195–214. Dedekind [2, p. 248, formula (31)], gave the lattice-theoretic projectivities involved. R. Remak, Jour. fur Math. 162 (1930), 1–16, showed that the groups were commutative. The author [1, p. 462], and [2, p. 119], got Remak's result lattice-theoretically; cf. also Ore, Duke Jour. 3 (1937), p. 174.

The correspondence from each element $a = [a_1, \cdots, a_r]$ of S to its i-component a_i is clearly a homomorphism $\theta_i : S \to S_i$. Moreover if θ_i is regarded as a congruence relation on S, then two elements are congruent modulo every θ_i if and only if they are identical, component by component. Hence

$$\bigwedge \theta_i = \theta_1 \frown \cdots \frown \theta_r = O.$$

Conversely, let $\theta_1, \cdots, \theta_r$ be congruence relations on an abstract algebra S. If we define the residue class mod θ_i which contains any $a \in S$ as the i-component a_i of a, then the correspondence $a \to [a_1, \cdots, a_r]$ is a homomorphism of S onto a subalgebra of the direct union $S_1 \times \cdots \times S_r$ of the algebras S_i of residue classes of S mod θ_i. Moreover every element of S_i is an i-component of some $a \in S$. Finally, the homomorphism $a \to [a_1, \cdots, a_r]$ is an isomorphism if and only if $\bigwedge \theta_i = O$.

Using a somewhat more elaborate notation, the same proof applies to subdirect unions having an infinite number of factors (cf. Thm. 4, Ch. II). Hence

THEOREM 9. *The representations of an abstract algebra A as a subdirect union correspond one–one to the sets of congruence relations on A satisfying $\bigwedge \theta_i = 0$.*

Now for any $a \neq b$, consider the partly ordered set $C(a, b)$ of all congruence relations θ on A, such that $a \not\equiv b \pmod{\theta}$. If T is any subchain of $C(a, b)$, we define the union τ of the $\theta \in T$ by the rule $x \equiv y\ (\tau)$ means $x \equiv y\ (\theta)$ for some $\theta \in T$. It is evident that $a \not\equiv b\ (\tau)$, and that (since A has finitary operations) τ is a congruence relation—cf. Thm. 4, Ch. II. Hence in $C(a, b)$, every subchain has an upper bound τ. Using (AC2) of Ch. III, §6, we infer that $C(a, b)$ has a *maximal* element σ.

We next consider H, the homomorphic image of A, mod σ. If ϕ is any congruence relation on H, then $a \equiv b\ (\phi)$, for otherwise σ could not be maximal. Hence the least congruence relation on H making $a \equiv b\ (\theta)$, is[11] a congruence relation ϕ_0 contained in every other congruence relation except 0. Hence if no $\phi_i = O$, $\bigwedge \phi_i \geqq \phi_0 > O$, and we conclude

THEOREM 10. *Every algebra A can be represented as a subdirect union of subdirectly irreducible algebras.*[12]

For the meet of the σ is O, since given $a \neq b$, $a \not\equiv b\ (\sigma)$ for some σ. And each $H = H(\sigma)$ is irreducible in the strong sense that in any isomorphic representation of H as a subdirect union, some one factor is isomorphic with H.

Ex. 1. Develop notation suitable for proving Thm. 9 in the case of infinitely many factors.

Ex. 2. Show that in Thm. 9, for algebras with permutable congruence relations, one gets a direct union if and only if $(\theta_1 \frown \cdots \frown \theta_{k-1}) \smile \theta_k = I$ for $k = 2, \cdots, r$—in case r is finite.

---

[11] We recall that being reflexive, symmetric, transitive, and enjoying the Substitution Property are all extensionally attainable (i.e., closure) properties—hence so is being a congruence relation, and ϕ_0 exists.

[12] This result is due to the author, Bull. Am. Math. Soc. 50 (1944), 764–768. Subdirect unions were first considered in the case of groups, by R. Remak, op. cit. in §5.

Ex. 3*. Show that Thm. 9, but not Thm. 10, is also valid for topological algebras, with infinitary operations. (Hint: try topological spaces.)

7. Kurosh-Ore Theorem. Theorem 9 makes one interested in the representations of an element (namely, O) of a modular lattice as a meet of larger elements. Ideal theory also involves such representations.[13]

Now we shall call an element a of a modular lattice L "meet-reducible" (for short, "reducible") if it is the meet $x \frown y$ of elements $x > a, y > a$ greater than itself; otherwise we shall call it "irreducible." A simple inductive argument shows that if L satisfies the ascending chain condition, then every $a \in L$ has a representation as a meet of irreducible elements. For in this case, we can assume by the generalized induction principle that every $x, y > a$ has such a representation.

Again, it is natural to call a component x_k in a "reduction" $a = x_1 \frown \cdots \frown x_r$ of a "redundant," if $a = x_1 \frown \cdots \frown x_{k-1} \frown x_{k+1} \frown \cdots \frown x_r$—and it is obvious that to any reduction of a there corresponds one, none of whose components is redundant. Such reductions will be called "irredundant."

LEMMA. *Let $a = x_1 \frown \cdots \frown x_r = x_1^* \frown \cdots \frown x_s^*$ be any two irredundant reductions of a into irreducible components. Then one can substitute for any x_i a suitable x_j^*, and get a new reduction of a.*

Proof. Set $y_i = x_1 \frown \cdots \frown x_{i-1} \frown x_{i+1} \frown \cdots \frown x_r$. Then by irredundancy, $y_i > a$, yet $x_i \frown y_i = a$. Now form $z_j = y_i \frown x_j^*$; clearly $y_i \geqq z_j \geqq a$—and, since $z_j \leqq x_j^*$, $a \leqq z_1 \frown \cdots \frown z_s \leqq x_1^* \frown \cdots \frown x_s^* \leqq a$. But by Thm. 6, Ch. V, the sublattice between $a = x_i \frown y_i$ and y_i is isomorphic to the sublattice between x_i and $x_i \smile y_i$—and since x_i is irreducible in the latter, so is a in the former. Hence some z_j is a, and $x_1 \frown \cdots \frown x_{i-1} \frown x_j^* \frown x_{i+1} \frown \cdots \frown x_r = a$.

THEOREM 11.[14] *The number of components in irredundant reductions of any element is independent of the reduction: in the preceding lemma, $r = s$.*

Proof. Choose r minimal, and replace the x_i by x_j^* one at a time. We get in the end $a = x_{j(1)}^* \frown \cdots \frown x_{j(r)}^*$, whence by the irredundancy of the x_j^* there are at least s $j(i)$, and $s \leqq r$. Hence by minimality, $s = r$.

COROLLARY. *Let A be any algebra whose congruence relations are permutable and satisfy the ascending chain condition. The number of factors in any irredundant representation of A as a subdirect union of subdirectly irreducible algebras is the same for all such representations.*

Proof. That any irredundant representation is finite, and the existence of such representations, follow from the ascending chain condition and Thm. 9.

[13] Partly because any "irreducible" ideal is "primary" in the sense of containing a power of a "prime" ideal. Cf. van der Waerden [1, Ch. XII].

[14] Historical note. Thm. 11 was proved for ideals by Emmy Noether, Math. Annalen 83 (1921), 24–66, §3. A different proof was given by R. Remak, Crelle's Jour. 163 (1930), 1–44. The first lattice-theoretic proof was given by A. Kurosh [1]; O. Ore [2], p. 270 gave a proof independently. The results of Exs. 3–4 below are due to R. P. Dilworth, Bull. Am. Math. Soc. 52 (1946), 659–663 and refs. given there.

The proof is completed by appeal to Thms. 11 and 2. By Thm. 1, the result holds for groups with operators, and for finite loops and loops satisfying $x^{-1}(xu) = (ux)x^{-1} = u$.

Ex. 1. Show that in the proof of the lemma, the y_i are in fact independent over a.

Ex. 2. Prove in detail that in any lattice satisfying the ascending chain condition, every element can be expressed as the meet of a finite number of meet-irreducible elements.

Ex. 3*. Show that in the lemma of §7, we can renumber the x_j^* so that every x_i^* can be substituted for x_i.

Ex. 4*. (a) Show that in the lemma, for each x_i, an x_j^* exists which can be substituted for x_i and such that x_i can also be substituted for x_j^*.

(b) Show that in one case, no renumbering can be found such that, for all i, x_i^* can be substituted for x_i and vice-versa.

8. Theorem of Ore. An even more important theorem, due to Ore,[15] is the following. Let us call an element e of a modular lattice a *direct join* of elements $a_1, \cdots, a_n$ (in symbols, $e = a_1 \times \cdots \times a_n$) when the a_i are independent and have the join e.

THEOREM 12. *Let L be any modular lattice of finite length. If I has two representations $a_1 \times \cdots \times a_m$ and $b_1 \times \cdots \times b_n$ as a direct join of indecomposable elements, then $m = n$ and the a_i and b_j are projective in pairs.*

Proof. Let $\bar{a}_i = a_1 \times \cdots \times a_{i-1} \times a_{i+1} \times \cdots \times a_m$ and $\bar{b}_j = b_1 \times \cdots \times b_{j-1} \times b_{j+1} \times \cdots \times b_n$; then $I = a_i \times \bar{a}_i = b_j \times \bar{b}_j$ for all i, j. If $I = b_j \times \bar{a}_i$ for some i, j we shall say that a_i is *replaceable* by b_j. We shall show that every a_i is replaceable by some b_j; without loss of generality, we assume $i = 1$.

Case I. If $a_1 \smile \bar{b}_j = \bar{a}_1 \smile b_j = I$ for some j, then by dimension

$$d[a_1] = d[I] - d[\bar{b}_j] + d[a_1 \frown b_j] = d[b_j] + d[a_1 \frown \bar{b}_j] \geqq d[b_j].$$

Similarly, $d[b_j] \geqq d[a_1]$, proving $d[a_1] = d[b_j]$, whence $d[a_1 \frown \bar{b}_j] = d[\bar{a}_1 \frown b_j] = 0$. We conclude $a_1 \frown \bar{b}_j = \bar{a}_1 \frown b_j = O$, and so a_1 and b_j are *mutually* replaceable.

Case II. Suppose $a_1 \smile \bar{b}_j < I$ for some j, say $j = 1$. Let q_h denote $(a_1 \smile \bar{b}_h) \frown b_h$. Since $a_1 \smile \bar{b}_1 \geqq b_1$ would imply $a_1 \smile \bar{b}_1 \geqq b_1 \smile \bar{b}_1 = I$, contrary to hypothesis, clearly $q_1 = (a_1 \smile \bar{b}_1) \frown b_1 < b_1$. Moreover since the b_h are independent and $q_h \leqq b_h$, $c = \bigvee_{h=1}^{n} q_h$ is the *direct* join of the q_h, and so $d[c] = \sum d[q_h] < \sum d[b_h] = d[I]$, whence $c < I$.

[15] Historical note. The analogous result for general finite groups was first given by J. H. M. Wedderburn, Annals of Math. 10 (1909), p. 173; the case of Abelian groups being due to L. Kronecker (Berl. Sitz. (1870), 881–889). A gap in Wedderburn's proof was filled by R. Remak, Crelle's Jour. 139 (1911), p. 293. Later papers by O. Schmidt; Krull, Math. Zeits. 23 (1925), 161–196; H. Fitting, ibid. 39 (1935), 16–40; and Korinek, Cas. Pest. mat. a fys. 66 (1937), 261–286, had extended the theorem to groups with operators. O. Ore made the proof purely lattice-theoretic [2, p. 272], thus paving the way for further generalizations—See also O. Ore, Duke Jour. 2 (1936), 581–596, and A. Kurosh, Izv. Akad. Nauk SSSR 7 (1943), 185–202, and 10 (1946), 47–72. The present new formulation was announced at the Princeton Bicentennial Conference (1946), with Theorems 3, 4, 6, 8.

Again, we get by induction on n, writing $a_1 \smile \bar{b}_h = d_h$,

$$
(7)\qquad
\begin{aligned}
c = \bigvee_{h=1}^{n} q_h &= (b_1 \frown d_1) \smile \left[\bigvee_{k=2}^{n} b_k \frown \bigwedge_{k=2}^{n} d_k\right] \\
&= d_1 \frown \left(b_1 \smile \left[\bigvee_{k=2}^{n} b_k \frown \bigwedge_{k=2}^{n} d_k\right]\right) && \text{by L5} \\
&= d_1 \frown \left(\bigvee_{k=1}^{n} b_k\right) \frown \bigwedge_{k=2}^{n} d_k && \text{by L5, since } \bigwedge_{k\neq 1} d_k \geqq b_1 \\
&= d_1 \frown I \frown \bigwedge_{k=2}^{n} d_k = \bigwedge_{k=1}^{n} (a_1 \smile \bar{b}_k) \geqq a_1 .
\end{aligned}
$$

Therefore $(c \frown \bar{a}_1) \smile a_1 = c \frown (\bar{a}_1 \smile a_1) = c$ by L5, and $c \frown \bar{a}_1 \frown a_1 = O$, whence $c = a_1 \times (c \frown \bar{a}_1)$.

It follows by induction on length that a_1 can be replaced by some factor $e_{h1} > 0$ of some q_h, in any representation of $c = q_1 \times \cdots \times q_n = a_1 \times (c \frown \bar{a}_1)$ as a direct join of indecomposable factors e_{hk} of the q_h; write $e = e_{h1}$ for short. Then $c = e \times (c \frown \bar{a}_1)$ by definition, whence

$$
\begin{aligned}
e \smile \bar{a}_1 &= e \smile (c \frown \bar{a}_1) \smile \bar{a}_1 \text{ (by L4)} \\
&= a \smile (c \frown \bar{a}_1) \smile \bar{a}_1 = c \smile \bar{a}_1 = I, \text{ by (7)}.
\end{aligned}
$$

But $d[e] = d[a_1]$, by replaceability in $c = a_1 \times (c \frown \bar{a}_1)$; hence $e \frown \bar{a}_1 = O$ and $I = e \times a_1$. Moreover $e = b_h$. For $e \frown (b_h \smile \bar{a}_1) \leqq e \frown \bar{a}_1 = O$, and by L5

$$e \smile (b_h \frown \bar{a}_1) = (e \smile \bar{a}_1) \frown b_h = I \frown b_h = b_h ,$$

whence e is a direct factor of $b_h = e \times (b_h \frown \bar{a}_h)$. But by hypothesis, b_h is indecomposable; hence $e = b_h$ and $I = b_h \times \bar{a}_h$. Hence a_1 is replaceable by b_h, where $h \neq 1$.

Case III. Suppose $a_1 \smile \bar{b}_j = I$ for all j, yet $\bar{a}_1 \smile b_j < I$ for all j—the only remaining possibility. Then, as in Case II, but with the roles of a_1 and b_1 interchanged, b_1 can be replaced by some $a_k \neq a_1$, say a_m (renumbering subscripts). Then $x \to (x \smile a_m) \frown \bar{a}_m$ is a perspectivity of $[O, \bar{b}_1]$ onto $[O, \bar{a}_m]$. Hence if b_j^* denotes $(b_j \smile a_m) \frown \bar{a}_m$, then $\bar{a}_m = a_1 \times \cdots \times a_{m-1} = b_2^* \times \cdots \times b_n^*$. By induction on length, a_1 is replaceable by some b_j^* in $[O, \bar{a}_m]$. Moreover $b_j \smile \bar{a}_1$ contains

$$b_j \smile a_m = (b_j \smile a_m) \frown (\bar{a}_m \smile a_m) = [(b_j \smile a_m) \frown \bar{a}_m] \smile a_m = b_j^* \smile a_m .$$

Hence it contains $b_j^* \smile a_2 \smile \cdots \smile a_{m-1} \smile a_m = \bar{a}_m \smile a_m$ (since a_1 is replaceable by b_j^* in $\bar{a}_m$); that is, $b_j \smile \bar{a}_1 = I$. But $d[a_1] = d[b_j^*] = d[b_j]$, the three being projective. Hence $I = b_j \times \bar{a}_1$, and a_1 is replaceable by b_j, q.e.d.

Using Theorem 4 and the Cor. of Thm. 5, we infer the

Corollary 1. *Let $A = A_1 \times \cdots \times A_m = B_1 \times \cdots \times B_n$ be any two representations of an algebra A as a direct union of indecomposable factors, where* (i) *A has a one-element subalgebra,* (ii) *all congruence relations on A are permutable,* *and* (iii) *the lattice of congruence relations on A has finite length. Then* $m = n$, *and the* A_i *and* B_j *are pairwise isomorphic.*

COROLLARY 2. *Let G be any group with operators, or loop satisfying* $x^{-1}(xu) = (ux)x^{-1} = u$; *suppose also the lattice of congruence relations on G has finite length. Then in any two representations of G as a direct union of directly indecomposable factors, the factors are pairwise centrally isomorphic.*[16]

Ex. 1. Show that if the central of G is the identity in Cor. 2, then the factors are equal. (Hint: If $c_0 = a_0b_0$, and every b or c is permutable with every a, then a_0 is in the center of G.)

Ex. 2. (a) Show that if the L of Thm. 12 is distributive, then the a_i and b_j are equal in pairs.
(b) State stronger versions of Cors. 1–2, valid in this case.
(c) Show that the results of Ex. 2 (a) hold more generally if the a_i, b_j are in the *center* of the lattice.

Ex. 3*. Show that neither the ascending nor the descending chain condition is enough to make Thm. 12 valid.[17]

Ex. 4*. Let A and B be the 2-element algebras, with a unary operation $'$, such that $0' = 0$ and $1' = 1$ in A, whereas $0' = 1$ and $1' = 0$ in B. Show that $A \times B$ and $B \times B$ are isomorphic, yet A and B are indecomposable and non-isomorphic. (B. Jónsson)

Problem 34. Is the Unique Factorization Theorem valid for all finite algebras with a one-element subalgebra?

9. Lattices of subgroups. Although it is the modular lattice of congruence relations (normal subgroups) on a group G which most directly characterizes the structure of G, the lattice $L(G)$ of *all* subgroups of G is also interesting. Of course, the two lattices are isomorphic if G is commutative.

Following Prüfer, we shall call a group G *generalized cyclic* if any two elements $a, b \in G$ are powers of a suitable third element $c = c(a, b)$ of G.

THEOREM 13. *The lattice* $L(G)$ *of all subgroups of a group G is distributive if and only if G is a generalized cyclic group.*[18]

Proof. Let G be a generalized cyclic group; by the one-sided distributive law, $L(G)$ is distributive if $A \frown (B \smile C) \leq (A \frown B) \smile (A \frown C)$ for any three subgroups A, B, C of G. But suppose $a = bc$ [$a \in A$, $b \in B$, $c \in C$]; by definition, b, c can be represented as powers $b = d^m$, $c = d^n$ of some third element d; hence $d^{m+n} = a$. If $m' = \text{l.c.m.}\ [m, m + n]$ and $n' = \text{l.c.m.}\ [n, m + n]$, then clearly $d^{m'} \in A \frown B$ and $d^{n'} \in A \frown C$; hence if $h = \lambda m' + \mu n' = \text{g.c.d.}$

[16] For a still more general result, see B. Jónsson and A. Tarski, *Direct decompositions of finite algebraic systems*, Notre Dame Mathematical Series, 1946. There the theorem is proved for any algebra with a binary operation $+$, an element 0 such that $0 + x = x + 0 = x$ for all x, and a structure lattice of finite length. See also R. Baer, *Direct decompositions*, Trans. Am. Math. Soc. 62 (1947), 62–98 and Bull. Am. Math. Soc. 54 (1948), 167–74.

[17] See W. Krull, Math. Zeits. 23 (1925), 161–196; O. Ore. op. cit.; B. Jónsson and A. Tarski, Abstract 51-9-150; I have not checked this result.

[18] This result is due to O. Ore, *Structures and group theory*. II, Duke Jour. 4 (1938), 247–269, Ch. 3.

(m', n'), $d^h \in (A \frown B) \smile (A \frown C)$. But by elementary number theory, $h = (m', n') = ([m, m + n], [n, m + n]) = [(m, n), m + n] = (m, n) \mid m + n$. Hence $a = d^{m+n} = d^{hk} = (d^h)^k \in (A \frown B) \smile (A \frown C)$ for some k.

Conversely, suppose $L(G)$ is distributive, let a, b be any two elements of G, and let m, n be any two integers. If A, B, C denote the subgroups generated by a, b, and $c = ab$ respectively, then $(A \smile B) \frown C = (A \frown C) \smile (B \frown C)$. But $A \frown C$ is generated by the smallest power $a^r = c^h$ of a which is also a power of c, and $B \frown C$ by $b^s = c^k$ likewise. Clearly a^r and b^s are permutable; hence the subgroup generated by them consists of the $a^{mr}b^{ns} = c^{mh+nk}$, and by hypothesis $a^{mr}b^{ns} = ab$ for some m, n; hence $a^{mr-1} = b^{1-ns}$. Therefore a^{mr-1} is permutable with b, hence with b^s, but $a^{mr} = (a^r)^m$ is permutable with b^s; hence so is a. Again, $b^{1-ns} = a^{mr-1}$ is permutable with a; hence so is $b = (b^s)^n b^{1-ns}$, and $ab = ba$. We conclude that a, b generate a *commutative* subgroup of G. Now, using the basis theorem for (possibly infinite) Abelian groups with two generators, this subgroup is cyclic or it has two *independent* generators a', b'. In the latter case, the subgroups generated by a', b', and $a'b'$ are not distributive, as can easily be checked directly.

It is also possible to determine all finite groups G, such that $L(G)$ is modular. This is certainly the case if all subgroups of G are normal; thus it is sufficient that G be generated by its center Z, and two other elements satisfying[19]

$$a^2 = b^2 = c, \qquad c^2 = 1, \qquad a^{-1}b^{-1}ab = c. \tag{8}$$

It is also clearly sufficient that all subgroups of G be *permutable*, as may be seen by inspecting the proof of Thm. 1, Ch. V. This condition is satisfied by the "modular p-groups" $G = \{y, b\}$, generated by a commutative subgroup Y whose elements satisfy $y^{p^m} = 1$, p a prime, and an element b of order p^r, where for some $n = ps \geq p$,

$$b^{-1}yb = y^n \text{ for all } y \in Y, \text{ where } n^{p^r} \equiv 1 \pmod{p^m}, \text{ and } p^s \geq 4 \text{ if } p = 2. \tag{9}$$

The modular law is also satisfied by the subgroups of so-called "modular pq-groups" $G = \{X, a\}$, generated by a commutative subgroup X whose elements satisfy $x^p = 1$ for some prime p, and an element a of prime-power order q^β which satisfies

$$a^{-1}xa = x^n \text{ for all } x \in X, \text{ where } n^q \equiv 1 \pmod{p}. \tag{10}$$

However, the subgroups of modular pq-groups need not be permutable. Conversely, Iwasawa has shown that every finite group G, such that $L(G)$ is modular, is a direct union of Hamiltonian groups, modular pq-groups, and modular p-groups as defined above.[20]

---

[19] Thus a, b generate the so-called *quaternion* group of Hamilton. Dedekind showed (Math. Annalen 48 (1897), 548–61) that "Hamiltonian" groups of the type just described were the only groups whose subgroups were all normal.

[20] K. Iwasawa, J. Fac. Sci. Tokyo 4 (1941), 171–199 and Jap. Jour. Math. 18 (1943), 709–28; see also A. W. Jones, Duke Jour. 12 (1945), 541–560. Quite recently, Marshall Hall has given similar characterizations of groups whose subgroup lattice is semi-modular and dually. Cf. Problem 12 of [LT].

Ex. 1. (a) Determine $L(G)$ if G is the dihedral group of symmetries of a regular pentagon, and show that it is modular.

(b) Same problem for the regular 15-gon, but show that $L(G)$ is non-modular.

(c) Determine $L(G)$, if G is defined by $x^7 = y^6 = 1, xy = yx^3$. Show that all chains have length 3, but that $L(G)$ is not modular. (It is neither upper nor lower semi-modular, in the sense of Ch. VII.)

(d) Let G be defined by $x^5 = y^4 = 1, xy = xy^2$. Show that $L(G)$ is upper, but not lower semi-modular. Show that it is non-modular.

Ex. 2. (a) Show that if $L(G)$ is modular, and H is any homomorphic image of any subgroup of G, then $L(H)$ is modular.

(b*) Is it true that if $L(G)$ and $L(H)$ are modular, then so is $L(G \times H)$?

Ex. 3*. Show that if G is finite, then the center of $L(G)$ consists of the normal and complemented Sylow subgroups of G.

Ex. 4. Represent the modular pq-groups as groups of transformations $\xi \to c\xi + \alpha$ of h-dimensional affine space over the Galois field of order p, in the notation of Ch. VII, §2.

Problem 35. What are the *neutral* elements of $L(G)$, if G is a finite group?

Problem 36. Find conditions on G which are necessary and sufficient for $L(G)$ to be semi-modular.[20] For its dual to be semi-modular (cf. Ch. VII, §5, Ex. 4).

10. Classification of groups by subgroup lattices. It has been shown by A. W. Jones (op. cit. supra) that the subgroup lattices of modular p-groups and of modular pq-groups are isomorphic to subgroup lattices of appropriate commutative groups. This emphasizes the fact that *non-isomorphic groups can have isomorphic subgroup lattices*.[21] However, the fact that all groups whose subgroup lattices are isomorphic with subgroup lattices of Abelian groups, and hence modular, are metabelian groups, shows that groups which have isomorphic subgroup lattices are usually very similar.

Thus for groups G whose order n can be factored into $k \leqq 4$ prime factors (counting repeated factors), the length of $L(G)$ is equal to k. This may be shown by noting that the alternating group of five letters is the only non-solvable such group.[22] Again, $L(G)$ is a chain if and only if G is cyclic of prime-power order. It seems likely that if G is simple, then it is determined to within isomorphism by $L(G)$. Much work remains to be done in this field.[23]

If we restrict ourselves to commutative groups, much can be said. Apart from cyclic Sylow subgroups, $L(G)$ completely determines G. Furthermore, every automorphism of $L(G)$ is induced by a group-automorphism of G. This result specializes, in the case of "elementary" Abelian groups of order p^n, which can be regarded as vector spaces of dimension n over finite fields, to a well known property of collineations in projective geometries, and is thus[24] related to the material in Chs. VII–VIII.

---

[21] For a striking example in point, see Ada Rottlaender, Math. Zeits. 28 (1928), 641–653; for the general problem, see R. Baer, Am. Jour. 61 (1939), 1–44, and Bull. Am. Math. Soc. 44 (1938), 817–820; also A. Kurosh, *Teori Grupp* (Russian) Moscow (1944), pp. 324–348.

[22] Cf. W. Burnside, *Theory of groups of finite order*, Cambridge Press (1897), p. 367.

[23] J. K. Senior has compiled an unpublished set of condensed diagrams of $L(G)$, in the case of p-groups G of low order. O. Ore, Duke Jour. 5 (1939), 431–460, has made partial classifications of solvable groups in terms of the lattices of normal and composition subgroups.

[24] Cf. R. Baer, *A unified theory of projective spaces and finite abelian groups*, Trans. Am. Math. Soc. 52 (1942), 283–343; also E. Inaba, Proc. Imp. Acad. Tokyo 19 (1943), 528–32.

Further, one can prove easily, using the Basis Theorem and characters, that *the lattice of all subgroups of any finite commutative group A is self-dual.*[25]

Ex. 1. Find a necessary and sufficient condition that $L(G)$ be isomorphic to $L(H)$, if G and H are cyclic groups of finite order.

Ex. 2. Show that the lattice of subgroups of the dihedral group of order $2p$ is isomorphic with the lattice of subgroups of the non-cyclic group of order p^2.

Ex. 3*. Show that the lattice of all characteristic subgroups of any Abelian group of odd finite order is distributive. Is it generated by two chains? (Hint: Try the subgroups of x satisfying $p^\alpha x = 0$ for some α, and satisfying $x = p^\alpha t$ for some t, using additive notation.)

Ex. 4. (a) Show that a finite group is hypercentral if and only if the intersection of its maximal proper subgroups contains its commutator-subgroup. (Wielandt)

(b*) Determine the groups G such that $L(G)$ is isomorphic to $L(H)$ for some hypercentral group H.

Ex. 5*. Show that if G is the symmetric or alternating group of degree $n > 4$, then $L(G)$ determines G to within isomorphism.

Problem 37. Find necessary and sufficient conditions on G in order that $L(G)$ be self-dual.

Problem 38. Find necessary and sufficient conditions on G in order that $L(G)$ be complemented.[26]

Problem 39. What is the largest integer k such that $L(G)$ has length k whenever G has k prime factors (not necessarily distinct)?

Problem 40. If $L(G)$ and $L(H)$ are isomorphic, and G is solvable, must H be solvable?

Problem 41. (a) Show that if S is simple, and if $L(G)$ and $L(S)$ are isomorphic, then the center of G is 1. Infer that the order of G is at most the number of automorphisms of $L(S)$.

(b) Use this result and Problem 39 to prove that G is isomorphic with S—or find a counterexample.

Problem 42. To what extent is a group determined to within isomorphism by the complete lattice of its *cosets*? (N. B. Every element is a coset.)

Problem 43 (I. Kaplansky). Is it true that if $L(G)$ has finite length, then G is finite?

---

[25] See A. Chatelet, *Les groupes Abéliens finis et les modules de points entiers*, Paris, 1925, pp. 143, 165, 168. The author, Proc. Lond. Math. Soc. 38 (1935), p. 389, showed that $L(A)$ had a dual automorphism of period two, carrying characteristic subgroups into characteristic subgroups. R. Baer, Bull. Am. Math. Soc. 43 (1937), 121–124, determined all infinite commutative groups A for which $L(A)$ was self-dual.

[26] Problems resembling Ex. 5 and Problem 38, but not equivalent to them, have been solved by R. Baer, Am. Jour. 61 (1939), p. 3, and P. Hall, Jour. Lond. Math. Soc. 12 (1937), 201–204. To solve Problem 40, it may be helpful to use P. Hall's Thm. that a group of order g is solvable if and only if it contains, for every m such that m and g/m are relatively prime, a subgroup of order m.

CHAPTER VII

SEMI-MODULAR LATTICES

1. Definition. A lattice L of finite length is called *semi-modular*[1] if and only if its elements satisfy

(ξ') If x and y cover a, and $x \neq y$, then $x \smile y$ covers x and y.

We have already seen (Ch. V, §2) that any semi-modular lattice satisfies the Jordan-Dedekind chain condition, and that the dimension function satisfies the inequality

$$(1) \qquad d[x \frown y] + d[x \smile y] \leqq d[x] + d[y].$$

From this it follows that

$$(2) \qquad \text{If } x \text{ covers } x \frown y, \text{ then } x \smile y \text{ covers } y.$$

For by (1), since $d[x] = d[x \frown y] + 1$, we get by cancellation $d[x \smile y] \leqq d[y] + 1$. But $d[x \smile y] = d[y]$ would imply $x \leqq y$, whence $x = x \frown y$ could not cover $x \frown y$. Conversely, (2) implies (1).

Following L. R. Wilcox,[2] we shall say that (x, y) is a *modular pair* when $x \geqq z$ implies $x \frown (y \smile z) = (x \frown y) \smile z$. In a modular lattice, evidently all pairs are modular.

LEMMA 1. *Elements x, y of a semi-modular lattice of finite length form a modular pair if and only if equality holds in* (1).

Proof. Suppose $u = x \frown (y \smile z) > (x \frown y) \smile z = t$ for some $z \leqq x$. Then (Ch. V, §1, Fig. 3a) $x \frown y \leqq t < u \leqq x$, yet $t \smile y = u \smile y$. This means that any connected chain from $x \frown y$ to x passing through t, u is *shortened* under the correspondence $s \to s \smile y$. But by (2) it goes into a connected chain; hence inequality holds in (1). Conversely, if x, y is a modular pair, then the transformation $s \to s \smile y$ of the interval $[x \frown y, x]$ has a single-valued inverse $s \smile y \to (s \smile y) \frown x$; hence connected chains go into connected chains of the same length; hence $d[x \smile y] - d[y] = d[x] - d[x \frown y]$, and equality holds in (1).

However, the condition that equality holds in (1) is symmetric on x and y; hence in a semi-modular lattice, if x, y is a modular pair, then y, x is a modular pair. Whereas if a lattice L of finite length is not semi-modular, we have y and z covering $a = y \frown z$, yet $y \smile z > x > z$ for some x, y, z. Then x, y is not a modular pair; yet y, x is a modular pair. For if $t \leqq y$, then $t \smile (x \frown y) =$

---

[1] Also, "Birkhoff lattices"; in [LT], "upper semi-modular lattices."

[2] *Modularity in the theory of lattices*, Annals of Math. 40 (1939), 490–505. Theorem 1 is due to Wilcox; the proof given below to I. Kaplansky and the author. Theorem 2 is new. Cf. R. P. Dilworth, *Ideals in Birkhoff lattices*, Trans. Am. Math. Soc. 49 (1941), 325–53, and S. MacLane [1], esp. p. 456, for semi-modular lattices of infinite length.

$t \smile a$ satisfies $a \leqq t \smile a \leqq y$. If $t \smile a = y$ certainly $t \smile (x \frown y) = y \geqq (t \smile x) \frown y$; if $t \smile a = a$, then $t \leqq a$ and so $t \smile (x \frown y) = a = x \frown y = (t \smile x) \frown y$. We conclude the following result.

THEOREM 1. *A lattice L of finite length is semi-modular if and only if the relation of modularity between pairs of elements of L is symmetric.*

This condition has the advantage of applying to lattices with continuous as well as discrete chains. So does the following condition.

THEOREM 2. *A lattice L of finite length is semi-modular if and only if:*
(γ) *if* $(x_0, y_0), (x_1, y_1), \cdots, (x_n, y_n)$ *is any maximal chain of the cardinal product* $[x \frown y, x] \times [x \frown y, y]$, *then* $x_0 \smile y_0, x_1 \smile y_1, \cdots, x_n \smile y_n$ *is a maximal chain of* $[x \frown y, x \smile y]$.

Proof. By definition of cardinal product, if (x_i, y_i) covers (x_{i-1}, y_{i-1}) in L, then either $x_i = x_{i-1}$ and y_i covers y_{i-1} or x_i covers x_{i-1} and $y_i = y_{i-1}$; in either case, if L is semi-modular, $x_i \smile y_i$ covers $x_{i-1} \smile y_{i-1}$ or equals it by (2); hence the $x_i \smile y_i$ form a maximal chain. Conversely, if L is not semi-modular, then (ξ') fails, and $a \smile a$, $a \smile y$, $x \smile y$ or $a \smile a$, $x \smile a$, $x \smile y$ fails to be maximal chain of the interval $[x \frown y, x \smile y]$.

We shall now show that (γ) holds in *any* modular lattice M. Let $\{x_\alpha\}$ and $\{y_\alpha\}$ be maximal chains in $[x \frown y, x]$ and $[x \frown y, y]$, respectively; then $\{x_\alpha \smile y_\alpha\}$ is a chain in $[x \frown y, x \smile y]$; let c be any cut in $\{x_\alpha \smile y_\alpha\}$; define $x_c = (c \smile y) \frown x$ and $y_c = (c \smile x) \frown y$. By L5, we have $[(x_\alpha \smile y_\alpha) \smile y] \frown x = (x_\alpha \smile y) \frown x = x_\alpha \smile (y \frown x) = x_\alpha$. Hence if $x_\alpha \smile y_\alpha \leqq c$, $x_\alpha \leqq [c \smile y] \frown x = x_c$, and if $x_\alpha \frown y_\alpha \geqq c$, $x_\alpha \geqq [c \smile y] \frown x = x_c$, lattice operations being isotone. Also, $x_\alpha = x_\alpha \frown x \leqq (x_\alpha \smile y_\alpha) \frown x = x_\alpha \smile (y_\alpha \frown x) \leqq x_\alpha \smile (y \frown x) = x_\alpha$, whence $x_\alpha \smile y_\alpha \leqq c$ implies $x_\alpha = (x_\alpha \smile y_\alpha) \frown x \leqq c \frown x$, and $x_\alpha \smile y_\alpha \geqq c$ implies $x_\alpha = (x_\alpha \smile y_\alpha) \frown x \geqq c \frown x$. Since $x_c \in \{x_\alpha\}$, $y_c \in \{y_\alpha\}$, we conclude $x_c \smile y_c = x_\alpha \smile y_\alpha$. Hence the same cut c in the set of α defines x_c and $c \frown x$—and, $\{x_\alpha\}$ being maximal, $x_c = c \frown x \in \{x_\alpha\}$. Similarly, $y_c = c \frown y \in \{y_\alpha\}$, where c is one of the α. Consequently,

$$c \leqq (c \smile y) \frown (x \smile c) = [(c \smile y) \frown (x \smile y)] \frown (c \smile x) \quad \text{since } c \leqq x \smile y$$

$$= [\{(c \smile y) \frown x\} \smile y] \frown (c \smile x) = [(c \smile y) \frown x] \smile [y \frown (c \smile x)] \quad \text{by L5 twice}$$

$$= x_c \smile y_c = (c \frown x) \smile (c \frown y) \leqq c.$$

We conclude $(x_c \smile y_c) \in \{x_\alpha \smile y_\alpha\}$, which is thus maximal, q.e.d.

Ex. 1. Show that in any lattice L (i) if L is modular, then (α) the relation of modularity between pairs of elements of L is symmetric, (ii) if (α) holds, then (2) holds, (iii) if (2) holds, then (ξ') holds.

Ex. 2*. Show that (ξ') implies (α) if any two elements of L can be joined by a finite maximal chain. Prove an analog of (1) in this case. (I. Kaplansky)

Ex. 3. Show that any lattice of finite length possesses an isotone function assuming the real values $0, \frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \cdots$, such that (1) holds.

Ex. 4. (a) Show that $1 \oplus (1 + R) \oplus 1$ is a lattice which satisfies (ξ') but not (2); here R is the chain of rational numbers. (I. Kaplansky)

(b) Show that $1 \oplus (R + R) \oplus 1$ satisfies (α) and its dual, but not the condition that all maximal chains connecting the same end points are isomorphic. (I. Kaplansky)

Problem 44. Does condition (γ) imply condition (α)? What can you say if one chain condition holds (cf. Wilcox, op. cit.)? Do condition (γ) and its dual imply modularity? What about lattices whose ideals satisfy (ξ') (cf. Dilworth, op. cit.)?

Problem 45. Can Ore's Thm. 12 of Ch. VI be extended to the symmetric elements of semi-modular lattices, if suitably modified?

2. Examples. Now let R be any associative ring with unity 1; consider the set of n-vectors $\xi = (x_1, \cdots, x_n)$, $\eta = (y_1, \cdots, y_n)$—with components $x_i \in R$. We define addition of n-vectors and multiplication of vectors by scalars $c \in R$ by the usual formulas.[3]

$$\xi + \eta = (x_1 + y_1, \cdots, x_n + y_n), \; c\xi = (cx_1, \cdots, cx_n).$$

The algebraic system thus defined is denoted $V(R; n)$, and called the n-dimensional vector space over R.

A linear combination of vectors $\xi_1, \cdots, \xi_r$ is defined to be any finite sum $c_1\xi_1 + \cdots + c_r\xi_r$ of scalar multiples $c_i\xi_i$ of the ξ_i. The set of linear combinations of a set X of vectors is called the *vector subspace* generated by X, and may be denoted $\bar{X}$; the vector subspace generated by the void set is defined as $(0, \cdots, 0)$. It is easily verified that the operation $X \to \bar{X}$ is a closure operation in the sense of Ch. IV, §1; hence the vector subspaces of $V(R; n)$ form a complete lattice. By Thm. 1 of Ch. V, this lattice is even modular; it is denoted $PG(R; n - 1)$ and called *the* $(n - 1)$*-dimensional projective geometry over* R.

The most interesting case occurs when R is a division ring; in this case, each nonzero vector ξ generates a minimal proper subspace, consisting of the various $c\xi$. For any $c\xi \neq 0$ generates a subspace including $c^{-1}(c\xi) = \xi$. These minimal proper subspaces are called *projective points*; they correspond to projective points under homogeneous coordinates, in the usual sense.[4]

Obviously every subspace of $V(R; n)$ is the join of the projective points which it contains; moreover if $\bar{\xi} \neq \bar{\eta}$, $\bar{\xi} \smile \bar{\eta}$ contains $\overline{\xi + \eta}$, which determines a third projective point; hence

THEOREM 3. *For any division ring R and any n, $PG(R; n - 1)$ is a modular lattice in which the join of two distinct points contains a third.*

An *affine subspace* of $V(R; n)$ is defined as a subset which contains, with any ξ, η, also all "affine combinations" $\xi + c(\eta - \xi)$; the void set is included as an affine subspace. It is easily verified that any nonvoid affine subspace is the transform of a vector subspace under a translation $\tau \to \tau + \xi$; moreover as in Ch. IV, §1, the affine subspaces of $V(R; n)$ form a complete lattice. This is denoted $AG(R; n)$, and called the *n-dimensional affine geometry over R.*

---

[3] As, for example, in N. Jacobson, *Theory of rings*, New York, 1943, esp. Ch. II, where more material may be found.

[4] See for example W. C. Graustein, *Introduction to higher geometry*, MacMillan, 1940 Ch. III.

Again, let R be a division ring. In $PG(R; n)$, let S be the vector subspace of all $(n + 1)$-vectors $(x_1, \cdots, x_n, 0)$; we call this the "hyperplane at infinity." Each vector $\xi \in V(R; n + 1) - S$ determines just one vector $(x_{n+1}^{-1}x_1, \cdots, x_{n+1}^{-1}x_n, 1)$ in the affine subspace A of vectors $(y_1, \cdots, y_n; 1)$; this is the usual correspondence between homogeneous and non-homogeneous coordinates. Moreover, this correspondence interchanges linear combinations and affine combinations; hence it interchanges vector subspaces not included in S and affine subspaces of A. In this way, it may be shown (we omit the details) that

THEOREM 4. *For any division ring R and any n, $AG(R; n)$ is isomorphic with the subset of those elements of $PF(R; n)$ which are not contained in a maximal proper element $S < I$.*

Using Ex. 4 below, one then easily shows that $AG(R; n)$ is always a semi-modular lattice.[5]

It is easy to show that any cardinal product, join-homomorphic image,[6] or convex sublattice of a semi-modular lattice of finite length is itself semi-modular. However, duals and sublattices of semi-modular lattices need not be semi-modular.

Other examples of semi-modular lattices are described in §§5–6, below.

Ex. 1. Show that any non-modular lattice contains a non-semi-modular sublattice.

Ex. 2. Show that unless R consists of 0, 1 alone, every "line" in $PG(R; n)$ contains at least four points.

Ex. 3. Show that if p is any point of $AG(R; n)$, the $x \geqq p$ form a modular lattice isomorphic with $PG(R; n)$. (Menger)

Ex. 4. Let M be any modular lattice, and $s < I$ any maximal proper element of M. Show that if we delete the $x \leqq s$ in M, we get a semi-modular lattice L. Show that if $p > 0$ in L, the $y \geqq p$ form a modular lattice.

Ex. 5. Show that if, in any semi-modular lattice L, we equate to I all elements with $d[x] \geqq n$ (n any fixed integer), we get a semi-modular lattice. Show that this is a join-homomorphic image of L. (S. MacLane)

Ex. 6. (a) Show that if R is the real number system, the portions of affine subspaces contained in any open convex subset S of $V(R; n)$ form a semi-modular lattice. (This gives n-dimensional *hyperbolic* geometry, if S is an n-sphere.)

(b**) Generalize to the case R is an ordered field, so far as possible.

Ex. 7. Generalize Thms. 3–4 to the case of infinite n.

Ex. 8. (a) Show that the "normal cosets" (i.e., cosets of normal subgroups) of a finite group G form a semi-modular lattice if and only if the normal subgroup generated by each element $a \in G$ (not the identity) is a minimal proper normal subgroup.

(b) Which finite groups have this property?

Problem 46. To what extent are the results of the last paragraph applicable to semi-modular lattices of infinite length, using conditions (α), (γ) of §1?

---

[5] This result and Thm. 4 are due to Menger [3]; Thms. 1–2 are due to Menger [1]–[2]. For Ex. 4 cf. Saul Gorn, *On incidence geometry*, Bull. Am. Math. Soc. 46 (1940), 158–67. See also C. J. Everett, *Affine geometry of vector spaces over rings*, Duke Jour. 9 (1942), 873–8.

[6] Let the homomorphism be $L \to L_1$, and let x_1 and y_1 cover a_1 in L_1. Let a be the largest antecedent of a_1, and x, y arbitrary antecedents of x_1, y_1. Form chains from a to $a \smile x$ and $a \smile y$; the elements which cover a in each will be antecedents x^* of x_1 and y^* of y_1. Hence $x^* \smile y^*$ will be an antecedent of $x_1 \smile y_1$, which thus covers x_1 and y_1.

3. Dependence and rank. From now on we consider only semi-modular lattices of finite length. A sequence $x_1, \cdots, x_r$ of elements of a semi-modular lattice is called *independent*[7] if and only if it satisfies the symmetric condition

$$d[x_1 \smile \cdots \smile x_r] = d[x_1] + \cdots + d[x_r]. \tag{3}$$

By (2), $d[x_1 \smile \cdots \smile x_r] \leqq d[x_1 \smile \cdots \smile x_r] + d[x_r] - d[(x_1 \smile \cdots \smile x_{r-1}) \frown x_r]$; hence in any case (by induction) $d[x_1 \smile \cdots \smile x_r] \leqq d[x_1] + \cdots + d[x_r]$. Equality holds if and only if (i) $(x_1 \smile \cdots \smile x_{r-1}) \frown x_r = 0$, (ii) $x_1 \smile \cdots \smile x_{r-1}$, x_r are a "modular pair" (cf. §1), and (iii) $x_1, \cdots, x_{r-1}$ are independent. In particular, *any subset of an independent set is independent.*

The most interesting case occurs when the x_i are points. In this case, we may call $d[\sup X]$ the *rank* of X. Since $x_1 \smile \cdots \smile x_{k+1}$ at most covers $x_1 \smile \cdots \smile x_k$, we have $d[x_1 \smile \cdots \smile x_{k+1}] = d[x_1 \smile \cdots \smile x_k] + 1$ or $d[x_1 \smile \cdots \smile x_k]$ according as $(x_1 \smile \cdots \smile x_k) \frown x_{k+1} = O$ or not. It is a corollary that

LEMMA 1. *A sequence $x_1, \cdots, x_r$ of points is independent if and only if $(x_1 \smile \cdots \smile x_k) \frown x_{k+1} = O$ for $k = 1, \cdots, r - 1$.*

It is a corollary, since condition (3) is symmetric, that

(4) the condition that $(x_1 \smile \cdots \smile x_k) \frown x_{k+1} = O$ for $k = 1, \cdots, r - 1$ is invariant under all permutations[8] of the x_i.

Again, let $x_1, \cdots, x_r$ be any sequence of points, independent or not. We can construct term-by-term a subsequence, none of whose members is contained in the join of the preceding, yet whose join is $x_1 \smile \cdots \smile x_r$—simply by deleting x_k if $x_k \leqq x_1 \smile \cdots \smile x_{k-1}$. We conclude

LEMMA 2. *Any set of points contains an independent subset of the same rank (i.e., with the same join).*

THEOREM 5. *Let X be a set of independent elements $x_i > O$ of a semi-modular lattice L of finite length. Then the x_i generate a sublattice isomorphic with the field of all subsets of X.*

Proof. Associate with each subset S of X, sup S. The set of all sup S is clearly closed under join. By the minimax inequality (Ch. II, §4) $\sup (S \frown T) \leqq \sup S \frown \sup T$, while by L1–L3, $\sup (S \smile T) = \sup S \smile \sup T$. By this and (1),

$$\begin{aligned} d[\sup S \frown \sup T] &= d[\sup S] + d[\sup T] - d[\sup S \smile T] \\ &= \sum_S d[x_i] + \sum_T d[x_i] - \sum_{S \smile T} d[x_i] = \sum_{S \frown T} d[x_i] = d[\sup S \frown T], \end{aligned}$$

---

[7] The concept of independence for points was formulated by H. Whitney [1], but not in lattice-theoretic terms. The author gave a lattice-theoretic interpretation in Am. Jour. 57 (1935), 800–4. See also T. Nakasawa, *Zur Axiomatik der linearen Abhängigkeit*, Rep. Tokyo Bunr. Daigaku 2 (1935), 235–55, and 3(1936), 45–69 and 123–36, where many results are proved; S. MacLane Am. Jour. 58 (1936), 236–40; *Über Abhängigkeitsräume*, by O. Haupt, G. Nobeling and Chr. Pauc., Jour. f. Math. 181 (1940), 193–217. Also R. Dilworth, *Dependence relations in a semi-modular lattice*, Duke Jour. 11 (1944), 575–87.

[8] Fr. Klein, *Birkhoffsche und harmonische Verbände*, Math. Zeits. 42 (1936), 58–81, discovered condition (4).

as can be calculated. Hence the minimax inequality is an equality, and meets correspond to set-products, as well as joins to set-unions. The condition $x_i > O$ guarantees that we have not merely a homomorphism, but an isomorphism.

Recently, using the theory of abstract linear dependence, Dilworth has proved the remarkable result that *every finite lattice is isomorphic with a sublattice of a semi-modular lattice.* (Cf. [LT, Problem 15].)

Ex. 1. (a) Show that in a semi-modular lattice L, $x_1, \cdots, x_r$ are independent if and only if the intervals $[O, x_i]$ generate a sublattice isomorphic with the cardinal product of the $[O, x_i]$.

(b) Infer that definition (3) of independence is equivalent to that of Ch. V, §5, in the case of modular lattices of finite length.

Ex. 2*. Correlate Fr. Klein's observation that independence is symmetric in a semi-modular lattice with Wilcox's condition that modularity of pairs be symmetric.

Ex. 3. Show that, in a semi-modular lattice, if points $p_1, \cdots, p_s$ are independent, and if $q_1, \cdots, q_{s+1}$ are independent, then some set $p_1, \cdots, p_s, q_j$ is independent. (H. Whitney)

Ex. 4. (a) Show that the conclusion of the Kurosh-Ore Theorem is not true in the semi-modular lattice of Fig. 7a.

(b*) Show that the conclusion of the Kurosh-Ore Thm. holds in a finite semi-modular lattice M if and only if the sublattice $L(a)$, generated by the elements p_i covering any $a \in M$, is modular.[8]

4. Matroid lattices. As in Ch. II, §6, a *complemented* lattice is one satisfying

L7. Given x, x' exists with $x \frown x' = O, x \smile x' = I$;

a *relatively complemented* lattice is one satisfying

L7R. Given $a \leqq x \leqq b$, y exists with $x \frown y = a, x \smile y = b$.

Obviously, any relatively complemented lattice of finite length is also complemented.

THEOREM 6. *A semi-modular lattice of finite length is complemented if and only if it satisfies*

L7′. *I is the join of points.*

It is relatively complemented if and only if

L7R′. *Every element X is the join of points.*

Proof. In any lattice of finite length, L7 implies L7′. For let a be the join of all points; $a' = O$ since it cannot contain a point. Conversely, let L be a semi-modular lattice (of finite length) satisfying L7′; let $a \in L$ be given. There exist in succession points $p_1 \not\leqq a$, $p_2 \not\leqq a_0 \smile p_1, \cdots$, until $a \smile p_1 \smile \cdots \smile p_r = I$. As in Lemma 1 of §3, $d[a \smile (p_1 \smile \cdots \smile p_r)] = d[a] + r$; hence

$$d[a \frown (p_1 \smile \cdots \smile p_r)] \leqq d[a] + d[p_1 \smile \cdots \smile p_r] - d[a \smile p_1 \smile \cdots \smile p_r]$$
$$\leqq a + r - (a + r) = 0.$$

[8] See R. P. Dilworth, *The arithmetical theory of Birkhoff lattices*, Duke Jour. 8 (1941), 286–99; also Trans. Am. Math. Soc. 49 (1941), 325–53.

It follows that $a' = p_1 \cup \cdots \cup p_r$ is a complement of a, and even that a, a' form a modular pair. Fig. 7a shows that in a general lattice, neither L7′ nor L7R′ implies L7, let alone L7R.

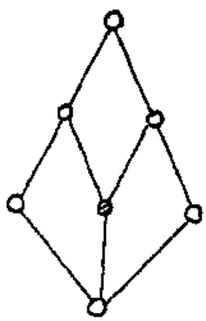

FIG. 7a

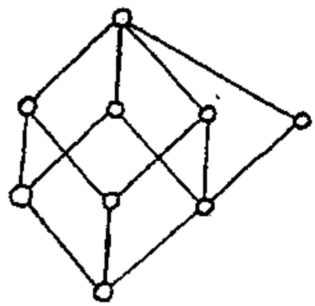

FIG. 7b

Again, in any lattice of finite length, L7R implies L7R′ by the preceding argument applied to the complemented lattice $[O, x]$. Conversely, let L be a semi-modular lattice satisfying L7R′; let $a \leqq x \leqq b$ be given. There exist in succession points $p_1, \cdots, p_r \leqq b$ such that $(x \cup p_1 \cup \cdots \cup p_k) \cap p_{k+1} = O$, $x \cup p_1 \cup \cdots \cup p_r = b$. As in Lemma 1 of §3 and in the preceding paragraph, if we let $z = p_1 \cup \cdots \cup p_r$, then $d[a \cup z] = d[a] + r$ and $d[x \cup z] = d[x] + r = d[b]$. Let $y = a \cup z$. Then $x \cup y = x \cup a \cup z = x \cup z = b$; while $x \cap y \geqq a$ and

$$d[x \cap y] \leqq d[x] + d[a \cup z] - d[x \cup y] = d[x] + d[a] + r - (d[x] + r) = d[a].$$

Hence $x \cap y = a$, and L7R *and* L7R′ *are equivalent if* (ξ') *holds.*

Fig. 7b shows that there exist semi-modular lattices which are complemented but not relatively complemented.

DEFINITION. *A relatively complemented semi-modular lattice is called a matroid lattice.*[10]

Any semi-modular lattice satisfies the "exchange axioms" of Steinitz and MacLane, as defined in (5) and (6) respectively,

(5) If p, q are points, and $a < a \cup q \leqq a \cup p$, then $a \cup p = a \cup q$.

(6) If p is a point, then either $p \leqq a$ or $a \cup p$ covers a.

THEOREM 7. *A lattice L of finite length is a matroid lattice, if and only if it satisfies* (A) L7R *or* L7R′, *and* (B) *either* (ξ') *or* (4) *or* (5) *or* (6).

[10] Following H. Whitney [1]. Matroid lattices are also called "exchange lattices," as in S. MacLane [1], where "exchange axioms" are discussed. Part of Thm. 6 was suggested to the author by I. Kaplansky; cf. [LT, §76]. See also L. R. Wilcox, *A note on complementation in lattices*, Bull. Am. Math. Soc. 48 (1942), 453–7.

Proof. Since L7R implies L7R′ in any lattice of finite length, it suffices to show that if L7R′ holds, then conditions (ξ'), (4), (5) and (6) imply each other cyclically. For then any of these conditions with L7R′ will imply (ξ') and L7R′, hence (ξ') and L7R, and hence that L is a matroid lattice.

First, (ξ') implies (4) as in §3, Lemma 1.

Next, (4) implies (5). Using L7R′, one easily obtains independent points $p_1, \cdots, p_r$ with $p_1 \smile \cdots \smile p_r = a$. Moreover since $a \smile q \leqq a \smile p$, the sequence $p_1, \cdots, p_r, p, q$ is not independent; hence by (4) neither is $p_1, \cdots, p_r, q, p$; hence $p \geqq (a \smile q) \frown p > O$; hence $p \leqq a \smile q$, and $a \smile p \leqq a \smile q$, giving $a \smile p = a \smile q$ by hypothesis and P2.

Then (5) implies (6). If $a < b \leqq a \smile p$, there exists by L7R′ a point q contained in b but not in a; clearly $a < a \smile q \leqq b$. By (5), $a \smile p = a \smile q \leqq b$; hence $a \smile p = b$, and $a \smile p$ covers a. Finally, (6) implies (ξ'). If x, y cover a, then by L7R′ there exist points p, q with $a < a \smile p \leqq x$, $a < a \smile q \leqq y$, whence $a \smile p = x$ and $a \smile q = y$. Hence $x \smile y = a \smile p \smile q$, which by (6) covers $x = a \smile p$ and $y = a \smile q$.

Ex. 1. (a) Show that in Fig. 7a, the shaded element has no complement.
(b) Show that the lattice of Fig. 7a is dually isomorphic to a sublattice of the lattice of all subgroups of the octic group.

Ex. 2. Show that every interval $[a, I]$ of a lattice of finite length satisfying L7′ is complemented.

Ex. 3. Show that if a', a'' are both complements of a, and if both (a, a') and (a, a'') are modular pairs, then $a' \nless a''$.

Ex. 4. Show that for any integer n and division ring R, $AG(R; n)$ and $PG(R; n)$ are matroid lattices.

Problem 47. Correlate conditions (E_5)–(E_6)–(E_7) of MacLane [1] with the conditions of §1.

5. Partition lattices; transcendence degree. It is easily seen that the projective geometries and affine geometries of §2 are matroid lattices: every element is a join of points. (Even 0 is the join of the void set of points!) Further, any cardinal product, lattice-homomorphic image, or interval sublattice of a matroid lattice is itself a matroid lattice.

THEOREM 8. *The set of all partitions π of any finite aggregate X is a matroid lattice.*[11]

Proof. Let X have n elements $x_1, \cdots, x_n$. Let $d[\pi] = n - n(\pi)$, where $n(\pi)$ is the number of disjoint subclasses into which π divides X. It is easy to show that the $\pi' \geqq \pi$ form an interval sublattice $[\pi, I]$ isomorphic to the lattice of all partitions of $n(\pi)$ objects; hence to prove (ξ'), we need only prove that if π' and π'' are distinct minimal partitions (equivalence relations), then $\pi' \smile \pi''$ covers both. But a minimal partition simply identifies two unequal elements;

[11] This result, together with most of the Exs. below, are due to the author ([3, §§16–22]; Abstract 40-11-323 of Bull. Am. Math. Soc. [LT §77]).

hence $\pi' \smile \pi''$ either identifies three elements, or identifies the elements of two distinct pairs. In either case, it covers π and π'. To show L7R$'$, we merely observe that if $x_i \equiv x_j \pmod{\pi}$, there exists a minimal partition π_{ij} which identifies x_i and x_j, but no other pair, whence $\pi_{ij} \leqq \pi$. It is then clear that $\pi = \bigvee \pi_{ij}$, for such π_{ij}; now use Thm. 7.

It has been pointed out by Ore that *symmetric partition lattice of degree n* just defined is somewhat analogous to affine geometry.[12]

It is also noteworthy that the symmetric partition lattices and their sublattices occur in many problems of algebra (cf. Thm. 4, Ch. II) and of combinatory analysis. Quite recently, P. Whitman has shown that *every lattice is isomorphic with a sublattice of the lattice of all partitions of some (infinite) class.*[13]

THEOREM 9. *The algebraically closed subfields of any field I form a matroid lattice.*

Proof. Let F be any algebraically closed subfield, and let H and K cover F. Choose x in H, y in K, neither in F. Then H is the set[14] of numbers algebraic over the ring $\{F, x\}$, K of those algebraic over $\{F, y\}$, and $H \smile K$ of those algebraic over $\{F, x, y\}$. Now if z is in $H \smile K$, then some polynomial $p(x, y, z) = 0$; if z is not in H then this polynomial must involve positive powers of y; hence y is algebraic over $\{F, x, z\}$. It follows that if $H < Z \leqq H \smile K$, then Z contains y, and so $Z = H \smile K$, which proves (ξ') and the Steinitz-MacLane "exchange axiom." Finally, the lattice satisfies L7R$'$: if $G > F$, choose a maximal set of numbers x_α of G which are algebraically independent over F; then the algebraic closures of the $\{F, x_\alpha\}$ will be points whose join is G.

We can define the transcendence degree of G over F as the lattice-theoretic dimension of G over F. Then the above theorems on dependence, rank, etc., include as corollaries most of Steinitz' theory of algebraic dependence; for example, the number of x_α is $d[G/F]$.

No satisfactory theory of functional dependence has yet been invented.

Ex. 1. (a) Show that the symmetric partition lattice of degree n is non-modular if $n > 2$.

(b) Show that the number $\pi(n)$ of partitions of n objects satisfies the recursion formula

$$\pi(n+1) = \sum_{i=0}^{n} \binom{n}{i} \pi(i).$$

(c) Show that $n!\pi(n)$ has the generating function[15] $e^{e^x - 1}$.

(d) Compute $\pi(n)$ for $n = 1, \cdots, 10$. ($\pi(10) = 115975$.)

[12] O. Ore, *Theory of equivalence relations*, Duke Jour. 9 (1942), 573–627, esp. Ch. IV.

[13] P. M. Whitman, *Lattices, equivalence relations, and subgroups*, Bull. Am. Math. Soc. 52 (1946), 507–22. Space forbids our giving the proof of this important result.

[14] We rely on the lemma: the set of numbers algebraic over any subring of I forms an algebraically closed subfield. For the algebraic background assumed, cf. van der Waerden [1, vol. 1, pp. 206–8]. Theorem 9 and the applications of it are entirely due to S. MacLane [1].

[15] Cf. L. Epstein, M. I. T. Jour. Math. Phys. 18 (1939), 153–73; also G. Williams, Am. Math. Monthly 52 (1945), 323–7.

Ex. 2. (a) Show that there is a join homomorphism mapping the matroid lattice 2^2 onto the chain 3.

(b) Prove that every lattice-homomorphic image of a matroid lattice is a matroid lattice. (Hint: Show that any point goes into a point or 0.)

Ex. 3. Show that any interval sublattice or cardinal product of matroid lattices is a matroid lattice.

Ex. 4*. (a) Show that the dual of the lattice of all subgroups of any p-group of finite order p^n is a semi-modular lattice.

(b) Show that it is not a matroid lattice unless the p-group is the elementary Abelian group of order p^n.

Ex. 5*. Show that the subgroups of any finite group which lie in a composition series (so-called "composition subgroups") form a sublattice of the lattice of all subgroups, whose dual is semi-modular.[16]

Ex. 6. (a) Show that the lattice of all partitions of n objects is isomorphic to a sublattice of the subgroup-lattice of the symmetric group of degree n. (Hint: Associate with π the permutations having the π-subsets as imprimitive sets.)

(b) Extend to the infinite case. (H. Löwig. Hint: Do the same, but take only permutations leaving all but a finite number of objects fixed.)

Ex. 7. (a) Show that the symmetric partition lattice of degree n has no proper congruence relations.

(b) Extend to n infinite. (O. Ore, op. cit., p. 626.)

Ex. 8*. (a) Show that π and π' are a modular pair if and only if the topological graph of π and π' (with π-subsets A_i and π'-subsets A_j as vertices, and an edge joining A_i and A_j if and only if $A_i \frown A_j' > 0$) is without cycles.[17]

(b) Infer that Wilcox's definition of semi-modularity is satisfied even for partitions of infinite sets.

(c) Try other conditions for semi-modularity.

Ex. 9. Show that the lattice of all partitions of any finite graph into connected subgraphs is semi-modular. When is it a matroid lattice? What is its center? Apply to the map coloring problem (Ch. I, §12).

Ex. 10*. Show that neither the symmetric partition lattices nor subgroup lattices satisfy any identical implications on lattice polynomials, except those satisfied by L1–L4. (Use Whitman's Theorem.)

Ex. 11. (a) Show that the partitions of any measure space into a finite number of disjoint measurable subsets form a semi-modular lattice.

(b) In what sense do the partitions into countable disjoint measurable subsets form a semi-modular lattice? Suppose sets of measure zero are ignored?

Ex. 12. (a) Show that the k-spheres and k-flats $[k = 0, 1, 2, \cdots, n-1]$ in Euclidean n-space I form, together with I and the void set O, a matroid lattice L_s of length $n+2$. (Note: A 0-sphere is a point pair.)

(b) Show that this is also true in spherical n-space and elliptic n-space, giving lattices L_s' and L_s''.

(c) Show that every "inversion" generates a lattice-automorphism of L_s'.

Ex. 13. (a) Using Ptolemaic projection, show that (for given n), L_s is isomorphic to a sublattice of L_s' obtained by deleting a single point.

---

[16] See. H. Wielandt, Math. Zeits. 45 (1939), p. 209–44. The fact that composition subgroups are closed under intersection is obvious.

[17] O. Ore, op. cit., p. 583; also P. Dubreil and M.-L. Dubreil-Jacotin, *Théorie algèbrique des relations d'equivalence*, Jour. de Math. 18 (1939), 63–96. For other lattice-theoretic aspects of partitions, see O. Boruvka, Rozp. Tridy Ceske Akad. 53 (1943), No. 23; Publ. Fac. Sci. Univ. Masaryk (1946), 1–37.

For Ex. 12, see S. Izumi, Proc. Imp. Acad. Tokyo 16 (1941), p. 515.

(b) Show further that, if p is any point of L'_s, the dual ideal of $x \geqq p$ in L_s is isomorphic with the $AG(R^*; n-1)$ of §2, where R^* is the real field.

(c) State a corresponding result about L_s.

Problem 48. Is any finite lattice isomorphic with a sublattice of a symmetric partition lattice of finite degree? Is this true of the dual of the symmetric partition lattice of degree 4?

Problem 49. Is every lattice of finite length isomorphic with a sublattice of a matroid lattice of finite length? Of the same length?

Problem 50. Which complete lattices are isomorphic with the lattice of *all* congruence relations of a suitable abstract algebra? (Thm. 4 of Ch. II shows that certain continuity laws hold; see also Ex. 4, §7, Ch. III.)

6. Plane geometries. Other important examples of matroid lattices are furnished by plane affine and projective geometries.

A *plane affine geometry* may be defined[18] combinatorially as a collection of points and of sets of points called lines, satisfying:

APG1. Any two distinct points p, q are on one and only one line $p \smile q$.

APG2. Given $p \smile q$ and $r \not\in p \smile q$, there exists just one line $r \smile s$ such that $p \smile q$ and $r \smile s$ have no common points.

APG3. There are three points not on a line.

It is easily shown that if the void set O and all points I are adjoined, one gets a matroid lattice A.

Two lines of A are called *parallel* if and only if they are identical or without common points. One shows easily that the relation of parallelism is an equivalence relation. For its definition is reflexive and symmetric. While if μ and $\mu' \neq \mu$ are both parallel to λ, they cannot have a common point p—otherwise there would be two lines through p parallel to λ, contradicting APG2.

It follows that we can adjoin to A a "line at infinity" λ_∞, containing exactly one point for each set of parallel lines. Two finite lines then always intersect exactly once—either on the finite plane or (if parallel) on λ_∞; moreover each finite line lies in just one set of parallel lines, and hence has just one point in common with λ_∞. Hence, after A is extended, APG2 may be replaced by

PG2′. Every pair of distinct lines has just one point in common.

PG2″. Every line contains three or more points. (For if one "line" of A contained just one point, by APG2 there is just one line through every other point, which is impossible by APG1 and APG3.)

A set of points and lines satisfying APG1, PG2′, PG2″ and APG3 is called a *plane projective geometry*, and we have proved

THEOREM 10. *Every plane affine geometry can be extended to a plane projective geometry by adding a "line at infinity."*

---

[18] As by E. Artin, *Coordinates in affine geometry*, Rep. Math. Colloq. Notre Dame, Indiana, 1940. The reading of this paper is strongly recommended.

We shall now show that plane affine geometries arise from coordinate systems more general than division rings.

We define a *point* to be a *number-pair* (x, y). Our lines we take to be (i) lines $x = c$ of infinite slope, and (ii) the lines $y = a + sx$ with "slope" s and "y-intercept" a. This definition involves a ternary operation on our "numbers."[19] Clearly lines of infinite slope are "parallel". If $(x, a + sx) = (x', a' + sx')$, then $x = x'$, $a + sx = a' + sx$; hence lines of the same finite "slope" are parallel if and only if

(i) $a + sx = a' + sx$ implies $a = a'$.

Further $x = c$ and $(x, a + sx)$ obviously have in common just $(c, a + sc)$. Hence to satisfy APG2, it is sufficient that

(ii) if $s \neq s'$, $a + sx = a' + s'x$ has just one solution.

Moreover APG3 is trivially satisfied. Hence our ternary operation $a + bc$ will define an affine plane geometry if and only if APG1 is satisfied, namely,

(iii) given $x, y, x' \neq x, y'$, we have $a + sx = y$ and $a + sx' = y'$, for exactly one pair a, s.

The smallest known system R satisfying (i)–(iii), but not a division ring, was discovered by O. Veblen and J. H. M. Wedderburn.[20] Its ternary operation $a + sx$ may be defined indirectly from binary addition and multiplication. Under addition, R is the elementary Abelian group of order 9; its general element is $m + n\alpha$ [m, n integers mod 3]. Here $1 = 1 + 0\alpha$ is a multiplicative unit and $(x + y)z = xz + yz$; hence multiplication is completely defined by $\alpha\alpha = 2$, $\alpha(\alpha + 1) = 2\alpha + 1$, $\alpha(\alpha + 2) = \alpha + 1$, $\alpha(2x) = 2(\alpha x)$.

Let P be a finite projective plane with $n + 1$ points on some line λ. If p is any point not on λ, the lines through p each intersect λ in just one point; hence there are n lines through p. This is also true of *any* line λ' not through p; but no λ' exhausts $P - \lambda$; hence *every line of P contains exactly $n + 1$ points.* Similarly, every point is on exactly $n + 1$ lines. Since every point not p is on just one line through p, and each of the $n + 1$ such lines contains n points other than p, P must contain exactly $n^2 + n + 1$ points.

Consequently the *affine* plane of n^2 points, obtained by deleting a "line at infinity" from P, has the following property. There are $n + 1$ successive ways $\pi_1, \cdots, \pi_{n+1}$ of dividing these n^2 points into rows ("parallel lines") of n elements, so that each pair of points is in the same row under one and only one π_i.

A more general combinatory problem is the following. Let m, n be integers such that $(n - 1)|(mn - 1)$; let $r = (mn - 1)/(n - 1)$. Let us try to find partitions $\pi_1, \pi_2, \pi_3, \cdots$ of mn objects into m rows of n objects, such that no two objects are in the same row more than once. After r times, each object will then have been in the same row with $r(n - 1) = mn - 1 =$ all other objects; hence r is the greatest possible number of such partitions. We define the (m, n)-

---

[19] We follow here the idea of Marshall Hall, *Projective planes*, Trans. Am. Math. Soc. 54 (1943), 229–77; cf. also Ruth Moufang, six papers in Math. Annalen, vols. 105–110 incl.

[20] *Non-Desarguesian and non-Pascalian geometries*, Trans. Am. Math. Soc. 84 (1907), 379–88.

Problem as the problem of finding such a set of partitions;[21] the set is called an (m, n)-System.

With *four* partitions π_1, π_2, π_3, π_4 having the type described of a set of n^2 elements, one can construct a so-called $n \times n$ *Eulerian square*, as follows. The rows and columns of the square are associated with the rows of π_1 and π_2 respectively; thus the (i, j)-space in the square is associated with the point p_{ij} falling in the ith row of π_1 and the jth row of π_2. The rows of π_3 and π_4 are numbered $k = 1, \cdots, n$ and $l = 1, \cdots, n$; the (i, j)-space is then filled by the symbol (k, l) when p_{ij} falls in the kth row of π_3 and the lth row of π_4.

Since $\pi_i \frown \pi_j = 0$, if $i \neq j$, each k and each l occurs exactly once in each row and each column; moreover no pair (k, l) occurs more than once. Such an array is called an Eulerian (or Graeco-Latin) square; if n is odd, it is easy to construct (cf. Ex. 1 below).

Using such square, one easily constructs a *magic square* by entering $(k - 1)n + 1$ in the square having the entry (k, l). For further details on Eulerian and magic squares, see P. J. MacMahon, *Combinatory analysis*, Cambridge University Press; also Rouse Ball, op. cit. supra, pp. 189–217; also the Exs. below.

Ex. 1. (a) Show that if n is odd, one can construct an $n \times n$ Eulerian square with (i, j)-entry $(i + n, j - n)$ mod n.

(b) Construct a 5×5 magic square.

Ex. 2. Using the Galois field of four elements, construct a 4×4 Eulerian square and a 4×4 magic square.

Ex. 3**. Show that it is impossible to construct a 6×6 Eulerian square. (M. G. Tarry)

Ex. 4*. An $n \times n \times n$ "magic cube" consists of the numbers $1, \cdots, n^3$ so arranged in a cubical array that the sum of the terms in any row parallel to an edge is constant.

(a) Show that, treating the cube as affine 3-space, if 6 points (a "complete hexangle") can be found on the "plane at infinity," such that no 3 points are collinear, integer-triples (k, l, m) can so be assigned to the positions (h, i, j) of the cube that no triple occurs twice and that k, l, m each assume each value exactly once in any row parallel to an edge $(h, i, j, k, l, m = 1, \cdots, n)$. (This defines a "Eulerian cube.")

(b) Show that this exists if and only if $n \geqq 5$. (Hint: A complete quadrangle has $6n - 5$ points, a complete pentangle, $10n - 20$.)

(c) Infer that if $p^k \geqq 5$, where p is a prime, then a $p^k \times p^k \times p^k$ magic cube exists.

Ex. 5. Show that the Cayley numbers satisfy (i)–(iii), and hence give coordinates for a non-Desarguesian geometry.[22]

Ex. 6. A set of points and lines may be called a "plane configuration," if no two points are on more than one line and no two lines have more than one common point.

(a) Show that any plane configuration not a projective geometry can be extended further by adding a line through any pair of points not previously intersecting.

(b) Show that any plane configuration can be extended to a plane projective geometry.[23]

---

[21] The (5,3)-problem ($r = 7$) is Kirkman's celebrated Schoolgirls problem. The $(2n + 1, 3)$-problem is closely related to the problem of Steiner's triple systems. For further known results, see Rouse Ball, *Mathematical recreations and essays*, Macmillan, 1942 (11th ed., revised by H. S. M. Coxeter), Ch. XI; also E. Netto, *Lehrbuch der Combinatorik*, Leipzig, 1901, Chs. X, XI.

[22] Cf. H. S. M. Coxeter, Abstract 52-7-222 Bull. Am. Math. Soc.

[23] M. Hall, *Projective planes*, loc. cit.

Ex. 7. Construct a complete multiplication table for the Veblen-Wedderburn algebra of nine elements.

Ex. 8. (a) Show that the symmetric partition lattice of degree n is a matroid lattice of length n, whose group of automorphisms is transitive on points.

(b) Show that the group of automorphisms is not transitive on lines.

Ex. 9. Show that $PG(R; n)$ and $AG(R; n)$ are matroid lattices, whose group of automorphisms is transitive on the elements of any given dimension.

Ex. 10*. Show that a finite plane projective geometry which satisfies Desargues' Theorem, satisfies Pascal's Theorem.

Ex. 11. Show that (i)–(iii) are implied by: (a) R is a commutative group under addition, (b) $(x + y)z = xz + yz$, (c) $xa = b$ and $ay = b$ $(a \neq 0)$ have unique solutions x, y, (d) $xa = xb + c$ $(a \neq b)$ has a unique solution x. (M. Hall)

Problem 51. Enumerate all finite plane geometries, and determine for which n there exist plane projective geometries of $n^2 + n + 1$ elements. (Hint: Letting R be a Galois field, they exist for $n = p^k$ (p any prime, k any positive integer), but not for $n = 6$.)

Problem 52. Which finite plane projective geometries are self-dual? Which have groups of automorphisms which are transitive (a) on points, (b) on lines? Do any of these conditions imply Desargues' Theorem?

Problem 53. Which (m, n)-Systems admit a group of automorphisms transitive on their elements (i.e., are "homogeneous")?[24]

Problem 54. Discuss topological matroid lattices, especially in case they are locally compact topological lattices[25] of finite length.

---

[24] See Problem 5 in Ch. I, §10, and the refs. given there.

[25] See L. R. Wilcox, Duke Jour. 8 (1941), 273–85; Haupt, Nöbeling, and Pauc, op. cit. in §3; A. Kolmogoroff, Annals of Math. 33 (1932), 163–76.

CHAPTER VIII

COMPLEMENTED MODULAR LATTICES

1. **Definition.** The present chapter will be concerned with *complemented modular lattices*—that is, with modular lattices L with O and I which satisfy L7. Every $x \in L$ has a "complement" x', such that $x \frown x' = O$ and $x \smile x' = I$. We shall first show that a complemented modular lattice is necessarily relatively complemented, in the sense of Ch. VII, §4. Indeed, let $a \leqq x \leqq b$ be given, and let x' be any complement of x. Then

$$(a \smile x') \frown b \frown x = (a \smile x') \frown x = a \smile (x' \frown x) = a \smile O = a,$$

$$x \smile a \smile (x' \frown b) = x \smile (x' \frown b) = (x \smile x') \frown b = I \frown b = b.$$

Hence $(a \smile x') \frown b = a \smile (x' \frown b)$ is a relative complement of x in the interval $[a, b]$. This proves

THEOREM 1. *Any complemented modular lattice is relatively complemented.*

COROLLARY. *For modular lattices of finite length, each of conditions* L7, L7R, L7′, L7R′ *of Ch.* VII, §4, *implies all the others.*

Proof. By Thm. 6 of Ch. VII, L7 and L7′ are equivalent and L7R and L7R′ are equivalent. We have just shown that L7 implies L7R; conversely, any lattice of finite length has an O and an I; in such a lattice L7R implies L7 trivially.

Incidentally, the implication L7 $\rightarrow$ L7R′ is an immediate corollary of the following

LEMMA. *The "differences" $d_k = x_k' \frown x_{k+1}$ between successive terms of any chain $O = x_0 < x_1 < \cdots < x_s$ are independent elements whose join is x_s.*

Proof. By induction on s, we can assume that $(d_1 \smile \cdots \smile d_{s-1}) \smile d_s$ is $x_{s-1} \smile (x_{s-1}' \frown x_s)$; by L5, this is $(x_{s-1} \smile x_{s-1}') \frown x_s = x_s$. The d_k are independent in the sense of Ch. V, §5, since

$$(d_1 \smile \cdots \smile d_{s-1}) \frown d_s = x_{s-1} \frown d_s = x_{s-1} \frown x_{s-1}' \frown x_s = O.$$

THEOREM 2. *Let L be any complemented metric lattice, and let x' be any complement of x in L. If $| x - y | < \epsilon$, then y has a complement y' which satisfies $| x' - y' | < \epsilon$.*

Proof. Let $t = x \frown y \leqq x$. We form the chain $O \leqq x' \leqq (t \smile x') \leqq x \smile x' = I$. By the Lemma, forming the chain $O \leqq t \leqq x \leqq I$, the elements t, $t' \frown x$, x' are independent elements whose join is I; hence if t' is any complement of t, $(t' \frown x) \smile x' = t^*$ is another. But by Ch. V, §7, (7), to replace x by t in $(t' \frown x) \smile x'$, will move it at most $| t - x |$; the substitution yields

$(t' \frown t) \smile x' = x'$; hence $| t^* - x' | \leqq | t - x |$. Similarly, we can find a complement y^* of y such that $| y^* - t^* | \leqq | y - t |$. By the triangle inequality

$$
\begin{aligned}
| y^* - x' | &\leqq | x - x \frown y | + | y - x \frown y | \\
&= v[x] - v[x \frown y] + v[y] - v[x \frown y] \text{ since } x, y \geqq x \frown y \\
&= v[x \smile y] - v[y] + v[y] - v[x \frown y] = | x - y |.
\end{aligned}
$$

This completes the proof.[1]

Ex. 1. Show that in any complemented modular lattice, all join-irreducible elements are atoms.

Ex. 2. Show that if z is a relative complement of x in $x \smile y$ or of $x \frown y$ in y, then it is a complement of $x \smile (x \smile y)'$.

Ex. 3. (a) Let L be a complemented, complete modular lattice in which every element is a join of atoms. Show without assuming chain conditions that the dual of L has the same property.

(b) Show that this is not true of all semi-modular lattices, even in the case of finite length.

Ex. 4. (a) Show that the modular lattice of all finite-dimensional subspaces of an infinite-dimensional vector space is relatively complemented, but not complemented.

(b) Show that it also satisfies L7R′.

(c) Construct modular lattices satisfying L7R, but not L7R′, and L7R′ but not L7R.

Ex. 5. Show that all relatively complemented lattices of eight or fewer elements are modular (H. Rubin).

2. Examples. Since set-complements satisfy L7, the algebra of all subsets of any class I forms a complemented modular lattice for the same reason, so does any field of subsets of I. Other similar examples are discussed in Ch. X.

Again, using L7′, we see that the linear subspaces of any finite-dimensional vector space (i.e., the projective geometries $PG(R; n)$ of Ch. VII, §2) form a complemented modular lattice. Similarly, so do the normal subgroups of any finite direct union of simple groups, and the ideals (resp. invariant subalgebras) of the direct sum of any finite set of simple rings (resp. linear algebras). More generally, so do the Ω-subgroups of any finite direct union of "simple" groups with a class Ω of operators. We shall see in §8 that these results apply equally to infinite-dimensional vector spaces, and arbitrary direct unions of groups with operators.

Complemented modular lattices are also important in representation theory. Let Ω be any set of linear operators, operating on a linear space I. Then the condition that the modular lattice M of Ω-invariant subspaces[2] of I be comple-

[1] *Bibliographical remarks.* Thms. 1–2 are due to von Neumann [2, Thm. 1.3]. Parts of the Cor. of Thm. 1 had been previously obtained by the author [1, Thm. 11.4] and [2, p. 745]; the rest is due to Ore [2, Ch. 3, §1]. The concept of a complemented modular lattice is due to the author [2]; cf. also K. Menger [2].

[2] I.e., subspaces X such that $x\omega \in X$ if $x \in X$ and $\omega \in \Omega$. It is well known that M is complemented if Ω is a finite group or semi-simple hypercomplex algebra, except perhaps when Ω is a group whose order is a multiple of the characteristics of the field of scalars for I. Cf. J. H. M. Wedderburn, *Lectures on matrices*, Am. Math. Soc. Colloq. Publications. vol. 17, New York 1934, pp. 165–9.

mented is by definition that if Ω can be "half-reduced" by one Ω-invariant subspace X, then Ω can be "fully reduced" by X and some complementary invariant subspace X'. This is clearly the condition that M be complemented, and the equivalence of this condition with the other conditions of the Cor. of Thm. 1 plays an important role in representation theory.

It may be easily shown that any dual, cardinal product, lattice-homomorphic image, or interval sublattice of a complemented modular lattice, is itself a complemented modular lattice.

Ex. 1. Let F be any (commutative) field, and n any positive integer. For any α, ξ in $V(F; n)$, define $\alpha \rho \xi$ to mean $a_1x_1 + \cdots + a_nx_n = 0$.

(a) Show that the polarity induced by this relation shows that the lattice of subspaces of $V(F; n)$ is dually isomorphic to itself, under an "involution."

(b) Show that if F is "formally real" (i.e., if $x_1^2 + \cdots + x_n^2 = 0$ implies $x_1 = \cdots = x_n = 0$), then the polarity carries each subspace X into a complementary subspace (cf. §8).

Ex. 2. Prove the statements of the last paragraph of §2.

Ex. 3*. Show that every complemented non-modular lattice L of finite length contains a complemented non-modular sublattice of five elements which includes the O and I of L. (R. P. Dilworth, Tohoku Math. Jour. 47 (1940), 18–23.)

3. Projective geometries as lattices. Let M be any complemented modular lattice of finite length; we define "points" in M as usual, and "lines" as elements of M which cover points. Then evidently

PG1. Two distinct points are in one and only one line.

Again, it is easy to prove

PG2. If a line λ intersects two sides of a triangle (not at their intersection), it also intersects the third side.

Proof. Let the two sides be $p \smile q$, $p \smile r$, and let the points of intersection be $q^* \leqq p \smile q$, $r^* \leqq p \smile r$. Since $q^* \neq p$, $\lambda = q^* \smile r^*$. To complete the proof, we compute

$$d[(q^* \smile r^*) \frown (q \smile r)] = d[q^* \smile r^*] + d[q \smile r] - d[q^* \smile r^* \smile q \smile r]$$
$$\geqq 2 + 2 - d[p \smile q \smile r] = 4 - 3 = 1,$$

where the inequality is obvious since $q^* \leqq p \smile q \smile r$, $r^* \leqq p \smile q \smile r$.

Definition. *A projective geometry is a system of points and lines satisfying* PG1, PG2, *and*

PG3. *Every line contains at least three points.*

It is called finite-dimensional if and only if

PG4. *There is a finite set of points such that any "flat" which contains them contains all space.*

A flat is a set of points which contains the line through p and q if it contains p and q.

It is evident that, for any $a \in M$, the set $S(a)$ of all points $p \leqq a$ is a flat.

Conversely, let S be any flat in M; we can write $s = \bigvee_S p_i = p_1 \cup \cdots \cup p_r$ as the join of a finite subset of $p_i \in S$; let $t = p_1 \cup \cdots \cup p_{r-1}$. If a point $q \leqq s = t \cup p_r$, then either $q \leqq t$—whence, by induction on r, we can assume $q \in S$—or $t < s$, in which case $p_r \leqq (q \cup p_r) \cap (t \cup p_r) = [(q \cup p_r) \cap t] \cup p_r$. Here $(q \cup p_r) \cap t$ is a point (or O, which is a trivial case) since

$$d[(q \cup p_r) \cap t] = d[q \cup p_r] + d[t] - d[q \cup p_r \cup t] = d[q \cup p_r] - 1 \leqq 1;$$

hence by induction (being in t) it is in S. Hence $q \in S$, so that $S = S(s)$, and M *is isomorphic to the lattice of flats of the associated projective geometry.*

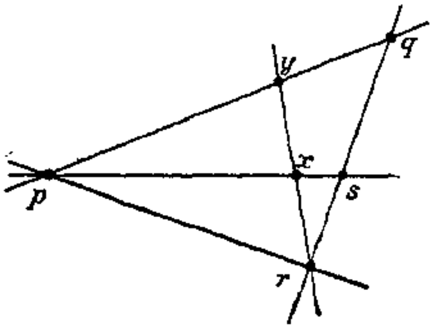

FIG. 8

Conversely, let P be any system satisfying PG1-PG2. We let $p \cup q$ denote the (unique) line through p and q. Postulate PG1 asserts that $p \cup q = q \cup p$, and further that if r is on $p \cup q$, then (since $p \cup r$ and $p \cup q$ both contain p and r) $p \cup r = p \cup q$.

THEOREM 3.[3] *The flats of any space satisfying* PG1-PG2 *form a complete complemented modular lattice, in which the "join" of any two flats S and T is the set of all points on lines $s \cup t$ joining S with T, provided neither S nor T is void and they are not both the same point.*

Proof. By Thm. 1, Ch. IV, the flats form a complete lattice. We next consider $S \cup T$. Suppose $p \in s \cup t$, $q \in s' \cup t'$ $[s, s' \in S; t, t' \in T]$, and $x \leqq p \cup q$. If we can show $x \leqq s'' \cup t''$ $[s'' \in S, t'' \in T]$, then we will know that the set of points on lines joining S and T is a flat. But (except in the cases noted) it clearly contains S and T, and is contained in any flat containing S and T; hence it will be the lattice-join of S and T, as asserted.

In general, let $X \vee Y$ denote the set of points on lines joining X and Y; we shall show that, for distinct points, not only is $p \vee q = q \vee p$ (which is obvious), but $p \vee (q \vee r) = (p \vee q) \vee r$; by symmetry and P2, it is enough to show that

[3] Theorem 3 is due to W. Prenowitz, *Projective geometries as multigroups*, Am. J. Math. 65 (1943), 235–56, and O. Frink [2]. For a generalization to descriptive geometries and matroid lattices, see W. Prenowitz, *Descriptive geometries as multigroups*, Trans. Am. Math. Soc. 59 (1946), 333–80. Also *Total lattices of convex sets and of linear spaces*, Annals of Math. 49 (1948), 659–88.

$p \vee (q \vee r) \leqq (p \vee q) \vee r$. But if $x \in p \vee (q \vee r)$, then $x \in p \vee s$, where $s \in q \vee r$. Now form $r \vee x$; it will intersect $q \vee r$ at some point y by PG2: Since $r \vee x$ meets two sides of the triangle pqs, it must meet the third. But $y \in p \vee q, x \in y \vee r = (p \vee q) \vee r$, completing the proof. (The case p, q, r collinear is trivial.)

Using these laws L2–L3, we have above

$$x \in (s \vee t) \vee (s' \vee t') = (s \vee s') \vee (t \vee t'),$$

so that $x \leqq s'' \vee t''$ for some $s'' \in s \smile s', t' \in t \smile t'$, as desired.

Finally, the lattice of flats is modular. Suppose $S \leqq U$, and let x be any point of $(S \smile T) \frown U$; then $x \in S \smile T$ and $x \in U$. By the preceding result x is on some $s \smile t$ [$s \in S$, $t \in T$], but $x \in U$; hence $x \smile s \in S \smile U = U$, and so $t \in U$. We conclude that x is on $S \smile (T \frown U)$, proving $(S \smile T) \frown U \leqq S \smile (T \frown U)$. By the one-sided modular law (Ch. II, §4, (4)), we get L5.

Further, L7′ is obvious, and so we have L7 if PG4 holds. This proves

Corollary 1. *The class of finite-dimensional complemented modular lattices is identical with the class of lattices of "flats" of systems satisfying* PG1, PG2, *and* PG4.

Corollary 2. *The finite-dimensional complemented modular lattices satisfying* PG3 *are the lattices of flats of the various finite-dimensional projective geometries.*

Ex. 1. Show directly that under the operation $\vee$, the points of projective n-space generate a semi-lattice.

Ex. 2. Show that a line with n points can be expressed as the "projective line" of all points with coordinates in some division ring, if and only if $n = p^k + 1$ for some prime p and positive integer k.

Ex. 3. Let L be the modular lattice of all Ω-subgroups of the direct union of an infinite number of simple groups with operators. Show that L7, L7R, L7′, and L7R′ all hold.

Ex. 4. (a) Show that if R denotes the real field, and Q the skew-field of quaternions, then $PG(Q; 2)$ is isomorphic with a sublattice of $PG(R; 11)$.

(b) Infer that no lattice-theoretic identity is equivalent to Pascal's Theorem.[4]

4. Perspectivity and projectivity. As first observed by von Neumann [2, p. 19], the concept of "transposed intervals" introduced in Ch. V to obtain theorems of the Jordan-Hölder type is essentially equivalent to the concept of "perspectivity" as defined in classical projective geometry. Moreover the latter concept applies in a simple fashion to any complemented modular lattice, as follows.

Definition. *Two elements a and b of a complemented modular lattice are "perspective" if and only if they have a common complement c, called an "axis of perspectivity" for a and b.*

[4] The statements of M.-P. Schutzenberger, C. R. Paris 221 (1945), 218–20, imply that the Desargues Theorem can be characterized by a combinatorial identity as follows. Let a_1, a_2, a_3, a_4 be given. Define $b_{12} = (a_1 \smile a_2) \frown (a_3 \smile a_4)$, etc., $c_{12} = (b_{13} \smile b_{24}) \frown (a_1 \smile a_2)$, etc. The condition is $c_{13} \leqq c_{23} \smile c_{12}$.

It is well known that in projective geometries any two equidimensional elements (points, lines, etc.) are perspective; we shall see shortly that this property characterizes exactly projective geometries from other complemented modular lattices of finite length.

THEOREM 4. *Two elements a and b are connected by a sequence of perspectivities if and only if the ideals $[O, a]$ and $[O, b]$ are projective.*

Proof. If a and b are perspective by c, then $[O, a]$, $[c, I]$, and $[O, b]$ are transposes in that order; hence $[O, a]$ and $[O, b]$ are projective. Since projectivity is a transitive relation, $[O, a]$ and $[O, b]$ are projective (in the sense of Ch. V) if they are connected by a sequence of perspectivities. Conversely, let $[O, a]$ and $[O, b]$ be projective, and let $[u \frown v, v]$ and $[u, u \smile v]$ be any adjacent intervals in the sequence of transpositions connecting (by definition) $[O, a]$ and $[O, b]$. Then by the Lemma of §1, any relative complements w of $u \frown v$ in v and w_1 of u in $u \smile v$ are perspective by any $(u \smile v)' \smile t$, where t is any relative complement of $u \frown v$ in u. (Proof: Consider the chains $O \leqq u \frown v \leqq u \leqq u \smile v \leqq I$ and $O \leqq u \frown v \leqq v \leqq u \smile v \leqq I$.) Hence, by induction, any relative complements of O in a and O in b are connected by a sequence of perspectivities. But a and b are the only such relative complements, q.e.d.

Ex. 1. Show that c is a relative complement of a in b (where $a \leqq b$), if and only if $c = a' \frown b$ for some complement a' of a.

Ex. 2. Show that a and b are perspective if d exists with $a \frown d = b \frown d = O$ and $a \smile d = b \smile d$.

Ex. 3. Show that, above, w and w_1 are actually perspective by $(u \frown v)' \smile u$.

5. Congruence relations and endomorphisms. It is evident that if a is a neutral element of any lattice (Ch. II, §10), then the principal ideal $[O, a]$ is a congruence module for the endomorphism $x \rightarrow x \smile a$. Conversely, if L is a relatively complemented lattice satisfying the ascending chain condition, then for any congruence relation θ, the ideal of elements $x \equiv O\ (\theta)$ is a principal ideal, $[O, a]$. Moreover by Ch. II, §6, $x \equiv y\ (\theta)$ in L if and only if some $w \leqq a$ is a relative complement of $x \frown y$ in $x \smile y$. But this implies

$$x \smile a = x \smile w \smile a \geqq (x \frown y) \smile w \smile a = x \smile y \smile a \geqq y \smile a,$$

and similarly $y \smile a \geqq x \smile a$, whence $x \smile a = y \smile a$. Conversely, $x \smile a = y \smile a$ and $a \equiv O\ (\theta)$ imply $x = x \smile O \equiv y \smile O = y\ (\theta)$. This proves the following result.

LEMMA 1. *In any relatively complemented lattice satisfying the ascending chain condition, every congruence relation is associated with a lattice-endomorphism $x \rightarrow x \smile a$.*

Combining with Thm. 13 of Ch. V, and the observation that any complemented modular lattice is relatively complemented, we get (cf. Thm. 3, Ch. II)

THEOREM 5. *The congruence relations on a complemented modular lattice L of finite length correspond one-one with the neutral elements a of L.*

The correspondence is, in fact, with the endomorphism $x \to x \smile a$ induced by a. We note here also a consequence of Ch. II, Thm. 9, Cor.

COROLLARY. *The following conditions on an element a of a complemented modular lattice are equivalent:* (i) *a is neutral,* (ii) *a is in the center.*

There follows immediately, comparing with Ch. I, §9, the following result.

LEMMA 2. *Any complemented modular lattice of finite length is a cardinal product of complemented modular lattices without proper congruence relations.*

Such lattices may be called *simple*, in the general sense that any algebra is "simple" if it has no non-trivial congruence relations (i.e., none except O and I). This definition of universal algebra includes as special cases the usual definitions of simple groups, simple rings, and simple linear algebras.

6. Factorization theorem. We next show that the only simple complemented modular lattices of finite length are **2** and projective geometries (more precisely, lattices consisting of the flats of a suitable projective geometry—which we shall call "projective geometries," by way of abbreviation).

LEMMA 3. *Two points p and q are perspective if and only if $p \smile q$ contains a third point s.*

Proof. Let a be the axis of perspectivity; then

$$d[a \frown (p \smile q)] = d[a] + d[p \smile q] - d[a \smile p \smile q] = d[I] - 1 + 2 - d[I]$$

and so $a \frown (p \smile q)$ is a third point on $p \smile q$. Conversely, if s is a third point on $p \smile q$, then, since p, s, and $(p \smile q)'$ are independent elements with join I, $e = (p \smile q)' \smile s$ is complementary to p; similarly, it is complementary to q, and so p and q are perspective.

Now let a be an axis of perspectivity for p and q, and b one for q and r. Let s and t be third points on $p \smile q$ resp. $p \smile r$. Then $u = (q \smile t) \frown (r \smile s)$ is by V1 a point; similarly, so is $(p \smile q) \frown (q \smile r)$—and in fact, a third point on $q \smile r$. Hence by Lemma 3, perspectivity between points is a transitive relation.[5] That is, two points are projective if and only if they are perspective.

It follows, by Thm. 10 of Ch. V, that in a "simple" complemented modular lattice L of finite length, all points are perspective. Hence, by Lemma 3, every line of L contains at least three points; i.e., PG3 is satisfied. Hence, by Lemma 2, we have

THEOREM 6. *Any complemented modular lattice of finite length is (uniquely) a direct union (i.e., cardinal product) of projective geometries.*

The case of **2**, consisting of the void set and a point alone, is exceptional; cf. Ex. 1 below.

COROLLARY. *Each of the following conditions on a complemented modular*

[5] This result is due to the author [2, Lemma 2]; perspective points were termed "conjoint." Thm. 6 below is due to the author (cf. [2, p. 747]; also Bull. Am. Math. Soc. **40** (1934), p. 209); it is also stated in Menger [3].

lattice L of finite length is necessary and sufficient that it be a projective geometry: (i) *L is simple,* (ii) *L is directly indecomposable,* (iii) *all points of L are perspective,* (iv) *all points of L are projective,* (v) *any two valuations of L are linearly dependent.*

We leave the details of proof to the reader. Slightly less trivial is the following result.

THEOREM 7. *In a projective geometry, the following conditions are equivalent:* (a) $d[x] = d[y]$, (b) *x and y are perspective,* (c) *x and y are projective.*

Proof. The implications $(b) \to (c) \to (a)$ are obvious, if we use V1. Now suppose $d[x] = d[y] = r$, and let $p_1, \cdots, p_r$ and $q_1, \cdots, q_r$ be bases for $x - x \frown y$ and $y - x \frown y$ respectively. Let $t_1, \cdots, t_r$ be third points on $p_1 \smile q_1, \cdots, p_r \smile q_r$. Then evidently

$$x \smile t_1 \smile \cdots \smile t_r = (x \frown y) \smile p_1 \smile t_1 \smile \cdots \smile p_r \smile t_r$$

$$= (x \frown y) \smile p_1 \smile q_1 \smile \cdots \smile p_r \smile q_r = x \smile y$$

and so by dimensionality, $x \frown y$, the p_i, the t_j, and $(x \smile y)'$ are independent elements whose join is I. Hence $(x \smile y)' \smile t_1 \smile \cdots \smile t_r$ and $x = (x \frown y) \smile p_1 \smile \cdots \smile p_r$ are complements; likewise, it and y are complements, whence x and y are perspective, proving $(a) \to (b)$, q.e.d.

Ex. 1. Interpret the statement: any complemented modular lattice of finite length is a direct union of a Boolean algebra 2^n with projective lines, planes, etc.

Ex. 2. Prove the Cor. of Thm. 6. Which conditions of this corollary are contained in Thm. 7?

Ex. 3. (a) Show that if a and a_1 are perspective in A, then they are also perspective in $A \times B$, for any B.

(b) Show that perspectivity is transitive (i.e., that perspectivity and projectivity are equivalent) in any complemented modular lattice of finite length.

Ex. 4. Show that, in a projective geometry of finite length, all lines contain the same number of points. (Hint: they are perspective.)

Ex. 5*. Show that not every modular lattice is isomorphic with a sublattice of a complemented modular lattice (Hint: Show first that if M is a sublattice of a complemented modular lattice all of whose prime quotients are projective, and if $[a, b]$ and $[a_1, b_1]$ are intervals of M of "length" three, then both or neither must define Desarguesian planes.[6]

Problem 55. Which modular lattices M can be represented as sublattices of complemented modular lattices L? If this is possible, can one make the length of L equal to that of M? (Dilworth-Hall)

7. Automorphisms as collineations; projectivities. Consider $PG(R; n)$ as the lattice of all subspaces of the $(n + 1)$-dimensional vector space $V(R; n + 1)$ of $(n + 1)$-vectors $\xi = (x_0, x_1, \cdots, x_n)$ with homogeneous coordinates in a division ring (i.e., field or skew-field) R. Evidently any lattice-*automorphism* of $PG(R; n)$ carries points into points, lines into lines, and collinear points into collinear points, all terms being taken in their usual projective sense. Such

[6] See M. Hall and R. P. Dilworth, *The imbedding problem for modular lattices*, Annals of Math. 45 (1944), 450–456; also for Problem 55.

transformations will be called *collineations*;[7] conversely, any collineation of $PG(R; n)$ is evidently a lattice-automorphism.

Let $x \to \omega(x)$ be any automorphism of R, and $A = \| a_{ij} \|$ be any $(n + 1) \times (n + 1)$ non-singular matrix with coefficients in R. Then the correspondence $\xi \to \eta$ of $V(R; n + 1)$ defined by

$$(1) \qquad y_i = a_{i0}\omega(x_0) + a_{i1}\omega(x_1) + \cdots + a_{in}\omega(x_n)$$

is called a *semi-linear* transformation.[8] Since it preserves linear dependence, though with altered coefficients, (1) defines a collineation (lattice-automorphism) of $PG(R; n)$. The following result is known.

THEOREM 8. *Every collineation of $PG(R; n)$ is given by a transformation of the form* (1), provided $n > 1$.

Sketch of proof. Let α: $\xi \to \alpha(\xi)$ be any collineation of $PG(R; n)$; using homogeneous coordinates, let $\epsilon_0, \cdots, \epsilon_n$ be unit vectors $(1, 0, \cdots, 0), \cdots, (0, 0, \cdots, 1)$ of $V_{n+1}(R)$. By a "projectivity" $\eta \to \zeta$, where $\zeta = (z_0, z_1, \cdots, z_n)$ is given by

$$(2) \qquad z_i = b_{i0}y_0 + b_{i1}y_1 + \cdots + b_{in}y_n,$$

we can reduce to the case $\alpha(\epsilon_i) = \epsilon_i$, and $(1, 1, \cdots, 1)$ goes into itself. But with reference to the ϵ_i the homogeneous coordinates of ζ are uniquely determined; thus $(\zeta \cup \epsilon_2 \cup \cdots \cup \epsilon_n) \cap (\epsilon_0 \cup \epsilon_1)$ projects η uniquely on the line $\epsilon_0 \cup \epsilon_1$. Comparing with $(\xi \cup \epsilon_2 \cup \cdots \cup \epsilon_n) \cap (\epsilon_0 \cup \epsilon_1)$, we establish one-one correspondences $x_i \leftrightarrow z_i$ between the coordinates of ξ and those of ζ. Moreover since the correspondence is a collineation, von Staudt's algebra of throws (see Veblen and Young [1, Ch. VI]) is preserved; hence the correspondences give ring-automorphisms ω_i with $z_i = \omega_i(x_i)$. Since $(1, 1, \cdots, 1)$ is invariant, all ω_i are equal, and $z_i = \omega(x_i)$. The proof is completed by observing that if A is the matrix inverse to the B of (2), then (1) is obtained explicitly.

Since $\omega^{-1}(\sum a_{ki}\omega(x_i)) = \sum \omega(a_{ki})x_i$, it is easily seen that the projectivities of $PG(R; n)$ form a normal subgroup of the group of all collineations. It may be characterized lattice-theoretically, as the subgroup generated by perspectivities.

8. Correlations and polarities; orthocomplementation. Again, let us define a *correlation* of $PG(R; n)$ as any *dual* automorphism of the corresponding lattice. If R^* is the ring anti-isomorphic[9] to R, then the correspondence

$$(3) \quad (x_0, x_1, \cdots, x_n) \leftrightarrow y_0\omega(x_0) + y_1\omega(x_1) + \cdots + y_n\omega(x_n) = 0$$

---

[7] The sharp distinction made here between collineations and projectivities is not always made in the literature.

[8] For a discussion of semi-linear transformations, see N. Jacobson, *Theory of rings*, New York, 1943; the concept is due to C. Segre (1889).

[9] I.e., obtained by reversing the order of multiplication, but preserving addition. Cf. Albert [1, p. 96], where there are considered "involutions," or correspondences satisfying not only $\omega(x + y) = \omega(x) + \omega(y)$ and $\omega(xy) = \omega(y)\omega(x)$, but also $\omega(\omega(x)) = x$.

is easily shown to be a dual isomorphism between $PG(R; n)$ and $PG(R^*; n)$. But if α and β are any two dual isomorphisms, then $\alpha^{-1}\beta$ is an isomorphism; hence the most general dual isomorphism of $PG(R; n)$ onto $PG(R^*; n)$ is given by

$$(4) \qquad (x_0, x_1, \cdots, x_n) \leftrightarrow \sum_{i,j} y_i a_{ij} \omega(x_j) = 0.$$

Further, since R^* may be defined lattice-theoretically (or "combinatorially") by the algebra of throws, we get

THEOREM 9. *A projective geometry $PG(R; n)$ $[n \geqq 2]$ has a dual automorphism if and only if the division ring R is anti-isomorphic with itself. In this case there is a one-one correspondence* (4) *between correlations and non-singular bilinear forms.*[10]

We may write $\eta A \xi^* = 0$ to denote the fact that ξ lies in the $(n - 1)$-flat determined, through (4), by η; it is a kind of perpendicularity between ξ and η. In case it is symmetric, the correlation is termed a *polarity*; as in Ch. IV, §5, it is the condition

L9. $$(x')' = x \qquad \text{for any flat } x.$$

Writing $$0 = \omega^{-1}(0) = \sum x_j b_{ji} \omega^{-1}(y_i) \qquad [b_{ji} = \omega^{-1}(a_{ij})]$$
and noting that the roles of i and j are symmetric, we see that it is sufficient (and essentially necessary) that ω be an *involution*, so that $\omega(\omega(x)) = x$, and that A be "Hermitian" in the sense that $\omega(a_{ij}) = a_{ji}$. Further, if A is *definite*, in the sense that $\sum x_i a_{ij} \omega(x_j) = 0$ implies $x_0 = x_1 = \cdots = x_n = 0$, then, again as in Ch. IV, §5,

L10. $$x \frown x' = O \qquad \text{and} \qquad x \smile x' = I.$$

DEFINITION. *A modular lattice is called orthocomplemented if and only if it admits a dual automorphism $x \to x'$ satisfying* L9, L10. (*Of course, any dual automorphism satisfies*

L8. $$(x \frown y)' = x' \smile y' \qquad \textit{and} \qquad (x \smile y)' = x' \frown y'.)$$

For example if Q is the quaternion ring, if $\omega(x)$ is the quaternion conjugate of x, then the "definite diagonal Hermitian form" $\sum y_i \omega(x_i) = 0$ defines $PG(Q; n)$ as an orthocomplemented modular lattice. In general, it may be proved[11] that *every* orthocomplemented $PG(R; n)$ can be obtained (to within isomorphism) as above from an involution $x \to \omega(x)$ of R, and a definite diagonal Hermitian form $\sum y_i a_i \omega(x_i) = 0$, with $\omega(a_i) = a_i$.

Geometrical interest also attaches to "null systems," or polarities such that

$$(5) \qquad \xi \leqq \xi' \quad \text{for every projective point } \xi.$$

---

[10] For Thm. 9, see J. von Neumann [3]; and G. Birkhoff and J. von Neumann, *The logic of quantum mechanics*, Annals of Math. 37 (1936), p. 835 and appendix. Artin has informed me that a proof of Thm. 9 was obtained, but not published, by H. Zassenhaus, for $n > 2$.

[11] G. Birkhoff and J. von Neumann, loc. cit. supra. J. von Neumann [3, Part III] has further related the existence of orthocomplements to that of "Hermitian" idempotents in the coordinatization by regular rings.

For facts about null systems, which are correlated with skew-Hermitian matrices, we refer the reader to the literature.[12]

In conclusion, we note that the *free* orthocomplemented modular lattice with two generators may be shown to be $2^4 \times PG(J_3, 1)$, and has 96 elements; $PG(J_3, 1) = 1 \oplus 4 \oplus 1$.

Ex. 1. Show that the free orthocomplemented modular lattice generated by a chain of length n is the Boolean algebra 2^n.

Ex. 2. Show that orthocomplementation is possible in a direct union of lattices, if and only if it is possible in every factor.

Ex. 3. Show that the lattice of all subspaces invariant under a finite group of linear transformations of a real vector space is orthocomplemented.

Ex. 4. Show that the lattice of all closed subspaces of Hilbert space is orthocomplemented but non-modular.

Ex. 5. Show that in real and complex projective geometry, every orthocomplementation is equivalent (i.e., isomorphic) to that given by the usual inner product.[13]

Ex. 6. (a) Show that, in a "null system," $p \leqq q'$ implies $p' \geqq q$, and generalize this result.

(b) Infer that no plane projective geometry, whether Desarguesian or not, can be made into a null system.

Ex. 7. (a) Show that any "null system" in $PG(R; n)$ contains a chain $O < x_1 < x_2 < \cdots < x_{n-1} < I$ in which x_{i+1} covers x_i and $x_i' = x_{n-i}$.

(b) Show that if we take these to be coordinate subspaces, we can make the first two rows and columns of the "polarity" matrix $\| a_{ij} \|$ consist of zeros, except that $a_{01} = 1, a_{10} = -1$.

(c) By induction, show that n is odd, and that we can make $a_{2i,2i+1} = 1 = -a_{2i+1,2i}$, and all other coefficients zero.

(d) Infer that R must be commutative.

Problem 56. Which non-Desarguesian plane projective geometries admit orthocomplements?

9. Neutral elements and ideals. We have seen (Thm. 5, Cor.) that being *neutral* is equivalent to lying in the *center* of L. One can show further

THEOREM 10. *An element is in the center of a complemented modular lattice L if and only if it has a unique complement.*[14]

Proof. In any lattice $L = M \times N$, $[I, O]$ can have only $[O, I]$ for complement; hence no element of the center can have more than one complement. Conversely, suppose a has a unique complement a', and that $u \frown a = O$. Then by hypothesis u, a, and any complement $(u \smile a)'$ of $u \smile a$ are independent elements with join I, hence $u \smile (u \smile a)' = a'$ and $u \leqq a'$. Thus a' contains every u with $u \frown a = O$. In particular, since $[(a \frown x)' \frown x] = O$ irrespective of x, $(a \frown x)' \frown x$ is included in a' as well as x, and

$$x = (a \frown x) \smile [(a \frown x)' \frown x] \leqq (a \frown x) \smile (a' \frown x) \leqq x \smile x = x.$$

[12] W. C. Graustein, *Introduction to higher geometry*, Macmillan, 1940, pp. 467–471; R. Brauer, *A characterization of null systems in projective space*, Bull. Am. Math. Soc. 42 (1936), 247–254; R. Baer, *Null systems in projective space*, ibid., 51 (1945), 903–906.

[13] In Exs. 4–5, we use the terminology of M. H. Stone, *Linear transformations in Hilbert space*, pp. 17–21.

[14] This result is due to J. von Neumann [2, Part I, Thms. 5.3–5.4]. The statement of Thm. 4.5 of [LT] is incorrect.

Hence $x = (a \frown x) \smile (a' \frown x)$, and every $x \in L$ can be written in the form $y \smile z$ $[y \leqq a, z \leqq a']$. It follows from Thm. 7 of Ch. V that L is the cardinal product $[O, a] \times [O, a']$.

We now generalize Theorem 5.

THEOREM 11. *The congruence relations on L correspond one-one with the neutral ideals N of L, or ideals containing with any element a all perspective elements.*

Proof. Suppose that N defines a congruence relation on L, as in Thm. 3, Ch. II, and that $a \in N$ and b are perspective, with the axis of perspectivity c. Then

$$b = b \frown I = b \frown (a \smile c) \equiv b \frown c = O \pmod N.$$

Hence $b \in N$, and N is neutral. Conversely, let N be neutral, and let $x \equiv y$ mean $x \smile a = y \smile a$ for some $a \in N$. This is an equivalence relation and even a join-homomorphism, for any ideal in any lattice (Ch. II, §6, Ex. 3). We wish to show that $x \equiv y$ implies $x \frown u \equiv y \frown u$ in a complemented modular lattice, if N is neutral. Since we are dealing with an equivalence relation, and $x \equiv x \smile a = y \smile a \equiv y$, we can reduce to the case $y = x \smile a$; hence *it is suffiient to show that*

$$(x \frown u) \smile a \equiv [(x \smile a) \frown u] \smile a = (x \smile a) \frown (u \smile a),$$

in any modular lattice. But setting $x = x_1$, $u = x_2$, $a = x_3$, this is equivalent to showing that $c_3 \equiv b_3$ in the free modular lattice with three generators (Ch. V, §3). By inspection, $[b_3, c_3]$ is however projective to part of x_3. Hence by Thm. 4, $x_3 = a$ and some element d containing $c_3 \frown b_3'$ are perspective. Hence

$$c_3 \frown b_3' \in N, \text{ and } b_3 \equiv b_3 \smile (b_3' \frown c_3) = c_3,$$

completing the proof.

A special discussion of congruence relations in metric complemented modular lattices may be found in S. Gorn, *Homomorphisms and modular functionals*, Trans. Am. Math. Soc. 51 (1942), 103–15.

Ex. 1. Show directly that an ideal of a complemented modular lattice is neutral in the sense of Thm. 11, if and only if it is neutral in the sense of Ch. V, §8, Ex. 3.

Ex. 2. Construct a modular lattice of ten elements, containing 3^2 as a sublattice, one of whose elements has a unique complement without being neutral. (M. Hall)

Ex. 3. Show that a complemented modular lattice of finite length is a projective geometry, if and only if O, I are the only elements with unique complements.

10. Continuous-dimensional projective geometries. A remarkable class of metric complemented modular lattices, whose dimension function varies continuously between zero and one, was discovered by von Neumann [1].

Let F be any field or skew-field. If a and a' are complementary $(n-1)$-dimensional elements of $PG(F; 2n-1)$, then the sublattices X and Y of $x \leqq a$ and $y \leqq a'$ are clearly isomorphic with $PG(F; n-1)$; hence they are isomorphic with each other. A typical case is furnished by letting a and a' be skew lines in projective space. Moreover since a and a' are independent, by Thm. 7 of Ch. V, the joins $x \smile y$ [$x \in X, y \in Y$] form a *sublattice* isomorphic to $XX = X^2$, in PG(F; $2n - 1$). But the following inference is obvious:

LEMMA 1. *The couples* $[x, x]$ *of* X^2 *form a sublattice of* X^2 *which is isomorphic with* X, *under an isomorphism which carries* O *into* O, I *into* I, *and multiplies lattice dimension* $d[x]$ *by two.*

(We note that $d[x]$ exceeds the ordinary geometrical dimension of x by one.) We conclude that $PG(F;\ n - 1)$ can be embedded isomorphically in $PG(F;\ 2n - 1)$, so that the "normalized dimension function" $d[x]/d[I]$ is preserved. Repeating the process, we get a sequence of extensions of $PG(F; 1)$,

$$PG(F; 1) \leqq PG(F; 3) \leqq PG(F; 7) \leqq \cdots \leqq PG(F; 2^n - 1) \leqq \cdots$$

in which the lattice operations and also the "normalized dimension function" $d[x]/d[I]$ are preserved.

Taking the union of these extensions, we get an enveloping *metric lattice* which contains elements of every conceivable dyadic lattice dimension $k/2^n$. By Thm. 14 of Ch. V, this is a metrically dense sublattice of a *complete* metric lattice, which will therefore contain elements of every dimension d, $0 \leqq d \leqq 1$. This last is the "continuous geometry" $CG(F)$ of von Neumann, having F as base field.[15]

THEOREM 12. *For any* F, $CG(F)$ *is a complemented modular and complete metric lattice, in which any two equidimensional elements are perspective.*

Sketch of proof. We first show that the metric completion $\bar{M}$ of any metric complemented modular lattice M is complemented. Indeed, given $a \in \bar{M}$, we can find $\{a_n\}$ in M such that $\delta(a_n, a) < 2^{n+1}$, whence $\delta(a_n, a_{n+1}) < 2^n$. By Theorem 2, to any complement a_n' of a_n there corresponds a complement a_{n+1}' of a_{n+1}, with $\delta(a_{n+1}', a_n) < 2^n$; it follows that a_n' is a convergent sequence, whose limit a' will (by formulas (7)–(7′) of Ch. V, §7) satisfy $a \frown a' = 0$, $a \smile a' = I$.

The proof that any two equidimensional elements are perspective is similar; we construct a convergent sequence of axes of perspectivity c_n for a_n, b_n. As in Thm. 2, we reduce to the case $a_{n+1} < a_n$ and its dual. Suppose a, b are perspective by c in M, and that $a > a_1$, $b > b_1$, with $\delta(a, a_1) = \delta(b, b_1) = \delta_1$. Then by hypothesis, $c \smile a_1$, $c \smile b_1$ will have a common complement q, with $d[q] = \delta_1$; and so a_1, b_1 will be perspective by $c \smile q$, where $\delta(c \smile q, c) = \delta_1$.

Dually, suppose $a_2 > a$, $b_2 > b$, with $\delta(a, a_2) = \delta(b, b_2) = \delta_2$. Then $d[a_2 \frown c] = d[b_2 \frown c] = \delta_2$; and any common *relative* complement r of $a_2 \frown c$ and $b_2 \frown c$ in c will satisfy $\delta(c, r) = \delta_2$. Further, a_2 and b_2 will be perspective by r.

Ex. 1. Let $L_1 \leqq L_2 \leqq L_3 \leqq \cdots$ be any sequence of metric lattices. Show that their union is a metric lattice.

---

[15] An interesting construction analogous to von Neumann's has been suggested by Aronszajn and Glivenko (Glivenko [2, p. 40]). All the results stated here are due to von Neumann.

Ex. 2. Let M be any metric lattice, and $\bar{M}$ its metric completion. Show that if M is complemented, then so is $\bar{M}$.

Ex. 3*. In the notation of Ex. 2, can you prove that if any two equidimensional elements are perspective in M, the same is true of $\bar{M}$? (The corresponding proposition for relative complements is straightforward.)

Ex. 4*. Let M be any irreducible complemented modular lattice of a finite length $n > 3$ which is also a compact topological lattice with $n + 1$ connected components under an extrinsic topology. Show that the coordinate-field of M, if of characteristic infinity, consists of the real, complex or quaternion numbers.[16]

Ex. 5*. Let M be any matroid lattice of finite length, which is also a locally compact topological lattice under an extrinsic topology. Define tangent lines and osculating planes to curves, so as to generalize the usual definitions. Generalize to tangent planes and (using circle-geometry) osculating circles.[17]

Ex. 6. Show that every automorphism of any of the PG(D; 2^{n-1}) generating $CG(D)$ can be extended to an automorphism of $CG(F)$.

Ex. 7.* (a) Show that in the (irreducible) complemented modular lattice of all subspaces of an infinite-dimensional vector space $V(R; \aleph_0)$, some elements x are projective with elements $y < x$.

(b) Infer that perspectivity is not transitive.

Ex. 8*. Show that the continuous geometry over the quaternion ring Q is lattice-isomorphic with the continuous geometry over the real field R^*, but not with that over the complex numbers. (von Neumann)

Problem 57. Is the completion by cuts of any complemented modular lattice necessarily modular? (See Ch. IX, §6, where refs. are given to proofs that the correspondence results for uncomplemented modular lattices is false.)

Problem 58. Need a complete complemented topological lattice be a topological lattice? (S. Gorn)

Problem 59. Is perspectivity transitive in every orthocomplemented modular lattice?

Problem 60. Characterize abstractly to within isomorphism, and as a metric group, the group of all isometries of $CG(F)$. Is it connected if F is real?

11. Converse results; coordinates in "regular rings." We know by Thm. 15 of Ch. V that $CG(F)$ is a topological lattice.

Von Neumann [2] has proved conversely that, in any complete, topological,[18] complemented modular lattice, whose center consists of O and I alone, one can introduce a dimension function, which becomes unique when "normalized" to make $d[O] = 0$, $d[I] = 1$.

To do this, he first defines $d[x] = d[y]$ as a relation which holds if and only if x and y are perspective. Then he proves that perspectivity is transitive, which justifies the use of the equality symbol. He then defines $d[x] \leqq d[y]$ to mean that x is perspective with a part of y. Then he proves that this relation simply orders his abstract "dimensional elements." Next, he defines addition of "dimensional elements," by making $x \frown y = O$ imply $d[x \smile y] = d[x] + d[y]$. He shows that this operation is commutative and associative. Finally, he shows

[16] See A. Kolmogoroff, Annals of Math. 33 (1932), 163–76.

[17] Cf. O. Haupt, G. Nobeling, and Chr. Pauc, op. cit. in Ch. VII, §3.

[18] He assumes continuity hypotheses involving any transfinite sequence. For additional literature, see I. Halperin, Trans. Am. Math. Soc. 44 (1938), 537–62; S. Gorn, Trans. Am. Math. Soc. 51 (1942), 103–16; and T. Iwamura, Jap. Jour. Math. 19 (1944), 57–71.

that the ordered additive system so constructed is isomorphic either with the system $0, 1/n, 2/n, \cdots, (n-1)/n, 1$, or with the continuum $0 \leqq x \leqq 1$ (the continuous-dimensional case). This justifies calling such a lattice an "abstract continuous geometry" in the latter case.

We have seen that any projective geometry of finite length $n > 3$ is isomorphic with the lattice $PG(n-1; D)$ of all subspaces of the n-dimensional linear space with coordinates in a suitable division ring D. J. von Neumann [3] has shown[19] that any abstract continuous geometry can be given analogous "ring-coordinates." We describe the analogy in the finite-dimensional case.

It is easily shown that $PG(n-1; D)$ is isomorphic with the lattice of all left-ideals of the "simple" ring of all $(n \times n)$ matrices over D. Moreover if R is any "semi-simple" ring in the usual sense, the lattice $L(R)$ of all its left-ideals is still complemented and modular. Conversely, one can obtain in this way all complemented modular lattices which satisfy Desargues' Theorem; cardinal products (direct unions) of lattices correspond to direct sums of rings. Thus von Neumann's "ring-coordinatization" has the outstanding advantage over von Staudt's "field-coordinatization," that it coordinatizes *reducible* (Desarguesian) complemented modular lattices.

A linear associative algebra R with finite basis is "semi-simple" in the usual sense if and only if it is "regular" in the sense that (6) every $a \in R$ has a "relative inverse" x, such that $axa = a$. Moreover this condition applies also to rings with an infinite basis or no basis over the center, giving a significant generalization.

It may be shown that two regular rings are isomorphic if and only if the complemented modular lattices of their left-ideals are isomorphic, and anti-isomorphic if and only if the latter are dually isomorphic. Also, two-sided ideals, which correspond in the usual "semi-simple" case to idempotents in the "center" of the ring, constitute the "center" of the lattice of left-ideals.

It may be shown that if the quotient I/O of an abstract continuous geometry can be divided into four mutually perspective parts, coordinates in a regular ring may be introduced; the added hypothesis is needed to exclude the non-Desarguesian case.

Proofs of all the preceding results may be found in von Neumann [3], where they were originally obtained.

Ex. 1. Prove that if $R + S$ is the direct sum of two regular rings, then the lattice $L(R + S)$ of left-ideals of $R + S$ is the direct union $L(R + S) = L(R) \times L(S)$ of the lattices of left-ideals of R and S independently.

Ex. 2*. Let $R \times S$ be the direct product of two regular rings. Show that $L(R \times S)$ may be described by the properties that it contains sublattices B and C which (i) are isomorphic with $L(R)$ and $L(S)$ respectively, (ii) have the same O and I as $L(R \times S)$, (iii) generate $L(R \times S)$, (iv) make (b, c) a distributive pair for all $b \in B, c \in C$, and (v) make $b \frown c = 0$ imply $b = 0$ or $c = 0$. (von Neumann)

Problem 61. Is a synthetic definition of $L(R \times S)$ in terms of $L(R)$ and $L(S)$ possible? Note Ex. 2. (von Neumann)

[19] For further literature, see F. Maeda, Jour-Sci. Hiroshima Univ. 8 (1939), 145–67, and 9 (1939), 73–84.

12. Atomic modular lattices. Consider the complete modular lattice $PG(R; d)$ of all vector subspaces of a vector space of infinite dimension d over a division ring R. (The "dimension" of a finite or infinite-dimensional vector space V is the number of elements in a basis of V.) Clearly each non-zero vector ξ generates a minimal proper subspace, the set of all scalar multiples of ξ. Hence in $PG(R; d)$, I is the join of "points" (actually, projective points)—i.e., L7′ holds. Further, as always with subalgebras (Ch. IV, §10, Ex. 3b), we have meet-continuity,

$$y_\alpha \uparrow y \text{ implies } x \frown y_\alpha \uparrow x \frown y. \tag{7}$$

We can now draw some lattice-theoretic inferences.

THEOREM 13. *In a complete modular lattice M satisfying* (7), L7′ *implies* L7, L7R, *and* L7R′.

Proof. Suppose the points of M to be well-ordered, as $p_1, p_2, p_3, \cdots, p_\omega, \cdots$. Define $a_\alpha = \bigvee_{\tau<\alpha} p_\tau$; then clearly $a_1 = 0$, $a_{\alpha+1} = a_\alpha \smile p_\alpha$, and, if λ is a limit-ordinal, $a_\lambda = \bigvee_{\alpha<\lambda} a_\alpha$. We shall first prove L7; by Thm. 1, this implies L7R.

We define $y_1 = 0$, and y_α recursively by transfinite induction as follows. (I) If $x \smile a_{\alpha-1} = x \smile a_\alpha$, set $y_\alpha = y_{\alpha-1}$. (II) If $x \smile a_\alpha \neq x \smile a_{\alpha-1}$, set $y_\alpha = y_{\alpha-1} \smile p_\alpha$. (III) If λ is a limit ordinal, set $y_\lambda = \bigvee_{\alpha<\lambda} y_\alpha$. We shall prove by induction that $x \frown y_\alpha = 0$, $x \smile y_\alpha = x \smile a_\alpha$; since some $a_\alpha = I$ by hypothesis L7′, this will give a complement of x. In Case I, $x \frown y_\alpha = x \frown y_{\alpha-1} = 0$, $x \smile y_\alpha = x \smile y_{\alpha-1} = x \smile a_{\alpha-1}$, by hypothesis and induction. In Case III, $0 = x \frown y_\alpha$ for all $\alpha < \lambda$ by induction, but $x \frown y_\alpha \uparrow x \frown y_\lambda$ by the hypothesis $y_\alpha \uparrow y_\lambda$ and (7); hence $x \frown y_\lambda = 0$. Similarly, $x \smile a_\alpha = x \smile y_\alpha \uparrow x \smile y_\lambda$ (cf. Ch. IV, §9); but $a_\alpha \uparrow a_\lambda$; hence $x \smile y_\lambda = x \smile a_\lambda$. In Case II, observe that x, $y_{\alpha-1}$, p_α are *independent* in the sense of Ch. V, §5, since $x \frown y_{\alpha-1} = 0$ by induction, and since $(x \smile y_{\alpha-1}) \frown p_\alpha = (x \smile a_{\alpha-1}) \frown p_\alpha$ (by induction) $\neq 0$ would imply $p_\alpha \leqq x \smile a_{\alpha-1}$ and $x \smile a_\alpha = x \smile a_{\alpha-1} \smile p_\alpha = x \smile a_{\alpha-1}$, contrary to hypothesis. Hence $x \frown y_\alpha = x \frown (y_{\alpha-1} \smile p_\alpha) = 0$. Finally, $x \smile y_\alpha = x \smile y_{\alpha-1} \smile p_\alpha = x \smile a_{\alpha-1} \smile p_\alpha$ (by induction) $= x \smile a_\alpha$, completing the proof of L7, and hence of L7′.

It remains to prove L7R′; we shall show by transfinite induction that every interval $[0, a_\alpha]$ satisfies L7R′; we can now assume L7 and L7R for all $a_\lambda = \bigvee_{\alpha<\lambda} p_\alpha$, and L7R′ for all a_λ preceding a_α.

Case I: $\alpha = 1$. This is trivial; even for α finite, we need only use the Cor. of Thm. 1.

Case II: $\alpha - 1$ exists. Let x' and $x \frown a_{\alpha-1}$, and let y be any relative complement of x' in $[0, a_{\alpha-1}]$, so that $x' \frown y = 0$, $x' \smile y = a_{\alpha-1}$. We shall write p for $p_{\alpha-1}$, for brevity.

Subcase IIa: $x \frown y > 0$. Write $x \frown y = q$; it is a point since x covers x' and $x' \frown y = 0$. Hence $x' < x' \smile q \leqq x$; but x covers x', whence $x' \smile q = x$. But x' is a join of points by induction; hence so is x.

Subcase IIb: $x \frown y = 0$. If $x \leqq a_{\alpha-1}$, then x is a join of points by induction on α. Otherwise $x \smile a_{\alpha-1} > a_{\alpha-1}$; but since $a_\alpha \geqq x \smile y \geqq x \smile x' \smile y = x \smile a_{\alpha-1} > a_{\alpha-1}$ and a_α at most covers $a_{\alpha-1}$, this implies $x \smile y = a_\alpha$ and (since $a_{\alpha-1} \smile p > a_\alpha$) $p \frown a_{\alpha-1} = 0$. Define $r = (p \smile y) \frown x$. If r were 0, then (since $p \frown y \leqq p \frown a_{\alpha-1} = 0$), p, y, x would be independent (Ch. V, §5), which is impossible since $(x \smile y) \frown p = a_\alpha \frown p > 0$. Hence $r > 0$; but since $(p \smile y) \frown x$ at most covers $(0 \smile y) \frown x = 0$, r is a point. Moreover

$$r \smile x' = [(p \smile y) \frown x] \smile x' = x \frown [p \smile y \smile x'] \text{ (by L5)}$$
$$= x \frown (p \smile a_{\alpha-1}) = x.$$

Hence x is a joint of points (x' is by induction).

Case III: λ is a limit-number. Every $x \leqq a_\lambda$ satisfies $x \frown a_\alpha \uparrow x \frown a_\lambda = x$ by (7). But each $x \frown a_\alpha$ is a join of points, by induction. Taking the join of all these points, we express $x = \sup (x \frown a_\lambda)$ as a join of points. This completes the proof of L7R′.

Definition. *A complete modular lattice which satisfies* (7) *and* L7′ (*and hence* L7, L7R, L7R′) *will be called atomic.*

Corollary (*Frink*). *The lattice of all subspaces of any vector space is a complete atomic modular lattice.*

Ex. 1. Show that for modular lattices of finite length, being atomic is equivalent to being complemented.

Ex. 2. (a) Show that if a complemented modular lattice L of finite length contains a chain C, then it contains a dual chain C consisting of complements of elements of C.

(b) Infer that if a complemented modular lattice M satisfies the ascending chain condition, then it satisfies the descending chain condition.

(c*) Is it true that if M is $\uparrow$-atomic in the sense of Ch. III, §4, then it is $\downarrow$-atomic?

Ex. 3. Let L consist of all finite-dimensional subspaces of an infinite-dimensional vector space V, and V itself. Show that L is a complete modular lattice satisfying L7′ and L7R′ but not (7), L7, or L7R.

Ex. 4*. Let D be the lattice of all dual ideals of a continuous geometry $CG(F)$. Show that D is not complemented, though all its elements are joins of points (atoms). (O. Frink)

13. Frink's decomposition theorems. We shall now summarize the proofs of some fundamental results due to Frink [2]; the reader is referred to Frink's paper for details.

First, since L7′ and (7) are obviously satisfied, we note as an immediate corollary of Thm. 13 that the flats of any system of points and lines satisfying PG1–PG2 form a complete atomic modular lattice. But conversely, exactly as in §3, the points and lines of any complete atomic modular lattice M satisfy PG1–PG2. Moreover M is isomorphic with the lattice of all the "flats" of this system. This generalizes Thm. 3, by establishing a one-one correspondence between systems satisfying PG1–PG2 and complete atomic modular lattices M.

Again, as in §6, one can divide the points of M uniquely into disjoint classes $S_1, S_2, S_3, \cdots$ of mutually perspective points. The flats of any class S_i of mutually perspective points satisfy PG3, and form what may be called an *atomic projective geometry*. One may show quite easily that M is a sublattice of the direct union (cardinal product) of these. We conclude

THEOREM 14. *Any complete atomic modular lattice is a sublattice of a direct union of atomic projective geometries—and conversely.*

Further, apart from certain finite projective lines and non-Desarguesian projective planes, coordinates in a division ring R can be introduced into any atomic projective geometry, through von Staudt's "algebra of throws." Now let d be the cardinal number of a maximal independent subset of S_i (the existence of this follows since independence is a property of finite character). Frink [2] has shown that if d is infinite, the atomic projective geometry is simply the $PG(R; d)$ of §12; the finite-dimensional case has already been discussed. Since we demonstrated the converse in the Cor. of Thm. 13, we have

THEOREM 15. *Apart from the well-known exceptional projective lines and non-Desarguesian projective planes, every atomic projective geometry is isomorphic with the lattice of all vector subspaces of the vector space $V(R; d)$ of a suitable dimension-number d over a suitable division ring R.*

Finally, let L be *any* complemented modular lattice, not necessarily atomic or complete. We first recall that, by Thm. 12 of Ch. V, the lattice of all ideals of L is modular—hence so is the lattice of all dual ideals of L. Next, we note that to be a proper dual ideal of L is equivalent to not containing O—and that this is a condition of finite character. Hence every proper dual ideal can be extended to a maximal proper dual ideal, which is "covered" by the improper dual ideal L. In particular, for any $a \neq I$ of L, the principal dual ideal of $x \geqq a'$ can be extended to a maximal proper ideal Q, which cannot contain a (or it would contain $a \frown a' = O$). Hence the intersection of all maximal dual ideals is I, the least dual ideal. We conclude by such reasoning that the lattice M of dual ideals is a modular lattice, in which every element is a join of points, *provided* that M is ordered by the *dual* of inclusion.

We cannot however conclude that (7) holds (though its dual does). But if we define a "point" as a maximal dual ideal, and a "line" as the intersection of two distinct maximal dual ideals, then PG1–PG2 are easy to prove. The "flats" form a complete atomic modular lattice.

We now associate with each element $a \in L$ the set $S(a)$ of all maximal dual ideals P, such that $a \in P$. It is easy to show that $S(a)$ is always a "flat," that $a > b$ implies $S(a) > S(b)$, and that $S(a \frown b)$ is the intersection of $S(a)$ and $S(b)$. Frink has shown further that $S(a \smile b)$ is the join of $S(a)$ and $S(b)$, the difficult point is to show that if $a \smile b \in P$, then there exist Q, R with $a \in Q$, $b \in R$, and such that P contains the set-intersection of Q and R.

Since the "flats" form a direct union of atomic projective geometries, by what we have already shown, we get the following final result.

THEOREM 16. *Any complemented modular lattice is isomorphic with a sublattice of a direct union of atomic projective geometries.*

Ex. 1. Show that L is a sublattice of the lattice M of all dual ideals of L. Why does not this yield Theorem 16?

Ex. 2. Prove in detail that M is complete, and that every element of M is a join of points.

Ex. 3. Show that if a maximal dual ideal fails to contain a, then it must contain a complement a' of a.

Ex. 4. In the proof of Thm. 16, show that $S(a \frown b)$ is the intersection of $S(a)$ and $S(b)$, and that $a > b$ implies $S(a) > S(b)$.

Problem 62. Find necessary and sufficient conditions that a modular lattice be isomorphic with a sublattice of a complemented modular lattice. (See Ex. 5, §6.)

Problem 63. If $CG(R)$ is represented as in Theorem 16, is there just one associated atomic projective geometry? Is it associated with the division ring R? (O. Frink)

CHAPTER IX

DISTRIBUTIVE LATTICES

1. Definition. Many important lattices satisfy the following three identities,

L6. $(x \frown y) \smile (y \frown z) \smile (z \frown x) = (x \smile y) \frown (y \smile z) \frown (z \smile x)$,
L6′. $x \frown (y \smile z) = (x \frown y) \smile (x \frown z)$,
L6″. $x \smile (y \frown z) = (x \smile y) \frown (x \smile z)$.

Definition. *A lattice will be called "distributive" if and only if it satisfies* L6, L6′, L6″ *identically.*

Theorem 1. *Each of the identities* L6, L6′, L6″ *implies* L5 *and both of the others.*[1]

Proof. L6′ implies L6″, for by direct computation,

$$(x \smile y) \frown (x \smile z) = [(x \smile y) \frown x] \smile [(x \smile y) \frown z] = x \smile [(x \frown z) \smile (y \frown z)]$$
$$= [x \smile (x \frown z)] \smile [x \smile (y \frown z)] = x \smile (y \frown z),$$

using L6′, L4 and L6′, together with L2. Again, L6″ implies L6. For by direct expansion,

$$\begin{aligned} &[(x \frown y) \smile (y \frown z)] \smile (z \frown x) \\ &\quad = [(x \frown y) \smile (y \frown z) \smile z] \frown [(x \frown y) \smile (y \frown z) \smile x] \\ &\quad = [(x \frown y) \smile z] \frown [(y \frown z) \smile x] && \text{by L3–L4} \\ &\quad = (x \smile z) \frown (y \smile z) \frown (y \smile x) \frown (z \smile x) && \text{by L6″ again} \\ &\quad = (x \smile y) \frown (y \smile z) \frown (z \smile x) && \text{by L1–L3} \end{aligned}$$

which is L6.

Finally, L6 implies L5 and L6′. We get L5 simply by setting $x \geqq z$ in L6, which reduces the left-hand side to $(x \frown y) \smile [(y \frown z) \smile z] = (x \frown y) \smile z$, and the right-hand side to $(x \smile y) \frown (y \smile z) \frown x = x \frown (y \smile z)$ dually. Then, abbreviating L6 to the form $u = v$, we get from the equality $x \frown u = x \frown v$,

[1] Historical note: It is curious that C. S. Peirce [1] should have thought that every lattice was distributive. He even said L6′, L6″ are "easily proved, but the proof is too tedious to give"! His error was demonstrated by Schroder [1, p. 282], who showed that L6′, L6″ were not implied by L1–L4, but (p. 286) implied each other and L6. A. Korselt (Math. Ann. 44 (1894), 156–157) gave another demonstration. Peirce at first [2] gave way before these authorities, but later (cf. E. V. Huntington [1, pp. 300–301]) boldly defended his original view.

Dedekind [1, p. 116] showed that each of L6′ and L6″ implied L5. Menger [3, p. 480] showed that L6 implied L5 and L6′ and L6′, L6″.

$x \frown (y \smile z)$ on the right-hand side by L4 and L2–L3. On the left-hand side, using L5, we get

$$x \frown ([y \frown z] \smile [(x \frown y) \smile (x \frown z)]) = (x \frown y \frown z) \smile (x \frown y) \smile (x \frown z)$$

But by L3–L4, this is $(x \frown y) \smile (x \frown z)$, completing the proof.

COROLLARY. *Any distributive lattice is modular.*

From Fig. 4 of Ch. V, it is evident that any non-distributive modular lattice contains a sublattice of five elements c, d, e_1, e_2, e_3 isomorphic with the lattice of Fig. 1c. Combining with Thm. 2, Ch. III, we conclude

THEOREM 2. *A lattice which is not distributive contains one of the examples of Figs.* 1c–1d, *p.* 6, *as a sublattice.*[2]

COROLLARY 1. *A lattice is distributive if and only if relative complements in it are uniquely determined.*

This means that, given $a \leqq x \leqq b$, at most one y exists satisfying $x \frown y = a$ and $x \smile y = b$.

Proof. In a distributive lattice, $x \frown u = x \frown v$ and $x \smile u = x \smile v$ imply $u = u \frown (x \smile v) = (u \frown x) \smile (u \frown v) = (v \frown x) \smile (u \frown v) = v \frown (u \smile x) = v$. Conversely, in both Fig. 1c and Fig. 1d, one element has two relative complements.

COROLLARY 2. *Any non-distributive modular lattice which satisfies either chain condition contains the first example of Fig.* 1c *as a sublattice in which x, u, v cover O.*

Proof. If the descending chain condition holds, then we find an $x^* \leqq x$ which covers O. Then $(x^* \smile u) \frown v$ and $(x^* \frown v) \smile u$ will provide the other examples; the role of e will be played by $[(x^* \smile u) \frown v] \smile x^* = (x^* \smile u) \frown (v \smile x^*)$. The covering conditions are guaranteed by Cor. 2 of Thm. 2, Ch. III. The case of the ascending chain condition may be treated dually.

Ex. 1. In any distributive lattice L, for given $a, b \in L$, let $J(a, b)$ denote the set of x such that $a \smile x = b \smile x$. Show that $J(a, b)$ is a dual ideal, and that the meet of $J(a, b)$ and its dual is either void or all of L.

Ex. 2. Show that any lattice in which

$$(x \smile y) \frown [z \smile (x \frown y)] = (x \frown y) \smile (y \frown z) \smile (z \frown x),$$

for all x, y, z, is distributive.

Ex. 3. Show that a lattice is distributive if and only if $x \smile (y \frown z) \geqq (x \smile y) \frown z$ for all x, y, z. (J. Bowden, 1936)

Ex. 4. Show that the two lattices of Figs. 1c–1d are the only non-distributive lattices of five elements.

Ex. 5. Obtain a short proof of Thm. 1, using Thm. 11 of Ch. V.

Ex. 6*. Without using §3, show that the following postulates characterize distributive

---

[2] G. Birkhoff, Proc. Camb. Phil. Soc. 30 (1934), p. 118. Corollary 1 is due to Bergmann [1, p. 273]; cf. also Ore [1, p. 414], condition (δ_2). The condition is related to ideas of R. Grassmann [1].

lattices: $a \frown a = a$, $a \frown b = b \frown a$, $a \smile b = b \smile a$, $a \frown (b \frown c) = (a \frown b) \frown c$, $a \frown (a \smile b) = a$, $a \frown (b \smile c) = (a \frown b) \smile (a \frown c)$. (Hint: Define $a \geqq b$ to mean $a \frown b = b$.)

Ex. 7. Show that L6 and L1–L3 imply $x \smile (x \frown y) = x \frown (x \smile y)$.

Ex. 8. Show that if O, I exist with $a \smile O = a \frown I = a$ for all a, then L2, L3, L6′–L6″ imply L1–L4. (E. V. Huntington [1, pp. 292–295])

Ex. 9. Show that if we add to a distributive lattice L new elements O, I satisfying $O < x < I$ for all $x \in L$, we get another distributive lattice.

2. Examples. Any chain is a distributive lattice: in any chain, each side of L6 is the middle one of the elements x, y, z. Again, the subsets of any aggregate I form a distributive lattice—and more generally, any ring of sets is a distributive lattice. Thus the open subsets of any topological space form a (complete) distributive lattice, and so do the closed ones.

Moreover any sublattice or cardinal product of distributive lattices is again distributive.[3] Hence so is any power D^X of any distributive lattice D with a partly ordered set X as exponent; in particular $\mathbf{2}^X$ is a distributive lattice for any partly ordered set X.

Therefore the lattice of the natural integers, ordered by divisibility, forms a distributive lattice: it is a sublattice of the direct product of a countable set of chains (consisting of the powers of the various primes $2, 3, 5, \cdots$). Hence so does the (isomorphic)[4] lattice of ideals of the ring of all algebraic integers of any extension of the rational field of finite degree.

The neutral elements (Ch. II, §10) of any lattice form a distributive sublattice. The dual of any distributive lattice is distributive. The Boolean algebras discussed in Ch. X are distributive. Finally, the lattice-ordered groups and vector lattices discussed in Chs. XIV–XV are distributive.

Ex. 1. (a) Show that the "Riemann" partitions of an interval into a finite number of non-overlapping subintervals form a distributive lattice.
(b) Is the analogous statement true in n dimensions?

3. Digression: alternative postulate systems. Following ideas of M. H. A. Newman [1], G. D. Birkhoff and the author[5] have developed a very brief set of postulates for distributive lattices.

THEOREM 3. *Any algebraic system which satisfies*

(1) $\quad a \frown a = a \quad$ *for all* a,

(2) $\quad a \smile I = I \smile a = I \quad$ *for some* I *and all* a,

(3) $\quad a \frown I = I \frown a = a \quad$ *for some* I *and all* a,

[3] It is shown in G. Birkhoff [3] that this is true for the family of lattices characterized by any identity or set of identities.

[4] See van der Waerden, vol. 2, p. 100. This is probably why Dedekind called distributive lattices "von Idealtypus."

[5] G. D. Birkhoff and G. Birkhoff, *Distributive postulates for systems like Boolean algebras*, Trans. Am. Math. Soc. 60 (1946), 3–11. Newman's ideas are related to some of M. H. Stone, *Postulates for Boolean algebras* . . . , Amer. J. Math. 57 (1935), 703–732.

(4) $a \frown (b \smile c) = (a \frown b) \smile (a \frown c)$ *and* $(b \smile c) \frown a = (b \frown a) \smile (c \frown a)$, *for all* a, b, c, *is a distributive lattice with* I.

Proof. We first show that, for all a, b,

$$(5) \qquad a = a \frown I = a \frown (a \smile I) = (a \frown a) \smile (a \frown I) = a \smile a,$$

$$(6) \qquad (a \frown b) \smile a = (a \frown b) \smile (a \frown I) = a \frown (b \smile I) = a \frown I = a,$$

and similarly

$$(6') \qquad a \smile (a \frown b) = a \smile (b \frown a) = (b \frown a) \smile a = a.$$

We are now able to prove, using (4), (1), and (6′),

$$(7) \qquad a \frown (a \smile b) = (a \frown a) \smile (a \frown b) = a \smile (a \frown b) = a,$$

and similarly

$$(7') \qquad a \frown (b \smile a) = (a \smile b) \frown a = (b \smile a) \frown a = a.$$

Now we can prove the commutative law

$$(8) \qquad \begin{aligned} a \smile b &= [a \frown (b \smile a)] \smile [b \frown (b \smile a)] = (a \smile b) \frown (b \smile a) \\ &\qquad\qquad \text{by (7)–(7′), (4),} \\ &= [(a \smile b) \frown b] \smile [(a \smile b) \frown a] = b \smile a \quad \text{by (4), (7)–(7′).} \end{aligned}$$

Preparatory to proving the associative law for joins, we show

$$\begin{aligned} a \frown [(a \smile b) \smile c] &= [a \frown (a \smile b)] \smile [a \frown c] = a \smile (a \frown c) = a \\ &\qquad\qquad \text{by (4), (7), (6′),} \end{aligned}$$

$$(9) \qquad b \frown [(a \smile b) \smile c] = [b \frown (a \smile b)] \smile [b \frown c] = b \smile (b \frown c) = b \quad \text{similarly,}$$

$$c \frown [(a \smile b) \smile c] = [c \frown (a \smile b)] \smile [c \frown c] = [c \frown (a \smile b)] \smile c = c$$

by (4), (1), (6). Now we prove the associative law for joins,

$$(10) \qquad \begin{aligned} a \smile (b \smile c) &= \{a \frown [(a \smile b) \smile c]\} \smile (\{b \frown [(a \smile b) \smile c]\} \\ &\qquad \smile \{c \frown [(a \smile b) \smile c]\}) \text{ by (9),} \\ &= [a \smile (b \smile c)] \frown [(a \smile b) \smile c] \text{ by (4) used twice,} \\ &= (a \smile b) \smile c \text{ similarly, by left-right symmetry.} \end{aligned}$$

We now prove the *dual* of (4), namely

$$(11) \qquad \begin{aligned} (a \smile b) \frown (a \smile c) &= [a \frown (a \smile c)] \smile [b \frown (a \smile c)] \\ &= a \smile [(b \frown a) \smile (b \frown c)] \text{ by (4),} \\ &= [a \smile (b \frown a)] \smile (b \frown c) = a \smile (b \frown c) \\ &\qquad \text{by (10), (6′).} \end{aligned}$$

(11′) $\qquad (a \frown b) \smile c = (a \smile c) \frown (b \smile c) \qquad$ by left-right symmetry.

We have already proved the dual (5) of (1), while (6) and (7) are dual. But these were the only laws used in proving (8), (10); hence exact duals of the proofs of (8), (10) yield the commutative and associative laws for meets.

(12) $\qquad a \frown b = b \frown a \quad \text{and} \quad a \frown (b \frown c) = (a \frown b) \frown c.$

This completes the proof of the laws L1, L2, L3, L4, L6 ordinarily used in defining a distributive lattice!

We shall now discuss some remarkable properties of the self-dual ternary operation[6] involved in L6,

(13) $\quad (a, b, c) = (a \frown b) \smile (b \frown c) \smile (c \frown a) = (a \smile b) \frown (b \smile c) \frown (c \smile a).$

We call (a, b, c) the *median* of a, b, c, since this is what it reduces to in the case of chains.

LEMMA 1. *In any distributive lattice,* $(a, x, b) = x$ *if and only if*

$$a \frown b \leqq x \leqq a \smile b.$$

Proof. If $a \frown b \leqq x \leqq a \smile b$, then clearly

$$(a \frown b) \smile (b \frown x) \smile (x \frown a) = (a \frown b) \smile [x \frown (b \smile a] = x.$$

The converse may easily be proved by the reader. In fact, if we define with W. D. Duthie,[7] the *segment* $\langle a, b \rangle$ joining a and b as the set of all x satisfying $a \frown b \leqq x \leqq a \smile b$, then

LEMMA 2. *The element* (a, b, c) *is the intersection of the three sets* $\langle a, b \rangle$, $\langle b, c \rangle$, $\langle c, a \rangle$.

Proof. By Lemma 1, (a, b, c) lies in all three sets. Conversely, if x lies on all three sets, then clearly

$$(a, b, c) = (a \frown b) \smile (b \frown c) \smile (c \frown a) \leqq x \leqq (a \smile b) \frown (b \smile c) \frown (c \smile a)$$
$$= (a, b, c).$$

One can easily define a distributive lattice with O, I in terms of the single ternary operation (a, b, c).

THEOREM 4. *Let A be any algebraic system with a ternary operation* (a, b, c), *and elements O, I, such that*

(14) $\qquad (O, a, I) = a, \qquad$ (15) $\qquad (a, b, a) = a,$

[6] This operation was first discussed in the case of Boolean algebras by A. A. Grau, *Ternary operations and Boolean algebra*, Ph.D. Thesis, Univ. of Michigan, 1944. It has been introduced into distributive lattices and applied to many logical problems by S. A. Kiss in his book *Lattice transformations and structures of logic*, New York, 1947. The present exposition follows S. A. Kiss and Garrett Birkhoff, *A ternary operation in distributive lattices*, Bull. Am. Math. Soc. 53 (1947), 749–52.

[7] *Segments of ordered sets*, by W. D. Duthie, Trans. Am. Math. Soc. 51 (1942), 1–14.

(16) $(a, b, c) = (b, a, c) = (b, c, a)$ *(Symmetry)*,

(17) $((a, b, c), d, e) = ((a, d, e), b, (c, d, e))$,

identically. Then if we define

(18) $a \smile b = (a, I, b)$ *and* $a \frown b = (a, O, b)$,

A is a distributive lattice in which (13) *holds.*

Proof. We first show that A is a distributive lattice, by use of Thm. 3. Indeed, (15) and (18) imply (1); (15) and (18), with (16), imply (2); (14) and (18), with (16), imply (3). While (17) implies the second identity of (4) if we set $b = I$ and $d = O$; the first follows by symmetry. (Note that the conditions of (16) imply the invariance of (a, b, c) under *all* permutations of its members.)

We now use Lemma 2 to show that in this distributive lattice, (a, b, c) has its usual meaning. But indeed

$$(a, (a, b, c), b) = ((a, c, b), a, b) = ((a, a, b), c, (b, a, b)) = (a, c, b) = (a, b, c),$$

by repeated use of (16), together with (17) and (15). Similarly $(a, (a, b, c), c) = (b, (a, b, c), c) = (a, b, c)$, whence by Lemma 1, (a, b, c) is the intersection of $\langle a, b\rangle$, $\langle b, c\rangle$, and $\langle a, c\rangle$—and so has its usual meaning.

Various other interesting properties of the ternary median operation (a, b, c) are described in exercises.

Ex. 1. (a) Show that, in any distributive lattice L, if (a, b, c) is defined by (13), then (15), (16), and (17) are valid.

(b) Show that if L has an O and an I, then (14), (18) hold.

Ex. 2. Let L be any distributive lattice of finite length, and define $\partial(a, b) = d[a \smile b] - d[a \frown b]$ as in Ch. V, §7.

(a) Show that $\langle a, b\rangle$ consists of the x such that $\partial(a, x) + \partial(x, b) = \partial(a, b)$.

(b) Infer that (a, b, c) gives to $\partial(a, x) + \partial(b, x) + \partial(c, x)$ its minimum value $\{\partial(a, b) + \partial(b, c) + \partial(c, a)\}/2$.

(c) Conclude that any homeomorphism of the *graph* of L is an automorphism of L with respect to the ternary operation (a, b, c).

(d) Infer that 2^n has $2^n(n!)$ automorphisms with respect to the ternary operation (a, b, c)—as contrasted with $n!$ ordinary automorphisms.

Ex. 3. Generalize Ex. 2a–2b to any distributive metric lattice.

Ex. 4. Show that in neither non-distributive lattice of five elements, does $\partial(a,x) + \partial(b,x) + \partial(c, x)$ assume a minimum at a unique x, for all a, b, c.

Ex. 5. (a) Prove the identity $(ab(cde)) = ((abc)d(abe))$ in distributive lattices.

(b) Show that this contains L6′ and L6″ as special cases.

Ex. 6*. Consider the algebras with two binary idempotent, commutative, associative, and mutually distributive operations, and two elements O and I satisfying $O \smile a = I \frown a = a$. Show that the "free" such algebra with one generator has exactly seven elements.[5]

Problem 64. Show that at least part of (16) can be dispensed with, if a suitable permutation of (17) is used.

[5] See E. Gonzales Baz, Bol. Soc. Mat. Mexicana, 4 (1947). For other generalizations of distributive lattices, see Gr. C. Moisil [1, pp. 1–5]; M. Smiley, Trans. Am. Math. Soc. 56 (1944), 435–47.

Problem 65. Prove or disprove the independence of the seven identities assumed as postulates in Theorem 3.

Problem 66. Extend the results of M. F. Smiley and W. R. Transue, Bull. Am. Math. Soc. 49 (1943), 280–287, to the case where there is no special "reference" element O.

4. **Representation theory: finite case.** We have observed that any ring of sets is a distributive lattice; in §§4–5 we shall prove converses of this fact. We first treat the case of finite length.

LEMMA 1. *In a distributive lattice L, if p is join-irreducible, then $p \leqq \bigvee_{i=1}^{k} x_i$ implies $p \leqq x_i$ for some i.*

Proof. The hypothesis implies $p = p \frown \bigvee_{i=1}^{k} x_i = \bigvee_{i=1}^{k} (p \frown x_i)$. Hence, since p is join-irreducible, $p = p \frown x_i$ for some i, which is to say $p \leqq x_i$ for some i.

LEMMA 2. *If L contains n join-irreducible elements $p_1, \cdots, p_n$ then $d[L] \geqq n$.*

Proof. Rearrange the p_i so that $p_i < p_j$ implies $i < j$; this is possible since partial ordering is anti-circular. Then the chain $0 < p_1 < p_1 \smile p_2 < \cdots < \bigvee_{i=1}^{n} p_i$ has length n, by Lemma 1.

THEOREM 5. *Let L be any distributive lattice of finite length n. Then the partly ordered subset X of join-irreducible elements $p_i > 0$ has order n, and $L = \mathbf{2}^{\check{X}}$.*

Proof. By finite induction, every a in L is the join $\bigvee_A p_i$ of the set A of the join-irreducible elements $p_i > 0$ which it contains. Also, if $p_i \leqq a$ and $p_j \leqq p_i$, then $p_j \leqq a$; that is, every set A is M-closed in X. But conversely, by Lemma 1, if A is M-closed, then $\bigvee_A p_i$ contains no p_k not in A. Hence the correspondence $a \leftrightarrow A$, which is obviously isotone, is one-one, and so an isomorphism. But as in Ch. I, §11, the set of A is isomorphic with the ring of "closed" subsets of the T_0-space defined by the dual $\check{X}$ of X, i.e., with $\mathbf{2}^{\check{X}}$. But it is immediate that $d[\mathbf{2}^{\check{X}}]$ is the order of $\check{X}$, completing the proof.

COROLLARY. *The number of (non-isomorphic) distributive lattices of length n is equal to the number of partly ordered sets of n elements.* (Ch. I, §3, Ex. 2(a).)

Ex. 1. Show that a distributive lattice of length n contains at most 2^n elements.

Ex. 2. Show that the set X of join-irreducible elements of a finite distributive lattice L is dually isomorphic to the set Y of meet-irreducible[9] elements of L.

Ex. 3. Show that for a modular lattice L of finite length to be distributive, each of the following conditions is necessary and sufficient; (a) every "simple" homomorphic image of L be 2, (b) L have $d[L]$ distinct prime congruence relations, (c) no two distinct quotients in the same chain be projective. (Hint: use Ch. V; cf. [LT, §94].)

Ex. 4*. Characterize abstractly the lattices of all sublattices of $\mathbf{2}^n$, n, and $\mathbf{2}^X$, where X is any partly ordered set.

Ex. 5. In Ch. II, §4, Ex. 5, show that joins in L correspond to set-unions in the representation if and only if L is distributive.

---

[9] M.-P. Schutzenberger, Comptes Rendus, 218 (1944), 218–219 has asserted that in any finite modular lattice, the number of join-irreducible elements equals the number of meet-irreducible elements.

Ex. 6*. Show that every finite distributive lattice is isomorphic with the lattice of all congruence relations on a suitable second finite lattice (R. Dilworth).

5. General representation theorem. We can also prove quite easily, using Thm. 10 of Ch. VI, the following general result.

THEOREM 6. *Any distributive lattice L (except* **1***) is isomorphic with a subdirect union of replicas of* **2**.

Proof. By Thm. 10, Ch. VI, L is a subdirect union of subdirectly irreducible distributive lattices. Hence it is sufficient to prove the

LEMMA. *The only subdirectly irreducible distributive lattice D (except* **1***) is* **2**.

Proof. Suppose D contained an element x not O or I. There would exist $r \in D$, not contained in x; hence $s = x \smile r > a$ would exist; dually, $t < a$ would exist in D. Hence the endomorphisms $u \to u \frown x$ and $u \to u \smile x$ of D would identify distinct elements. But as in Cor. 1 of Thm. 2, $u \frown x = v \frown x$ and $u \smile x = v \smile x$ imply $u = v$; hence the correspondence $d \to (d \frown x, d \smile x)$ would give a subdirect reduction of D. We conclude that D can contain no element not O or I, which clearly implies the lemma.

COROLLARY. *Any distributive lattice L is isomorphic with a ring of sets.*[10]

Proof. The case $L = \mathbf{1}$ is trivial. If $L \neq \mathbf{1}$, then L can be represented as a subdirect union of replicas of **2**, each of which we shall call a *point*, and denote p_α. With each $a \in L$ we associate the function f, such that $f(p_\alpha) = 1$ if the p_α-component of a is I, and $f(p_\alpha) = 0$ otherwise. This is the characteristic function of the set A of p_α such that the p_α-component of a is I. Since A determines all the p_α-components of a, the correspondence is one-one. Moreover join and meet in L obviously correspond, for each p_α-component, to union and intersection for the corresponding sets; this is simply the familiar calculus of characteristic functions. Hence we have exhibited an isomorphism, completing the proof.

Ex. 1. Show that any isomorphism of a distributive lattice L (not **1**) with a ring of sets corresponds to a representation of L as a subdirect union of replicas of **2**.

6. Ideals. We have already seen (Ch. II, §§5–6 and Ch. V, Thm. 12) that the ideals of any lattice L themselves form a lattice. Moreover it is easy to show that in this lattice, $J \frown K$ is simply the set of all $s \frown t$ with $s \in J$, $t \in K$. If L is *distributive*, it is also true that $J \smile K$ is also the set of all $s \smile t$ [$s \in J$, $t \in K$]. For clearly the intersection of all ideals in L containing J and K contains every such $s \smile t$. But conversely, since $(s \smile t) \smile (s_1 \smile t_1) = (s \smile s_1) \smile$

[10] G. Birkhoff [1, Thm. 25.2]. An interesting historical discussion of the type of construction used in the original proof has been made by M. H. Stone, *The representation of Boolean algebras*, Bull. Am. Math. Soc. 44 (1938), 807–816. The first example of its use was perhaps given by A. Tarski, *Une contribution à la théorie de la mesure*, Fund. Math. 15 (1930), 42–50.

$(t \smile t_1)$, while $x \leqq s \smile t$ implies $x = x \frown (s \smile t) = (x \frown s) \smile (x \frown t) = s_1 \smile t_1$ $[s_1 \in J, s_2 \in K]$, the set of all $s \smile t$ $[s \smile J, t \in K]$ is an ideal which contains J and K.

In summary, if L is a distributive lattice, then the operations $\frown$ and $\smile$ can be interpreted in the sense of the calculus of complexes.[11]

We saw in Ch. V, Thm. 12, that the ideals of any modular lattice themselves formed a modular lattice. We now prove similarly

THEOREM 7. *The ideals of any distributive lattice themselves form a distributive lattice under set-inclusion (or, isomorphically, the calculus of complexes).*

Proof. By the one-sided distributive law (3) of Ch. II, §4, $H \frown (J \smile K) \geqq (H \frown J) \smile (H \frown K)$. But every element $s \frown (t \smile u)$ $[s \in H, t \in J, u \in K]$ of $H \frown (J \smile K)$ is also an element $(s \frown t) \smile (s \frown u)$ of $(H \frown J) \smile (H \frown K)$; hence the reverse inequality holds.[12]

We have also already defined principal ideals and closed ideals. The principal ideals of any lattice L trivially form a sublattice of the lattice of all ideals of L, which is isomorphic with L itself. On the other hand, the closed ideals of L do not form a sublattice. Indeed, examples have been given independently by Cotlar, Funayama and Dilworth,[13] of distributive lattices whose completions by cuts are not even modular.

We now define a new type of ideal: prime ideals. This is the exact analog of the concept of prime ideal in ring theory, if we regard $\frown$ as signifying multiplication.

DEFINITION. *An ideal P of a lattice L is prime if and only if*

(19) $$x \frown y \in P \text{ implies } x \in P \text{ or } y \in P.$$

THEOREM 8. *Each of the following conditions is necessary and sufficient that an ideal J of a lattice L be prime:* (i) *the complement $L - J$ of J be a dual ideal,* (ii) *J be the set of antecedents of* 0 *under a lattice-homomorphism $L \to \mathbf{2}$.*

Proof. In any event, $x \in J$, $y \in J$, $u \in L - J$, $v \in L - J$ imply: $x \frown y$, $x \smile y$, and $x \frown u$ in J, while $x \smile u$ and $u \smile v$ are in $L - J$. The only question is as to $u \frown v$. To assert $u \frown v \in L - J$ is equivalent to (19), since it excludes $u \frown v \in J$, $u \notin J$, $v \notin J$, and by substitution in the definitions it is also easily seen to be equivalent to (i) and (ii). (The cases P void and $P = L$ are exceptional in the preceding considerations.)

It follows that the "points" in any representation of a (distributive) lattice

[11] This is a concept of universal algebra, first defined by Frobenius for groups. If $S_1, \cdots, S_n$ are any non-void subsets of an algebra with an n-ary operation f_i, then $f_i(S_1, \cdots, S_n)$ is the set of all $x = f_i(s_1, \cdots, s_n)$, with $s_1 \in S_1, \cdots, s_n \in S_n$.

[12] Most of the results of the present section are essentially due to Stone [3]; cf. also Tarski [1]; Tarski, Ann. Soc. Pol. Math. 15 (1937), 186–9; and Moisil [1]. We recall that what we here call "closed" ideals were previously called "normal" ideals.

[13] M. Cotlar, Revista Univ. Nac. Tucumán (A) 4 (1944), 105–157; N. Funayama, Proc. Imp. Acad. Tokyo 20 (1944), 1–2. The question was raised by H. MacNeille [2]; Dilworth's example is unpublished.

L as a ring of sets correspond uniquely to "prime ideals" of L, and that two points correspond to the same prime ideal if and only if one is redundant. Further, the "perfect" representation, in which each prime ideal occurs once and only once, plays a special role. Further details may be found elsewhere.[14]

Ex. 1. Show that a lattice is a chain, if and only if all its ideals are prime.

Ex. 2. Show that every ideal in a distributive lattice is neutral.

Ex. 3. Show that the modular, non-distributive lattice of five elements has two ideals J, K whose join is not $J \smile K$ in the sense of the calculus of complexes.

Ex. 4. (a) Show that a principal ideal $a \frown L$ of a distributive lattice L is prime, if and only if a is meet-irreducible.

(b) Show that if L has finite length n, then L has exactly n prime ideals, apart from the void set and L itself.

(c) Prove that every maximal ideal of a distributive lattice is prime. (Cf. Ch. X, §6).

7. Unique decomposition theorem. Let L be any distributive lattice, and let

$$a = x_1 \smile \cdots \smile x_r = y_1 \smile \cdots \smile y_s$$

be any two representations of an element $a \in L$ as a join of join-irreducible elements. Then by Lemma 1 of §4, given x_i, some $y_j \geqq x_i$, and similarly some $x_k \geqq y_j$. Hence, unless x_i is *redundant* in the sense that $x = x_1 \smile \cdots \smile x_{i-1} \smile x_{i+1} \smile \cdots \smile x_r$, we have $x_i = y_j = x_k$, whence $k = i$. Thus if the decompositions are irredundant, then the x_i and y_j are equal in pairs, $r = s$, and we conclude

Lemma 1. *In a distributive lattice, the representation of an element as an irredundant join of join-irreducible elements is unique (and dually).*

But if the descending chain condition holds, it is easy to prove the existence of such a representation, whence we have

Theorem 9. *In a distributive lattice L which satisfies the descending chain condition, each element has one and only one representation as an irredundant join of join-irreducible elements. (And dually, if L satisfies the ascending chain condition.)*

Now let P be the partly ordered set of all join-irreducible elements of L; clearly P itself satisfies the descending chain condition. We define a "crown" in P as a finite subset $X = (x_1, \cdots, x_r)$ of P such that $x_i \leqq x_j$ in X implies $x_i = x_j$. Then by Theorem 9, there is a one-one correspondence between the "crowns" of P and the elements of L, given by $(x_1, \cdots, x_r) \leftrightarrow x_1 \smile \cdots \smile x_r$. Moreover $x_1 \smile \cdots \smile x_r \leqq y_1 \smile \cdots \smile y_s$ if and only if every x_i is continued in some y_j.

Conversely, if P is an abstract partly ordered set satisfying the descending chain condition, then the finite "crowns" of P form a distributive lattice L satisfying the descending chain condition, if we define $(x_1, \cdots, x_r) \leqq (y_1, \cdots, y_s)$ to mean that every x_i is contained in some y_j. Moreover the join-irreducible

[14] Ch. XI, §2; also M. H. Stone, Mat. Sbornik 43 (1936), 765–72.

elements of L are the one-element crowns. One may thus prove the following result, generalizing Thm. 5.

THEOREM 10. *There is a one-one correspondence between distributive lattices L satisfying the descending chain condition, and partly ordered sets P satisfying the ascending chain condition. Under this correspondence, P is isomorphic to the subset of join-irreducible elements of L (and dually).*

Ex. 1. Show that in a distributive lattice L, the representation $a = x_1 \frown \cdots \frown x_r$ of a as a meet of meet-irreducible elements is irredundant unless $x_i > x_j$ for some i, j.

Ex. 2. (a) Show that if L is a modular, non-distributive lattice satisfying the descending chain condition, then Lemma 1 is false. (Hint: use $I = x \smile u = x \smile v$ in the lattice of Fig. 1c; decompose further as long as possible and eliminate redundant components. Any factor of the second decomposition contained in u must be contained in x or v and hence in O, whereas the first decomposition has a factor not O contained in u.)

(b) Show that in the non-modular lattice of Fig. 7a, the conclusion of Thm. 9 holds.

(c*) Show that if L is a lattice of finite length, then Lemma 1 holds in L if and only if L is a semi-modular lattice in which every modular sublattice is distributive.[15]

Ex. 3. Show that in Thm. 10, the crowns of P "covering" a given crown $(x_1, \cdots, x_r)$ may all be obtained by adjoining an element $t \in P$ which covers some x_i or is minimal, and discarding redundant elements.

Ex. 4. In Thm. 10, represent L as a ring of subsets of P. (Hint: Take sets of all t contained in the elements of a crown.)

Ex. 5. Show that if a partly ordered set satisfies the descending chain condition, then so do its "crowns," under the partial ordering of Thm. 10.

Ex. 6. Show that in Thm. 10, P is isomorphic with the set of prime ideals of L.

8. **Applications to algebra and algebraic geometry.** Combining Thm. 9 above with Thm. 9 of Ch. VI, we get immediately the following result.

THEOREM 11. *Let A be any abstract algebra, whose congruence relations form a distributive lattice satisfying the ascending chain condition. Then A and its homomorphic images have unique representations as subdirect unions of subdirectly irreducible factors.*

This result holds if A is any finite lattice (Ch. II, Thm. 5), semi-simple group, group of square-free order, or semi-simple hypercomplex algebra.

We have a more interesting application to algebraic geometry. An *algebraic variety* V in affine n-space over a field F is defined as the set of all points $(x_1, \cdots, x_n)$ which satisfy a suitable set $J(V)$ of polynomial equations $p_i(x_1, \cdots, x_n) = 0$ with coefficients in F. If V and W are algebraic varieties defined by r equations $p_i = 0$ and s equations $q_j = 0$ respectively, then it is easily shown that the rs equations $p_iq_j = 0$ are satisfied by points in V *or* W, and no others, while the $r + s$ equations $p_i = 0$, $q_j = 0$ are satisfied by points on V *and* W, and by no others. Hence the algebraic varieties form a ring of sets (distributive lattice).

[15] R. P. Dilworth, *Lattices with unique irreducible decompositions*, Annals of Math. 41 (1940), 771–7; see also *Ideals in Birkhoff lattices*, Trans. Am. Math. Soc. 49 (1941), 325–53; and A. Monteiro, Comptes Rendus 225 (1947), 846–8. Thms. 9–10 and Ex. 2(a) are due to the author.

Furthermore, it is easily shown that the ideals of the polynomial ring $F(x_1, \cdots, x_n)$ satisfy the ascending chain condition (van der Waerden [1, vol. 2, p. 25]); moreover the correspondence between varieties and the equations which they satisfy is a polarity. Hence, as in Ch. IV, the algebraic varieties satisfy the descending chain condition. We conclude that the hypotheses of Thm. 9 apply, whence *every algebraic variety has a unique expression as an irredundant sum of a finite number of irreducible components.*

Finally, let L be any modular lattice which satisfies the descending chain condition. If we identify elements x and y of L whenever the interval $[x \frown y, x \smile y]$ has finite length, we obtain a proper homomorphic image L_1 of L. Repeating this process, we obtain a sequence of homomorphic images $L > L_1 > L_2 > \cdots$, which were first discussed abstractly by Ore;[16] we let $0 < \theta_1 < \theta_2 < \cdots$ denote the corresponding sequence of congruence relations on L.

In the case of algebraic varieties, one may show that the *dimension* of a variety V is the least k such that $V \equiv 0 \bmod \theta_k$. Dually, if $J(V)$ is the ideal of polynomial equations satisfied by all $(x_1, \cdots, x_n) \in V$, and $F(x_1, \cdots, x_n)$ is the ring of all polynomials in $x_1, \cdots, x_n$ with coefficients in F, then k is the *transcendence degree* of the quotient ring (residue class ring) $F(x_1, \cdots, x_n)/J(V)$.

Ex. 1. Let J be any ideal in an extension F of finite degree of the rational field R. Show that J has one and only one irredundant expression as a meet of meet-irreducible ideals.

Ex. 2. (a) Show that if the congruence relations on A satisfy the ascending chain condition and are permutable, but the lattice of congruence relations is not distributive, then the conclusion of Thm. 11 is not true in A. (Hint: see Ex. 2(a) of §7.)

(b) Let A be a group with operators, whose lattice of congruence relations has finite length. Show that the conclusion of Thm. 11 holds unless A has a homomorphic image with two "independent" Ω-isomorphic Ω-subgroups S and T. (See [LT, §103, end].)

Ex. 3*. Let X denote the set of prime intervals of a lattice L of finite length, quasi-ordered by the relation $[q, p] \geqq [s, r]$ in X means that $u \geqq r > s \geqq v$ in L for some interval $[v, u]$ projective to $[q, p]$. Show that the lattice of congruence relations on L is[17] isomorphic with 2^X.

Problem 67. Generalize Ex. 3 to lattices L merely satisfying one chain condition.

9. **General finite distributivity.** The proofs by induction of the usual generalized distributive laws of ordinary algebra apply to distributive lattices, provided sums are interpreted as joins and meets as products, or dually. For example, by induction on n, we have

$$
\begin{aligned}
x \frown \bigvee_{j=1}^{n} y_j &= x \frown \left(\bigvee_{j=1}^{n-1} y_j \smile y_n\right) = \left(x \frown \bigvee_{j=1}^{n-1} y_j\right) \smile (x \frown y_n) \\
&= \bigvee_{j=1}^{n-1} (x \frown y_j) \smile (x \frown y_n) = \bigvee_{j=1}^{n} (x \frown y_j), \quad \text{and dually.}
\end{aligned} \tag{20}
$$

---

[16] Ore [1, pp. 421–424]; see also [LT, §56]. For algebraic varieties in general, see A. Weil, *Foundations of algebraic geometry*, New York, 1947.

[17] M. Funayama, *On the congruence relations on lattices*, Proc. Imp. Acad. Tokyo 18 (1942), 530–531. The basic remark is that every congruence relation θ is the join of the "join-irreducible" congruence relations $\theta(p, q)$ generated by the relation $p \equiv q$ for some prime interval $[q, p]$.

Similarly, by induction on m, we obtain

$$\bigvee_{i=1}^{m} x_i \frown \bigvee_{j=1}^{n} y_j = \bigvee_{i,j} (x_i \frown y_j), \text{ and dually.} \tag{21}$$

Finally, using induction on the number r of terms, we can derive the *generalized* distributive law,

$$\bigwedge_{h=1}^{r} u_{h,k} = \bigvee_{f} \left[\bigwedge_{h=1}^{r} u_{h,f(h)} \right], \quad \text{and dually.} \tag{22}$$

Here f runs through all the functions which associate, with each h, a unique $k = 1, \cdots, n(h)$.

THEOREM 12. *Any lattice polynomial ϕ of elements $x_1, \cdots, x_m$ of a distributive lattice L, can be written in the form,*

$$\bigwedge_{h=1}^{r} \left[\bigvee_{k=1}^{n(h)} x_{i(h,k)} \right],$$

and also dually.[18]

Proof. By repeated use of the generalized distributive law, we can replace $\bigwedge \bigvee$ by $\bigvee \bigwedge$ and conversely. Hence we can replace any $\bigwedge \bigvee \bigwedge \bigvee \cdots$ by $\bigwedge \bigwedge \bigvee \bigvee \cdots$, and this in turn (using the associative law) by $\bigwedge \bigvee$. The conclusion is now obvious by induction.

10. Free distributive lattices. We shall now determine the free distributive $FD(n)$ lattice generated by n symbols $x_1, \cdots, x_n$. The expression for this becomes neater if we adjoin an O and an I.

In the first place, by Thm. 12, we can write every element of $FD(n)$ in the form $\bigvee_{\sigma \in F}(\bigwedge_{i \in \sigma} x_i)$, where the σ denote sets of x_i, and F denotes a set of σ. Moreover by L1–L3, since meets and joins are determined by the *sets* of elements involved, each element is determined by this expression. Again, if $\sigma^* \geqq \sigma$, then

$$\bigwedge_{i \in \sigma} x_i \smile \bigwedge_{j \in \sigma^*} x_j = \bigwedge_{i \in \sigma} x_i;$$

hence every element of $FD(n)$ can be written in the form $\bigvee_{\sigma \in F^*}(\bigwedge_{i \in \sigma} x_i)$, where F^* contains, with any subset σ, all $\sigma^* \geqq \sigma$. We shall call such a family, *J-closed*.

This establishes a many-one correspondence, which clearly preserves order, between the set of all F^* and the elements of $FD(n)$. We introduce I to correspond to the case that F^* is void, and O for the case that F^* contains the void set σ_0 and no others. Hence the correspondence must be an isomorphism, if different F^* correspond to different elements, in one realization. We now exhibit such a realization.

Indeed, let $L = 2^n$ be the family of all subsets σ of $x_1, \cdots, x_n$, and let X_i denote the subset of L which contains x_i if and only if $x_i \in \sigma$. Then X_i will

[18] This principle, together with formulas (1)–(3), has been known almost since Boole; see Boole [2, pp. 72–5]. Cf. G. Birkhoff [1, Thm. 16.3].

be J-closed; hence this will be true of all subsets of the ring generated by the X_i. Moreover $\bigwedge_{i\in\tau} X_i$ will contain σ if and only if every x_i $[i \in \tau]$ is in σ—i.e., if and only if $\sigma \geqq \tau$. Hence $\bigvee_{\tau\in G}(\bigwedge_{i\in\tau} X_i)$ contains σ if and only if $\sigma \geqq \tau$ for some τ—hence, if G is J-closed, if and only if $\sigma \in G$. Hence different J-closed G determine different families of sets σ, and the correspondence is an isomorphism. This proves

THEOREM 13. *The free distributive lattice generated by n symbols, with O and I adjoined, is isomorphic with the ring of all J-closed subsets of the lattice 2^n of all subsets of n points.*[19]

By Thm. 8 of Ch. I, since 2^n is self-dual, we infer immediately the following

COROLLARY. *The free distributive lattice generated by n symbols, with O and I adjoined, is 2^{2^n}.*

Ex. 1. For what X is 2^X the free distributive lattice with n generators, without O and I adjoined?

Ex. 2. Show that the sublattice, generated by a finite subset of n elements of a distributive lattice, contains at most 2^{2^n} elements, and hence is finite.

Ex. 3. Let $f(n)$ denote the number of elements of $FD(n)$. Show that $f(1) = 3, f(2) = 6$, $f(3) = 20, f(4) = 168, f(5) = 7581$, and[20] $f(6) = 7{,}828{,}354$.

Problem 68. Find an analog of Thm. 13 for an infinite set of generators—noting chain conditions.

11. **Infinite distributivity.** The natural generalizations of the distributive laws (20)–(22) of §9 are the relations

$$(20')\qquad x \frown \bigvee_B y_\beta = \bigvee_B (x \frown y_\beta), \quad \text{and dually,}$$

$$(21')\qquad \bigvee_A x_\alpha \frown \bigvee_B y_\beta = \bigvee_{AB} (x_\alpha \frown y_\beta), \quad \text{and dually, and}$$

$$(22')\qquad \bigwedge_C [\bigvee_{A_\gamma} u_{\gamma,\alpha}] = \bigvee_F [\bigwedge_C u_{\gamma,\phi(\gamma)}], \quad \text{and dually.}$$

In (22′), F is the class of all single-valued functions ϕ, assigning to each $\gamma \in C$ a value $\phi(\gamma) \in A_\gamma$. These "infinite distributive laws" do *not* hold in every distributive lattice. However, their validity may be correlated with concepts already introduced.

THEOREM 14. *In any complete distributive lattice L, identity* (20′) *is equivalent to* (21′), *and to the condition that L is a topological lattice.*[21]

---

[19] This result is essentially due to Th. Skolem [1]; see also *Uber gewisse "Verbande" oder "Lattices,"* Avh. Norske Vid. Akad. Oslo (1936), pp. 1–16.

[20] The problem of determing $f(n)$ was proposed by Dedekind [1, p. 147], who found $f(4)$. R. Church, Duke Jour. 6 (1940), 732–4, found $f(5) = 7581 = 3\cdot 7\cdot 19^2$. Using computing machines, M. Ward found $f(6)$; see Abstract 52-5-135 in Bull. Am. Math. Soc. (1946). No divisibility properties of $f(n)$ in general are known.

[21] Thm. 14, for countable sets, is due to von Neumann [2, Appendix 1 of Part III]; see also A. Tarski [3, p. 510, footnote].

Proof. We reduce the labor of proof by half, using the Duality Principle. Using (20′) twice, we get

$$\bigvee_A x_\alpha \frown \bigvee_B y_\beta = \bigvee_A (x_\alpha \frown \bigvee_B y_\beta) = \bigvee_A (\bigvee_B (x_\alpha \frown y_\beta)) = \bigvee_{AB} (x_\alpha \frown y_\beta),$$

where the last step follows from the generalized associative law. Hence (20′) implies (21′); the converse is obvious. Again, by the Lemma of Ch. IV, §9, for L to be a topological lattice, it is sufficient that $x_\alpha \uparrow x$ imply $a \frown x_\alpha \uparrow a \frown x$, and dually, and this is an immediate consequence of (20′). Conversely, in a complete topological lattice, let Γ be the set of finite subsets G of a set B. Then the $z_G = \bigvee_G y_\beta \to \bigvee_B y_\beta$. Hence the $x \frown z_G \to x \frown \bigvee_B y_\beta$. But for each G, we have by (20), $x \frown z_G = \bigvee_G (x \frown y_\beta) = u_G$. And again by continuity the $u_G \to \bigvee_B x \frown y_\beta$. We infer that the two limits are the same.

Ex. 1. (a) Show that, in case A, B are restricted to be countable, Thm. 14 holds in any distributive σ-lattice. (Cf. [LT, §102].)

(b) State the appropriate generalization of Thm. 14 to distributive lattices which are $\aleph$-complete for a given cardinal number $\aleph$.

Ex. 2. (a) Let L be any complete distributive lattice in which half of (20′) holds. Show that the unrestricted joins of finite meets of elements of L form a subset closed under unrestricted union and finite intersections.

(b) Apply to the concept of a "sub-base" of open sets of a topological space.

(c) Dualize, and apply to "sub-bases" of closed sets.

Ex. 3. Show that, although (22′) contains (20′)–(21′) as special cases, it is not implied by them. What about the case of chains?

Problem 69. Try to characterize all lattices in which (22′) holds unrestrictedly. (Suggestions: See Ch. X, §9; try to introduce "cuts" in chains as points, etc.)

12. Pseudo-complemented lattices. Topological distributive lattices, and many others, are relatively pseudo-complemented in the following sense.[22]

DEFINITION. *By the pseudo-complement $a * b$ of an element a relative to an element b in a lattice L is meant an element c such that $a \frown x \leqq b$ if and only if $x \leqq c$. A lattice in which $a * b$ exists, for all a, b, is called relatively pseudo-complemented. The element $a * 0$ is called the pseudo-complement of a, and denoted a^*.*

Thus a^* is simply the greatest element disjoint from a, in case such an element exists.

THEOREM 15. *A complete lattice L is relatively pseudo-complemented if and only if it satisfies the first half of (20′).*

Proof. Suppose that L satisfies the first half of (20′), and let a, b, be given. Let B denote the set of all y_β satisfying $a \frown y_\beta \leqq b$. Then $a \frown \bigvee_B y_\beta = \bigvee_B (a \frown y_\beta) \leqq b$; hence $\bigvee y_\beta = c$ satisfies $a \frown c \leqq b$, and $a \frown y_\beta \leqq b$ implies $y_\beta \leqq c$; hence $a * b$ exists. Conversely, suppose that L is relatively pseudo-complemented, and let $b = \bigvee_B (a \frown y_\beta)$. Clearly $a \frown y_\beta \leqq b$ for every y_β;

[22] Cf. [LT, §124]; also G. Birkhoff [1, p. 459]. Our definition is the dual of the definition of a Brouwerian logic by McKinsey and Tarski [2].

hence every $y_\beta \leqq a * b$, and $\bigvee_B y_\beta \leqq a * b$. Substituting in the identity $a \frown (a * b) \leqq b$, we obtain $a \frown \bigvee_B y_\beta \leqq b = \bigvee_B (a \frown y_\beta)$; but the reverse inequality holds in any complete lattice, which finishes the proof.

Corollary. *Any relatively pseudo-complemented lattice is distributive, and any topological distributive lattice is relatively pseudo-complemented.*

Since the subalgebras of any abstract algebra satisfy the first half of (20′)—i.e., have a continuous join operation,—the ideals of any distributive lattice form a relatively pseudo-complemented lattice. Similarly, the open subsets of any topological space form a relatively pseudo-complemented lattice (see Ch. XI, §5). Again (Ch. XII, §7), Brouwerian logics are intimately related to relatively pseudo-complemented lattices.

The correspondence $a \to a^*$ is clearly a Galois connection in any relatively pseudo-complemented lattice L. Since also the relation $x \frown y = O$ is symmetric, we infer by Ch. IV, §6,

$$(23)\qquad \begin{array}{l} a \leqq a^{**}, \quad a^* = a^{***}, \quad a \leqq b \text{ implies } a^* \geqq b^*, \\ (a \smile b)^* = a^* \frown b^*, \text{ and } (a \frown b)^* \geqq a^* \smile b^*. \end{array}$$

Further, the "closed" elements of L satisfying $a = a^{**}$ form a complete lattice A, in which joins are given by the new operation $a \vee b = (a \smile b)^{**}$, while the meet operation is the same as in L. Since $(a \smile a^*)^* = a^* \frown a^{**} = O$, $a \vee a^* = O^* = I$, and

$$(23')\qquad a \frown a^* = O \quad\text{and}\quad a \vee a^* = I.$$

Next, suppose $x \frown a \frown b = 0$ in L; define $y = x \frown a^{**} \frown b^{**} \leqq x$. Clearly $y \frown a \frown b = 0$; but this implies $y \frown a \leqq b^*$; since $y \frown a \leqq b^{**}$, we infer $y \frown a = 0$. Similarly, from $y \frown a = 0$ we infer $y \leqq a^* \frown a^{**} = 0$. We conclude that $x \frown a \frown b = 0$ implies $x \frown a^{**} \frown b^{**} = 0$, or $(a \frown b)^* \leqq (a^{**} \frown b^{**})^*$. But the reverse inequality is obvious from (23). Using (23) again in the resulting equality, we get

$$(23'')\qquad (a \frown b)^* = (a^{**} \frown b^{**})^* = ((a^* \smile b^*)^*)^* = a^* \vee b^*.$$

By (23)–(23″), the correspondence $a \to a^{**}$ is a homomorphism of L onto A, which is thus a complemented distributive lattice. We shall now describe the associated congruence relation on L.

Let D be the set (dual ideal) of all $d \in L$ satisfying $d^* = 0$; we shall call such elements "dense." Clearly $d \in D$ is equivalent to $d = a \smile a^*$ for some a, and to $d^{**} = I$. We now state our final result.

Theorem 16 (Glivenko[23]). *In any pseudo-complemented distributive lattice L, the correspondence $a \to a^{**}$ is a closure operation in L, and a lattice-homomorphism*

[23] V. Glivenko, Acad. Royale Belg., Bull. Sci. vol. 15 (1929), 83–8; see also Stone [3, p. 66].

of L onto the complete Boolean algebra of "closed" elements. Moreover $a^{**} = b^{**}$ if and only if $a \frown d = b \frown d$ for some "dense" d satisfying $d^{**} = I$.

Proof. We have proved all but the last sentence already. Suppose $a \frown d = b \frown d$, where $d^{**} = I$. Then

$$a^{**} = a^{**} \frown I = a^{**} \frown d^{**} = (a \frown d)^{**} = (b \frown d)^{**} = \cdots = b^{**}.$$

Conversely, suppose $a^{**} = b^{**}$; set $d = (a \smile b^*) \frown (a^* \smile b)$. Then $d^{**} = (a^{**} \vee b^*) \frown (a^* \vee b^{**}) = (b^{**} \vee b^*) \frown (a^* \vee a^{**}) = I$, by what we have already proved. Moreover

$$a \frown d = a \frown (a \smile b^*) \frown (a^* \smile b) = a \frown (a^* \smile b)$$

$$= (a \frown a^*) \smile (a \frown b) = a \frown b.$$

Similarly, $b = a \frown b$, completing the proof.

Ex. 1. Show by direct computations that identities (23) hold in any relatively pseudo-complemented lattice.

Ex. 2. In each of the two non-distributive lattices of five elements, find a, b such that a^*b does not exist.

Ex. 3. Find a, b in $L = 2^2 \oplus 1$ such that $(a \frown b)^* > a^* \smile b^*$.

Ex. 4. (a) Show that the elements of any finite distributive lattice form a pseudo-complemented lattice.

(b) Prove that every chain is relatively pseudo-complemented.

Ex. 5. (a) Show that the ideals of any distributive lattice form a complete pseudo-complemented lattice. (M. H. Stone)

(b) Show that the congruence relations on any lattice form a pseudo-complemented lattice.

Ex. 6. Show that the open subsets of any topological space form a pseudo-complemented lattice.

Ex. 7. Show that if every interval sublattice of a lattice L is pseudo-complemented, then L is distributive.

Ex. 8. Show that any distributive lattice is isomorphic with a sublattice of a relatively pseudo-complemented lattice.

Problem 70. What is the most general pseudo-complemented distributive lattice in which $a^* \smile a^{**} = I$ identically? (M. H. Stone)

13. Distributive functionals; relation to wave equation. We shall now characterize those valuations which determine *distributive* metric lattices.

This is easy; since $x \smile (y \frown z) \leqq (x \smile y) \frown (x \smile z)$ in any lattice, a metric lattice will be distributive if and only if $v[x \smile (y \frown z)] = v[(x \smile y) \frown (x \frown z)]$ identically. But in any metric lattice, we have by V1 of Ch. V, §6,

$$v[x \smile (y \frown z)] = v[x] + v[y] + v[z] - v[y \smile z] - v[x \frown y \frown z],$$

$$v[(x \smile y) \frown (x \smile z)] = v[x \smile y] + v[x \smile z] - v[x \smile y \smile z].$$

Substituting and transposing, we get the equivalent symmetric condition

$$v[x \cup y \cup z] - v[x \cap y \cap z] = v[x \cup y] + v[y \cup z] + v[z \cup x] - v[x] - v[y] - v[z]. \tag{24}$$

This condition is not self-dual, but by V1 again,

$$v[x \cup y] + v[y \cup z] + v[z \cup x] - v[x] - v[y] - v[z] = v[x] + v[y] + v[z] - v[x \cap y] - v[y \cap z] - v[z \cap x].$$

Hence (24) is equivalent to the *self-dual*, symmetric condition

$$2\{v[x \cup y \cup z] - v[x \cap y \cap z]\} = v[x \cup y] + v[y \cup z] + v[z \cup x] - v[x \cap y] - v[y \cap z] - v[z \cup x]. \tag{25}$$

Valuations satisfying (25) will be called *distributive* valuations. We conclude

THEOREM 17. *A metric lattice is distributive if and only if its valuation is distributive.*

The concept of a valuation bears an interesting relation to the two-dimensional wave equation, $\partial^2 v/\partial x^2 = \partial^2 v/\partial t^2$. It is well known that if the characteristics $r = x + t$, $s = x - t$ are used as independent variables, the wave equation assumes the simple form $\partial^2 v/\partial r \partial s = 0$. The general solution is then given by

$$v(r, s) = f(r) + g(s),$$

subject to suitable differentiability conditions.

But now recall that the characteristics partially order the space-time of independent variables.[24] Under this partial ordering, $(r, s) \leqq (r_1, s)$ if and only if $r \leqq r_1$ and $s \leqq s_1$. Hence $(r, s) \cup (r_1, s_1) = (\text{Max}\,(r, r_1), \text{Max}\,(s, s_1))$, and dually, giving the distributive lattice R^{*2}, where R^* denotes the chain of real numbers. We can now state the connection.

THEOREM 18. *A real-valued function satisfies the wave equation in two-dimensional space-time, if and only if it is a valuation for the lattice defined by the usual partial ordering of relativistic time.*

Indeed, suppose that v is a valuation. Then $(r, s) = (r, O) \cup (O, s)$ and $(O, O) = (r, O) \cap (O, s)$. Hence $v(r, s) = v(r, O) + [v(O, s) - v(O, O)] = f(r) + g(s)$. Conversely, if $v(r, s) = f(r) + g(s)$, then

$$\begin{aligned} v &= v[(r, s) \cup (r_1, s_1)] + v[(r, s) \cap (r_1, s_1)] \\ &= v[\text{Max}\,(r, r_1), \text{Max}\,(s, s_1)] + v[\text{Min}(r, r_1), \text{Min}\,(s, s_1)] \\ &= f(\text{Max}\,(r, r_1)) + f(\text{Min}\,(v, r_1)) + g(\text{Max}\,(s, s_1)) + g(\text{Min}\,(s, s_1)) \\ &= f(r) + f(r_1) + g(s) + g(s_1) = v(r, s) + v(r_1, s_1). \end{aligned}$$

This completes the proof.

[24] See Ex. 1 of §2, Ch. I. Physically, $(x, y) \leqq (x_1, y_1)$ means that a light-signal can be transmitted from (x, y) to (x_1, y_1).

It would be interesting to know how this principle can be generalized; the problem is not easy. Thus, although the characteristics define a natural partial ordering for any hyperbolic differential equation, this does not define a lattice except in the two-dimensional case. Again, the characteristics vary from solution to solution in the non-linear case.

If we try to generalize the lattice, we run up against the difficulty that we do not know how to define the concept of an *analytic lattice*, in a significant way. These questions are extremely interesting.

Ex. 1. What identity on valuations is yielded by L6?

Ex. 2. Show that any finite metric distributive lattice is isomorphic to a ring of sets, under an isomorphism which makes $v[x]$ equal the measure of the set corresponding to x.

Ex. 3. Show that any product of endomorphisms of the form $x \to x \smile c$ or $x \to x \frown c$ can be written in the form $x \to (x \smile a) \frown b$, for suitable a, b.

Ex. 4. (a) Using Ex. 3, show that if intervals $[x, y]$ and $[x_1, y_1]$ are projective, in a distributive lattice, then $x_1 = (x \smile a) \frown b$ and $y_1 = (y \smile a) \frown b$, for some a, b.

(b) Infer that $x_1 \leqq x$, $y_1 \leqq y$ imply $x = x_1$, $y = y_1$,—i.e., that in a distributive lattice, *no interval can be projective to a proper part of itself* [LT, §98].

Problem 71. Let L be a lattice with a valuation which satisfies (25), and is such that $v[t]$ is not constant on an interval $[x, y]$ unless $x = y$. Show that L is distributive. (Suggestion: Decompose the valuation into positive and negative parts.)

CHAPTER X

BOOLEAN ALGEBRAS

1. Definition. Historically, the first lattices considered were the complemented distributive lattices studied by Boole [1], and named in his honor.[1] Obviously, all the results of Chapter VIII apply to Boolean algebras (cf. Exs. 1–2 below).

There is a close connection between the distributive law and unicity of complementation, already noted in Ch. IX, Thm. 2, Cor. 1. One proves easily[2]

THEOREM 1. *In a distributive lattice, complementation is unique and is orthocomplementation. Hence, in any Boolean algebra, we have*

L8. $(x \frown y)' = x' \smile y'$ *and* $(x \smile y)' = x' \frown y'$.

L9. $(x')' = x$, *as well as*

L10. $x \frown x' = O$ *and* $x \smile x' = I$.

Proof. If $a \smile x = I$ and $a \frown y = O$, then

$$x = O \smile x = (a \frown y) \smile x = (a \smile x) \frown (y \smile x) = I \frown (y \smile x) = y \smile x.$$

If also $a \frown x = o$ and $a \smile y = I$, then similarly $y = y \smile x$, whence $x = y$. This proves unicity. But by L2, the relation of complementarity is symmetric, and so $(a')' = a$. Again, if $a \leqq b$, then $a \smile a' = I$ and $a \frown b' \leqq b \frown b' = O$. Hence, as above, $a' = b' \smile a'$, and $b' \leqq a'$. That is, the correspondence $a \rightarrow a'$ is a dual automorphism, completing the proof.

From this theorem it follows directly that any Boolean algebra is dually isomorphic with itself. It is a second corollary that any lattice-automorphism of a Boolean algebra preserves complementation: the operation of complementation is *intrinsic*.

THEOREM 2. *The complemented elements of any distributive lattice form a sublattice.*

Proof. If x and y are complemented, then

$$(x \frown y) \frown (x' \smile y') = (x \frown y \frown x') \smile (x \frown y \frown y') = O \smile O = O,$$

and dually. Hence $x \frown y$ has the complement $x' \smile y'$, as in L8. Dually, $x \smile y$ has the complement $x' \smile y'$, completing the proof.

---

[1] Thus even in 1897, A. N. Whitehead wrote (*Universal algebra*, p. 35) that "Boolean algebra is the only known member of the non-numerical genus of universal algebra."

[2] The result goes back to R. Grassmann; see Schröder [1, pp. 299, 305, 352]. Cf. the Cor. of Ch. VIII, §5; also §13 below, for related results and extensions.

Ex. 1. Prove that every interval $[a, b]$ of a Boolean algebra L is a Boolean algebra, in which the meanings of $\leqq$, $\frown$, $\smile$ are the same as in L, but complements in $[a, b]$ are "relative complements" in L.

Ex. 2. (a) Show that in any Boolean algebra of finite length, every element is the join of points.

(b) Conversely, show that if L is a distributive lattice of finite length in which I is a join of points, then L is a Boolean algebra.

Ex. 3. Show that any lattice-homomorphism θ of a Boolean algebra A onto a Boolean algebra B preserves complementation—i.e., that if a', b' are any complements of $a \in A$ and $b = \theta(a) \in B$, then $\theta(a') = b'$.

Ex. 4. Find a modular lattice of six elements in which the complemented elements do not form a sublattice.

2. Examples. The subsets of any aggregate I form a Boolean algebra· the set-theoretic operations of sum, product, and complement become the lattice-theoretic operations of join, meet and complement. More generally, any field of sets is a Boolean algebra, under the same interpretations. Boolean algebras also arise in many other ways, from which we select a few examples.

Example 1. The center of any lattice is a Boolean algebra. (Ch. II, §§9–10.)

Example 2. Consider the class of all binary relations between the elements of two classes I and J. There is a one-one correspondence between relations ρ and subsets R of the product-class $I \times J$: $x\rho y$ if and only if $(x, y) \in R$. Hence the binary relations between I and J form a Boolean algebra.

This Boolean algebra is discussed in detail in Ch. XIII, §§5–6. Other examples of Boolean algebra arising in set theory and logic are discussed in Chs. XI–XII. For the present, we note only the following additional abstractly defined examples.

Any cardinal product of Boolean algebras is a Boolean algebra. So is any "subalgebra" of a Boolean algebra—i.e., any subset closed with respect to all three Boolean operations. So also is any lattice-homomorphic image of a Boolean algebra: it is a distributive lattice, and the equations $x \frown x' = O$, $x \smile x' = I$ are preserved.

Ex. 1. Show that the neutral elements of any complemented lattice form a Boolean algebra.

Ex. 2. Show that any complete lattice is a join-homomorphic image of a Boolean algebra. (Hint: Consider the correspondence $S \to \bigvee_S x_\alpha$ for subsets of L.)

Problem 72. Find necessary and sufficient conditions on a lattice L, that its congruence relations should form a Boolean algebra.

3. Boolean rings. M. H. Stone[3] has shown that one can subsume the theory

[3] Historical note. Boole originally characterized Boolean algebra as the algebra of 0 and 1 [1, p. 37], but he did not realize the significance of addition modulo two. Relations between Boolean algebras and rings of characteristic two were noted by P. J. Daniell, Bull. Am. Math. Soc. 23 (1916), 446–50; B. A. Bernstein, Trans. Am. Math. Soc. 26 (1924), 171–4; Gegalkin, Mat. Sbornik 35 (1928), 311–73; O. Frink, Bull. Am. Math. Soc. 34 (1928), 329–33; H. Whitney, Annals of Math. 34 (1933), 405–14. But Stone [2], [3] was the first to establish the one-one correspondence between Boolean algebras and a clear-cut family of rings, described in Thm. 3.

of Boolean algebras under the general theory of rings—actually, of commutative rings of characteristic two, in the usual sense.

To motivate this, we recall the notion of the "characteristic function" f_X of a set X in a space I: the function defined on the points $p \in I$, and satisfying $f_X(p) = 1$ or 0 according as $p \in X$ or $p \in X'$. Then $f_X f_Y = f_{X \frown Y}$, and $f_X + f_Y = f_{(x \frown y') \smile (x' \frown y)}$ mod 2. Thus, relative to *meets* $XY = X \frown Y$ and *symmetric differences* $X + Y = (X \frown Y') \smile (X' \frown Y)$, the elements of the Boolean algebra A defined by any field of sets form a ring $R(A)$ of characteristic two, with unit I satisfying $IX = XI = X$ for all X. Moreover in $R(A)$, $XY = YX$ and $XX = X$ identically: the ring is commutative, and all its elements are idempotent.

Actually, in any ring, the identity $xx = x$ implies $x + y = (x + y)(x + y) = xx + yx + xy + yy = x + y + yx + xy$, and so it implies $xy + yx = 0$. Setting $x = y$, we get $x + x = 0$, and $x = -x$. Using this, we get $xy - yx = 0$, and so $xy = yx$. Hence $xx = x$ implies both $xy = yx$ and $x + x = 0$. This suggests the following definition.

DEFINITION. *A "Boolean ring" is a ring whose elements are all idempotent.*

THEOREM 3. *There is a one-one correspondence between Boolean algebras and Boolean rings with unit. Under this, inclusion corresponds to divisibility, lattice meets to ring products, $O = 0$, $I = 1$, and*

(1) $$x + y = (x \frown y') \smile (x' \frown y) \text{ and } x \smile y = x + y - xy.$$

Proof. Let R be any Boolean ring with unit 1. If one defines $x \geqq y$ to mean $xy = y$, then clearly (i) $1 \geqq x \geqq 0$ for all x, (ii) $x \geqq x$ by idempotence, (iii) if $x \geqq y$ and $y \geqq x$, then $x = yx = xy = y$ by hypothesis and commutativity, (iv) if $x \geqq y$ and $y \geqq z$, then $x = xy = x(yz) = (xy)z = xz$, and so $x \geqq z$, (v) $x \geqq xy$, since $x(xy) = (xx)y = xy$, (v′) similarly, using commutativity, $y \geqq xy$, (vi) if $x \geqq z$ and $y \geqq z$, then $xyz = xz = z$ and so $xy \geqq z$, (vii) the correspondence $x \rightleftarrows 1 - x$ is obviously one-one; moreover since $xy = y$ implies $(1 - y)(1 - x) = 1 - y - x + xy = (1 - x)$, it inverts inclusion; hence it is a dual automorphism.

Hence our definition makes R into a partly ordered set with O and I (by (i)–(iv)), in which $x \frown y$ exists and is xy (by (v)–(vi)), whence (by (vii)) $x \smile y$ exists and is $1 - (1 - x)(1 - y) = x + y - xy$, as in (1). Also, if we define $x' = 1 - x$, then $x \frown x' = x(1 - x) = 0$ and $x \smile x' = x + (1 - x) + x(1 - x) = 1$; hence our definition makes R into a complemented lattice. Finally,

$$\begin{aligned} x \frown (y \smile z) &= x(y + z - yz) = xy + xz - xyz \\ &= xy + xz - xyxz = (x \frown y) \smile (x \frown z), \end{aligned}$$

and so R is a Boolean algebra.

Conversely, in any Boolean algebra A, define as by (1)

$$x + y = (x \frown y') \smile (x' \frown y) = (x \smile y) \frown (x' \smile y').$$

Obviously $O + x = x, x + y = y + x$ and $x + x = O$. Again, one easily computes $(x + y)' = (x' \frown y') \smile (x \frown y)$, and, using this,

$$(x + y) + z = (x \frown y' \frown z') \smile (x' \frown y \frown z') \smile (x' \frown y' \frown z) \smile (x \frown y \frown z).$$

By left-right symmetry, this is also equal to $x + (y + z)$. Hence addition is commutative and associative, O is an identity, and every element is its own inverse; hence A is a commutative group under addition. Further, multiplication as defined by $xy = x \frown y$ is obviously idempotent, commutative, and associative, and I is a multiplicative unit.

It remains to check the distributive law, as follows:

$$\begin{aligned} xz + yz &= [x \frown z \frown (y' \smile z')] \smile [(x' \smile z') \frown y \frown z] \\ &= [x \frown z \frown y'] \smile [x' \frown y \frown z] \\ &= [(x \frown y') \smile (x' \frown y)] \frown z = (x + y)z. \end{aligned}$$

This completes the proof; further results are assigned as exercises.[4]

Ex. 1. (a) Show that the idempotent elements of any commutative ring form a Boolean subring.

(b) Show that any commutative ring is also a ring under the "dual operations"

$$x \circ y = x + y - xy \quad \text{and} \quad x \oplus y = x + y - 1.$$

Ex. 2. Show that, under the correspondence of Thm. 3, $a \frown b$ corresponds to l.c.m.(a, b), $a \smile b$ to g.c.d. (a, b), automorphisms to automorphisms, Boolean subalgebras to subrings, ideals to ideals, and lattice-theoretic prime ideals to ring-theoretic prime ideals.

Ex. 3. Generalize Thm. 3 to a correspondence between all Boolean rings and all relatively complemented distributive lattices with 0.

4. Digression: postulate theory. Boolean algebra can be defined by widely varying postulate systems. We shall mention only a few of these,[5] although their comparative study gives an excellent idea of the power of postulate theory.

Perhaps the most remarkable system is due to Newman[6] [1]. Let A be any algebra with two binary operations, which satisfies the following postulates:

N1. $a(b + c) = ab + ac$. N1′. $(a + b)c = ac + bc$.

N2. $\exists 1$, such that $a1 = a$ for all a.

N3. $\exists 0$, with $a + 0 = a = 0 + a$, for all a.

N4. To each a corresponds at least one a', such that $aa' = 0$ and $a + a' = 1$.

[4] Most of these are due to Stone [2], [3, Thm. 4 ff]. Others are due to R. Vaidyanathaswami, Jour. Ind. Math. Soc., Vol. II (1937), No. 6; A. L. Foster, Trans. Am. Math. Soc. 59 (1946), 166–87, where further results may be found.

[5] For the literature prior to 1933, see E. V. Huntington, *Postulates for the algebra of logic*, Trans. Am. Math. Soc. 35 (1933), 274–304 (corrections pp. 557, 971, ibid.).

[6] We follow the exposition of G. D. Birkhoff and G. Birkhoff, Trans. Am. Math. Soc. 60 (1946), 3–11. The existence of a common theory of Boolean algebras and rings was indicated earlier by E. T. Bell, Trans. Am. Math. Soc. 29 (1927), 597–611. For further related work, see Newman, Jour. Lond. Math. Soc. 17 (1942), 34–47, and 19 (1944), 28–31; also R. B. Braithwaite, ibid. 17 (1942), 180–92.

It will be observed that neither idempotence, commutativity, nor associativity of either operation is assumed. We now prove

(T1) $$aa = aa + 0 = aa + aa' = a(a + a') = a1 = a.$$

With a little more computation, we prove

(T2) $$(a')' = a \text{ for all } a \text{ and all } (a')'.$$

Proof.
$$\begin{aligned}(a')' &= 0 + (a')'(a')' \\ &= a'(a')' + (a')'(a')' = (a' + (a')')(a')' \\ &= 1(a')' = (a + a')(a')' = a(a')' + 0 \\ &= 0 + a(a')' = aa' + a(a')' \\ &= a(a' + (a')') = a1 = a.\end{aligned}$$

It is a corollary that

(N4′) $a'a = 0$ and $a' + a = 1$;

and another, that complements are unique. (For if a' is any complement of a, then $a' = ((a')')'$, for any $((a')')'$.) Further

(T3) $$a0 = 0 = 0a, \text{ for all } a.$$

Proof. $0 = aa' = a(a' + 0) = aa' + a0 = 0 + a0 = a0$, and $0 = bb' = (0 + b)b' = 0b' + bb' = 0b' + 0 = 0b'$. But by T2 every $a = b'$, where $b = a'$.

It is a corollary that if $0 = 1$, then

$$0 = 0 + 0 = a + a\cdot 0 = 0 + a\cdot 1 = a\cdot 1 = a, \text{ for all } a.$$

Hence, except in this trivial one-element case, $0 \neq 1$. We shall assume $0 \neq 1$ from now on. It is another corollary that

(N2′) $$1a = (a + a')a = aa + a'a = a + 0 = a, \qquad \text{for all } a.$$

Hence there is *complete left-right symmetry in the properties of addition and multiplication.*

We now define $1 + 1 = 2$, $(1 + 1) + (1 + 1) = 2 + 2 = 4$, and call the left-multiples $y2$ of 2 *even* elements. Note that $4 = 2 + 2 = 2\cdot 1 + 2\cdot 1 = 2(1 + 1) = 2\cdot 2 = 2$, by T1. Next

(T4) x is even if and only if $x + x = x$.

For clearly $y2 + y2 = y(2 + 2) = y2$; conversely, if $x = x + x$, then $x + x\cdot 1 + x1 = x(1 + 1) = x2$.

(T5) Any multiple xt or ux of an even element is even.

For if $x = x + x$, then $xt = (x + x)t = xt + xt$ and $ux = u(x + x) = ux + ux$ for all t, u.

(T6) The correspondence $x \to x + x = x2$ is an idempotent endomorphism: $(x + y)2 = x2 + y2$, $(xy)2 = (x2)(y2)$, and $(x2)2 = x2$.

Proof. $(x + y)2 = x2 + y2$; $(x2)2 = x2 + x2 = x(2 + 2) = x2$, and

$$(x2)(y2) = (x + x)(y + y) = (x + x)y + (x + x)y$$

$$= (xy + xy) + (xy + xy) = (xy)2 + (xy)2 = (xy)2, \text{ by T4.}$$

It is a corollary that *the even elements form a subalgebra B*, in which addition is idempotent. In this subalgebra, we have

$$a + 1 = (a + 1)(a + a') = (aa + a) + (aa' + 1a')$$

$$= (a + a) + (0 + a') = a + a' = 1$$

for all a. By left-right symmetry, $1 + a = a$. But this result, (T1), N1–N4, and (N4′), (N2′) imply by Thm. 3 of Ch. IX that the subalgebra B is a Boolean algebra, in which 2 acts as I. Complements in B are relative complements in A.

Similarly, one may show that the "odd" elements, satisfying the equivalent conditions $x = y2'$, $x = x2'$, $x + x = 0$, form a subalgebra which is commutative ring with unity satisfying $1 + 1 = 0$,—i.e., a non-associative Boolean ring. Moreover A is the direct union of these subalgebras. For the details, the reader is referred to either of the articles previously mentioned. This implies

THEOREM 4. *Any "Newman algebra" satisfying* N1–N1′, N2, N3, N4 *is the direct union of a Boolean algebra and a (possibly non-associative) Boolean ring.*

What we have proved in detail shows that

COROLLARY. *Identities* $a \smile a = a$, $a \smile 0 = 0 \smile a = a$, $I \frown a = a$, L6′–L6″, *and* L10 *are postulates for a Boolean algebra.*

Another noteworthy postulate system for Boolean algebra is in terms of Sheffer's[7] *stroke-operation*

(2) $$x \mid y = x' \frown y' \text{ (binary rejection).}$$

All Boolean operations can be expressed in terms of this single binary operation (cf. Ex. 2c below); thus

(3) $$x' = x \mid x, \quad x \frown y = (x \mid x) \mid (y \mid y), \quad x \smile y = (x \mid y) \mid (x \mid y).$$

However, the postulate systems for this operation so far developed are not

---

[7] H. M. Sheffer, *A set of five independent operations for Boolean algebras*, Trans. Am. Math. Soc. 14 (1913), 481–8. Recently A. H. Diamond and J. C. C. McKinsey have shown that no postulate system for Boolean algebra can involve only two variables and identities (Bull. Am. Math. Soc. 53 (1947), 959–62).

particularly elegant. Thus Sheffer proposed defining $a' = (a \mid a)$, and postulating $(a')' = a$, $(a \mid (b \mid b')) = a'$, $(a \mid (b \mid c))' = (b' \mid a) \mid (c' \mid a)$.

The ternary *median* operation

$$(x, y, z) = (x \frown y) \smile (y \frown z) \smile (z \frown x) = (x \smile y) \frown (y \smile z) \frown (z \smile x) \tag{4}$$

of Ch. IX, §3 can also be used as a basis for Boolean algebra.[8] We note here, for reference in Ch. XIV, only the following result.

THEOREM 5. *Every group-translation $x \to x + a$ in a Boolean algebra A is an automorphism for the median operation* (4).

Proof. By direct computation in (1), we get

$$\begin{aligned}(x + a) \frown (y + a) &= [a' \frown (x \frown y)] \smile [a \frown (x \smile y)'],\\ (x + a) \smile (y + a) &= [a' \frown (x \smile y)] \smile [a \frown (x \frown y)'].\end{aligned} \tag{5}$$

By induction, we infer that for any lattice polynomial $p(x_1, \cdots, x_n)$,

$$p(x_1 + a, \cdots, x_n + a) = [a' \frown p(x_1, \cdots, x_n)] \smile [a \frown g(x_1, \cdots, x_n)],$$

where g is the complement of the dual of p. Hence if p is *self-dual*, like (x, y, z), we have $p(x_1 + a, \cdots, x_n + a) = p(x_1, \cdots, x_n) + a$.

This completes the proof. Other results are given as exercises below[9].

Ex. 1. Show that the following postulates on meet and complement serve to define a Boolean algebra: (a) $x \frown y' = z \frown z'$ if and only if $x \frown y = y$, (b) $x \frown y = y \frown x$, (c) $x \frown (y \frown z) = (x \frown y) \frown z$.

Ex. 2. (a) Prove that the median operation satisfies $(a, b, c)' = (a', b', c')$ in any Boolean algebra.

(b) Give a set of postulates for Boolean algebra, based on Thm. 4, involving meets and complements only.

(c) Develop a system involving only Sheffer's stroke-symbol.

Ex. 3. (a) Show that $x + y = x \frown y + x \smile y$ in any Boolean algebra, if $+$ denotes symmetric difference.

(b) Show that any finite distributive lattice with the property of Thm. 5 is a Boolean algebra.

Ex. 4. Show that any system which satisfies $a \frown a = a \smile a = a$, $a \smile b = b \smile a$, $a \smile (x \frown a) = a$, $x \smile a = I$, $a \frown (b \smile c) = (a \frown b) \smile (a \frown c)$, $(a \smile b) \frown c = (a \frown c) \smile (b \frown c)$ is a Boolean algebra.

Ex. 5. Let R be any commutative ring with unity in which $1 + 1 = 0$ and $x(1 - x)y(1 - y) = 0$. Show that the identity $a = (a - aa) + aa$ decomposes every $a \in R$ *uniquely* into the sum of a nilpotent and an idempotent component.

Ex. 6. Using only N1–N4 and their consequences, prove

(a) $a + b = (a + b)(b + b') = (a + 1)b + ab' = \cdots = b + a$.

---

[8] See A. A. Grau, Bull. Am. Math. Soc. 53 (1947), 567–72; also S. Kiss [1]. Thus the algebra of logic of Kiss has a different group (in the sense of F. I. Mautner, *Logic as invariant theory*, Am. Jour. 68 (1946), 345–84) than the usual propositional calculus.

[9] For Ex. 1, see Lee Byrne, Bull. Am. Math. Soc. 52 (1946), 269–72; also Huntington, op. cit. supra, fourth set. Ex. 4 is due to M. H. Stone, Am. Jour. 57 (1935), 703–32. Ex. 5 is due to A. L. Foster, Trans. Am. Math. Soc. 59 (1946), 166–87. For Ex. 6, see Newman [1]. Ex. 7 is very difficult; see M. H. A. Newman [1, Thm. 1b], and also Jour. Lond. Math. Soc. 19 (1944), 28–30.

(b) $1 + (1 + c) = [1 + (1 + 1)]c + (c' + c') = \cdots = (1 + 1) + c$, by right-multiplying by $c + c'$, expanding, and using (a) to infer $1 + (1 + 1) = (1 + 1) + 1$.

(c) $1 + (b + c) = (1 + b) + c$, using Part (b) and a similar right-multiplication by $b + b'$.

(d) $a + (b + c) = (a + b) + c$, using Part (c).

Ex. 7*. Show that, in Thm. 4, condition $0 + a = a$ is redundant.

5. Representation theory. The representation theory for distributive lattices, given in §§4–5 of Ch. IX, has a significant specialization to the case of Boolean algebras. We know (Ch. VIII, Thm. 1) that the only elements $p_i > 0$ of a complemented modular lattice which are join-irreducible are its points. Hence if L is complemented, the X of Thm. 5, Ch. IX, is totally unordered. We conclude

THEOREM 6. *Every Boolean algebra of finite length n is isomorphic with the field of all subsets of a set of n elements.*

Thus, in particular, there is just one Boolean algebra of length n; it is $\mathbf{2}^n$.

Again, in the Cor. of Thm. 6 of Ch. IX, we can delete the points not in I and those in O, and so get an isomorphic representation in which O corresponds to the void set, and I to all space. But in such a representation, complements must by L10 correspond to complements. We conclude Stone's result

THEOREM 7. *Any Boolean algebra is isomorphic with a field of sets.*

Thus any postulate system for Boolean algebra is *ipso facto* a complete postulate system for the algebra of classes under finite union, finite intersection, and complementation.

Ex. 1. Show that every Boolean algebra which satisfies the descending chain condition is finite.

Ex. 2. Show that every distributive lattice is isomorphic with a sublattice of a complemented distributive lattice.

Ex. 3*. Prove the result of Ex. 2, without assuming the Axiom of Choice or any theorem depending thereon.[10]

6. Ideal theory. In a distributive lattice, every ideal is neutral. Hence we have as an immediate corollary of Thm. 11, Ch. VIII, the following result.

THEOREM 8. *The ideals of any Boolean algebra A correspond one-one to its congruence relations θ; each θ corresponds to the ideal J of $x \equiv 0 \pmod{\theta}$.*

We could also infer this result from the theory of rings (Ex. 1 below). But it is so important that we shall give a special, less technical, proof of the fact that every ideal J determines a congruence relation in A. Combined with Thm. 3 of Ch. II, this will give an independent proof of Thm. 8.

Proof. Given J, we define $x \equiv y\ (J)$ to mean that $x \cup t = y \cup t$ for some

[10] This result may be found in H. M. MacNeille, *Lattices and Boolean rings*, Bull. Am. Math. Soc. 45 (1939), 452–5; also in MacNeille [1]. For Thm. 7, see M. H. Stone [1], [3]; N. Dunford and M. H. Stone, Revista Ciencias Lima 43 (1941), 447–53; O. Frink, Bull. Am. Math. Soc, 47 (1941), 755–6.

$t \in J$; this relation is clearly reflexive and symmetric. It is transitive, for if $x \smile t = y \smile t$ and $y \smile u = z \smile u$ $[t, u \in J]$, then $x \smile (t \smile u) = y \smile t \smile u = y \smile u \smile t = z \smile u \smile t = z \smile (t \smile u)$, for some $t \smile u \in J$. Hence it is an equivalence relation. Again, suppose $x \equiv y$ (J). Then, for any a, $a \smile x \smile t = a \smile y \smile t$; hence $a \smile x \equiv a \smile y$ (J), and the substitution property for joins holds. Moreover all this applies to any lattice. Further, if $x \equiv y$ (J), then $(a \frown x) \smile t = (a \smile t) \frown (x \smile t) = (a \smile t) \frown (y \smile t) = (a \frown y) \smile t$, and we have a congruence relation for meets and joins. Finally, $x \equiv 0$ (J) implies $x \leqq x \smile t = 0 \smile t = t$ for some $t \in J$, hence $x \in J$, and conversely; hence J is the set of all $x \equiv 0$ (J), q.e.d.

Incidentally, we note that any lattice-homomorphism carries complements into complements, by L10. Hence $x \equiv y$ (J) implies $x' \equiv y'$ (J), and lattice-homomorphisms have the substitution property for all three Boolean operations.

We recall from Ch. IX, §6, that the ideals of any distributive lattice themselves form a distributive lattice; moreover joins and meets of ideals may be interpreted in the sense of the calculus of complexes. These, and all other results of Ch. IX, §6, apply *a fortiori* to Boolean algebras. We note here, and in Exs. 3–6 below, properties of ideals in Boolean algebras which are not true in all distributive lattices.

First, an ideal of a Boolean algebra A is *prime* if and only if it is *maximal* (Stone [3]). Indeed, if P is prime in a Boolean algebra, for any $a \notin P$, we have $a' \in P$ since $a \frown a' = O \in P$; hence any ideal $J > P$ contains some $a \notin P$ and a', and so I. Conversely, suppose that M is maximal, with $x \frown y \in M$ and $x \notin M$. Then $x \smile M$ contains I; hence, for some $z \in M$, $x \smile z = I$, and $y = y \frown I = y \frown (x \smile z) = (y \frown x) \smile (y \frown z) \in M \smile M = M$. Hence M is prime, q.e.d.

For any subset X of a Boolean algebra A, let X^* denote the set of all $a \in A$ such that $a \frown x = 0$ for all $x \in X$. Evidently $a \frown x' = 0$ for all $x \in X$ if and only if $a \leqq x$ for all $x \in X$—i.e., if and only if a belongs to the *closed ideal* whose upper cut is x (Ch. IV, §7). Again, if J is an ideal of A, then J^* is the pseudo-complement of J in the distributive lattice of all ideals, in the sense of Ch. IX, §12. Hence an ideal of a Boolean algebra is closed if and only if it is the pseudo-complement of some other ideal.

We now define an ideal J to be *dense* if and only if $J^* = 0$. This means that, for any $a > 0$ of A, we can find $x > 0$ in J such that $x \frown a > 0$—hence $y = x \frown a > 0$ in J with $y \leqq x$. Using this condition, one shows easily that the intersection of any two dense ideals is dense. Again, if J is dense and $K \geqq J$, then evidently K is dense. Hence the *dense ideals form a dual ideal in the distributive lattice of all ideals of A.*

Again, since $(K \smile K^*)^* = K^* \frown (K^*) = 0$ for any ideal K, $K \smile K^*$ is always dense. Moreover $(K^*)^* \frown (K \smile K^*) = ((K^*)^* \frown K^*) \smile ((K^*)^* \frown K^*) = K$; hence, modulo this dual ideal, every ideal is congruent to its closure $(K^*)^*$. We next show that, conversely, any ideal $K \frown D$ congruent to a closed ideal K modulo a "dense" ideal has K for closure. Indeed, $((K \frown D)^*)^* \leqq (K^*)^* = K$, clearly. While for any $b \in (K \frown D)^*$ and $a \in K$, $a \frown b > 0$ would imply $0 < d \leqq a \frown b \leqq a \in K$ for some $d \in D$, hence $d \in K \frown D$; but $d \leqq a \frown b \leqq b \in (K \frown D)^*$; hence $d = 0$, a contradiction. Hence every $a \in K$ satisfies $a \frown b = 0$ for all $b \in (K \frown D)^*$, and $K \leqq (K \frown D^*)^*$.

Hence there is a lattice-homomorphism of the distributive lattice of all ideals onto the lattice of closed ideals, whence the latter is also a distributive lattice. In this lattice, K and K^* are complementary, since $K \frown K^* = 0$, and the join $((K \smile K^*)^*)^* = O^* = I$ of K and K^* in the lattice (not a sublattice) of closed ideals is I. Hence (cf. Ch. IX, Thm. 16, and Ch. XI, §5)

THEOREM 9 (Glivenko-Stone[11]). *The completion by cuts $\bar{A}$ of any Boolean algebra A is a Boolean algebra; moreover the correspondence $J \rightarrow (J^*)^*$ is a lattice-homomorphism of the lattice of all ideals of A onto $\bar{A}$.*

Ex. 1. Prove Thm. 8 as a corollary of the corresponding proposition for rings.

Ex. 2. Show that any ideal in a distributive lattice L with 0 consists of the set of all elements congruent to 0 under a suitable congruence relation.

Ex. 3. Show that every ideal of a Boolean algebra A is principal, if and only if A is finite.

Ex. 4*. Show that any ideal of a Boolean algebra A is the intersection of the prime ideals which contain it.

Ex. 5. (a) Show that an ideal J of a Boolean algebra A is principal if and only if $J \smile J^* = A$.

(b) Infer that the closed ideals of A cannot be a sublattice of the lattice of all ideals, unless A is complete, so that every closed ideal is principal.

Ex. 6. (a) Show that, if K is any principal ideal of a Boolean algebra A, there exists a subalgebra S of A containing exactly one representative from each residue class of A.

(b*) Show that this need not be true for arbitrary ideals, except with rather special Boolean algebras.[12]

Ex. 7. Show that a distribution lattice is a Boolean algebra if and only if every prime ideal is maximal. (L. Nachbin)

Problem 73. Find necessary and sufficient conditions, in order that the correspondence between the congruence relations and (neutral) ideals of a lattice be one-one.

7. Subalgebras; automorphisms. A subalgebra of a Boolean algebra is a sublattice which contains with any x, also x', and hence O and I. It is easy to determine the subalgebras of a finite Boolean algebra $A = \mathbf{2}^n$. Indeed, any subalgebra S of A will be itself a Boolean algebra of finite length, whose "points" will be independent elements of $\mathbf{2}^n$ (disjoint subsets of I) whose join is I—that is, they will be the subsets into which some *partition* divides I. Conversely, the subsets into which any partition divides I are the indivisible or "atomic" members of a field of sets, so that the correspondence between subalgebras of $\mathbf{2}^n$ and partitions of I is one-one. Finally, $S \leqq T$ if and only if its "points" are joins of "points" of T—that is, if and only if T effects a subpartition of the partition effected by S. In summary[13]

[11] This result goes back to V. Glivenko, *Sur quelques points de la logique de Brouwer*, Bull. Acad. Sci. Belg. (1929), 183–88, and M. H. Stone [3, Thm. 28]. See also K. Gödel, Ergebnisse eines Kolloquiums, Vienna 4 (1933), 35–40.

[12] This result is due to J. von Neumann and M. H. Stone, Fund. Math. 25 (1935), 353–78.

[13] This result is due to the author [3, Thm. 21]. The generalization to closed Boolean subalgebras and sublattices of any $2^{\aleph}$ may be found in the author's *On rings of sets*, Duke Jour. 3 (1937), 443–54.

THEOREM 10. *The lattice of all subalgebras of any finite Boolean algebra* $\mathbf{2}^n$ *is dually isomorphic with the lattice of all partitions of* n *elements.*

A corresponding result is true for the lattice of all *closed* subalgebras of $\mathbf{2}^{\aleph}$, for any cardinal number $\aleph$; these are the "complete fields of sets" of a set of $\aleph$ points.

Again, for any n, every permutation of the n points of $A = \mathbf{2}^n$ induces a unique automorphism on A. Moreover every automorphism of A permutes its points. Hence *the group of automorphisms of* $\mathbf{2}^n$ *is the symmetric group* I *on* n *letters.* In particular, $\mathbf{1}$ and $\mathbf{2}$ are the only finite Boolean algebras without proper automorphisms.

Conversely, let $\phi(x_1, \cdots, x_r)$ be any operation on subsets x_i of a class I of n elements, which is permutable with every $\gamma \in \Gamma$, so that

$$(6) \qquad \phi(x_1\gamma, \cdots, x_r\gamma) = \gamma[\phi(x_1, \cdots, x_r)], \quad \text{for all} \quad \gamma \in \Gamma.$$

The Boolean subalgebra S of $\mathbf{2}^n$ generated by $x_1, \cdots, x_r$ defines a partition π of I into subclasses $a_1, \cdots, a_s$, as in Thm. 10. Moreover the subgroup Σ of all $\gamma \in \Gamma$ satisfying $x_i\gamma = x_i$ for all i is the largest group having the a_i for sets of transitivity, in the sense of group theory. Hence if $y = \phi(x_1, \cdots, x_r)$, so that, by (6), $y\gamma = y$ for all $\gamma \in \Sigma$, y must be a union of a_i, so that $y \in S$ is a Boolean function of the x_i. From this it follows that *Boolean operations on finite sets are precisely those invariant under the symmetric group of point-permutations.*[14]

Ex. 1. Show that the finite subalgebras of any Boolean algebra correspond one-one to the "partitions" of I into disjoint parts whose sum is I.

Ex. 2. (a) Show that the relation $\alpha s = s$ between permutations α and subsets s of n points defines a "polarity" between the closed subalgebras of $\mathbf{2}^n$, and a sublattice of the lattice of all subgroups of the symmetric group.

(b) Show that $\alpha s = s$ defines a similar polarity between certain sublattices of $\mathbf{2}^n$ and certain subsystems of the semigroup of all single-valued transformations of n points.

Ex. 3*. Show that the italicized statement at the end of §7 remains true if the word "finite" is omitted, and infinitary "Boolean" operations are allowed.

Problem 74. Does every infinite Boolean algebra A admit a proper automorphism?[15]

Problem 75. (M. Ward). Does there exist a (finite) lattice, not a Boolean algebra, which has a dual automorphism S of period two, permutable with every lattice-automorphism? Must S be unique? What about non-Desarguesian projective geometries?

---

[14] See F. I. Mautner, *An extension of Klein's Erlanger Program: Logic as invariant theory*, Am. Jour 68 (1946), 345–84. Note that the ternary median operation admits a larger group, by Thm. 5.

The propositions involving n variables have been enumerated by G. Pólya, Jour. Symbolic Logic 5 (1940), 98–102.

[15] This would probably imply that if $\alpha(s) = s$ for all automorphisms α of A such that $\alpha(x_1) = x_1, \cdots, \alpha(x_r) = x_r$, then s must be a Boolean function of the x_i.

8. Free Boolean algebras. We shall now determine the free Boolean algebra generated by n symbols. This question can be restated as follows. By a "Boolean function" of variables $x_1, \cdots, x_n$ is meant one built up from the three basic functions: join, meet, and complement. We ask: what are the different Boolean functions of the x_i, and how does one combine them? The answer was given by Boole himself [1, pp. 72–5].

To get the answer,[16] first form the 2^n "elementary" Boolean functions f_i: $x_{i1} \frown \cdots \frown x_{in}$—where x_{ij} is either x_j or x_j', depending on i. For example, if $n = 2$, form $f_1 = x_1 \frown x_2$, $f_2 = x_1 \frown x_2'$, $f_3 = x_1' \frown x_2$, $f_4 = x_1' \frown x_2'$. Next observe that distinct f_i are disjoint: if $i \neq k$, then $f_i \frown f_k \leqq x_j \frown x_j'$ for some j, whence $f_i \frown f_k = 0$.

Then associate with each non-void set S of f_i the function $g_S = \bigvee_{i \in S} f_i$, and define g_0 as 0. We shall prove: (1) $g_O = O$ and $g_I = I$, (2) $g_{S \frown T} = g_S \frown g_T$, $g_{S \smile T} = g_S \smile g_T$, and $g_{S'} = (g_S)'$, (3) every Boolean function of the x_i is a g_S.

Proof of (1). By definition, $g_0 = 0$, while by the general distributive law,

$$I = \bigwedge_{j=1}^{n} (x_j \smile x_j') = \bigvee_{i=1}^{2^n} \bigwedge_{j=1}^{n} x_{ij} = \bigvee_{i \in I} f_i .$$

Proof of (2). $g_S \smile g_T = g_{S \smile T}$ by definition and L1–L3. Again, $g_S \frown g_T$ is the join of the $f_i \frown f_k$ $[i \in S, k \in T]$ by the general distributive law, while $f_i \frown f_k$ is 0 unless $i = k$. Hence $g_S \frown g_T = \bigvee f_i \frown f_i$ $[i \in S, i \in T]$, which by L1 is $\bigvee f_i$ $[i \in S \frown T]$, or $g_{S \frown T}$, q.e.d. It follows that $g_S \smile g_{S'} = I$ and $g_S \frown g_{S'} = 0$, whence $g_{S'} = (g_S)'$.

Proof of (3). By (2), every Boolean function of g_S is itself a g_S; hence it suffices to show that the x_i are g_S—and, by symmetry, that x_1 is. But by the general distributive law, if X_1 denotes the set of i such that $x_{i1} = x_1$,

$$x_1 = x_1 \frown \bigwedge_{j=2}^{n} (x_j \frown x_j') = \bigvee_{i \in X_1} f_i .$$

It follows that every Boolean function is a g_S; we shall now show that distinct g_S represent distinct functions. Let I consist of all points with n coordinates, each 0 or 1 (the vertices of an n-dimensional cube). Denote by x_j the set of points with jth coordinate 1. Then each f_i will represent a different point: the point with jth coordinate 0 or 1 according as x_{ij} is x_j' or x_j. Hence distinct sets S determine distinct g_S in this case, and a fortiori in a free Boolean algebra. We conclude

THEOREM 11. *The free Boolean algebra with n generators is isomorphic with the algebra 2^{2^n}.*

Ex. Show that though the free lattice with two generators is a Boolean algebra, it is not the free Boolean algebra with two generators.

---

[16] Another procedure is given in Birkhoff-MacLane, pp. 320–3, which involves a less sophisticated use of logic.

9. Boolean equations. As shown in Ch. XII, §3, any family of propositions in classical logic may be written in the form of a set of equations, with coefficients in a Boolean algebra. We shall now discuss the solution of such equations—or, what amounts to the same thing, their reduction to the simplest possible canonical form. This problem engaged much of the attention of mathematical logicians of the nineteenth century, because it corresponds to making the maximum logical simplification of a series of assertions.[17]

One procedure is the following. Any equation $p = q$ can be reduced to the form $r = (p' \frown q) \smile (p \frown q') = 0$. Two simultaneous equations $r = 0$ and $s = 0$ are equivalent to the single equation $r \smile s = 0$. Hence exactly $2^{2^{m+n}}$ inequivalent systems of assertions about m classes, involving n properties, can be made. If we use $a_1, \cdots, a_n$ to denote the properties, and $x_1, \cdots, x_m$ to denote the classes which we are trying to describe, we can systematize as in §8 by writing down an *arbitrary subset of the set of all* 2^{m+n} *elementary statements*

$$\begin{gathered} a_1 \frown \cdots \frown a_n \frown x_1 \frown \cdots \frown x_m = 0, \\ a_1 \frown \cdots \frown a_n \frown x_1 \frown \cdots \frown x_m' = 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ a_1' \frown \cdots \frown a_n' \frown x_1' \frown \cdots \frown x_m' = 0. \end{gathered}$$

This is an entirely systematic procedure.

In virtue of §3, we can also write every equation using *ring* notation; this is especially useful with *linear* equations. Thus consider

$$(7) \qquad ax = b, \quad \text{which is equivalent to} \quad ax + b = 0.$$

Multiplying through by $1 + a = 1 - a$, we get $0 = b + ab$; hence (7) has no solution unless $b = ab$. In this case, it reduces to $a(x + b) = 0$. Multiplying by b, we get $abx + ab = 0$, or $x \geqq ab$. Further, $0 = a(x + ab)$, whence $x + ab \leqq 1 + a$. Writing $x = ab + t$, we get $t \leqq 1 + a$. Conversely, any $x = ab + t$ with $t = (1 + a)t$ satisfies $a(ab + (1 + a)t) = aab = b$ if $b = ab$. We conclude that (7) has *no* solution unless $b \leqq a$, and if $b \leqq a$, the general solution is $x = ab + t$, where $t \leqq a'$.

We can *eliminate* from a system of simultaneous linear equations, using the Euclidean algorithm,[18] applied to row-equivalent matrices. We illustrate by the case of the equations

$$(8) \qquad ax + by = c, \qquad dx + ey = f.$$

---

[17] See E. Schröder [1, Vol. 1, p. 475 ff]; L. Couturat, *The algebra of logic* (translated), Chicago and London (1914), p. 57 ff.

[18] The observation that $a \smile b = a + b + ab =$ g.c.d. (a, b) is due to E. T. Bell, op. cit. in §4. For equivalence of matrices in Euclidean rings, see N. Jacobson [1, p. 43]. For Boolean matrices in general, see L. Loewenheim, Math. Annalen 73 (1913), 245–72, and 76 (1919), 223–36; J. H. M. Wedderburn, Annals of Math. 35 (1934), 185–94; Gr. C. Moisil, Ann. Sci. Univ. Jassy, Sect. I, 27 (1941), 181–240. The procedure in the special case of chains modulo two, in combinatorial complexes, is well known.

Adding d times the first equation to the second, we replace (8) by the equivalent system (8′) $ax + by = c$, $(d + ad)x + (e + bd)y = (f + cd)$. Now adding the second of these to the first, we get

$$(a \smile d)x + (b + e + bd)y = (c + f + cd). \tag{9}$$

Adding $(d + ad)$ times (9) to (8′), we get

$$(e + bd + de + ade)y = f + cd + df + adf. \tag{9′}$$

Equations (9)–(9′) are equivalent to (8), which we have thus "reduced" to triangular form.

The further theory of "Boolean matrices," or matrices whose coefficients lie in a fixed Boolean ring, is developed in exercises. In Ch. XIII, §7, a related theory of matrices with coefficients in a Boolean algebra is developed.

Ex. 1. (a) Call two Boolean matrices "equivalent" if one can be obtained from the other by a sequence of additions of one row or column to another. Prove that any $m \times n$ Boolean matrix $A = \| a_{ij} \|$ is equivalent to one and only one "canonical" Boolean matrix, satisfying $a_{ij} = 0$ if $i \neq j$, and $a_{11} \geqq a_{22} \geqq a_{33} \geqq \cdots$. (Here $a_{11} = \bigvee a_{ij}$, etc.)

(b) Interpret as a systematic way of solving simultaneous linear equations.

Ex. 2. Show that (8) has no solution unless

$$(1 + a)(1 + b + c)df + (1 + b + ae)cd + (1 + e)f = 0.$$

Ex. 3. (a) Let S be a set of nr points, formed of n disjoint subsets $S_1, \cdots, S_n$, each having r points. Interpret $n \times n$ matrices with coefficients in 2^r as "linear" transformations of S.

(b) Develop a corresponding theory of "affine" transformations. Do these leave the ternary median operation invariant?

10. Infinite distributivity. We shall now show that the infinite distributive law $x \frown \bigvee_B y_\beta = \bigvee_B (x \frown y_\beta)$ is valid in any Boolean algebra. Indeed, $x \frown \bigvee_B y_\beta$ is clearly an upper bound to every $x \frown y_\beta$; hence we need only show that $x \frown \bigvee_B y_\beta$ is contained in every upper bound u to the $x \frown y_\beta$. But if $x \frown y_\beta \leqq u$ for all β, then $y_\beta = (y_\beta \frown x) \smile (y_\beta \frown x') \leqq u \smile x'$ for all β, and so

$$x \frown \bigvee_B y_\beta \leqq x \frown (u \smile x') = (x \frown u) \smile (x \frown x') = x \frown u \leqq u.$$

This completes the proof.[19] We infer, by Thm. 14 of Ch. IX, §11, and the Duality Principle, the following result.

THEOREM 12. *Any complete Boolean algebra is a topological lattice, satisfying the infinite distributive laws*

$$x \frown \bigvee_B y_\beta = \bigvee_B (x \frown y_\beta), \quad \bigvee_A x_\alpha \frown \bigvee_B y_\beta = \bigvee_{AB} (x_\alpha \frown y_\beta), \quad \text{and dually.} \tag{10}$$

[19] See von Neumann [2, II, Appendix, p. 7]; also Tarski [3, p. 510, footnote]. For Thm. 13 see also O. Ore, Annals of Math. 47 (1946), p. 70.

Since the completion of a Boolean algebra by cuts is a complete Boolean algebra (Thm. 9), while completion by cuts preserves g.l.b. and l.u.b. whenever they are defined, we see that the infinite distributive laws (10) are valid in any Boolean algebra when their terms are defined.

This is not true of the distributive law (22′) of Ch. IX, §11. In fact, the construction of §8 above, extended transfinitely, yields the following remarkable result of Tarski [1, pp. 195–7].

THEOREM 13. *If a Boolean algebra A is completely distributive, then it is isomorphic with the algebra $2^{\aleph}$ of all subsets of some aggregate.*

Explanation. A lattice will be called "completely distributive," if and only if law (22′) of Ch. IX, §11, holds without restriction on the number of terms involved.

Proof. Let x_α denote the general element of A; make the expansion $I = \bigwedge_A (x_\alpha \smile x'_\alpha) = \bigvee \theta_\phi$, where θ_ϕ denotes the most general $\bigwedge_A x_{\phi\alpha}$ $[x_{\phi\alpha} = x_\alpha \text{ or } x'_\alpha]$; (22′) justifies this expansion. We first show that each θ_ϕ not 0 covers 0. Indeed, if $x_\alpha < \theta_\phi$, then (since $x_{\phi\alpha} = x$ would imply $\theta_\phi \leqq x_\alpha$, contradicting $x_\alpha < \theta_\phi$) $x_{\phi\alpha} = x'_\alpha$, and so $x_\alpha = x_\alpha \frown \theta_\phi \leqq x_\alpha \frown x'_\alpha = 0$. Hence the $\theta_\phi > 0$ are points; this is Tarski's central idea.

Moreover each $x_\alpha = x_\alpha \frown I = x_\alpha \frown \bigvee \theta_\phi = \bigvee(x_\alpha \frown \theta_\phi)$ is the join of the "points" $\theta_\phi > 0$ which it contains (for either $\theta_\phi \leqq x_\alpha$ and $x_\alpha \frown \theta_\phi = \theta_\phi$, or $x_\alpha \frown \theta_\phi < \theta_\phi$ and $x_\alpha \frown \theta_\phi = 0$). Again, a join $g_S = \bigvee_S \theta_\phi$ of points contains no point p not in S, since

$$g_S \frown p = \bigvee_S (\theta_\phi \frown p) = \bigvee_{\phi \in S} 0 = 0$$

unless $p \in S$, again by (10). This establishes a one-one order-preserving correspondence between the sets S of points and the different elements g_S of A, q.e.d.

Note that the "and dually" of (22′) is redundant, in this proof.

Ex. 1. Show by direct computation that the identity (22′) of Ch. IX, §11, implies (20′) and (21′).

Ex. 2. Show that not every complemented modular lattice is topological. (Hint: Consider the lattice of all subspaces of an infinite-dimensional vector space.)

Ex. 3. Show that every translation $x \to x + a$ of a Boolean algebra is a homeomorphism with respect to the interval topology. (Hint: Use Thm. 5, and define the interval $[a \frown b, a \smile b]$ as the set of all x such that $(a, x, b) = x$.) What of the order topology?

Ex. 4. Define a fundamental sequence in a Boolean algebra as one such that $x_m - x_n \to 0$ in the order topology, and a *null sequence* as one such that $x_n \to O$.

(a) Show that, modulo null sequences, the fundamental sequences of any Boolean algebra A form a σ-complete Boolean algebra,[20] in which A is dense.

(b*) Extend to fundamental and null directed sets; also to the interval and star topologies.

(c*) Does one obtain in any of these ways the completion of A by cuts?

Problem 76. Do the order topology and interval topology coincide for a complete Boolean algebra?

[20] See H. Loewig, *Intrinsic topology and completion of Boolean algebras*, Annals of Math. 42 (1941), 1138–96.

Problem 77. In a σ-complete Boolean algebra, do $x_{i,j} \to x_i$ for all i, and $x_i \to 0$, imply the existence of $j(i)$ such that $x_{i,j(i)} \to 0$? (This relates to Ex. 4a.)

11. Boolean σ-algebras; Theorem of Loomis. We shall now prove a representation theorem for *Boolean σ-algebras*—i.e., σ-complete Boolean algebras.

THEOREM 14 (Loomis[21]). *Any Boolean σ-algebra A is a σ-homomorphic image of a σ-field of sets.*

Proof. Let I be the class of all functions P which select, from each pair of complements a, a' of A, one of the two terms; we shall call these "points." With each $a \in A$, we associate the set $\tau(a)$ of all points P such that $a \in P$. These sets $\tau(a)$ are closed under complementation, since $\tau(a') = [\tau(a)]'$. Hence they generate a σ-field of subsets of I under countable union and intersection. Let N be the family of finite or countable intersections $\bigwedge \tau(a_j)$, for which $\bigwedge a_j = O$ in A. Let J be the σ-ideal generated by N; it will consist of the $t \leqq \bigvee n_i$, for countable subsets $\{n_i\}$ of N. We shall show that Φ/J is isomorphic to A, under the correspondence $\tau: a \to \tau(a)$.

First, τ is a σ-homomorphism of A onto all of Φ/J. For if $a = \bigvee a_i$, then $a' \frown a_i \leqq a' \frown a = O$ for all i and $O = a \frown a' = a \frown (\bigvee a_i)' = a \frown \bigwedge a_i'$. Hence by definition of N and J, every $\tau(a') \frown \tau(a_i) \in N$, and $\tau(a) \frown \bigwedge \tau(a_i') \in N$. By the former,

$$\tau(a') \frown [\bigvee \tau(a_i)] = \bigvee [\tau(a') \frown \tau(a_i)] \in J.$$

By the latter, $\tau(a) \frown [\bigvee \tau(a_i)]' = \tau(a) \frown \bigwedge \tau(a_i') \in N$. Hence the symmetric difference between $\tau(a) = \tau(\bigvee a_i)$ and $\bigvee \tau(a_i)$ lies in J. A dual argument works for meets.

This σ-homomorphism will be an isomorphism if $\tau(a) \in J$ implies $a = O$. This we shall now show with the help of a "diagonal process," thereby completing the proof.

If $\tau(a) \in J$, then as above $\tau(a) \leqq \bigvee_i(\bigwedge_j(a_{ij}))$, where $\bigwedge_j a_{ij} = O$ for all I. Hence, for any function $j(i)$, by the isotone law (Ch. II, Thm. 2),

$$\text{(A)} \qquad \tau(a) \leqq \bigvee_i \tau(a_{i,j(i)}), \text{ whence } \tau(a') \geqq \bigwedge_i \tau(a'_{i,j(i)}).$$

Now suppose $a \neq O$. Then $a' < I$, and so

$$I > a' = a' \smile O = a' \smile \bigwedge a_{1j} = \bigwedge (a' \smile a_{1j}).$$

Hence some $a' \smile a_{1,j(1)} < I$. Repeating the process

$$\begin{aligned} I > a' \smile a_{1j} &= a' \smile a_{1,j(1)} \smile O \\ &= (a' \smile a_{1,j(1)}) \smile \bigwedge a_{2,j} = \bigwedge (a' \smile a_{1,j(1)} \smile a_{2,j}). \end{aligned}$$

[21] L. Loomis, *On the representation of σ-complete Boolean algebras*, Bull. Am. Math. Soc. 53 (1947), 757–60. We copy Loomis' proof almost verbatim. See also A. A. Liapounoff, Doklady URSS 53 (1946), 395–8.

By this "diagonal process," we get a function $j(i)$ such that, for all n,

$$I > a' \smile a_{1,j(1)} \smile \cdots \smile a_{n,j(n)}.$$

This sequence can contain neither a nor a complementary pair; hence we can form a point P which contains a and every $a'_{i,j(i)}$. Clearly $P \in \tau(a)$, yet $P \notin \bigvee_i \tau(a_{i,j(i)})$ (since no $\tau(a_{i,j(i)})$ contains P and union in Φ is set-union). This contradicts (A), and completes the proof.

Ex. 1. (a) Show that a subset J of a Boolean σ-algebra A corresponds to the family of all sets failing to contain a point under some σ-homomorphism of A onto a σ-field of sets, if and only if it is a "σ-prime ideal," in the sense that $\bigwedge_{i=1}^{\infty} a_i \in J$ if every $a_i \in J$ and $\bigwedge_{i=1}^{\infty} a_i \in J$ if and only if some $a_i \in J$.

(b) Infer that A is isomorphic with a σ-field of sets if and only if the intersection of its σ-prime ideals is 0.

Ex. 2. Let a Boolean σ-algebra A be generated by a subset G. Show that an element p of A is a "point" if and only if, for all $g \in G$, $p \frown g = 0$ or $p \leqq g$.

Ex. 3. (a) Define the "free Boolean σ-algebra with $\aleph$ generators" for any cardinal number $\aleph$ (in the sense of the Foreword on Algebra), and prove its existence.

(b) Using Thm. 14, show that it is isomorphic with a σ-field of sets.

Problem 78. Prove (or disprove) that if a Boolean σ-algebra A is generated by a subset G, then every $a > 0$ in A contains some finite or countable meet $\bigwedge g_i > 0$ of elements of G.

Problem 79. Prove (or disprove) that the free Boolean σ-algebra with countably many generators is isomorphic with the field of all Borel subsets of the Cantor discontinuum.

Problem 80. Generalize Thm. 14 to cardinal numbers other than countable infinity.

12. Measure algebras. In measure theory, one usually discusses metric Boolean algebras in which $v[O] = 0$. These are usually defined as Boolean algebras with positive functional $v[x]$ satisfying

$$(11) \qquad v[x \smile y] = v[x] + v[y] \quad \text{if} \quad x \frown y = 0.$$

Setting $x = y = O$ in (11), we get (after cancellation) $v[O] = 0$. Moreover by induction, we get

$$(11') \qquad v\left[\bigvee_{i=1}^{n} x_i\right] = \sum_{i=1}^{n} v[x_i] \quad \text{if all} \quad (x_1 \smile \cdots \smile x_{k-1}) \frown x_k = O.$$

A Boolean algebra with a measure which is countably additive, in the sense that

$$(11'') \qquad v\left[\bigvee_{i=1}^{\infty} x_i\right] = \sum_{i=1}^{\infty} v[x_i] \quad \text{if all} \quad (x_1 \smile \cdots \smile x_{k-1}) \frown x_k = O,$$

is usually called a *measure algebra*. For this it is necessary and sufficient that $v[x]$ be continuous.

Any finite measure algebra M can be easily realized geometrically. If the points of M are $p_1, \cdots, p_r$, we let p_k correspond to the half-closed interval

$$v[p_1] + \cdots + v[p_{k-1}] \leqq x < v[p_1] + \cdots + v[p_k],$$

on the real axis. This may be extended, using (11), to a measure-preserving isomorphism ("isometric isomorphism") between M and a field of elementary subsets of the x-axis. Thus *a complete basis for measure theory, with respect to finitary union, intersection and complementation, is given by any set of postulates for Boolean algebra, if* (11) *is added.*[22]

We shall now construct a highly homogeneous, universal separable measure algebra which plays a central role in measure theory, and is the prototype for the continuous-dimensional projective geometries already discussed.

THEOREM 15. *There is, up to isometric isomorphism, only one complete separable measure algebra without points and satisfying $v[I] = 1$; we shall denote it $\bar{M}$. Every separable measure algebra is, after change of scale, isometrically isomorphic with a subalgebra of $\bar{M}$. The automorphisms of $\bar{M}$ are transitive on the elements x not O or I; for any real number c, the isometric automorphisms*[23] *are transitive on the elements satisfying $v[x] = c$.*

Proof. Let A be any separable measure algebra, with a countable dense subset $x_1, x_2, x_3, \cdots$. Then A satisfies $w[I] = 1$ for the new valuation $w[x] = v[x]/v[I]$, which clearly amounts simply to a change of scale. Let X_n denote the finite subalgebra of A generated by $x_1, \cdots, x_n$; we represent it by finite sums of line intervals as above. The union U of the X_n can also be so represented; moreover unless A contains a point, *every* finite sum of line intervals (with its ordinary measure) is a metric limit of elements of U. Hence if we let M denote the metric Boolean algebra of finite sums of half-open intervals of the interval $[0, 1)$, we see that the metric completion (cf. Ch. V, §9) $\bar{M}$ of M not only contains U, but is isometrically isomorphic with $\bar{U} = A$ if A is complete and without points. That $\bar{M}$ *is* a metric Boolean algebra follows from Ch. VIII, Thm. 12; in fact, the proof given there can be simplified using L6.

Since the closed ideals $[0, x]$ of $\bar{M}$ are complete and without points, they are always isometrically isomorphic after a change of scale. The remainder of Thm. 15 can easily be proved by using this fact and the fact that any isomorphism of $[0, x]$ with $[0, y]$ and $[0, x']$ with $[0, y']$ can be extended to an automorphism of $\bar{M}$.

Measure algebras and measure theory will be discussed further in Ch. XI, §§8–11.

Ex. 1. (a) Show that, in any Boolean algebra, (11) is equivalent to V1 and $v[O] = 0$, while V2 is equivalent $v[x] \geqq 0$.

(b) Show that (11″) is equivalent to (11) and the continuity of $v[x]$ in the order-topology.

---

[22] See G. Birkhoff, Proc. Camb. Phil. Soc. 30 (1934), 115–22, for the case of distributive lattices; H. P. Evans and S. C. Kleene, Am. Math. Monthly 46 (1939), p. 141.

[23] The first two statements of Thm. 15 are due to C. Carathéodory, Ann. Scuo. Norm. Sup. Pisa 8 (1939), 105–30, and P. Halmos and J. von Neumann, Annals of Math. 43 (1942), 332–50. The group of automorphisms was discussed by P. R. Halmos, Trans. Am. Math. Soc. 55 (1944), 1–18. See also Problem 85, Ch. XI, §10.

Ex. 2. Prove from (11) that $v[a_1' \frown a_2' \frown \cdots \frown a_n']$ equals[24]

$$v[I] - \sum v[a_i] + v[a_i \frown a_j] - \cdots + -(1)^n v[a_1 \frown a_2 \frown \cdots \frown a_n].$$

Ex. 3.* Show that any metric distributive lattice is isometrically isomorphic with a sublattice of a Boolean algebra, provided $v[x]$ is bounded.

Ex. 4*. Construct $\bar{M}$ by completing metrically the union of the nested sequence $2^1 \leqq 2^2 \leqq 2^4 \cdots$, suitably normed—by analogy with Ch. VIII, §10. Represent in terms of coordinate subspaces of $CG(F)$.

Ex. 5*. Show that any isometry between finite subsets of $\bar{M}$ can be extended to a self-isometry of all of $\bar{M}$. A "generalized Boolean algebra" is a relatively complemented distributive lattice with **0**. Construct a universal separable metric generalized Boolean algebra, as a sublattice of the cardinal product of countably many replicas of $\bar{M}$.

13. Lattices with unique complements. Using the technique of free lattices, Dilworth [1] has proved that *every lattice is a sublattice of a lattice with unique complements.* (A lattice "with unique complements" is a lattice in which each element has one and only one complement.) It follows that lattices with unique complements need not be distributive, or even modular (see Ex. 2 below). Nevertheless, non-distributive lattices with unique complements cannot be finite.

THEOREM 16. *Let L be any complete, atomic lattice with unique complements. Then L is isomorphic with the Boolean algebra of all subsets of its points.*[25]

Proof. To each set S of points of L, associate the join $x(S)$ of the $p \in S$, and the meet $y(S)$ of the complements p' of the $p \in S$. It will follow by generalized associativity (Ch. IV, §4) that $x(S \smile T) = x(S) \smile x(T)$ and $y(S \smile T) = y(S) \frown y(T)$. Again, the complement of $x(I)$ can contain no point (we let I denote both the set of all p and the biggest element of L). Hence $[x(I)]'$ is O, and $x(I) = [[x(I)]']' = O' = I$. Dually, $y(I) = O$.

Again, the complement p' of any point p is covered by I; that is, $x \geqq p'$ implies $x = p'$ or $x = I$. For if $x \geqq p$, then $x \geqq p \smile p' = I$; and if not, then $x \frown p < p$ will be O while $x \smile p \geqq p' \smile p = I$, whence $x = p'$. Hence (i) if p and q are distinct points, then $p \leqq q'$. For unless $p \leqq q'$, $p \frown q' = O$ and $p \smile q' = I$ (since p covers O and I covers q')—implying $q' = p'$ and so $q = p$. It is a corollary of (i) that $x(S) \leqq y(S')$.

From this crucial inequality, we infer (ii) $x(S) \frown x(S') \leqq y(S') \frown y(S) = y(S \smile S') = y(I) = O$. Thus $x(S)$ contains no point not in S, whence distinct sets S determine distinct $x(S)$, and the partly ordered system of the $x(S)$ is isomorphic with the atomic Boolean algebra of all sets S.

It remains to show that every $a \in L$ is an $x(S)$. But denote by S the set

[24] Various important applications of this identity are made by Uspensky and Heaslet, *Elementary number theory*, p. 105. Ex. 3 is due to M. F. Smiley, Trans. Am. Math. Soc. 56 (1944), 435–47.

[25] G. Birkhoff and M. Ward, Annals of Math. 40 (1939), 609–10. Observe that the only "atomic" assumption used is the assumption that every $a > 0$ contains a point.

of points $p \in L$, with $p \leqq a$. Evidently $a \frown x(S')$ will contain only points in S and in S'; hence $a \frown x(S') = O$. On the other hand, $a \smile x(S') \geqq x(S) \smile x(S') = x(S \smile S') = I$; hence a is the unique complement $[x(S')]'$ of $x(S')$. But this is $x(S)$, by (iii) and the equality $x(S) \smile x(S') = I$, completing the proof.

Again, an orthocomplemented lattice with unique complements is necessarily a Boolean algebra.

THEOREM 17. *If every a in a lattice L has a unique complement a', and if $a \to a'$ is a dual automorphism, then L is a Boolean algebra.*

Proof. We first show that $b \geqq a$ implies $(b \frown a') \smile a = b$ and dually $(a \smile b') \frown b = a$. Indeed, setting $c = b \frown a'$, evidently $c \frown a = O$. Also $(c \smile a)' \frown b = [(b' \smile a) \frown a'] \frown b = (b' \smile a) \frown (a' \frown b) = O$ since $b' \smile a$ and $(b' \smile a)' = b \frown a'$ are orthocomplements. Again, since $c \smile a = (b \frown a') \smile a \leqq b \smile b = b$, clearly $(c \smile a)' \smile b \geqq b' \smile b = I$. We conclude $(c \smile a)' = b'$, whence $c \smile a = b$. This is our first conclusion; dually, $(a \smile b') \frown b = a$.

Now suppose $x \frown y = a$, $x \smile y = b$, and form $e = b' \smile (x \frown a')$. Using the result just obtained twice, and $y = a \smile y = b \frown y$ also,

$$e \smile y = b' \smile (x \frown a') \smile a \smile y = b' \smile x \smile y = b' \smile b = I,$$

$$e \frown y = [b' \smile (x \frown a')] \frown b \frown y = x \frown a' \frown y = a' \frown a = O.$$

It follows that y is the (unique) complement of e, so that even *relative* complements are unique. The proof is completed by recalling Cor. 1 of Thm. 2, Ch. IX.

Ex. 1. Show that $(a')' = a$ in any lattice with unique complements.

Ex. 2. Show that any *modular* lattice with unique complements is a Boolean algebra. (See Thm. 10, Ch. VIII.)

Ex. 3. Show that a complete, atomic lattice L is a Boolean algebra if and only if every element of L has a unique complement.

Ex. 4. Show that a complete Boolean algebra A is atomic if and only if it is completely distributive.

Ex. 5. Show that in the non-modular five-element lattice, every element a has a complement a' such that $a \frown x = O$ implies $x \leqq a'$.

Ex. 6. Let L be any lattice such that every $a \in L$ has a complement, and such that $a \frown x = O$ implies $x \leqq a'$ for *all* complements a' of a. Prove that

(a) Each a has a unique complement a'.

(b) If $a \leqq b$, then $a \frown b' = O$, and so $b' \leqq a'$.

(c) L is a Boolean algebra. (See Huntington [1].)

CHAPTER XI

APPLICATIONS TO SET THEORY

1. Elementary and Borel sets. Let I_n denote the closed unit n-cube—i.e., the set of all points $x = (x_1, \cdots, x_n)$ with n real coordinates x_i, $0 \leqq x_i \leqq 1$. Let $B(I_n)$ denote the complete, completely distributive Boolean algebra of all subsets of I_n.

The simplest figures in I_n are the closed "n-rectangles" of points $(x_1, \cdots, x_n)$ satisfying $a_k \leqq x_k \leqq b_k$ $[k = 1, \cdots, n]$ for some fixed set of $2n$ real numbers a_k, b_k.

Definition. *The Boolean subalgebra of $B(I_n)$ generated by n-rectangles consists of the elementary subsets of I_n; the σ-subalgebra of I_n generated by n-rectangles consists of the Borel subsets of I_n.*

The concepts of elementary and Borel sets play a fundamental role in set theory.

By subtracting the faces, edges, vertices, etc., from a closed rectangle, we get its interior expressed as a difference of closed rectangles—hence any open rectangle is an elementary set. But any open set in I_n can be expressed as a countable union of open rectangles—namely, of open rectangles defined by *rational* coordinates a_k, b_k. It follows that any open or closed set is a Borel set. Hence if we define a *Borel set* in an arbitrary topological space as a set in the σ-subalgebra of sets generated by open and closed sets, we get a valid generalization of the preceding definition.

Euclidean n-space requires no separate discussion, since it is homeomorphic with an open rectangle of I_n, under a correspondence which preserves the concept of coordinate rectangle.

Ex. 1. Show that $B(I_1)$ is isomorphic to $B(I_n)$ for all finite n, and also to the Boolean algebra of all subsets of Euclidean n-space.

2. Compact spaces and distributive lattices. We shall now correlate topological spaces with distributive lattices; this theory is due entirely to Wallman [1]. Let I be any T_1-space (see the Foreword on Topology). The closed subsets of I form a complete distributive lattice (Ch. IV, Thm. 3).

Theorem 1. *Any topological space I is determined to within homeomorphism by the distributive lattice $L(I)$ of all its closed subsets.*

For by C4 the points of I are the elements covering O ("atoms") of $L(I)$. And the closure $\bar{S}$ of any subset of I consists of the points $p \in I$ corresponding to atoms contained in the join (in $L(I)$) of atoms corresponding to points of S.

THEOREM 2. *A compact T_1-space I is determined to within homeomorphism by any sublattice S of the lattice of its closed subsets which is a basis.*

Sketch of proof. We may define each point in I as a maximal dual ideal in S—i.e., as a maximal family Φ of the basis, no finite subfamily of which has a void intersection. That the intersection of such a family of closed subsets should be a point is one definition of compactness. Each element $a \in S$ is made to determine the "closed" subset of all "points" Φ with $a \in \Phi$, and the topology of I then determined by taking this as a basis of closed sets.

Wallman has shown that an abstract distributive lattice with O and I is isomorphic with a basis of closed subsets of a bicompact T_1-space, if and only if it has the "disjunction property": given $S > T$, there exists an X such that $S \frown X > O$ yet $T \frown X = O$.

Moreover, if S is any sublattice of the lattice of all closed subsets of a T_1-space I, which is a basis of closed subsets, we may define a compact space I^* from S as in Thm. 2. This will be the Čech bicompactification of I, and hence will have the same (Čech) dimension and homology groups as I.

In the separable case, we may take S to be countable, and hence as the limit of an increasing sequence of finite sublattices. This remark suggests Alexandroff's characterization of separable compact spaces by sequences of "finite coverings" (abstract complexes), each a refinement of the last. By using directed sets of finite coverings, we get similarly all compact spaces; see Tukey [1].

The interested reader will find many additional results in the literature;[1] see also §7.

Ex. 1. (a) Show that an abstract complete distributive lattice is the lattice of all closed subsets of a T_1-space if and only if, given $s > t$, there exists a p covering O, such that $p \leqq s$ yet $p \frown t = O$.

(b) Prove directly that $x \smile \bigwedge u_a = \bigwedge (x \smile u_a)$ holds.

Ex. 2. (a) Let L be any complete distributive lattice satisfying the infinite distributive law of Ex. 1b, and let S be any subset of L. Show that the class of arbitrary intersections of finite unions of elements of L is closed under finite union and arbitrary intersection.

(b) Apply to the concept of a *sub-base* of closed sets.

Ex. 3. Consider the lattice of all T_1-topologies which can be imposed on an abstract set.[2] Show that every such topology can be extended to a maximally strong T_1-topology, and that every maximally strong T_1-topology is compact. (E. Hewitt)

Ex. 4. Show that the closure operator on the closed subsets of a normal Hausdorff space X, regarded as a subset of its compactification, is a lattice-isomorphism.

---

[1] H. Terasaka, *Über die Darstellung der Verbande*, Proc. Imp. Acad. Tokyo 14 (1938), 306–11; J. W. Alexander, *A theory of connectivity for gratings*, Annals of Math. 39 (1938), 883–912; A. N. Milgram, Reps. Notre Dame Colloq. (1940); E. Livenson, Mat. Sbornik 7 (1940), 309–12; R. Vaidyanathaswamy, Proc. Ind. Acad. Sci. 16 (1942), 379–86; N. Matsuyama, Proc. Imp. Acad. Tokyo 13 (1937), and 19 (1943), 426–8; A. Pereira Gomes, *Sobre a Nocao dec Espaco Compacto*, Porto (1945) and Portugaliae Math. 5 (1946), 207–17; G. Higman, Quar. Jour. 19 (1948), 27–32.

[2] For this concept, see G. Birkhoff, Fund. Math. 26 (1936), 156–66; E. Hewitt, Duke Jour. 10 (1943), 309–33; R. Arens, Annals of Math. 47 (1946), 480–95; M. E. Shanks, Am. Jour. Math. 56 (1944), 461–9; V. S. Krishnan, Jour. Ind. Math. Soc. 10 (1946), 37–56.

Ex. 5*. Let L be any complete lattice, and let G be a semigroup of isotone transformations γ of L. We say that $a \in L$ is *closed* under G if and only if $a\gamma \leqq a$ for all $\gamma \in G$.

(a) Show that being closed is a "closure" property.

(b) Show that if L consists of the topologically closed subsets of a compact space, and the γ are continuous, then any "closed" $a \in L$ contains a "minimal" closed $m > O$. (These correspond to the "central motions" of G. D. Birkhoff.)

3. Boolean spaces and Boolean algebras. By Thm. 2, any compact T_1-space is characterized topologically by any "basis" of closed sets. But a closed set has a closed complement if and only if it disconnects the space. Hence a T_1-space has a Boolean algebra for a basis of closed sets, if and only if it is *totally disconnected*.[3]

LEMMA. *A compact space X is totally disconnected if and only if it is zero-dimensional.*

Proof. Let X be totally disconnected, and let U be any open set containing a point p of X. For each $q \in U'$, there exists an open-and-closed set $S(q)$ containing q but not p. But U' is compact (since X is); hence some *finite* union $S(q_1) \smile \cdots \smile S(q_n)$ will contain U'. Its complement $V = \bigwedge S'(q_i)$ will be a neighborhood of p contained in U and having a void boundary. The existence of such a V however defines X as zero-dimensional. Conversely, any zero-dimensional space is trivially totally disconnected.

Moreover any Boolean algebra has Wallman's disjunction property. Hence it can be regarded as a basis of closed sets of a totally disconnected compact T_1-space. Conversely, the field of all open and closed subsets of any such space I forms a Boolean algebra $A(I)$ which characterizes I to within homeomorphism. We conclude

THEOREM 3 (Stone[4]). *There is a many-one correspondence between Boolean algebras A and totally disconnected (i.e., zero-dimensional) compact T_1-spaces I, under which elements of A correspond to open-and-closed subsets of I, and points of I to prime ideals of A.*

For this reason, Stone has called zero-dimensional compact spaces *Boolean* spaces.

Ex. 1. Show that, above, I affords the "perfect" representation of $A(I)$ by a field of sets.

Ex. 2.* (a) Show that Theorem 3 can be extended so as to express a correspondence between *generalized* Boolean algebras and totally disconnected *locally* bicompact spaces. (M. H. Stone)

(b) What about Thm. 2 and locally bicompact spaces?

Ex. 3. Show that Problem 74 of Ch. X, §7, is equivalent to the following unproved conjecture of topology: Every zero-dimensional compact space has a proper homeomorphism.

---

[3] The usual definition of total disconnectedness, that any two points fall in complementary closed sets, is equivalent (cf. Lemma 2, §5) to the assertion that any closed set is the intersection of open closed sets.

[4] M. H. Stone [4], which was the pioneer article in the field discussed in §§2–4.

4. Theorem of Kaplansky. Consider next the lattice L of all real-valued functions defined and continuous on a compact Hausdorff space X. We shall say that a prime ideal P in L is *associated* with a point $x \in X$, when $f \in P$ and $g(x) < f(x)$ imply $g \in P$.

LEMMA 1. *Each prime ideal P is associated with one and only one point of X.*

Proof. Suppose P were associated with no point of X. Then for each $x \in X$ we would have functions f, g with $g(x) < f(x)$ yet $f \in P$, $g \in L-P$. Since X is compact and the set $Y(f,g)$ on which $g(y) < f(y)$ is open, we would have a finite number of pairs $f_1, g_1, \cdots, f_n, g_n$ such that

$$X = \bigvee Y(f_i, g_i) \leqq Y(\bigvee f_i, \bigwedge g_i).$$

This would imply $\bigvee f_i > \bigwedge g_i$, which is impossible since $\bigvee f_i \in P$, $\bigwedge g_i \in L-P$, one being an ideal and the other a dual ideal.

Hence P is associated with at least one point $x \in X$; suppose it were associated with two points, say x and y. Choose $f \in P$, $g \in L-P$. Since any compact Hausdorff space is normal, we can construct h so that $h(x) < f(x)$, $h(y) > g(y)$. But this would require h to be in both P and $L-P$.

LEMMA 2. *Two prime ideals P, Q are associated with the same point $x \in X$, if and only if $P \frown Q$ contains a prime ideal.*

Proof. Suppose P, Q are both associated with x. Choose $f \in P$, $g \in Q$, and let a be any number smaller than $f(x)$ or $g(x)$. Then the set of all h satisfying $h(x) \leqq a$ forms a prime ideal R contained in $P \frown Q$. Conversely, let P, Q, R be prime ideals and $P \frown Q \geqq R$; suppose they are associated with x, y, z. Choose any $f \in R$, $g \in L-P$; if $x \neq z$, h will exist with $h(z) < f(z)$, $h(x) > g(x)$. Then $h \in R \frown (L-P)$, which is impossible; hence $x = z$. Similarly, $y = z$, and so $x = y$.

LEMMA 3. *Let f_0 be a fixed function in L, and S any subset of X. Then a point x is in the closure $\bar{S}$ of S if and only if some prime ideal $P(x)$ associated with x contains the intersection $A(S)$ of the prime ideals containing f_0 which are associated with points of S.*

Proof. If $x \in \bar{S}$, we choose $\alpha > f_0(x)$ and let P consist of all f with $f(x) \leqq \alpha$; clearly P is a prime ideal associated with x. Now $g \in A(S)$ implies $g(y) \leqq f_0(y)$ for all $y \in S$ (since each such inequality defines a prime ideal including f_0), and so $g(x) \leqq f_0(x)$, whence $g(x) \in P$. Hence $A(S) \leqq P$. Conversely, suppose $x \notin \bar{S}$, and let P be any prime ideal associated with x. For any $f \in L-P$ we may find (again by normality of X) a function g such that $g(y) = \operatorname{Inf}_{z \in S} f_0(z) - 1$ on S, yet $g(x) > f_0(x)$. Then g is in $A(S)$ but not in P.

THEOREM 4 (Kaplansky[5]). *Any compact Hausdorff space X is determined to within homeomorphism by the lattice L of its continuous functions.*

---

[5] I. Kaplansky, *Lattices of continuous functions*, Bull. Am. Math. Soc. 53 (1947), 617–22. I have copied Kaplansky's proof; Kaplansky's article also essentially includes Exs. 2–4 below. See also O. Ore, Annals of Math. 47 (1946), p. 72.

Proof. Call two prime ideals in L "equivalent" if their intersection contains a third prime ideal. Lemmas 1–2 show that the classes of "equivalent" prime ideals in L may be interpreted as "points" of X. Lemma 3 shows that the topology of X can be expressed in terms of inclusion relations among these prime ideals.

COROLLARY 1. *X is determined by the ring*[6] *R of continuous real functions on X.*

Proof. $f \geqq g$ if and only if $(f - g) = h^2$ in R.

COROLLARY 2. *X is determined by the Banach space $C(X)$ of continuous real functions on X.*

Proof. Let e be an "extreme point" on the unit sphere S of $C(X)$—i.e., a point not an interior point of a segment lying on S. Then $e(x) = 1$ on S and $e(x) = -1$ on S', where S and S' are complementary closed sets. Hence if we define $f > g$ to mean that $f \neq g$ and $\|(f - g)/\|f - g\| - e\| \leqq 1$, we preserve order on S, invert it on S', and so obtain a lattice isomorphic with L above, thus determining X.

The lattice of all continuous functions on a Hausdorff space will be considered further in Ch. XV.

Ex. 1. Show that if f, g are continuous functions on a Hausdorff space, then so are $f \frown g$ and $f \smile g$.

Ex. 2*. (a) Extend Thm. 4 to continuous functions from X to any chain R without O or I which "separates" X in the sense that, given $h \neq y$ in X and $\alpha \neq \beta$ in R, there exists a continuous function f from X to R with $f(x) = \alpha, f(y) = \beta$.

(b) Similarly, extend Thm. 4 to any chain R such that X is "R-normal" in the sense that for any disjoint closed subsets S, T of X and any α, β in R, there exists a continuous f equal to α on S and to β on T.

Ex. 3*. Using Ex. 2(b), give a new proof of Thm. 3.

Ex. 4*. Show that L in Thm. 4 is a cardinal product $L = MN$ if and only if X is the sum of closed sets Y and Z, where M is associated with Y and N with Z as in Thm. 4.

Problem 81. Give necessary and sufficient conditions in order that an abstract lattice be the lattice of all continuous real-valued functions on a compact Hausdorff space.[7]

5. Pseudo-complements and regular open sets. Let X be any topological space, and let L be the complete distributive lattice of all its open subsets. We shall study the topological significance of the results of Ch. IX, §12.

If T is open and $S \frown T = 0$, then[8] $\bar{S} \frown T = 0$ and so $T \leqq \bar{S}'$; while $S \frown \bar{S}' \leqq \bar{S} \frown \bar{S}' = 0$; hence, for any $S \in L$, $\bar{S}'$ is the pseudo-complement S^* of S in L. Further, since $S^{**} = \bar{S}'^{-\prime}$, which is by definition the interior of $\bar{S}$, we see that $S = S^{**}$ if and only if S is the interior of its closure—i.e., a so-called "regular" open set. Otherwise, $S > S^{**}$, and the boundary of S contains interior points of S.

[6] Cor. 1 is due to I. Gelfand and A. N. Kolmogoroff, Doklady URSS 22 (1939), 11–15; Cor. 2 to Stone [4, p. 469].

[7] For the corresponding result for Banach spaces, see R. F. Arens and J. L. Kelley, Trans. Am. Math. Soc. 62 (1947), 499–508.

[8] We let both $\bar{S}$ and S^- denote the topological closure of S. The results given here are sketched in [LT, §124].

We get as a corollary of this result and Thm. 15 of Ch. IX,

THEOREM 5. *Let X be any T_0-space. The correspondence $S \to \bar{S}'^{-\prime}$ is a lattice homomorphism of the lattice of all open sets of X onto the complete Boolean algebra B of "regular" open sets of X.*

Again, $S^{**} = I$ if and only if $\bar{S}'^{-\prime} = I$, which is equivalent to $\bar{S}'^{-} = O$, or $\bar{S}' = O$, or $\bar{S} = I$—i.e., if and only if S is a *dense* open set. Since $N = S'$ is closed, this implies $N^{-\prime -} = (S')^{-\prime -} = S''^{-} = \bar{S} = I$.

DEFINITION. *A set T which satisfies $\bar{T}'^{-} = I$ is called nowhere dense.*

By Thm. 15 of Ch. IX, dense open sets satisfying $S^{**} = I$ form a dual ideal. But a closed set C is nowhere dense if and only if $C'^{-} = \bar{C}' = I$—i.e., if and only if its open complement C' is dense. Hence nowhere dense closed sets form an ideal. Again, clearly a set T is nowhere dense if and only if its closure $\bar{T}$ is; hence *nowhere dense sets form an ideal.*

LEMMA 1. *If X and Y are open, $X^{**} = Y^{**}$ if and only if the difference between X and Y is nowhere dense.*

Proof. By Thm. 15 of Ch. IX, $X^{**} = Y^{**}$ if and only if $X \frown D = Y \frown D$, where D is a dense open set. But by Boolean ring algebra, this means $O = X \frown D + Y \frown D = (X + Y) \frown D$, i.e., that the (symmetric) difference $X + Y$ between X and Y lies in the nowhere dense complement of the dense open set D, or equivalently, that $X + Y$ is nowhere dense.

Since $X^{**} \geqq X > O = O^{**}$, we infer that

COROLLARY. *No non-void open set X is nowhere dense.*

THEOREM 6. *If X is a subset of Euclidean space without isolated points, then the Boolean algebra A of "regular" open sets of X is the completion by cuts of the free Boolean algebra B_∞ with countable generators.*

Proof. The proof will apply generally to any T_1-space with a countable basis of regular open sets, a_i. Indeed, the a_i and their pseudo-complements a_i^* generate a replica of the free Boolean algebra B_∞ with countable generators, which may also be defined as the limit of $\mathbf{2} \leqq \mathbf{2}^2 \leqq \mathbf{2}^4 \leqq \cdots \leqq \mathbf{2}^{2^n} \leqq \cdots$. Clearly every $a \in A$ defines a cut in B_∞; x is in the lower half of the cut if and only if $x \leqq a$, and in the upper half if and only if $x \geqq a$. Again, unless $b \leqq a$ in A, $b - \bar{a}$ is a non-void (since a, b are regular) open set which contains some $a_i > 0$ in b but not in a; hence different elements of A correspond to different cuts in B_∞. Finally, every cut L, U in B_∞ corresponds to some $a \in A$. For take the set of all $x_i \leqq b$ for all $b \in U$, the upper half of the cut. Then the regular hull $(\bigvee x_i)^{**} \leqq b^{**} = b$ for all $b \in U$. But $x_i \in L$ in B_∞ if and only if $x \leqq b$ for all $b \in U$—i.e., if and only if $x \leqq (\bigvee_L x_i)^{**} \in A$, completing the proof.

LEMMA 2. *Let X be a Boolean space. Then the lattice of open subsets of X is isomorphic with the lattice of ideals of the Boolean algebra A of open-and-closed subsets of X.*

Proof. If J is an ideal of A, form the open join $S(J) =' \bigvee S_\alpha$ of the open-and-closed subsets S_α of X corresponding to $s_\alpha \in J$. Suppose T open and closed but not an S_α. Then no finite union $\vee_F S_\alpha$ of S_α contains T; hence no finite closed intersection $T \frown (\vee_F S_\alpha)' = T \frown \wedge S_\alpha'$ is void; but X is compact; hence $T \frown \wedge_J S_\alpha'$ is non-void, and T is *not* contained in $S(J)$. Hence J equals the ideal $K(S(J))$ of all $T \leqq S(J)$. Conversely, let U be any open set in X; $K(U)$ is an ideal in A. Moreover since X is zero-dimensional, each point $p \in U$ has an open-and-closed neighborhood $S_\alpha(p) \leqq U$. Hence $S(K(U))$, which is obviously contained in U, equals U.

The isomorphism of Lemma 2 transforms Thm. 9 of Ch. X into a special case of Thm. 5 above.

Ex. 1. Show that the "interior" operation $X \to X'^{-\prime}$ is a closure operation in the dual of the lattice of all subsets of any topological space.

Ex. 2. Show that a set N is nowhere dense if and only if, whenever S has a non-void interior, $S \frown N'$ has a non-void interior.

Ex. 3. Show that the intersection of two "regular" open sets must be regular, but that the union of two regular open sets need not be regular.

Ex. 4. Show that the Boolean algebra associated with the Cantor set is B_ω (Stone [4, p. 393]).

6. Sets of first category. A subset of a topological space X is said to be of *first category* (Baire) when it can be expressed as a sum of countable nowhere dense sets.

It is obvious that the subsets of first category in X are a σ-ideal J in the Boolean algebra A of all subsets of X. Moreover since Borel sets are generated by open sets, it follows from Lemma 1 and induction that every Borel set is congruent to a "regular" open set, modulo J. (Any open set S is congruent to S^{**}, while a closed set C is congruent to $C'^* = C'^{-\prime}$, modulo a nowhere dense boundary of first category.)

LEMMA. *In a complete metric space, or in a locally compact space, no two distinct "regular" open sets are congruent modulo a set of first category.*

Proof. We easily reduce to the case $R = A \frown B$ and $S = A \vee B$ of regular open sets $S > R$. Then $S \frown R^* > 0$ is regular and open, which reduces us to the case $S > 0$. Suppose $N_1 \smile N_2 \smile N_3 \smile \cdots$, where the N_i are nowhere dense. Then, by Ex. 2 of §5, $S \frown N_1' = S_1$ contains a closed sphere of radius at most 1/2; by induction, $S_k \frown N_{k+1}' = S_{k+1}$ contains one of radius at most $1/2^{k+1}$. The metric limit of the S_k will be in S but not in $\vee N_k$, which takes care of the complete metric case. In the locally compact case, we use compact S_k instead; we leave the details to the reader.

Combining the preceding results, we conclude[9]

THEOREM 7. *In any complete metric or locally compact space X, the Boolean σ-algebra of Borel sets of X, modulo sets of first category, and the lattice of open sets, modulo nowhere dense sets, are both isomorphic with the complete Boolean algebra of "regular" open sets of X.*

---

[9] Much of this result is due to S. Ulam and the author (Proc. Olso Congress (1936), vol. 2, p. 37). Thm. 6 above is largely due to H. M. MacNeille.

COROLLARY. *If X is a (locally) complete metric space satisfying the second countability axiom, then the quotient-algebras of Thm. 7 are isomorphic with the completion by cuts of B_∞.*

Ex. 1. Describe the algebra of "regular" open sets of X, if X is the sum of an "open" subset of Euclidean space and of discrete points.

Ex. 2*. The same, if X is Hilbert space under the metric topology—under the weak topology.

Problem 82. Find necessary and sufficient conditions on a Boolean algebra, for it to be isomorphic with the lattice of all "regular" open sets of a suitable T_1-space—of a suitable metric space.

7. Abstract closure algebras. McKinsey and Tarski [1] have given an interesting postulational discussion of the closure operation in topological spaces. It is clear that the subsets of any T_0-space form a closure algebra in the following sense.

DEFINITION. *A closure algebra is a Boolean algebra with a closure operation satisfying conditions* C1, C2, C3* *of the Foreword on Topology, and also* $\bar{0} = 0$.

Thus neither the existence of points, nor the infinite distributive law (22′) of Ch. IX, §11 are postulated. Though it is not yet clear how much of topology can be derived without postulating these further laws,[10] we can present a few positive results.

In any Boolean algebra B, the correspondence $x \to x \frown a$ is, for any fixed $a \in B$, a lattice-homomorphism of B onto the ideal A of all $y \leqq a$. Moreover A becomes a closure algebra, if one defines the *relative* closure of each $y \leqq a$ by

$$(1) \qquad \bar{y}_a = \bar{y} \frown a.$$

This we may call[11] the *relativization* of B, relative to a.

LEMMA 1. *The correspondence $x \to x \frown a$ is an endomorphism of B onto A, regarded as a closure algebra, if and only if a is open.*

Proof. The condition to be tested is that $\bar{x} \frown a = ((x \frown a)^-)_a$, which is $(x \frown a)^- \frown a$. Setting $x = a'$, this implies $a'^- \frown a = \bar{0} \frown a = 0$, or $a'^- \leqq a'$. This asserts that a' is closed, i.e., that a is "open." Conversely, if a is open, then $(x \frown a')^- \frown a \leqq a'^- \frown a = a' \frown a = 0$, whence

[10] Thus the important concept of isolated points almost certainly cannot be defined. However, it seems probable that Betti groups, dimensionality, and compactness can be treated. Still more general related systems have been discussed by J. Ridder, Verh. Ned. Akad. Wet., Sect. I 18 (1944), No. 4, 43 pp; and by O. Ore, Duke Jour. 10 (1943), 761–85, Annals of Math. 44 (1943), 514–33, and ibid. 47 (1946), 56–72, but these systems seem applicable mainly to algebraic problems.

[11] The nature of this operation was first stressed by C. Kuratowski, *Topologie*, Warsaw, 1933. Kuratowski also essentially derived Theorem 8 below; see Fund. Math. 3 (1922), 182–99.

$$\bar{x} \frown a = [(x \frown a) \smile (x \frown a')]^{-} \frown a = [(x \frown a)^{-} \smile (x \frown a')^{-}] \frown a$$

$$= [(x \frown a)^{-} \frown a] \smile [(x \frown a')^{-} \frown a] = (x \frown a)^{-} \frown a.$$

COROLLARY. *If a is open, the $x \in B$ which satisfy $x \frown a = 0$ or $x \geqq a$ form a closure subalgebra of B, isomorphic with the direct union $\mathbf{2} \cdot A_1$, where A_1 is the relative closure algebra of all x with $x \leqq a'$ (i.e., $x \frown a = 0$).*

For these are the elements mapped onto 0 and a in the preceding lemma.

We can now easily construct the *free closure algebra with one generator x.* It lies in the intersection of the subalgebras defined as in the preceding corollary by the "interior" $x'^{-\prime}$ of x and that $\bar{x}'$ of x'. Apart from components in $\mathbf{2}^2$, each element of it is therefore defined by its component on the closed *boundary* $b = (x'^{-\prime} \smile x^{-\prime})' = x^{-} \frown x'^{-}$ of x. But on this, $x_b^{-} = x_b'^{-} = b$; hence the components define a *four-element* closure algebra C defined by two points p, q, with $\bar{p} = \bar{q} = I$. Thus

THEOREM 8 (Kuratowski). *The free closure algebra with one generator is $\mathbf{2}^2 C$, and contains sixteen elements.*

What is perhaps more interesting, the results of §5 can be derived in any closure algebra, as shown in McKinsey and Tarski [2].

THEOREM 9. *The open elements of any closure algebra form a relatively pseudo-complemented lattice (Brouwerian logic).*

Indeed, the proofs given in §5 are valid as they are written. It is a corollary that the "regular" open sets form a Boolean algebra, etc., etc.

Tarski and McKinsey ([1, p. 149], and [2, p. 155]) have given representation theorems which show that closure operations in topological spaces have no algebraic properties not implied in the preceding definition. See also W. D. Puckett, Duke Jour. 14 (1947), 289–96.

Ex. 1. Show that, in the distributive lattice L of "open" elements of a closure algebra, $a^{-\prime}$ is a pseudo-complement of a, for any $a \in L$.

Ex. 2. (a) Define a closure algebra B to be "compact" if and only if every family of "closed" elements of B whose finite meets are non-void has a lower bound $s > 0$. Prove that every $a \in B$ defines a compact relative closure algebra, in this case.

(b) Define B to be "locally compact" if it contains a family of open sets with compact closures, whose join is I. Show that every regular open subset of a locally compact B is locally compact—or disprove it.

Ex. 3. Formulate a Duality Principle for topological spaces, interchanging closure and interior.

Ex. 4*. Show that the free closure algebra with n generators is infinite, for any $n > 1$.

Ex. 5*. Show that if, in the "free" closure algebra with n generators, $f \frown g = 0$, then $f^{-} \frown g^{-} = 0$.

Problem 83. Define the element 0 to be (-1)-dimensional in a closure algebra B. Define B to be "at most n-dimensional" if and only if, for any compact $c \in B$ and open $r > c$, one can find s, with $c \leqq s \leqq r$, whose boundary is "at most $(n-1)$-dimensional" in its relative topology. How much of dimension theory applies if B is (locally?) compact?

8. Measure theory. Much of the essence of measure theory is contained in the abstract considerations presented below. This formulation is due to the genius of C. Carathéodory;[12] we reserve for §9 the applications to special cases.

Suppose given a Boolean algebra A, a subalgebra S of A, and a non-negative valuation (measure function) $v[x]$, defined on S. We admit $+\infty$ as a possible value, but require $v[O] = 0$. For example, A might consist of all subsets of the infinite line, S might include all finite sums of intervals (with or without end points), and $v[x]$ might be the sum of the lengths of the intervals composing x.

We define an *outer measure* on A, by

$$(2) \qquad m^*[a] = \operatorname{Inf} \sum_{i=1}^{n} v[x_i], \quad \text{for} \quad x_i \in S \quad \text{with} \quad \bigvee_{i=1}^{n} x_i \geqq a.$$

Such finite sets of x_i will be called *coverings* of a.

Whether or not $v[x]$ is additive, we have

$$(3) \qquad a \leqq b \text{ implies } m^*[a] \leqq m^*[b],$$

$$(4) \qquad m^*[0] = 0,$$

$$(5) \qquad m^*[a \smile b] \leqq m^*[a] + m^*[b].$$

In general, any real-valued function defined on a Boolean algebra will be called an *outer measure* if it satisfies (3)–(5).

In such a system, we call *a measurable* when

$$(6) \qquad m^*[b] = m^*[a \frown b] + m^*[a' \frown b] \text{ for all } b \in A.$$

LEMMA 1. *The measurable elements of A form a Boolean subalgebra M of A, on which m^* is additive.*

Proof. By (6), since $(a')' = a$, if $a \in M$, then $a' \in M$. Again, if $a, c \in M$, then for all $b \in A$,

$$\begin{aligned} m^*[b] &= m^*[b \frown a] + m^*[b \frown a'] \\ &= m^*[b \frown a \frown c] + m^*[b \frown a \frown c'] + m^*[b \frown a' \frown c] + m^*[b \frown a' \frown c'] \\ &\geqq m^*[b \frown (a \frown c)] + m^*[(b \frown a \frown c') \smile (b \frown a' \frown c) \smile (b \frown a' \frown c')] \\ &= m^*[b \frown (a \frown c)] + m^*[b \frown (a \frown c)']. \end{aligned}$$

Hence $a \frown c \in M$, and M is a subalgebra of A. The additivity of m^* for ele-

[12] *Über das lineare Mass von Punktmengen*, Gott. Nachr., Math.-Phys. Klasse (1914); *Vorlesungen über reelle Funktionen*, Leipzig, 1927, Ch. V; *Entwurf fur eine Algebraisierung des Integralbegriffs*, S.-B. Bayer. Akad. (1938), 27–69; *Die Homomorphieen von Somen*, Ann. Scuo. Norm. Sup. Pisa 8 (1939), 105–30. See also J. Ridder, Acta Math. 73 (1941), 131–73; M. F. Smiley, Trans. Am. Math. Soc. 56 (1944), 435–47; A. Pereira Gomes, Portugaliae Math. 5. (1946) 1–120.

ments $a, b \in M$ follows as in Ch. X, §12, from the fact that if $a \frown b = 0$, then $m^*[a \smile b] = m^*[(a \smile b) \frown a] + m^*[(a \smile b) \frown a'] = m^*[a] + m^*[b]$.

In M, we call $m^*[a]$ the *measure* of a, and write it $m[a]$. We have shown that

$$\text{(7)} \qquad \text{if } a \frown b = 0, \text{ then } m[a \smile b] = m[a] + m[b].$$

Further, if m^* is defined by (2) from a valuation, one can show that all $a \in S$ are measurable (see Lemma 2 below), and that $m[a] = v[a]$.

We can define a second outer measure on A, by replacing the *finite* sums of (2) by *countable* sums,

$$\text{(2')} \qquad m^{**}[a] = \operatorname{Inf} \sum_{i=1}^{\infty} v[x_i], \quad \text{for} \quad x_i \in S \quad \text{with} \quad \bigvee_{i=1}^{\infty} x_i \geqq a.$$

Just as before, we infer (3)–(4); moreover (5) can be strengthened to

$$\text{(5')} \qquad m^{**}\left[\bigvee_{i=1}^{\infty} a_i\right] \leqq \sum_{i=1}^{\infty} m^{**}[a_i].$$

Hence (6) and Lemma 1 apply.

We now use the hypothesis that $v[x]$ is additive.

LEMMA 2. *Any $a \in S$ is measurable.*

Proof. Given any covering $\bigvee x_i \geqq b$ of any $b \in A$, we can construct coverings of $b \frown a$ and $b \frown a'$ by the $x_i \frown a$ resp. $x_i \frown a'$, where by hypothesis $\sum v[x_i] = \sum v[x_i \frown a] + \sum v[x_i \frown a'] \geqq m^{**}[b \frown a] + m^{**}[b \frown a']$. Since $m^{**}[b] = \operatorname{Inf} \sum v[x_i]$, for $\bigvee x_i \geqq b$, we infer

$$m^{**}[b] \geqq m^{**}[b \frown a] + m^{**}[b \frown a'].$$

Combining with (5), we get (6).

Unlike the finitely additive outer measure given by (2), that given by (2′) need not satisfy $m^{**}[a] = v[a]$ for all $a \in S$. To compensate, we have

LEMMA 3. *If A is any Boolean σ-algebra with an outer measure satisfying* (5′), *then the measurable elements form a σ-subalgebra in which*

$$\text{(7')} \qquad \textit{if all} \quad (a_1 \smile \cdots \smile a_{n-1}) \frown a_n = 0, \textit{then } m\left[\bigvee_{k=1}^{\infty} a_k\right] = \sum_{k=1}^{\infty} m[a_k].$$

Proof. By Lemma 1, the measurable elements form a subalgebra M; suppose $c_1, c_2, c_3, \cdots \in M$; if we can prove $\bigvee c_i \in M$, we will have shown that M is a σ-subalgebra. Define $d_n = c_1 \smile \cdots \smile c_n$, $c = \bigvee_{i=1}^{\infty} c_i$, $r_n = c \frown d_n'$, and $a_n = d_n \frown d_{n-1}'$; the a_n are thus disjoint elements, and $\bigvee_{i=1}^{n} a_i = d_n = \bigvee_{i=1}^{n} c_i$. We wish to prove $c \in M$—i.e., $m^{**}[b] = m^{**}[c \frown b] + m^{**}[c' \frown b]$. The case $m^{**}[c \frown b] = \infty$ is trivial, since then $m^{**}[b] \geqq m^{**}[c \frown b] = \infty$. Otherwise $\sum_{k=1}^{\infty} m^{**}[b \frown a_k] = \operatorname{Sup} m^{**}[b \frown d_n] < \infty$, so that, given $\epsilon > 0$, we can make $\sum_{k=n}^{\infty} m^{**}[b \frown a_k] < \epsilon$ by choosing n large enough. Hence, by Thm. 12 of Ch. X and (5′),

$$m^{**}[b \frown r_n] = m^{**}\left[b \frown \bigvee_{k=n}^{\infty} a_k\right] = m^{**}\left[\bigvee_{k=n}^{\infty} (b \frown a_k)\right] \leqq \sum_{k=n}^{\infty} m^{**}[b \frown a_k] < \epsilon.$$

By Lemma 1, every d_n is measurable, and so

$$m^{**}[b] + \epsilon > m^{**}[b \frown d_n] + m^{**}[b \frown d_n'] + m^{**}[b \frown r_n].$$

By (3), $d_n'^{**}[b \frown c'] \leqq m^{**}[b \frown d_{n'}]$, and by (5),

$$m^{**}[b \frown c] = m^{**}[b \frown (d_n \smile r_n)] \leqq m^{**}[b \frown d_n] + m^{**}[b \frown r_n].$$

Substituting, $m^{**}[b \frown c'] + m^{**}[b \frown c] < m^{**}[b] + \epsilon$ for all $\epsilon > 0$, which proves that $c \in M$.

To prove (7′), we need only note that by (3),

$$m^{**}\left[\bigvee_{k=1}^{\infty} a_k\right] \geqq \operatorname{Sup} m^{**}\left[\bigvee_{k=1}^{n} a_k\right] = \operatorname{Sup}\left(\sum_{k=1}^{n} m^{**}[a_k]\right) = \sum_{k=1}^{\infty} m^{**}[a_k],$$

while the reverse inequality is guaranteed by (5′).

LEMMA 4. *If outer measure is defined, in a Boolean σ-algebra, by (2′), then every measurable element is congruent to a countable meet of countable joins of elements of S, modulo an element of measure zero. The finite joins of elements of S are dense in M.*

Proof. Let $a \in M$ be given; we can find, for each m, a countable set of $x_{m,n} \in S$ such that $y_m = \bigvee_{n=1}^{\infty} x_{mn} \geqq a$, yet

$$m^{**}[y_m] \leqq \sum_{n=1}^{\infty} m^{**}[x_{mn}] \leqq \sum_{n=1}^{\infty} v[x_{mn}] \leqq m^{**}[a] + 2^{-m}$$

Set $z = \bigwedge_{m=1}^{\infty} y_m \in M$; clearly $z \geqq a$; yet $m^{**}[z] \leqq m^{**}[a]$. It follows that $m^{**}[(z \frown a') \smile (z' \frown a)] = 0$, proving the first assertion. Since we can make $\bigvee_{n=1}^{r} x_{mn}$ arbitrarily close to y_m, we get the second result.

COROLLARY. *If S is countable, then the measure algebra defined by M, modulo elements of measure zero, is separable.*

Ex. 1. Prove that (7) holds if a *or* b is measurable.

Ex. 2. (a) Prove that if $m^*[a] = 0$, then a is measurable.
(b) Prove that if a is measurable, then $m^*[a] + m^*[a'] = m^*[I]$, for any outer measure.
(c)* Prove that if $m^*[I]$ is finite, then $m^*[a] + m^*[a'] = m^*[I]$ if and only if a is measurable.

Ex. 3. (a) Show that $m_*[a]$ is g.l.b. $m[x]$, for measurable $x \leqq a$, with any outer measure.
(b) Show that if $m[I]$ is finite, then the "inner measure" $m^*[a] = m[I] - m^*[a']$ is l.u.b. $m[y]$, for measurable $y \leqq a$.

Ex. 4. Let A be the Boolean algebra of all subsets of the set I of rational numbers r, $0 \leqq r \leqq 1$. Let S be the subalgebra of finite sums of intervals, with their usual measure. Show that $m_{**}[I] = 0$, though $v[I] = 1$.

Ex. 5. Show that if we repeat the process of defining outer measure by (2) or (2′), but using M and $m[x]$ in place of S and $v[x]$, we get the same outer measure back again.

9. Applications. The most important application of the theory of §8 is to the case that A consists of the subsets of Euclidean n-space, S consists of the "elementary" subsets in the sense of §1, and $v[x]$ is the n-dimensional volume of x, in the elementary sense.[13]

In this case, the construction of (2) and Lemma 1 defines what is usually called "Jordan content." The construction of (2′) gives classical Borel-Lebesgue measure, in n dimensions. Since (by compactness) any covering of a closed rectangle by elementary sets determines one by open rectangles which has arbitrarily little greater total volume, we see that in this case $m^{**}[x] = v[x]$ for elementary sets. Thus *Borel-Lebesgue measure is a direct extension of elementary volume.*

Again, we could have replaced S by the *countable* field of sets (Boolean subalgebra of A) generated by n-rectangles bounded by rational coordinates, without altering $m^{**}[x]$ in A. Hence, by the Cor. at the end of §8, the measure algebra defined by Lebesgue measurable sets in Euclidean n-space is *separable.* Since it obviously contains no indivisible elements of positive measure, we conclude

THEOREM 10. *The "measure algebra" of measurable subsets of the unit cube in Euclidean n-space $[n \geqq 1]$, modulo sets of measure zero, is the $\bar{M}$ of Thm.* 15, *Ch.* X.

Incidentally, Lemma 3 of §8 shows that every Borel set is measurable, while Lemma 4 shows that, conversely, every measurable set is congruent modulo a null set to an intersection of countable open sets, which is a Borel set of class G_δ.

COROLLARY. *The Borel subsets of the unit cube in m-space, modulo sets of measure zero, form the metric completion of B_∞. (Cf. Thm. 7, Corollary.)*

Again, consider Daniell's theory[14] of measure on the countable-dimensional torus of points $x = (x_1, x_2, x_3, \cdots)$ $[x_i \text{ mod } 1]$. Let π_n denote the slicing up of this torus into the $2^{n(n-1)/2}$ "generalized rectangles" R: $k(R)/2^{n-i} \leqq x_i < (k(R)+1)/2^{n-i}$ $[i = 1, 2, \cdots, n]$. The π_n define a sequence of finite Boolean algebras with measure functions. The union of these is countable; now, by applying (2″), we get Daniell measure. Moreover, since the torus is compact, we have as before $m^{**}[x] = v[x]$. Hence, as above, the algebra of Daniell measurable subsets of the countable-dimensional torus, modulo sets of Daniell measure 0, is isometrically isomorphic with $\bar{M}$.

In the measure theory associated with the Radon-Stieltjes theory of integration, on the other hand, one has a subalgebra of $\bar{M}$ in which lumps or "atoms" of positive measure are allowed.

---

[13] It is easy to show that if $v[x]$ is to be invariant under translation, then the "value" of a rectangle must be proportional to the product of the lengths of its sides; hence we are led inevitably to the usual elementary measure. We omit the proof that the volume so defined is a valuation.

[14] P. J. Daniell, *Integrals in an infinite number of dimensions*, Annals of Math. 20 (1919), 281–8; B. Jessen, Seventh Scand. Math. Congress Oslo (1929), 127–38; R. E. A. C. Paley and N. Wiener, *Fourier Transforms in the complex domain*, Am. Math. Soc. Colloquium Publ., vol. 19 (1934), Ch. IX.

Problem 84. Characterize abstractly, as measure algebras, (a) the natural extension of Daniell measure to a torus of uncountably infinite dimensions, (b) the measure algebra of sets of finite p-dimensional measure in Euclidean q-dimensional space, in the sense of Hausdorff.[15]

10. Measure sometimes impossible. We shall now show that, although a finitely additive measure can be constructed in any Boolean algebra, there are many important (infinite) Boolean algebras in which no countably additive measure is possible. For example, it is improbable that a countably additive measure can be constructed on the interval $0 \leqq x \leqq 1$, which gives all points zero measure.

THEOREM 11. *Any finitely additive measure function defined on a subalgebra S of a Boolean algebra A can be extended*[16] *to one defined on all of A.*

Proof. Since our conditions are of finite character (Ch. III), it suffices to show that an extension from any $S < A$ to a larger subalgebra is possible. But let $a \notin S$ be given; the elements $(a \frown b) \smile (a' \frown c)$ $[b, c \in S]$ form such a subalgebra. We define explicitly

$$
\begin{aligned}
&m_1[a \frown b] = \operatorname{Inf} m[s] \text{ for } s \geqq a \frown b \text{ in } S,\\
(8)\qquad &m_1[a' \frown c] = \operatorname{Sup} m[t] \text{ for } t \leqq a' \frown c \text{ in } S,\\
&m_1[(a \frown b) \smile (a' \frown c)] = m_1[a \frown b] + m_1[a' \frown c].
\end{aligned}
$$

We shall show that this is an extension, as desired.

$$m_1[a \frown b] + m_1[a' \frown b] = \operatorname{Inf}_s\{m[s] + \operatorname{Sup}_t m[t]\}.$$

But given $s \geqq a \frown b$, $s' \frown b \leqq (a' \smile b') \frown b = a' \frown b$ is a t of the desired kind. Hence, for any admissible s, we have

$$m[s] + \operatorname{Sup}_t m[t] \geqq m[s] + m[s' \frown b] \geqq m[s \smile (s' \frown b)] = m[s \smile b] \geqq m[b].$$

Hence $m_1[a \frown b] + m_1[a' \frown b] \geqq m[b]$, for any $b \in S$. By duality, we get the reverse inequality, proving $m_1[b] = m[b]$.

It remains to prove that m_1 is additive; it is enough to show that a-components are additive—that for all $b, c \in S$, $(a \frown b) \frown (a \frown c) = 0$ implies $m_1[(a \frown b) \smile (a \frown c)] = m_1[a \frown b] + m_1[a \frown c]$. For any $\epsilon > 0$, we can find $t \geqq a \frown b$, $u \geqq a \frown c$ in S, with $m[t] < m_1[a \frown b] + \epsilon$, $m[u] < m_1[a \frown c] + \epsilon$, hence

$$m[t \smile u] \leqq m[t] + m[u] \leqq m_1[a \frown b] + m_1[a \frown c] + 2\epsilon.$$

Since $t \smile u \geqq (a \frown b) \smile (a \frown c)$, $m_1[(a \frown b) \smile (a \frown c)] \leqq m_1[a \frown b] + m_1[a \frown c]$. Conversely, for any $v \geqq (a \frown b) \smile (a \frown c) = a \frown (b \smile c)$ in S,

---

[15] F. Hausdorff, *Dimension und ausseres Mass*, Math. Annalen 79 (1919), 157–79.

[16] This result is due essentially to A. Tarski, Fund. Math. 15 (1930), 42–50. For related results, see Exs. 1–3 below; also A. Tarski, Fund. Math. 32 (1938), 45–63, and 33 (1945), 51–65.

we have $m[v] \geqq m[v \frown b \frown c'] + m[v \frown c]$, since the two are disjoint. By straight Boolean algebra, $v \frown b \frown c' \geqq a \frown b$; thus since $a \frown c \frown c' = 0 = a \frown b \frown c$,

$$\begin{aligned} v \frown b \frown c' &\geqq a \frown (b \smile c) \frown (b \frown c') \\ &= (a \frown b \frown c') \smile (a \frown b \frown c) = a \frown b. \end{aligned}$$

Hence $m[v \frown b \frown c'] \geqq m_1[a \frown b]$; similarly, $m[v \frown c] \geqq m_1[a \frown c]$. Hence every $m[v] \geqq m_1[a \frown b] + m_1[a \frown c]$, and

$$m_1[(a \frown b) \smile (a \frown c)] = \operatorname{Inf} m[v] \geqq m_1[a \frown b] + m_1[a \frown c], \text{ q.e.d.}$$

We now come to negative results.

THEOREM 12. *In any measure algebra, we have, for any countable set of elements* x_i $[i = 1, 2, 3, \cdots]$,

$$(9) \qquad \operatorname*{Inf}_{0 < y_i \leqq x_i} \left(\bigvee_{i=1}^{\infty} y_i \right) = 0, \quad \textit{unless points (of positive measure) exist.}$$

Moreover if, for all i, $\bigvee_j a_j^i = I$, *and* $m[I] > 0$, *then*

$$(10) \qquad m\left[\bigwedge_i \left(\bigvee_{j=1}^{r(i)} a_j^i \right) \right] > 0 \textit{ for some function } r(i).^{17}$$

Proof of (9). Unless points exist, we can find, for any $\epsilon > 0$, y_i with $0 < y_i \leqq x_i$, such that $m[y_i] < \epsilon/2^i$. It follows that $m[\bigvee_{i=1}^{\infty} y_i] \leqq \sum_{i=1}^{\infty} m[y_i] < \epsilon$. Hence as we vary the choice of y_i, $m[\bigwedge(\bigvee_{i=1}^{\infty} y_i)] < \epsilon$ for all $\epsilon > 0$, and $\bigwedge(\bigvee_{i=1}^{\infty} y_i) = 0$.

Proof of (10). For each $\epsilon > 0$ and i, we can choose $r(i)$ so large that $m[\bigvee_{j=1}^{r(i)} a_j^i] > m[I] - \epsilon/2^i$. It follows that $m[\bigwedge_i \bigvee_{j=1}^{r(i)} a_j^i] > m[I] - \epsilon$. This proves (10′) if $m[I] > 0$; it even proves

$$(10') \qquad \bigvee_{r(i)} [m \bigwedge_i \bigvee_{j=1}^{r} a_j^i] = m[I].$$

The preceding results can be stated more simply if we identify elements whose symmetric difference has measure zero.

COROLLARY 1. *The algebra of Borel sets modulo sets of first category is not isomorphic with any measure algebra.*

For if we let the x_i be the intervals with rational end points, then $\bigvee y_i = I$ for any choice of y_i with $0 < y_i \leqq x_i$. Comparing with the Cors. of Thms. 7, 10, we obtain

[17] Condition (9) and Cors. 1–2 are due to S. Ulam and the author—see Proc. Oslo Congress (1936), vol. 2, p. 37; also J. von Neumann [2, Part IV]. For an interesting related result, see E. Szpilrajn, Fund. Math. 22 (1934), p. 304. Condition (10) and Thm. 13 are due to S Banach and C. Kuratowski, Fund. Math. 14 (1929), 127–31; Banach, ibid. 15 (1930), 97–101; Ulam ibid., 16 (1931), 140–50.

COROLLARY 2. *The completion by cuts of the metrized free Boolean algebra with countable generators is not isomorphic with its metric completion.*

THEOREM 13. *If the Continuum Hypothesis is true, then no non-trivial countably additive measure can be defined for all subsets of the continuum, such that every point has measure zero.*

Proof. Form the class of all single-valued functions α: $\alpha(i) = j$ from the positive integers to the positive integers. There are $2^{\aleph_0}$ of these; hence if the Continuum Hypothesis is true, we can well-order the set A of α so that each α has countably many predecessors. Now reject all α such that, for some $\beta < \alpha$ in A, $\alpha(i) < \beta(i)$ for all i. The residual set B of unrejected β has the property that to every $\alpha \in A$ corresponds a $\beta \in B$, with $\beta < \alpha$ and $\alpha(i) \leqq \beta(i)$ for all I (since the relation is transitive and A well-ordered). Again, if B were countable, then we could enumerate its members $\beta_1, \beta_2, \beta_3, \cdots$; defining $\beta^*(k) = \beta_k(k) + 1$, we would get a new unrejected β^*, contrary to hypothesis. Hence B is uncountable. By the Continuum Hypothesis again, it is therefore in one-one correspondence with the continuum, so that points of the continuum can be denoted p_β $[\beta \in B]$. Now let X_k^i denote the set of all points p_β with $\beta(i) = k$; clearly $\bigvee_{k=1}^{\infty} X_k^i = I$, for all i, since $\beta(i)$ has some value. Hence, by (10), for some $r(i)$, $m[\bigwedge_i(\bigvee_{j=1}^{r(i)} X_j^i)] > 0$. But some $\beta_0 \in B$ satisfies $\beta_0(i) \geqq r(i)$ for all i. And $\beta(i) \leqq r(i) \leqq \beta_0(i)$ for all i will imply $\beta \leqq \beta_0$ in B; the set of these predecessors of β_0 is however always countable. Hence $\bigwedge_i (\bigvee_{j=1}^{r(i)} X_j^i)$ contains only *countably* many points p_β, and must have measure zero. This contradiction proves the theorem.

S. Ulam (loc. cit.) has proved the impossibility of such a measure under still weaker hypotheses.

Ex. 1. Using the representation theorem, prove directly that any distributive lattice has a finitely additive measure not identically zero.

Ex. 2. Using Thm. 11, prove that, in the case of the Boolean algebra of all subsets of the continuum, we can in addition make all finite sets have measure zero.

Ex. 3*. Extend Thm. 11 to distributive lattices L with 0, in the case of bounded measure functions. (Suggestion: Show that linear functionals on the space (B) of bounded functions on the set I representing L are the Riemann integrals of bounded measure functions on I—and use Banach's extension theorem.)

Ex. 4. Show that no metric distributive lattice with I can have an uncountable family of disjoint elements.

Problem 85. Find necessary and sufficient conditions for a Boolean algebra to be isomorphic with a measure algebra, modulo elements of measure zero.[13]

Problem 86. Prove the impossibility of a non-trivial countably additive measure for all subsets of the continuum, which gives all points measure zero, without assuming the Continuum Hypothesis.

---

[13] See Thm. 15 of Ch. X and the refs. given above; also D. Maharam, Trans. Am. Math. Soc. 51 (1942), 164–93, and Annals of Math. 48 (1947), 154–67.

CHAPTER XII

APPLICATIONS TO LOGIC AND PROBABILITY

1. Algebra of attributes. The present chapter will be devoted exclusively to *Algebraic* aspects of logic and probability. No attempt is made to treat the more controversial aspects of these fields, nor to resolve the paradoxes of set theory. As only two of our results are theorems of lattice theory, much of the material will be presented informally.

We begin by describing the classical Boolean algebra of attributes. The concept of an *attribute* (also called "property" or "quality") of an object is so fundamental, that no definition of it in more fundamental terms is possible.[1] Attributes are usually designated by adjectives (viz., red, liquid, dead, etc.) or generic nouns (viz., beast, tree, ocean, etc.). It is easily seen that, in their logical effect, adjectives and generic nouns are equivalent—to say, "water is liquid" is tantamount to saying "water is a liquid."

One can *combine* attributes by the conjunctions *and, or* (viz., red and liquid, red or liquid); one can also construct the negative of any attribute by using the word *not* (viz., not red). One can also relate attributes by inclusion; thus the attribute of being an ocean includes the attribute of being liquid ("every ocean is liquid").

Boole's First Law. Let attributes be designated by letters, "and," "or," "not" by the symbols $\smile$, $\frown$, $'$ respectively, and "every x is y" by "$x \leqq y$." Then attributes form a Boolean algebra.

This proposition can be verified by comparison of L1–L7 with rules of inference presented in textbooks on formal logic, or by direct introspection.

The reader will readily see that this is not a deductive "proof" of a mathematical theorem. In fact, we are simply reformulating some of the fundamental assumptions of classical logic, in a form adapted to mathematical analysis.[2]

We shall now derive some useful corollaries from Boole's First Law and our preceding work. Thus the postulate theory of Ch. X, §4, shows that effectively equivalent systems of axioms for formal logic can be found, which vary widely in appearance. For example, "or" and "not" can be defined in terms of "and" alone.

---

[1] Thus Boole [2, p. 27, Prop. I] asserts that all reasoning can be reduced to the discussion of objects and their attributes. Biology affords excellent illustrations of combinations of attributes (e.g., mammal, vertebrate, carnivorous, cannibal, quadruped, etc.).

[2] Further consideration of the matter brings out the real difficulty: any purely logical analysis of logic involves "reasoning in a circle" in its very essence. The only escape from this circle consists in an objective study of the implications of these assumptions.

Bibliographical note. For physiological correlations with Boolean algebra, see A. Householder and H. D. Landahl, *Mathematical biophysics of the central nervous system*

Again (Ch. X, Thm. 11), exactly 2^{2^n} different attributes can be compounded from given ones, by use of and, or, and not. Finally, Boolean algebra implies *all* the identities valid for finite sets of attributes under "Boolean" combination by and, or, and not. For the free Boolean algebra with n generators can be realized by sets (Ch. X, §8), and hence (§2 infra) by attributes of belonging to suitable sets. Hence no (finite) identity not true in every Boolean algebra can be true for attributes in general.

Indeed, using Ch. X, §8, it is easy to show that the finite identities of Boolean algebra are maximal, in the sense that if one adjoins any additional independent identity, then *every* identity may be proved.[3] One may interpret this result as follows. The classical logic of attributes cannot be *strengthened* without giving rise to absurdities; it can only be *weakened*.

Ex. 1. Base a system of verbal rules for formal logic in postulates for Sheffer's stroke operation.

Ex. 2. Define "or" and "not" on terms of "and" alone. (Hint: Define $\leq$ first.)

2. Boole's dual isomorphism; critique. It is natural to identify each attribute x with the class $\hat{x}$ of all objects (or "things") having that attribute. Moreover, by definition of set-product, the set of objects having both attribute x and attribute y is the set-product of the set $\hat{x}$ and the set $\hat{y}$. Similar arguments for the other two cases prove

$$(1) \qquad \widehat{x \smile y} = \hat{x} \frown \hat{y}, \quad \widehat{x \frown y} = \hat{x} \smile \hat{y}, \quad \widehat{(x')} = (\hat{x})';$$

the correspondence $x \to \hat{x}$ is a dual homomorphism.

Conversely, with each class X of objects, we may associate the attribute a_X of "membership in X"; moreover $\hat{a}_X = X$ for all X. We may say that two attributes are "objectively equivalent" if they determine the same class; this will lead to the following result of Boole [2, pp. 28, 43].

Boole's Second Law. The correspondence $x \to \hat{x}$ is a dual isomorphism between the Boolean algebra of classes and that of attributes, provided objectively equivalent attributes are identified.

This dual isomorphism affords the standard way of passing back and forth between the subjective world of mind (attributes), and the objective world of matter. But it must be admitted that, if carried to its logical extreme, it involves one in conclusions which common sense rejects, and in well-known mathematical paradoxes as well.

Thus the concept of "the class of all objects" is patently meaningless. Not being omniscient, we simply do not know what it is—e.g., did it include mesons in 1850?[4] Again, "the class of all ordinal numbers" is well-ordered; let τ denote its ordinal number; τ cannot exist (by Thm. 4 of Ch. III, and the sentence

[3] See K. Gödel, Monats. Math. u. Phys. 37 (1930), 349–60.

[4] The philosophical absurdity of a literal acceptance of the dogmas of formal logic is exposed, from the point of view of common sense, in F. C. S. Schiller's *Formal logic*, MacMillan, 1931; the dual isomorphism between intension and extension receives specific attention on pp. 33–36.

following it); this is a mathematical paradox, at least if one accepts the Axiom of Choice.

Various plausible conventions have been proposed by mathematical logicians for avoiding such paradoxes; each has its merits; but none has been proved indispensible. These conventions will not be discussed below.

Instead, we shall consider in §§4–9 various alternative models for the algebra of logic, which can be motivated by physical or psychological arguments. It is entirely possible that different physical theories may permit differing algebras of logic. Indeed, this possibility has been widely accepted on a philosophical level, with respect to the theory of relativity and quantum mechanics (the Uncertainty Principle).[5]

Judgment of the relative utility of these non-Boolean algebras of logic may not be possible for many years.

3. Propositional calculus. But before turning our attention to non-Boolean algebras of logic, we shall describe the Boolean algebra of propositions.[6] For any propositions x, y one can denote the propositions "x and y," "either x or y (or both)," and "not x," by $x \smile y$, $x \frown y$, and x', respectively. Under this notation, the identities of Boolean algebra relate logically equivalent statements. Thus (L2) "John sleeps and Henry walks" is true or false according as "Henry walks and John sleeps" is true or false. In summary, we get

Boole's Third Law. Propositions form a Boolean algebra.

Applications of Boolean algebra may be made to the propositional calculus, similar to those described at the end of §1.

In classical logic, all propositions are either true or false. Moreover $x \smile y$ is true if and only if x and y are both true; $x \frown y$ is true if x or y is true; of x and x', one is true and the other false. Hence we get the

Fourth Law. True propositions form a (proper) *prime ideal* in the Boolean algebra of all propositions: the complementary dual ideal consists of false propositions.

The resulting propositional calculus will clearly apply *only* to systems in which all propositions are demonstrably true or demonstrably false; thus it need not apply to questions of fact where there is limited evidence. In such systems the compound proposition "x implies y" ("if x, then y"), which is denoted $x \to y$, has a very special meaning. Clearly $x \to y$ is true or false according as "y or not-x" is true or false; thus, following Whitehead and Russell, one can identify $x \to y$ with $x' \frown y$, *if* one identifies propositions which are both true or both false. This is reasonable if one's only interest is in determining the class of all true propositions in a single system.

In such systems, one can similarly denote "x is equivalent to y" by $x \sim y$,

[5] We recall also the sharp distinction between inductive and deductive logic.

[6] Synonyms for proposition are: "sentence," "statement," "theorem." The propositional calculus deals with compound sentences like: "John sleeps and Henry walks," "Johns sleeps or Henry walks," "John sleeps not."

and identify it with "x implies y and y implies x"—i.e., with the symmetric difference $(x \to y) \smile (y \to x) = x + y$ of x and y. One can also show that many compound propositions p are "tautologies," that is, true by virtue of their logical structure alone. This amounts algebraically to saying that $p \sim 0$. The simplest tautology is $x \frown x'$ ("x or not-x"). It is a simple exercise in Boolean algebra to show that the following are also tautologies,

$$I \to x,\ x \to 0,\ x \to x,\ x \sim x,\ x \to (y \to x),$$

$$(x \sim y) \sim (y \sim x),\ (x \sim 0) \frown (x \sim I),\ (x \to y) \frown (y \to x), \tag{2}$$

$$[(x \to y) \smile (y \to z)] \to (x \to z),\ (x' \to I) \to x.$$

The legitimacy of assuming these tautologies in mathematical logic is discussed in §6.

Ex. 1. (a) Using Boolean algebra, give formal proofs of the "tautologies" (2).
(b) Write sentences in ordinary words, which correspond to them.

Ex. 2. Show that "x unless y," "x and/or y," and "if not-y, then x" have the same meaning. To what does "x or y, but not both," correspond?

Ex. 3. (a) Develop postulates for the Whitehead-Russell algebra of propositions in terms of the unary operation x' and the binary operation $x \to y$.
(b) Show that, in terms of implication alone, one cannot define x'.
Hint: 0, x form an "implication subalgebra."

Ex. 4. Let $2^n = A$ be any finite Boolean algebra, and let P be any prime ideal of A. Show that, for a fixed point a and a variable subset S of a class C of n elements, the proposition $a \in S$ gives an isomorphic representation of (A, P) in terms of a calculus of propositions.

4. A model from classical mechanics. By Thm. 13 of Ch. X, the identification of attributes with classes which is accepted in classical formal logic (Boole's Second Law) is tantamount to an assumption that the generalized distributive law (22') of Ch. IX is valid. By Thm. 16 of Ch. X, it is tantamount to the assumption that there exist *maximal* attributes, true only of a single element (hence corresponding to proper names); this we may call the Atomistic Hypothesis.

The Atomistic Hypothesis must however be avoided in typical physical applications, as we shall now see.

Consider the n-body problem, as usually treated.[7] The "state" of a system Σ of n bodies at any time t_0 can be expressed by $6n$ real numbers: each body has three coordinates of position and three of velocity. Moreover this description is complete, in the sense that the state of Σ at any later (or earlier!) time t is determined by these numbers and the laws of mutual attraction and repulsion.

In summary, the "state" (or phase) of Σ may be represented by a point in $6n$-dimensional Cartesian space; the space of all such points is called the *phase-space* I of Σ. Each attribute of Σ defines a set in this phase-space: the set of all "states" in which Σ has the given attribute. Thus according to Boolean

[7] These bodies may represent either the planets and their satellites (celestial mechanics), or the molecules of a gas (statistical mechanics).

logic, there should be a one-one correspondence between the subsets of I and attributes of Σ.

But this is physically absurd. Thus, since the accuracy of measurements is limited, one can never know by experiment whether the kinetic energy of Σ, measured in ergs, is a rational number.

The correspondence may also be mathematically inconvenient, in that (by Thm. 13 of Ch. XI) it is probably incompatible with the principle, essential in statistical mechanics, that *every* significant attribute has a probability, where probability is countably additive.

Without prolonging the discussion, we may assert that dictates of mathematical consistency and physical plausibility[8] strongly suggest making "attributes" correspond to measurable subsets, ignoring sets of measure zero.

The resulting system is of course the universal separable measure algebra of Thm. 15, Ch. X. It is a *continuous* Boolean algebra, which avoids the dubious Atomistic Hypothesis. However, on the finite level, it is a strictly Boolean logic; it even satisfies the infinite distributive laws of Ch. X, Thm. 12. It admits a non-trivial, countably additive probability function—being, in fact, the model on which most modern probability theories are based (see §9).

5. A model from quantum mechanics. The logic of quantum mechanics is more complicated. According to the generally accepted mathematical theory,[9] the "state" of a system may be represented by a point ψ in complex Hilbert space, which thus acts as a "phase-space" I. Moreover observable quantities correspond to self-adjoint operators A on I.

If A has a *discrete* spectrum, the theory of the attributes definable in terms of A is simple. There are countable orthogonal eigenstates $\psi_1, \psi_2, \psi_3, \cdots$, such that $\psi_i A = \lambda_i \psi_i$. Any given "state" ψ can be expanded as $\psi = \sum c_i \psi_i$, where the ψ_i are characteristic states associated with different eigenvalues λ_i. The *a priori* probability that an observation of ψ will yield the measurement λ_i is then $|c_i|^2 = c_i c_i^*$. The most general physical attribute definable in terms of A is of the form

$$\lambda \in L, \qquad L \text{ any subset of the spectrum.} \tag{3}$$

This is a "true or false" statement *a posteriori*. The corresponding *a priori* probability that an observation of ψ will yield a measurement $\lambda \in L$ is then

$$P_L = \sum_{\lambda_i \in L} |c_i|^2. \tag{4}$$

This has the formal properties of probability (§9).

---

[8] Von Neumann has remarked that, since a set is measurable if and only if it has density 0 or 1 almost everywhere, we select precisely those attributes upon whose truth or falsity we can pronounce, with arbitrary nearness to certainty, by making sufficiently accurate measurements. Also, all known attributes (viz., of having temperature, pressure, etc., within fixed limits), correspond to Borel (hence measurable) sets.

[9] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Berlin, 1931; or P. A. M. Dirac, *Wave Mechanics*, Oxford Press, 1930. The ideas of the present section are due to von Neumann and the author, *The logic of quantum mechanics*, Annals of Math. 37

It is apparent that the *statements* definable in terms of A form the atomic Boolean algebra of all subsets of a countable set; whereas the *predictions* involving A are purely statistical.

Next, suppose that A has a continuous spectrum; the case of the x-coordinate of position is typical. To each elementary *statement* of the form $x > \alpha$ (α any real number) corresponds a *closed subspace* S_α of Hilbert space; we let E_α denote orthogonal projection onto S_α. For given ψ, the *prediction*

$$(3') \qquad x \in L_\alpha, \quad \text{where } L_\alpha \text{ is the set of } x > \alpha,$$

has a probability of being fulfilled which is given by

$$(4') \qquad P_\alpha = |\psi E_\alpha|^2 = \psi E_\alpha E_\alpha^* \psi^*.$$

Under countable union, intersection, and complementation, the L_α generate the σ-field Φ of all *Borel subsets* L of the spectrum (Ch. XI, §1). The corresponding operations on the complete lattice of closed subspaces of Hilbert space give a Boolean algebra of closed subspaces, S_L, which is actually Φ modulo sets of measure zero as in §4. Orthogonal projections E_L onto the S_L are, in turn, generated by the E_α under multiplication, addition modulo two ("Boolean addition"—Ch. X, §3), and passage to the limit; the resulting Boolean ring is also isomorphic to the non-atomic Boolean algebra of §4.

Hence, if A has a continuous spectrum, the *a posteriori* statements about A correspond to Borel subsets L of the spectrum, modulo sets of measure zero. The a priori probability of the prediction $\lambda \in L$ is given, in quantum theory, by

$$(4'') \qquad P_L = |\psi E_L|^2 = \psi E_L E_L^* \psi^*.$$

More generally, if $A, B, C, \cdots$ are any set of permutable observables, we know that each statement L corresponds to a closed subspace S_L of Hilbert space. In the absence of physical evidence, we shall make the following

Hypothesis. The linear sum of any two closed subspaces which correspond to observable attributes, itself corresponds to an observable attribute.

It will follow that any linear sum $X \smile Y$, orthogonal complement X', or intersection $X \frown Y = (X' \smile Y')'$ of such closed subspaces will correspond to an observable attribute. That is, *the logic of quantum mechanics is an orthocomplemented modular lattice.*

Thus the distributive law of logic disappears, even on the finite level. (Infinite distributivity has already disappeared in the model of §4.) Specifically *the distributive law is satisfied by simultaneously observable attributes, but no others.* (Two quantities are "simultaneously observable" in quantum mechanics, if and only if the associated linear operators are permutable; the proof of the preceding statement follows from Ex. 2 below.) It is noteworthy that these results would remain valid if we replaced the preceding Hypothesis by the hypothesis that every closed subspace of Hilbert space corresponded to an observable attribute. In any case, a priori probabilities are presumably given by (4).

The preceding questions will be treated in greater detail by Mme. Paulette Destouches-Février in *Recherches sur la structure des théories physiques*, to be published by Presses Universitaire.

Ex. 1. (a) Show that, in any orthocomplemented modular lattice M, the sublattice generated by any chain and its complements form a Boolean algebra.

(b) Show that, if M is metric, a complete Boolean is generated if limits are included.

(c) Correlate with the logic of quantum mechanics.

Ex. 2. Let E, F denote orthogonal projections onto closed subspaces S, T of Hilbert space.

(a) Show that $EF = FE$ if and only if $S \frown T$, $(S \frown T)' \frown S$, and $(S \frown T)' \frown T$ are orthogonal. (Here X' denotes the orthogonal complement of X.)

(b) Show that if $EF = FE$, then both denote orthogonal projection onto $S \frown T$, while $E + F + EF$ denotes projection onto $S \smile T$.

(c) Infer that if a family of closed subspaces satisfies (a), then the orthocomplemented sublattice which they generate is a Boolean algebra.

(d) Extend to a complete Boolean algebra.

Ex. 3. Show, by elementary logic, for simultaneously observable attributes, "x and (y or z)" has the same probability as "(x and y) or (x and z)".

Ex. 4. Show that, for simultaneously observable attributes, L is a "probability function" in the sense of §9.

6. Metaphysical objections to Boolean logic. In §§4–5 we have discussed algebras of attributes suggested by the needs of theoretical physics. We shall now discuss propositional calculi suggested by purely metaphysical objections to the Boole-Whitehead algebra of logic described in §§1–3.

Thus the principle that "a false proposition implies every proposition," which is expressed in the tautology $I \to x$ of §3, seems philosophically unsatisfactory.[10] So does the tautology $(p \to q) \smile (q \to p)$, which asserts that "of any two propositions p, q, either p implies q or q implies p."

In the same skeptical vein, one may question the validity of proofs by contradiction. Why should the disproof (or "reductio ad absurdum") of "not-p", imply the truth of "p"? Such negative proofs seem particularly unsatisfactory when "p" asserts the existence of a number, but the disproof of "not-p" indicates no procedure for finding it.

Brouwer and his "institutionist" school implacably reject all such "nonconstructive" proofs. And indeed, one cannot defend proofs by contradiction if one admits the existence of "undecidable" propositions, for which neither "p" nor "not-p" is demonstrable. There is some evidence for the existence of undecidable propositions.

Thus Skolem and Gödel[11] have constructed a plausible and consistent logical

[10] In this connection, the following anecdote is appropriate. Russell is reputed to have been challenged to prove that the (false) hypothesis $2 + 2 = 5$ implied that he was the Pope. Russell replied as follows: "You admit $2 + 2 = 5$; but I can prove $2 + 2 = 4$; therefore $5 = 4$. Taking two away from both sides, we have $3 = 2$; taking one more, $2 = 1$. But you will admit that I and the Pope are two. Therefore, I and the Pope are one, q.e.d."

[11] K. Gödel, *Über unentscheidbare Sätze* ⋯, Monatsh. f. Math. u. Phys., 38 (1931), 173–98. The question remains whether there do not exist perfectly "valid" methods of proof, excluded by this particular logical system.

system, in which such undecidable propositions exist concerning ordinary integers! The existence proof itself is however non-constructive, and depends on admitting the existence of uncountably many "propositions," but only countably many "proofs."

Though no specific undecidable "genuinely mathematical" proposition is known, it is entirely possible that the Continuum Hypothesis (and the Axiom of Choice) are undecidable, in the following precise sense. There may exist one system of transfinite numbers, otherwise perfectly consistent with logic, in which the Continuum Hypothesis holds—and another system in which it fails.[12] In other words, ordinary logic may not be *categorical*—it may not determine the arithmetic of transfinite numbers up to isomorphism.

However, the author will venture the opinion that no logical system will be accepted as final which admits undecidable propositions.

7. Brouwerian logic; Lewis' strict implication. Motivated by such metaphysical considerations, a noteworthy algebra of logic has been developed, in which the identity $(x')' = x$ is denied, and replaced by the weaker inequality $(x')' \leqq x$. That is, $x \to (x')'$ is admitted, but $(x')' \to x$ denied. Namely, we have Heyting's formulation of intuitionist or Brouwerian logic,[13] which may be phrased as follows.

DEFINITION. *A Brouwerian logic is the dual of a relatively pseudo-complemented lattice.* (*See Ch.* IX, §12.)

In such a lattice, we denote the dual of $a * b$ by $a \to b$, and the relation of $x = 0$ (i.e., tautologies) by $\vdash x$. Since $x \to y$ is the least element t such that $x \smile t = y$, clearly $\vdash x \to y$ if and only if $x \geqq y$.

Using this relation, it is easy to derive Heyting's postulates, which are:

$$\vdash a \to (a \smile a),\ \vdash a \smile b \to b \smile a,\ \vdash (a \to b) \to (a \smile c \to b \smile c),$$

$$\vdash [(a \to b) \smile (b \to c)] \to (a \to c),\ \vdash b \to (a \to b),\ \vdash [a \smile (a \to b)] \to b,$$

$$\vdash a \to (a \frown b),\ \vdash a \frown b \to b \frown a,\ \vdash [(a \to c) \smile (b \to c)] \to (a \frown b \to c),$$

$$\vdash a^* \to (a \to b),\ \vdash [(a \to b) \smile (a \to b^*)] \to a^*.$$

It is a corollary that the system of closed subsets of any topological space (technically, T_0-space) may be regarded as a complete Brouwerian logic.[14]

---

[12] K. Gödel, Proc. Nat. Acad. Sci. 24 (1938), 556–7, and 25 (1939), 220–4; also K. Gödel, *The consistency of the Continuum Hypothesis*, Princeton, 1940.

[13] A. Heyting, *Die formalen Regeln der intuitionistischen Logik*, S. B. Preuss. Akad. Wiss. (1930), 42–56; also *Mathematische Grundlagenforschung, Intuitionismus, Beweistheorie*, Berlin, 1935. The lattice-theoretic interpretation is due to the author [LT, §§161–2], and has been extensively developed in McKinsey and Tarski [2]. See also A. Kolmogoroff, Mat. Sbornik 37 (1930), p. 39; Johánnson, Compositio Math. 4 (1936), p. 119; Tarski [3]; and S. Pankajam, Jour. Ind. Math. Soc. 5 (1941), 49–61; 6 (1942), 51–62, 102.

[14] See M. H. Stone [5]; A. Tarski, *Der Aussagenkalkül und die Topologie*, Fund. Math. 31 (1938), 103–34. An analogous relation for Lewis' implication is indicated by Tsao-Chen Tang, Bull. Am. Math. Soc. 44 (1938), p. 737.

Conversely, any *complete* atomistic Brouwerian logic would appear to be isomorphic with the system of all closed subsets of a suitable T_0-space.

By Glivenko's Thm. 16 of Ch. IX, one can also associate, with any Brouwerian logic, a Boolean logic.

Another interesting algebra of logic is furnished by Lewis' calculus of "strict implication," which may be defined as follows.[15]

In any Boolean algebra A, we may define $p \to q = p' \frown q$ as before (in words, p implies q "materially.") We define $p \prec q$ (in words, p implies q "strictly") to be O if $p \geqq q$ (i.e., if $p' \frown q = 0$), and I otherwise. Thus the elements $p \to q$ and $p \prec q$ are equivalent in a two-element Boolean algebra—but they are not equivalent in general, even though $p \prec q = 0$. We may also define $\Diamond p$ as the element $p \prec I$, and get an interesting algebraic system.

Ex. 1. Prove Heyting's postulates in detail.

Ex. 2. Prove that a complete lattice is a base for a Brouwerian logic if and only if it satisfies the following distributive law: $a \smile \bigwedge x_\alpha = \bigwedge (a \smile x_\alpha)$. [LT, Thm. 8.4.]

Ex. 3. Let T be any prime ideal of "true" propositions in a Brouwerian logic. What happens if one adjoins to T all x such that x^* is not in T? All x with $x^* = I$?

Ex. 4. Show that $(p \prec q) \smile (q \prec p)$ does not hold generally in Lewis' logic of strict implication.

Ex. 5. (a) Show that any Brouwerian logic which satisfies the identity $(x^*)^* = x$ is a Boolean algebra in which $x^* = x'$ and $x^*y = x' \frown y$.

(b) Show that the same is true if $x \frown x^* = 0$.

Ex. 6. (a) Show that any finite distributive lattice is a Brouwerian logic.

(b) Show by consideration of the lattices $1 \oplus 2^2$ and $1 \oplus 2^2 \oplus 1$, that the binary operations $\smile$ and $\to$ in a Brouwerian logic cannot, in general, be expressed as algebraic functions of $\frown$ and $*$[LT, p. 130].

Ex. 7. Let L be the modular lattice of all subspaces of Hilbert space, and let x^*y consist of all sums of a vector of y and a vector orthogonal to x. To what extent is the dual of this system analogous to Brouwerian logic?

Problem 87. Can one obtain a treatment of quantifiers in Lewis' system, by interpreting $\vdash \Diamond p$ appropriately?

8. Modal logic. Generally speaking, the Boole-Whitehead propositional calculus applies to *two-valued* deductive logic, in which every proposition is demonstrably true or demonstrably false. The alternative calculi discussed in §§5 and 7 can only be valid where other categories of propositions are admitted. Theories of logic which admit more than the two categories of "true" and "false" propositions constitute what is usually called "modal" logic, and the categories which they admit are called "modes" or "truth values."

Modal logic is very ancient. Thus Aristotelian logic recognized[16] four modes:

---

[15] C. I. Lewis and C. H. Langford, *Symbolic logic*, New York, 1932; see also E. V. Huntington, Bull. Am. Math. Soc. 40 (1934), 729–35; A. Tarski, Bull. Am. Math. Soc. 44 (1938), 737–44; K. Chandrasekharan, Math. Student 12 (1944), 14–24; J. C. C. McKinsey, Jour. Symbolic Logic 9 (1944), 42–45, 6 (1941), 117–34, and 9 (1944), 42–45. The remarks on this subject in [LT] are erroneous.

[16] A detailed discussion of several truth-value systems is given by Lewis and Langford, op. cit. supra, Ch. VII, see also the end of Gr. C. Moisil [1].

necessary, contingent, possible, impossible. Modern logic seems to stress th true, undecidable, and false. In the theory of probability, the scale of tr values runs through all numbers from zero to one.[17]

Interesting algebraic systems, describing propositional calculi with sim ordered sets of modes, have been proposed by Lukasiewicz and Tarski, and Post. I refer the reader to an extensive literature for their detailed discussio

Most systems of modes studied in the past have been simply ordered by degree of truth which they ascribe to propositions. All others known to me h formed distributive lattices and hence subdirect unions of two-valued log The author can see no valid reason for this emphasis on simple orderin It would seem worthwhile to construct propositional calculi based on non-tributive lattices of truth-values—say, on the two non-distributive lattices five elements. In my own attempts to do this, I have been troubled by problem as to how the truth-values of p and q should determine the tru values of $p \rightarrow q$ and p'.

We shall now turn our attention to the classical theory of probabilit which is by far the most important case.

9. Probability and measure. Everyone talks about probability, but nob can say what it is, to the satisfaction of others.[20] We shall follow the m influential mathematical school, and identify it with measure,[21] on a postulatio basis.

DEFINITION. *A probability algebra is a measure algebra* (Ch. X, §12) *in wh* $p[I] = 1$.

From any measure algebra with $m[I] \neq 0$, one can get a probability algebra setting $p[x] = m[x]/m[I]$. Hence the two theories are coextensive on the pur

---

[17] The author's opinion that probability may be regarded as a kind of modal logic shared by J. Venn, who wrote "the modals are the nearest counterpart to probability wh was afforded by the old systems of logic" (*The logic of chance*, London, 1888).

[18] For the Lukasiewicz-Tarski system, see J. Lukasiewicz and A. Tarski, *Mehrwerti Systeme der Aussagenkalkül*, C. R. de la Société des Sciences et Lettres de Varsovie 23 (1930), 1–21; also ibid., p. 51; O. Frink, Am. Math. Monthly 45 (1938), p. 212; Gr. C. Moi Ann. Sci. Univ. Jassy, Section I, 25 (1939), 341–84; 26 (1940), 431–66; 27 (1941), 86–98.] the Post system, see E. Post, Am. Jour. 43 (1921), 163–85; D. L. Webb, Proc. Nat. Ac Sci. 21 (1935), 252–4; P. C. Rosenbloom, *Post Algebras. I. Postulates and general theo* Am. Jour. 64 (1942), 167–88. For both, see S. B. Rosser and A. R. Turquette, Jour. Sy bolic Logic, 10 (1945), 61–82. See also Gr. C. Moisil, Disquis. Math. Phys. 1 (1941), 307-2 (1948), 3–98.

[19] J. M. Keynes, *A treatise on probabilities*, London, 1929, p. 39, has even suggested t the modes of probability form a partly ordered system. This view is shared by B. Koopman, *The axioms and algebra of intuitive probability*, Annals of Math. 41 (1940), 271–

[20] This philosophical uncertainty is well illustrated in Math. Reviews 7 (1946), pp. 1 93; also in J. M. Keynes, op. cit. supra.

[21] See A. Kolmogoroff, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin, 19 Ergebnisse series; H. Cramér, *Mathematical methods of statistics* Princeton, 1946. See a P. R. Halmos, Am. Math. Monthly 51 (1944), 493–510; K. Yawada, Jap. Jour. Math. 8 (194 887–92.

algebraic level. One can even give a direct identification, using "geometrical probabilities," by the following example.

Example 1. Let a circular disc of radius $1/2\pi$ be spun. For each subset S of the rim, let $p[S]$ be the probability that, when the disc comes to rest, the radius in a fixed (say, east) direction will cut the circumference at a point of S. Clearly $p[S]$ is simply the measure of S.

It may be objected that, owing to the limited accuracy of measurement, this experiment cannot be carried out physically. However, by the construction of Ch. X, §12, paragraph two, we can certainly realize any *finite* probability algebra in this way, arbitrarily closely. And the physical meaning of the infinite, on an empirical level, is extremely dubious. On a strictly empirical level, the most general example is perhaps the following.

Example 2. Let a repeatable experiment E have possible eventualities $h_1, \cdots, h_m$. Let A be the Boolean algebra of all attributes X definable by Boolean operations from the h_i. Finally let $p_n[X]$ denote the proportion of the first n trials of E having the attribute X. Then, for each n, $p_n[X]$ is a probability.

Now imagine the experiment repeated, in order, an infinite number of times. We may call the attribute X *statistically regular* if and only if, as $n \rightarrow \infty$, $p_n[X]$ approaches a numerical limit $p_\infty[X]$, called the *frequency* of X. Then one can show that, with respect to $p_\infty[X]$, the statistically regular attributes form a Boolean subalgebra, over which p_∞ is *finitely* additive. It need not, however, be countably additive,[22] in general.

The probability that a positive integer "chosen at random" will belong to a set S is quite similar. Let $p_n[S]$ denote the fraction of the first n integers belonging to S. Then the limit $p_\infty[S]$ of the $p_n[S]$ defines a finitely additive measure function. Using Cesaro means, one can greatly extend the class of measurable sets (cf. Ch. XI, Thm. 11). Is this a "probability"? That, in the author's opinion, is a matter of taste; but our definition excludes it.

We can identify the concept of probability as frequency with the concept of probability as measure in many cases. These resemble the following well-known example, due essentially to E. Borel.

Example 3. Let E consist of choosing one of the digits $0, \cdots, 9$ at random. Imagine this experiment repeated an infinite number of times.

We can write the result of this hypothetical infinite sequence of experiments as a single infinite decimal. Excluding the (infinitely improbable) decimals ending in an infinite sequence of 9's, we can therefore establish a one-one correspondence between sequences of experiments and points on the interval $0 \leqq x < 1$. Hence we can define a countably additive *measure* function $m[X]$ for these sequences of experiments.

[22] This is the foundation of probability according to the school of R. von Mises, *Probability, statistics, and truth*. These examples may explain why some writers omit the postulate of countable additivity. (E.g., E. Tornier, *Wahrscheinlichkeitsrechnung und allgemeine Integrationstheorie*, Leipzig, 1936.)

We shall now identify this measure with probability. By an "elementary statement" we mean a statement $S_{i,j}$ of the form: the ith repetition of E gave the value j. This corresponds to the set $X_{i,j}$ of experiments with ith digit equal to j; clearly $p[S_{i,j}] = 1/10$. Hence the finite or countable Boolean combinations of "elementary statements" correspond to the Borel subsets of the interval, and a unique "probability function" is definable for each such statement, equal to the measure of the corresponding subset of the interval.

By Thm. 15 of Ch. X, the preceding example is universal, for probability algebras generated by a finite or countable number of statements.

The algebra of probability also involves another operation, that of taking *weighted means*, as we may show by the following simple example.

Let a large square be subdivided into areas $a_1, \cdots, a_n$; and let P and Q denote the experiments of throwing a penny into the square from opposite sides. Let $p[a_i]$ and $g[a_i]$ be the probabilities that the penny will land in a_i under P and Q, respectively. Then any weighted mean $\lambda p + \mu g$ of p, g $[\lambda > 0, \mu = 1 - \lambda > 0]$ can be realized by the following experiment. A disc, divided into sectors of $2\pi\lambda$ and $2\pi\mu$ radians, is spun in a fixed horizontal plane, and a penny is then tossed into the square from side P or side Q, depending on which sector comes to rest opposite a fixed point.

The mathematical properties of this operation are discussed from a technical point of view in Ch. XV, §13; it plays a fundamental role in discussions of abstract Markoff processes and ergodic theory (Ch. XVI). We note here only that under it *the algebra of probability becomes a normed vector lattice.*

Ex. 1. Show that a probability algebra is either finite or uncountably infinite.

Ex. 2*. Let E be the experiment of turning a roulette wheel, as in Example 1. Let elementary statements be of the form "the ith trial of E gave a point in the measurable subset S." Using Daniell measure, prove the existence of a probability algebra generated by such elementary statements.

Ex. 3. Define the "direct sum" of measure algebras A and B, to consist of the direct union $A \times B$, where $m[a, b] = m[a] + m[b]$ for all $a \in A$, $b \in B$. Show that this is a measure algebra.

Ex. 4*. Define the "direct product" of two probability algebras of A and B as the set of all finite unions $\vee a_i \frown b_i$ where if $i \neq j$, either $a_j \frown a_i = 0$ or $b_i \frown b_j = 0$; define $p[\vee a_i \frown b_i] = \Sigma p[a_i]p[b_i]$.

(a) Show that, if equality is suitably defined, this is a probability algebra.

(b) Show that this is a special case of the concept of the direct product of rings, in the case of finite Boolean rings.

(c) Relate to "independent probabilities."

(d) Express the Law of Large Numbers abstractly, in terms of corresponding concept of "direct power."

Problem 88. Develop an algebra of probability for quantum mechanics, corresponding to the algebra of attributes of §5. We know that, for "orthogonal" closed subspaces, $p[S \frown T] + p[S \smile T] = p[S] + p[T]$. We need to characterize angles, and probability as a quadratic functional.

CHAPTER XIII

LATTICE-ORDERED SEMIGROUPS

1. Definition; ideal-theoretic interpretation. The concept of a lattice-ordered semigroup, or l-semigroup, arose naturally in ideal theory.[1] The following classical example is especially instructive.

Example 1. Let F be the normal extension field formed by adjoining to the rational numbers the roots of a polynomial equation; let E be the subring of all algebraic *integers* of F. A Dedekind *ideal* of F is a non-void subset H of F such that if $a, b \in H$ and $r \in E$, then $a \pm b \in H$ and $ra \in H$.

Since this is a closure property, the ideals of F form a complete lattice under set-inclusion. If H and K are two ideals, then $H \frown K$ is their intersection (which is never void, since zero is in every ideal), and the set of all sums $x + y$ $[x \in H, y \in K]$ is the join $H \smile K$ of H and K. The *product* HK of H and K is defined as the smallest ideal containing all products xy $[x \in H, y \in K]$.

With respect to these three operations, the Dedekind ideals of F satisfy all the conditions which are about to be defined abstractly.

Definition. *By a multiplicative lattice, or m-lattice, we mean a lattice L with a binary multiplication satisfying*

(1) $$a(b \smile c) = ab \smile ac \text{ and } (a \smile b)c = ac \smile bc.$$

A zero of an m-lattice L is an element 0 satisfying

(2) $$0 \frown x = 0x = x0 = 0 \text{ for all } x \in L.$$

A unity of L is an element e satisfying

(3) $$ex = xe = x \text{ for all } x \in L.$$

An infinity of L is an element I satisfying

(4) $$I \smile x = Ix = xI = I \text{ for all } x \in L.$$

L is called commutative or associative if

(5) $$xy = yx, \text{ or } \qquad (6) \quad x(yz) = (xy)z$$

for all $x, y, z \in L$. If L is conditionally complete and satisfies the unrestricted distributive laws

(1′) $$a \bigvee b_\alpha = \bigvee (ab_\alpha) \text{ and } (\bigvee a_\alpha)b = \bigvee (a_\alpha b),$$

[1] R. Dedekind, Ges. Werke, vol. III, pp. 62–71. The further development is due largely to Ward and Dilworth [1], Dilworth [1], and J. Certaine [1]; see also G. Birkhoff [6, §27]; Ward, Annals of Math. 39 (1938), 558–68; and Ward and Dilworth, ibid. 40 (1939), 328–38 and 600–8.

it is called a complete m-lattice, or cm-lattice. An associative m-lattice with unity is called a lattice-ordered semigroup, or l-semigroup; if complete, it is called a cl-semigroup.

It is easily verified that, in Example 1, the Dedekind ideals form a commutative cl-semigroup with zero. Thus (1′) follows because $\bigvee K_\alpha$ is the set-union of the finite ideal unions of the K_α ; the ideal consisting of the number 0 alone satisfies (2).

THEOREM 1. *In any m-lattice we have*[2]

$$a \leqq b \quad \textit{implies} \quad xa \leqq xb \quad \textit{and} \quad ay \leqq by \quad \textit{for all} \quad x, y, \tag{7}$$

$$(a \frown b)(a \smile b) \leqq ba \smile ab \textit{ for all } a, b. \tag{8}$$

If the m-lattice has a unity e, then

$$a \smile b = e \textit{ implies } a \frown b = ba \smile ab, \textit{ and} \tag{9}$$

$$a \smile b = a \smile c = e \textit{ implies } a \smile bc = a \smile (b \frown c) = e. \tag{10}$$

If it has an element $z \leqq e$ satisfying $zx = xz = z$ for all x, then this z is a zero.

Proof: Ad (7): $a \leqq b$ implies $by = (a \smile b)y = ay \smile by$.
Ad (8): $(a \frown b)(a \smile b) = (a \frown b)a \smile (a \frown b)b \leqq ba \smile ab$, by (7).
Ad (9): if $a \smile b = e$, then, by (8), $a \frown b \leqq ba \smile ab$. But by (7), $ba \leqq ea = a$, $ba \leqq b$, $ab \leqq a$, $ab \leqq b$; hence $ba \smile ab \leqq a \frown b$, proving (9).
Ad (10): clearly $e \geqq a, b, c$, whence $a \smile bc \geqq a \geqq aa, ba, ac$. Hence

$$e = e \smile ee \geqq a \smile bc \geqq aa \smile ba \smile ac \smile bc = (a \smile b)(a \smile c) = ee = e.$$

Again, since $b \geqq bc$, $c \geqq bc$, we have $b \frown c \geqq bc$, so that $a \smile (b \frown c) \geqq a \smile bc = e$, proving (10). The final assertion follows immediately since, for all $x \in L$, $z = zx \leqq ex = x$, whence $z = z \frown x = x \frown z$.

DEFINITION. *Let G be any m-lattice. We define the right-residual $h{:}k$ of h by k as the largest x (if it exists) satisfying $xk \leqq h$; the left-residual $h{::}k$ of h by k is the largest y satisfying $ky \leqq h$. An m-lattice in which such residuals always exist is called a residuated lattice.*

The m-lattice of Example 1 is residuated; $H{:}K$ is the set of all $x \in F$ such that $xk \in H$ for all $k \in K$. This is an ideal, since $(x \pm y)k = kx \pm ky$ and $(rx)k = r(xk)$ $[r \in E]$.

This somewhat modifies the terminology of Ward-Dilworth [1], in which a residuated lattice was defined as a commutative l-semigroup in which $e \geqq x$ for all x. This last assumption corresponds to the usual distinction in ideal theory between *integral* ideals $K \leqq E$ of F, and *fractional* ideals not so contained. The integral Dedekind ideals of F are the ordinary ideals of E in the usual modern sense.[3]

[2] Formulas (7)–(10) are in Certaine [1, p. 39]; they generalize somewhat earlier results of Dedekind, Ward, and Dilworth.

[3] See van der Waerden [1], Albert [1], or Birkhoff-MacLane.

DEFINITION. *The elements $x \leqq e$ of an m-lattice will be called integral. If every element is contained in e, the m-lattice will be called integral.*

We shall now show that the integral ideals in Example 1 form an integral residuated lattice. More generally, we have

THEOREM 2. *In any cm-lattice, $h:k$ exists if some x satisfies $xk \leqq h$.*

Proof. Let u be the join of all x_α such that $x_\alpha k \leqq h$. Then $uk = (\bigvee x_\alpha)k = \bigvee (x_\alpha k) \leqq h$.

COROLLARY 1. *The integral elements of any cm-lattice form an "integral" residuated lattice.*

COROLLARY 2. *Any cm-lattice with zero is residuated.*

Proof. $0k = 0 \leqq h$ for all h, k.

We quote without proof the following result (Dedekind, loc. cit.; Dilworth [1, p. 428], Certaine [1, pp. 67–8] all contributed).

THEOREM 3. *In any residuated lattice, we have*
(i) $(\bigwedge a_\alpha):b = \bigwedge (a_\alpha:b)$ *and symmetrically,*
(ii) $a:(\bigvee b_\beta) = \bigwedge (a:b_\beta)$ *and symmetrically,*
(iii) $a \geqq cb$, $a:b \geqq c$, *and* $a::c \geqq b$ *are equivalent,*
(iv) $(ab):b \geqq a$ *and* $(ba)::b \geqq a$.

If multiplication is associative, then also

(v) $(a::b):c = (a:c)::b$ *is the largest x with $bxc \leqq a$,*
(vi) $(a:(bc)) = (a:c):b$ *and symmetrically.*

In (i)–(ii), the existence of the left-hand side implies that of the right-hand side.

Note that although l-semigroups satisfy a principle of left-right symmetry, the Duality Principle does not apply to them.

Ex. 1. Let G be the lattice **2** with elements $0, I$, multiplication being defined by $00 = 0$, $0I = I0 = II = I$. Show that G is a cl-semigroup.

Ex. 2. Show that if (1′) is assumed for the void set of K_α, then the lattice O is a multiplicative zero.

Ex. 3. Show that the "positive" elements $x \geqq e$ of an l-semigroup form an l-semigroup in which *no* residuals except $x:e = x$ exist. (J. Certaine)

Ex. 4. Show that, for any $a < e$ of an l-semigroup, the x satisfying $a \cup x = e$ form an l-semigroup.

Ex. 5. Show that, for any fixed element a of a residuated lattice, the correspondence $x \to a:x$ is a Galois correspondence in the lattice of all elements satisfying $x = a:(a:x)$.

Ex. 6. Show that the non-negative rational integers $0, 1, 2, \cdots$ form a residuated lattice, if $\leqq$ has its usual meaning and $m + n$ is taken as the "product" of m and n.

Ex. 7. Show that the positive integers form a residuated lattice, if multiplication is ordinary multiplication, and (lattice-theoretically) $m \leqq n$ means "m is a divisor of n."

Ex. 8. Show that the ideals $K > 0$ in the rational field form a cl-semigroup, in which, if H denotes the ideal of all fractions whose denominators are powers of a fixed prime p, $E:H$ does not exist.

Ex. 9. Let G be any commutative cl-semigroup. Show that the largest residuated lattice contained in G consists of all $a \in G$ such that $xa \leqq e$ for some $x \in G$.

Ex. 10*. Construct an l-semigroup of ten or fewer elements in which $a \smile b = e$, yet $ab \neq ba$. (Certaine)

Ex. 11*. Construct a commutative l-semigroup of five elements in which $ab \neq (a \frown b)(a \smile b)$. (Certaine)

2. Related interpretations. We can enormously generalize Example 1 in the following way.

Example 2. Let R be any system with a binary multiplication xy, and possibly other binary operations $x + y, x - y, \cdots$, with respect to which multiplication is distributive, so that $a(b \pm c) = ab \pm ac$, $(a \pm b)c = ac \pm bc$. For lack of a better word, we shall call such a system a *ringoid*; ordinary rings and distributive lattices are included as very special cases. As in the case of rings, we define a *module* of R to be a subset H such that $a, b \in H$ imply $a \pm b \in H$; as in the cases of rings and distributive lattices, we define an *ideal* to be a module H such that $a \in H$ implies $xa \in H$ and $ay \in H$ for all $x, y \in R$.

THEOREM 4. *The modules of any ringoid R form a residuated cm-lattice, in which the ideals form a residuated cm-sublattice.*

Proof. Since being a module is a closure property, the modules of R form a complete lattice, in which meets are set-products. Again, the join $K \smile L$ of two modules consists of all combinations by $\pm$ such as $[(y_1 - z_1) + (y_2 - z_2)] - y_3$, etc., of $y_i \in K$ and $z_i \in L$. We define the *product* HK of two modules as the module generated by products xy $[x \in H, y \in K]$. Clearly $HK \leqq H(K \smile L)$ and $HL \leqq H(K \smile L)$; hence $HK \smile HL \leqq H(K \smile L)$. But conversely, $H(K \smile L)$ is generated by combinations of the form

$$x\{[(y_1 - z_1) + (y_2 - z_2)] - y_3\} = [(xy_1 - xz_1) + (xy_2 - xz_2)] - xy_3$$

in $HK \smile HL$; hence $H(K \smile L) \leqq HK \smile HL$. By symmetry, we get (1). From this (1′) follows since $\bigvee K_\alpha$ is the set-union of finite joins of K_α; hence the modules are a *cm*-lattice. In this *cm*-lattice, the void set is a zero; hence by Cor. 2 of Thm. 2, the *cm*-lattice is residuated.

In this *cm*-lattice, any join or meet of modules which are ideals is itself an ideal. This is trivial for meets (= set-products); for joins, it follows from the identity displayed above. Using this fact, the proofs of (1)–(1′) given above for module products apply equally to ideal products, if the ideal product of two ideals H and K is the ideal generated by products xy $[x \in H, y \in K]$. (If multiplication is associative, this is also the module product defined above.)

If R has no operations except multiplication, the "modules" form the Boolean algebra of all subsets ("complexes") of a system with binary multiplication, under Kronecker multiplication of complexes. In the case of groups and loops, the non-void subsets form a *cm*-lattice, which is not, however, usually residuated.

If R is a ring, the non-void modules and ideals form *residuated cm-lattices with zero* consisting of the ring-zero. The same remark applies to the subalgebras and invariant subalgebras of any linear algebra. In these cases, if multiplication is associative, right-residuals are left-ideals and left-residuals are right-ideals.

If R is a distributive lattice, we infer that the ideals form a residuated *cm*-lattice. Moreover in this case, as in the case of rings with unity, R is a unity for the *cm*-lattice—which is therefore an *integral* residuated *cm*-lattice with zero (M. Ward, Duke Jour. 3 (1937), 627–36).

But we already know that the ideals of any distributive lattice form a relatively pseudo-complemented distributive lattice. We can generalize this result as follows; we omit the proof.

THEOREM 5. *A lattice is an m-lattice when xy is defined as $x \frown y$, if and only if it is distributive. It is a residuated lattice if and only if it is relatively pseudo-complemented.*

COROLLARY. *A Brouwerian logic may be defined as the dual of a lattice with O, I, which is residuated under lattice meets.*

This result gives a remarkable connection between ideal theory, topology (the algebra of open sets), and mathematical logic.[4]

Again, it is well-known that multiplication in Lie algebras is analogous to the operation of forming the commutator $[a, b] = a^{-1}b^{-1}ab$ in groups. This can be based on the following analog of Thm. 4.

Example 3. Let L be the lattice of all non-void normal subgroups of any group G; define $[M, N]$ as the subgroup generated by all commutators $x^{-1}y^{-1}xy$ $[x \in M, y \in N]$. Then L is a commutative residuated *cm*-lattice with zero 1 (the group identity).

Proof. Since $[M, N]$ is invariant under all inner automorphisms, it is normal. Since $y^{-1}x^{-1}yx = y^{-1}(x^{-1}(y^{-1})^{-1}xy^{-1})y$, $[M, N] = [N, M]$. Since

$$x^{-1}(yz)^{-1}x(yz) = (x^{-1}z^{-1}xz)z^{-1}(x^{-1}y^{-1}xy)z,$$

we have $[L, M \smile N] = [L, M] \smile [L, N]$. By symmetry, we have (1), from which (1′) follows as in Thm. 4. The rest of the proof is trivial.

The concepts of nilpotent rings, "hypercentral" groups, etc., extend to any residuated lattice L with zero 0 and I; for simplicity, we restrict ourselves to the commutative case. We define $I^r = I$, $I^{n+1} = II^n$ recursively, ${}^0I = 0$, and ${}^{n+1}I = ({}^nI):I$ recursively. We shall say that L is *nilpotent* if some $I^n = 0$; in this case L contains a "nilpotent" chain of the form

$$(*)\qquad I = a_0 > a_1 > a_2 > \cdots > a_r = 0, \text{ with } a_iI = a_{i+1}.$$

But for any such chain, we can easily prove by (7) and induction, that $I^{i+1} \leqq a_i \leqq {}^{r-i}I$. It follows that $I^{r+1} = 0$ and ${}^rI = I$. Hence if we call the sequence

$$I > I^2 > I^3 > \cdots > I^n = 0$$

[4] It is due to G. Birkhoff [6, Thm. 46], and J. Certaine [1, Thm. 9.5].

the *lower* central series of L, and the dual sequence

$$^0I < {}^1I < {}^2I < \cdots < {}^mI = I$$

the *upper* central series of L, we have $n \leqq r + 1$ and $m \leqq r$. Hence both $n - 1$ and m are equal to the length r of the shortest nilpotent chain. We conclude

THEOREM 6. *In any nilpotent residuated lattice, the upper and lower central series have the same length r. If $I = a_0 > a_1 > \cdots > a_r$ is any nilpotent chain, then*

$$I^{i+1} \leqq a_i \leqq {}^{r-i}I \textit{ for all } i. \tag{11}$$

For the further theory of commutation, the reader is referred to H. Zassenhaus, *Gruppentheorie*, pp. 43–4, 105–7, and 119; also P. Hall, Proc. Lond. Math. Soc. 36 (1933), 29–95, and Ex. 1 below.[5]

Ex. 1. Prove that Example 3 satisfies the identity
$[L, [M, N]] \leqq [[L, M], N] \smile [[L, N], M]$ of P. Hall.

Ex. 2. Prove that if $C' = II$ and $C^{m+1} = C^mC^m$, then
$C^m = 0$ implies $I^{2^m} = 0$. (P. Hall)

Ex. 3. Show that if, in a ringoid, $0a = a0 = 0$ for all a, then $0 \pm 0 = 0$.

Ex. 4. Show that Example 2 includes the case of "multiplicative ideals" in the sense of ideal theory.

Ex. 5. Extend Thm. 4 to S-modules, or modules H which, for some subset S of R, contain all products sx and xs [$x \in H, s \in S$].

Problem 89. Develop an analog of Theorem 6 applicable to the case of transfinite r.

Problem 90. Develop an analog of Theorem 6 for the non-commutative, non-associative case.

3. Integral m-lattices. We have seen that the ideals of any ring E with unity 1 form an integral m-lattice with unity $e = E$ and zero 0. In any such lattice, one can prove some properties of relatively prime or "coprime" ideals, familiar in the theory of commutative rings.

DEFINITION. *A maximal element of an integral m-lattice L is an element covered by e; a prime element is an element p such that $xy \leqq p$ implies $x \leqq p$ or $y \leqq p$. Two elements $a, b \in L$ are coprime if $a \smile b = e$.*

LEMMA 1. *If a, b are coprime, then*

$$x = xa \smile xb = (x \frown a) \smile (x \frown b) \textit{ for all } x. \tag{12}$$

Proof. We begin by noting that, since $xy \leqq xe = x$ and $xy \leqq ey = y$, we have

$$xy \leqq x \frown y, \text{ for all } x, y. \tag{13}$$

[5] A somewhat analogous treatment of the Jordan-Hölder Theorems has been given by R. J. Duffin and R. S. Pate, Duke Jour. 10 (1943), 743–50.

We then infer (12) from the sequence of inequalities

$$x = xe = x(a \smile b) = xa \smile xb \leqq (x \frown a) \smile (x \frown b) \leqq x.$$

LEMMA 2. *If a, b are coprime and $a \frown b \leqq x$, then*

$$x = (x \smile a) \frown (x \smile b) = (x \frown a) \smile (x \frown b). \tag{14}$$

Proof. In any lattice, $(x \frown a) \smile (x \frown b) \leqq x \leqq (x \smile a) \frown (x \smile b)$. Under the present hypotheses, by (12) and (1),

$$\begin{aligned}(x \smile a) \frown (x \smile b) &= a[(x \smile a) \frown (x \smile b)] \smile b[(x \smile a) \frown (x \smile b)]\\ &\leqq a(x \smile b) \smile b(x \smile a) = (ax \smile ab) \smile (bx \smile ba).\end{aligned}$$

Again, since $ax \leqq a \frown x$ and $ab \leqq a \frown b = a \frown (a \frown b) \leqq a \frown x$, $ax \smile ab \leqq a \frown x$. Similarly, $bx \smile ba \leqq b \frown x$. Substituting, $(x \smile a) \frown (x \smile b) \leqq (a \frown x) \smile (b \frown x)$, completing the proof.

THEOREM 7. *If a, b are coprime, then the interval $[a \frown b, e]$ is lattice-isomorphic with the cardinal product $[a, e] \times [b, e]$.*

Proof. Given $a \frown b \leqq x \leqq e$, define $t = x \smile a$ and $u = x \smile b$; clearly $t \in [a, e]$ and $u \in [b, e]$. Conversely, given $t \in [a, e]$ and $u \in [b, e]$, form $\phi(t, u) = t \frown u$; these are single-valued correspondences from $[a \frown b, e]$ to $[a, e] \times [b, e]$ and conversely. By Lemma 2, $\phi(x \smile a, x \smile b) = x$; conversely, since $a \leqq t$,

$$t \leqq (t \frown u) \smile a \leqq (t \smile a) \frown (u \smile a) = t \smile a \text{ (since } u \smile a = e) = t;$$

similarly, $u = (t \frown u) \smile b$; hence the correspondences are inverse. But they are obviouly isotone; hence they are both isomorphisms.

THEOREM 8. *Every complemented integral m-lattice L is a Boolean algebra, with $xy = x \frown y$.*

Proof.[6] Let $a \in L$ be arbitrary, and a' any complement of a. Then by Thm. 7, a and a' are in the center of L; hence L is a Boolean algebra. Further, by (12) and distributivity,

$$x \frown a = (xa \smile xa') \frown (xa \smile x'a) = xa \smile (x \frown x')a \smile x(a' \frown a) \smile (xa' \frown x'a).$$

All terms but the first are 0, whence $x \frown a = xa$, q.e.d.

We now assume the ascending chain condition.[7] With each maximal element m_i of L we associate the set M_i of all *einartig* elements satisfying $x \smile m_j = e$ for all maximal m_j except possibly m_i. Since every $x < e$ is contained in at

[6] Ward-Dilworth [1, Thm. 7.31]; Certaine [1, Thm. 10.5].

[7] This holds in algebraic number theory and with polynomial ideals, together with the commutative and associative laws of multiplication. Incidentally, the ideals of any ring form a modular lattice. But no important consequences of these additional conditions are known. They have been studied by H. Grell, Math. Annalen 97 (1927), 490–523; W. Krull, Math. Zeits. 28 (1928), 481–503; W. Krull, *Idealtheorie*, Ergebnisse series, Berlin, 1935.

least one maximal element, by the chain condition, each M_i consists of e and all x contained in m_i and no *other* maximal element.

In the case of algebraic number theory, the maximal ideals are the prime ideals, and the einartig ideals are the prime-power ideals. Indeed, in any integral m-lattice, every maximal element m is prime, since $xy \leqq m$ and $x \nleqq m$ imply $x \smile m = e$, whence $y = ey = (x \smile m)y = xy \smile my \leqq m$.

Hence the following result may be regarded as a partial generalization of the Fundamental Theorem of Ideal Theory.

THEOREM 9. *Let L be any integral m-lattice satisfying the ascending chain condition. The sublattice S generated by the sets M_i of einartig elements is the cardinal product $M_1 \times M_2 \times M_3 \times \cdots$ of the M_i.*

Proof.[8] By (10), each M_i is an interval sublattice (dual ideal) closed under multiplication. Again, if $x \in M_i$ and $y \in M_j$ $[i \neq j]$, then $x \smile y$ is not contained in any maximal element, and so $x \smile y = e$. The same remark holds, by (10), if $x = x_1 \frown \cdots \frown x_n$ $[x_i \in M_i]$ and $y \in M_{n+1}$. Hence, by Thm. 7 and induction, the interval sublattice generated by the M_i is their cardinal product. In the presence of the ascending chain condition, we can extend this result to an infinite number of factors, provided all but a finite number of "components" are e.

Caution. Though the M_i are closed under multiplication, their cardinal product need not be.

Ex. 1. Show that any m-lattice which satisfies the ascending chain condition is a residuated cm-lattice.

Ex. 2. (a) Show that any lattice with O and I becomes a residuated cm-lattice if we define $xy = O$, $x{:}y = I$.

(b) Show that if we adjoin an $e > I$, we get an integral, residuated cm-lattice (Ward-Dilworth).

(c) Show that any isotone multiplication in a chain defines an m-lattice.

(d) Show that O, 1, ∞ form an m-lattice under multiplication, whether the "indeterminate" product $0\infty = \infty 0$ is defined as 0, 1, or ∞!

Ex. 3. Show that, in a residuated integral m-lattice, p is prime if and only if $p{:}x > p$ implies $x \leqq p$.

Ex. 4*. Show that the free modular lattice with three generators cannot be made into an integral m-lattice. (Ward-Dilworth)

Ex. 5*. Show that the following conditions on an integral m-lattice are equivalent and imply distributivity: (i) $(a{:}b) \smile (b{:}a) = e$, (ii) $a{:}(b \frown c) = (a \smile b) \smile (a \smile c)$, (iii) $(b \smile c){:}a = (b{:}a) \smile (c{:}a)$.

Ex. 6*. Let s be any ideal in an integral m-lattice satisfying the ascending chain condition. Define the *radical* of s as the join r of all x such that $x^n \leqq s$ for some $n = n(x)$.

(a) Show that $r^n \leqq s$ for some n.

(b) Show that if s is *primary*, in the sense that $ab \leqq s$ and $a \nleqq s$ imply $b^n \leqq s$ for some n, then r is a prime ideal.

Ex. 7. Give a short direct proof of Thm. 8, based on Newman's Thm. 4, Ch. X.

Ex. 8*. Show that if $1{:}(1{:}x) = x$ and $1{:}(xy) = (1{:}x)(1{:}y)$ in an integral residuated m-lattice L, then L is a commutative l-group. (Certaine)

---

[8] See G. Birkhoff, Bull. Am. Math. Soc. 40 (1934), 613–19; Ward-Dilworth [1, Thm. 8.3].

Problem 91. Develop a theory of subdirectly irreducible integral m-lattices.

Problem 92. Develop a theory of m-lattices in which also $a(x \frown y) = ax \frown ay$ and $(x \frown y)a = xa \frown ya$.

4. Isotone, semicontinuous, and subharmonic functions. Consider the class N of all real functions $f(x)$ of a real variable x, such that $x \geqq y$ implies $f(x) \geqq f(y)$. Such functions may be called *isotone* or *non-decreasing*. If we define $f \geqq g$ to mean $f(x) \geqq g(x)$ for all x, then we get the lattice R^R (Ch. I, §7), where R is the real number system. We can make $N = R^R$ into an m-lattice in either of two ways.

We can let fg denote the *composite* function $g(f(x))$, giving an associative, non-commutative multiplication. Then $fg \smile fh$ and $f(g \smile h)$ both assign to each x the larger of $g(f(x))$ and $h(f(x))$; and $fh \smile gh$ and $(f \smile g)h$ both assign the larger of $h(f(x))$ and $h(g(x))$; hence we define an m-lattice.

This construction gives an m-lattice C^C from any chain C. Note that, with chains, an isotone function is the same as a join-endomorphism. It is this class of operators which gives an m-lattice in the general case.

Example 4. The join-endomorphisms of any lattice L form an l-semigroup M.

Indeed, we have $x(\theta \smile \theta_1) = x\theta \smile x\theta_1$, which is a join-homomorphism since

$$(x \smile y)(\theta \smile \theta_1) = (x \smile y)\theta \smile (x \smile y)\theta_1 = x\theta \smile y\theta \smile x\theta_1 \smile y\theta$$

$$= x(\theta \smile \theta_1) \smile y(\theta \smile \theta_1).$$

Multiplication is usual endomorphism multiplication. Thus

$$x(\theta \smile \theta_1)\theta_2 = (x\theta \smile x\theta_1)\theta_2 = x\theta\theta_2 \smile x\theta_1\theta_2 = x(\theta\theta_2 \smile \theta_1\theta_2),$$

$$x\theta(\theta_1 \smile \theta_2) = x\theta\theta_1 \smile x\theta\theta_2 = x(\theta\theta_1 \smile \theta\theta_2).$$

This completes the proof.

We can also let our auxiliary operation consist of forming the *sum* $h = f + g$ of two functions defined by $h(x) = f(x) + g(x)$ for all x. The class of all isotone real functions is closed under addition and join. The fact that it forms an l-semi-group is therefore a corollary of the following principle.

Example 5. Let G be any complete l-group; we write the group operation $+$ and the identity as 0. Let S be any subset of G which contains 0, which contains $x + y$ if it contains x and y, and which contains $\bigvee x_\alpha$ whenever all x_α exist and have an upper bound. Then S is a complete l-semigroup.

Indeed, (1)–(1′) hold in any l-group (Ch. XIV, §10). The rest of the proof is obvious.

For the same reason, the class of all *upper semicontinuous* real functions forms a complete commutative l-semigroup, if the group operation is taken as addition. So does the class of all *subharmonic* functions of one, two, or more variables. So, incidentally, does the class of all nowhere positive subharmonic functions, etc., etc.

In the case of subharmonic functions, the residual $0:a$ has an interesting interpretation. It is the join of all subharmonic functions having the same boundary values as the superharmonic function $-a$; hence it is *harmonic.* Generally, harmonic functions are subharmonic functions h with additive subharmonic inverses, and all $h:a$ are also harmonic (have inverses).

Ex. 1. Prove that the join-endomorphisms of any chain form a distributive lattice.

Problem 93. Is the lattice of all join-endomorphisms of an arbitrary lattice semi-modular?

5. Algebra of relations. Let Γ be any class of elements $\alpha, \beta, \gamma, \cdots$. By a binary (or dyadic) *relation* on Γ is meant any rule r which says, of each ordered pair (α, β) of elements of Γ, that either the relation r holds between α and β (in symbols, $\alpha r \beta$), or that it does not hold (in symbols, $\alpha r' \beta$).

If Γ consists of n elements $\alpha_1, \cdots, \alpha_n$, one can establish a one-one representation of relations r on Γ by "relation matrices" $\| r_{ij} \|$ of zeros and ones. This is defined by

$$(15) \qquad r_{ij} = \begin{cases} 1 & \text{if} \quad \alpha_i r \alpha_j \\ 0 & \text{if} \quad \alpha_i r' \alpha_j \quad \text{(i.e., otherwise).} \end{cases}$$

Thus the *equality* relation e corresponds to the identity matrix, $e_{ii} = 1$ and $e_{ij} = 0$ if $i \neq j$. The *null* relation O corresponds to the zero matrix, $O_{ij} = 0$ for all i, j; the *universal* relation I to the matrix $I_{ij} = 1$ for all i, j.

We define $r \leqq s$, corresponding to the logical concept "r implies s," as follows

$$(16) \qquad r \leqq s \text{ means that } \alpha r \beta \text{ implies } \alpha s \beta.$$

Thus in the finite case, it means $r_{ij} \leqq s_{ij}$ for all i, j. Using the relation matrix representation (which is easily extended to the infinite case), one sees

LEMMA 1. *Under inclusion, the relations on a fixed class Γ of $\aleph$ elements form the atomic Boolean algebra $2^{\aleph^2}$. We can therefore define $r \frown s$, $r \smile s$, and r' as usual. Thus r' has the meaning of paragraph one, and $\alpha(r \smile s)\beta$ means either $\alpha r \beta$ or $\alpha s \beta$. Again, a relation r is reflexive if and only if $r \geqq e$.*

Besides these Boolean operations, we have the fundamental operation of (relative) *multiplication* of relations, defined by

$$(17) \qquad \alpha(rs)\beta \quad \text{means} \quad \alpha r \gamma \quad \text{and} \quad \gamma s \beta \quad \text{for some} \quad \gamma \in \Gamma.$$

Thus a relation r is *transitive* if and only if $r^2 \leqq r$. It is a one-one transformation if and only if $rx = xr = e$ for a suitable "inverse" x; moreover in the case of transformations (one-one or not), (17) reduces to the usual definition of transformation multiplication.[8]

[8] This is why I have adopted the terminology of multiplication and products, instead of the older terminology of relative multiplication and relative products. I have also abandoned the older notation $(r;s)$ in favor of the more compact notation rs.

I shall now list some fundamental laws of the algebra of relations,[10] which supplement the Boolean identities already covered in Lemma 1.

THEOREM 10. *The relations on Γ form a Boolean cl-semigroup $R(\Gamma)$ with zero* 0, *identity e, and largest element I, under inclusion and multiplication. Moreover*

$$rs \leqq e' \text{ implies } sr \leqq e', \tag{17}$$

$$e':(e':r) = r \quad \text{for all} \quad r, \tag{18}$$

$$e':(rs)' = (e':s')(e':r'), \tag{19}$$

$$\text{if } r > 0, \text{ then } I\, r\, I = I. \tag{20}$$

Proof. All statements except (17)–(20) are obvious. It is a corollary that *all identities of Thm.* 1 *and Thm.* 3 *apply to the algebra of relations.* We now prove (17)–(20).

If $rs \leqq e'$, then $r_{ik}s_{ki} = 0$ for all i, k; this means that $r_{ik} = 1$ implies $s_{ki} = 0$. This implies $s_{ki}r_{ik} = 0 = (sr)_{kk} = 0$ for all k, i, whence $sr \leqq e'$, proving (17).

Further, if we set $s_{ki} = 0$ when $r_{ik} = 1$, and 1 otherwise, $sr \leqq e'$; hence the largest $s = e':r$ satisfying $sr \leqq e'$ is obtained from r by transposing subscripts and interchanging zeros and ones. If we do this twice, we obviously get r, proving (18). We postpone the proof of (19), but prove (20) by noting that if $r > 0$, then some $r_{ij} = 1$, whence every $(IrI)_{hk} \geqq I_{hi}r_{ij}I_{jk} = 1$.

Law (18) is closely related to the properties of the *converse* $\breve{r}$ of a relation r, usually defined by

$$\alpha\, \breve{r}\, \beta \quad \text{if and only if} \quad \beta\, r\, \alpha. \tag{21*}$$

Since $e':r$ is obtainable from r by permuting subscripts and interchanging zeros and ones, we have

$$\breve{r} = e':r'. \tag{21}$$

Hence we do not need to treat conversion as an undefined operation, though it is usually so treated. We now obtain (19) as another way of writing

$$\breve{rs} = \breve{s}\breve{r}, \tag{19'}$$

whose proof is trivial. This proves Theorem 10; we define a *relation algebra* as any system satisfying the conditions of Thm. 10.

In any residuated lattice, for any fixed element a, the correspondence $r \to a:r$ inverts inclusion. By (18), the correspondence $r \to e':r$ is its own inverse, and so one-one; hence it is a dual automorphism. Hence

$$\breve{r} = e':r' = (e':r)'. \tag{22}$$

---

[10] See C. S. Peirce, Mem. Am. Acad. Arts. Sci. 9 (1870), 317–78; E. Schroder [1, vol. III]; J. C. C. McKinsey, Jour. Symbolic Logic 5 (1940), 85–97; A. Tarski, ibid. 6 (1941), 73–89.

Further, $r \to \breve{r}$ is the product of two dual automorphisms, and so a lattice-automorphism, giving

$$(23)\qquad \overbrace{r \frown s} = \breve{r} \frown \breve{s}, \qquad \overbrace{r \smile s} = \breve{r} \smile \breve{s}, \qquad \breve{r}' = \overbrace{(r')}.$$

This is obvious from (21*), but we have preferred to prove the result as a corollary of Theorem 10, from (18).

We shall now discuss the implications of (17). It obviously implies $e':r = e'::r$—that the residual $e':r$ is left-right symmetric. It also implies

$$(24)\qquad \text{If } (r_1r_2 \cdots r_{n-1})r_n \leqq e', \text{ then } r_n(r_1r_2 \cdots r_{n-1}) \leqq e';$$

in other words, *the n-ary relation $r_1r_2 \cdots r_n \leqq e'$ is invariant under cyclic permutations.*

Ex. 1. (a) Show that a relation is symmetric if and only if $r = \breve{r}$, and transitive if and only if $r^2 \leqq r$.

(b) Show that a partial ordering may be defined as a relation p satisfying $p \frown \breve{p} = e$ and $p^2 = p$.

(c) What do $p \frown \breve{p} = 0$ and $p^2 \leqq p$ imply (cf. Chap. I, §1, Ex. 1)? What about $p \frown \breve{p} = 0$ and $p^2 = p$?

(d) What do $a^2 = a = \breve{a}$ and $a \geqq e$ signify?.

Ex. 2. (a) Show that, for all r, $r\breve{r}$ is symmetric.

(b) Show that $\breve{r} = r'$ is strictly impossible.

In Exs. 3–5, base your conclusions on Thm. 10 alone.

Ex. 3. Prove that, if $ax = xa = e$ for some x, then $x = \breve{a}$, so that $a\breve{a} = \breve{a}a = e$.

Ex. 4. (a) Show that $pt \leqq e'$, $p \leqq (e':t)$, and $p' \geqq \breve{t}$ are equivalent.

(b) Show that $rs \frown t = 0$ if and only if $rst \leqq e'$. Infer that it implies $st \frown \breve{r} = 0$.

Ex. 5. Show that, if $r > 0$, then $r\breve{r} \frown e > 0$, whence $r\breve{r} > 0$. (Hint: Use Ex. 4.)

6. Structure and representation theory. We know (Ch. X, Thm. 7) that any Boolean algebra is isomorphic with a subalgebra of the Boolean algebra of all subsets of a suitable class of points. Also, any homomorphic image, subalgebra, or direct union of Boolean algebras is itself a Boolean algebra. We shall now show that one cannot hope for a similar theorem about relation algebras.

LEMMA 2. *Every Boolean m-lattice R with $0, e, I$ which satisfies (20) is simple—that is, it has no proper homomorphic images exept itself and the one-element algebra $0 = e = I$.*

Proof. Let θ be any congruence relation on R. Unless θ is the equality relation, some $r > 0$ satisfies $r \equiv 0 \pmod{\theta}$, by Thm. 8, Ch. X. Hence, by (20), $I = IrI \equiv I0I = 0 \pmod{\theta}$, and so (again by Thm. 8 Ch. X) every $x \equiv 0 \pmod{\theta}$.

But (20) holds in every subalgebra of a relation algebra, which contains 0, e, I—i.e., is closed under these zero-ary operations. On the other hand, (20) is violated in the direct union of two relation algebras; hence *the direct union of two relation algebras is not isomorphic to a subalgebra of a relation algebra,* even though the corresponding fact is true in Boolean algebra and in matrix algebra.

It follows that the concept of a "relation algebra" is ambiguous. All the laws of Thm. 10 are preserved under the formation of subalgebra and (trivially) homomorphic image—but if we wish to consider the class of algebras generated by $R(\Gamma)$ under these operations *and* direct union, we must use different postulates.[11]

Again, it is not known whether or not every abstract algebra satisfying the conditions of Thm. 10 is isomorphic with a subalgebra of some $R(\Gamma)$. (Though it is known that every "simple" matrix algebra with finite basis is a full matrix algebra over a division ring.) Most discussions define a "subalgebra" as a subset containing 0, e, I, and closed under Boolean operations, multiplications, and conversion. The results of §5 suggest requiring closure under residuation, of which conversion is a special case.

We illustrate the possible complexity of subalgebras of relation algebras by the 32-element subalgebra of the 512-element algebra of all relations on three elements, generated by 0, e, I and the first matrix of Fig. 9. This has for mini-

$$\begin{matrix} 0&1&1\\ 0&0&0\\ 0&0&0 \end{matrix},\quad \begin{matrix} 1&0&0\\ 0&0&0\\ 0&0&0 \end{matrix},\quad \begin{matrix} 0&0&0\\ 0&1&0\\ 0&0&1 \end{matrix},\quad \begin{matrix} 0&0&0\\ 1&0&0\\ 1&0&0 \end{matrix},\quad \begin{matrix} 0&0&0\\ 0&0&1\\ 0&1&0 \end{matrix}$$

Fig. 9

mal elements the other relation matrices of Fig. 9. A more symmetrical example is the following.

Example 6. The subsets $S, T, U, \cdots$ of any group G form a relation algebra, if we let $\breve{S}$ denote the set of all inverses of elements of S, and ST the set of all products st $[s \in S, t \in T]$.

We represent this system as a subalgebra of the algebra $R(G)$ of all relations on G, as follows. We identify each S with the relation σ: $x\sigma y$ means that $y \in xS$, in other words, that $xs = y$ for some $s \in S$. We leave it to the reader to verify that $S \frown T$, $S \smile T$, S', and $\breve{S}$ have the right meanings.

Though we cannot obtain a representation theorem for general relation algebras, we can reconstruct $R(\Gamma)$ as a relation algebra, by using a trick from the Wedderburn theory of semisimple algebras.

Definition. *A left-ideal element of a relation algebra R is an element x such that $Ix \leqq x$.*

Since $I(Ix) = (II)x \leqq Ix$, every Ix is a left-ideal element; since $I(x \smile y) = Ix \smile Iy \leqq x \smile y$, if x and y are left-ideal elements so is $x \smile y$.

Lemma 3. *The left-ideal elements of any Boolean m-lattice R with I satisfying* (17)–(19) *form a Boolean subalgebra closed under multiplication.*

Proof. If Ix is a left-ideal element, then $Ix \frown t = 0$ implies $x\breve{t} \frown I = 0$ by Ex. 4, §5, hence $0 = x\breve{t} = x(\breve{t}I) \frown I = Ix \frown It$, by Ex. 4 again. Therefore

[11] Both McKinsey (op. cit) and Tarski (op. cit. XXXII) assume (20). The logical difficulties (decision problem, elimination problem) of the algebra of relations are discussed in Tarski, op. cit., pp. 88–9, and in references cited there. Note also H. Behmann, Math. Annalen 86 (1922), 163–229, esp. §19; W. Ackermann, ibid., 110 (1934), 390–413; and Hilbert-

the complement of Ix, which is the largest element disjoint from Ix, is a left-ideal element. Since $x \smile y$ is a left-ideal element if x and y are, it follows that the left-ideal elements are a Boolean subalgebra. Finally, any right-multiple xy of a left-ideal element x satisfies $I(xy) = (Ix)y \leqq xy$.

Now let $m_1, \cdots, m_s$ be the *minimal* left-ideal elements of R. For any $r \in R$, define $r_{ij} = 1$ if $m_i r \geqq m_j$, and $r_{ij} = 0$ otherwise. (In the latter case, $m_i r \frown m_j = 0$.) One can prove that $r_{ji} = 0$ if and only if $\tilde{r}_{ij} = 0$ (by Ex. 4 again.) Moreover $(r \smile s)_{ij} = r_{ij} \smile s_{ij}$. To prove that the representation is homomorphic we must *assume* that every $\tilde{m}_i m_j$ covers 0 (is an atom); this is however true if $R = R(\Gamma)$. It is not true in Example 6.

Ex. 1. Show that the preceding construction "represents" the direct union $R(\Gamma) \times R(\Gamma^*)$ of two relation algebras as a "subalgebra" of $R(\Gamma + \Gamma^*)$, except that I has an altered meaning.

Ex. 2. In any relation algebra A, let the "points" be $p_1, \cdots, p_n$. Define $q_{ij} = p_i I p_j$. Discuss the "representation" of A so obtained. (Thus if (20) is assumed, $q_{ik} q_{kj} = q_{ij}$.)

Problem 94. Obtain a set of postulates on the operations of relation algebra, satisfied by an algebra if and only if it is a subalgebra of an $R(\Gamma)$, closed under: (a) 0, e, I, Boolean operations, and conversion, (b) same, plus residuation, (c) same, where the new I can be different from the old I.

7. Boolean matrices. The relation algebra $R(\Gamma)$ can also be regarded as the algebra of all *join-endomorphisms* of the Boolean algebra A of all subsets of Γ. To establish this interpretation, it is convenient to represent the elements of A as characteristic functions $f = (f_1, \cdots, f_n)$. Then the transform $g = fr$ of f under the endomorphism corresponding to $r = \| r_{ij} \|$ is defined by $g_j = \bigvee f_i r_{ij}$. This suggests considering, as analogs of relation algebras, the m-lattices of join-endomorphisms of given distributive lattices—and possibly of other lattices, though the author does not know when the join-endomorphisms of non-distributive lattices form lattices.

Another analog of relation algebras is furnished by the $n \times n$ matrices with coefficients r_{ij} in a fixed Boolean algebra A. These form a Boolean algebra if we define

$$(24) \qquad (r \smile s)_{ij} = r_{ij} \smile s_{ij}, \; (r \frown s)_{ij} = r_{ij} \frown s_{ij}, \; (r')_{ij} = r'_{ij}.$$

We can also define (relative) *multiplication* by

$$(25) \qquad (rs)_{ij} = \bigvee_k (r_{ik} \frown s_{kj}).$$

We can define 0, I, e by

$$(26) \qquad 0_{ij} = O \text{ and } I_{ij} = I \text{ for all } i, j$$

$$(26') \qquad e_{ii} = I, \text{ and } e_{ij} = O \text{ if } i \neq j.$$

This always defines an l-semigroup, and it defines the algebra of relations already discussed in case A is the two-element Boolean algebra **2**.

We shall not discuss such Boolean linear associative algebras further here.[12]

[12] See J. H. M. Wedderburn, Annals of Math. 35 (1934), 185–94; also Ch. X, §9.

CHAPTER XIV

LATTICE-ORDERED GROUPS

1. Definition; positive elements. We shall be concerned below with lattice-ordered groups, or *l-groups*, in the following sense.

DEFINITION. *An l-group G is* (i) *a lattice,* (ii) *a group, in which* (iii) *the inclusion relation is invariant under all group-translations $x \to a + x + b$. If G is a partly ordered set satisfying* (ii) *and* (iii), *it is called a partly ordered group, or po-group.*

We shall use the additive notation for the group operation below, in place of the multiplicative notation of Ch. XIII. Corresponding to the use of $a + b$, we shall let $-a$ denote the group inverse of a, $a - b$ denote $a + (-b)$, $-a + b$ denote $(-a) + b$, and na denote $a + \cdots + a$ (n summands).

In any *po*-group, condition (iii) is obviously equivalent to

$$(1) \qquad x \geqq y \text{ implies } a + x + b \geqq a + y + b, \quad \text{for all} \quad a, b \in G.$$

In an l-group, it is equivalent to the distributive laws

$$(2) \quad a + (x \smile y) = (a + x) \smile (a + y) \text{ and } (x \smile y) + b = (x + b) \smile (y + b),$$

or to their duals; we leave the proof to the reader.[1]

Hence *any l-group is an l-semigroup* in the sense of Ch. XIII, and all the results of that chapter are valid. However, it will almost always be easier to prove results about l-groups directly.

DEFINITION. *An element a of an l-group G is called positive if $a \geqq 0$. The set of all positive elements of G will be denoted G^+.*

THEOREM 1. *Any po-group G is determined to within isomorphism by the set G^+ of its positive elements, since*

$$(3) \qquad a \leqq b,\ b - a \in G^+, \text{ and } -a + b \in G^+ \text{ are equivalent conditions.}$$

Moreover (i) $0 \in G^+$, (ii) *if* $x, y \in G^+$, *then* $x + y \in G^+$, (iii) *if* $x, y \in G^+$ *and* $x + y = 0$, *then* $x = y = 0$, (iv) *for all* $a \in G$, $a + G^+ = G^+ + a$. *Conversely, if G is any group, and G^+ is a subset of G satisfying* (i)–(iv), *then condition* (3) *defines G as a po-group.*

Proof. We get (3) easily from (1); thus $a \leqq b$ implies $0 = a - a \leqq b - a$. Condition (i) is trivial; moreover since $s \geqq 0$, $t \geqq 0$ imply $s + t \geqq s + 0 \geqq$

[1] The distributive law (2) was used to define commutative l-groups by M. H. Stone [6]. The foundations of the general theory of l-groups were first given in G. Birkhoff [6].

$0 + 0 = 0$, (ii) holds. Under the hypotheses of (iii), $0 = x + y \geqq x, y \geqq 0$ by (3), whence $x = y = 0$, proving (iii). Finally, by (3), $a + G^+$ and $G^+ + a$ both define the set of all $x \geqq a$, proving (iv).

Conversely, let G be a group, and G any subset of G which fulfills the conditions listed; define $x \geqq y$ by (3). Then conditions (i), (ii), (iii) imply the rules P1, P3, P2 defining a partly ordered set, respectively. Again, suppose $x - y \in G^+$, and use (iv) in the form (iv′) $G^+ = -a + G^+ + a$. Then

$$(a + x + b) - (a + y + b) = a + x + b - b - y - a$$

$$= a + (x - y) - a \in G^+;$$

hence (1) holds, so that G is a *po*-group.

Remark. Conditions (i)–(ii) assert that G^+ is a semigroup. Condition (iv), in the form (iv′), asserts that G^+ is invariant under all inner automorphisms of G. The easiest way to show that a given system is an *l*-group is usually to verify these conditions, and then to use the following result.

THEOREM 2. *A po-group G is an l-group if and only if, for all $a \in G$, $a \smile 0 = a^+$ exists.*

Proof. If G is an *l*-group, then obviously $a \smile 0$ exists for all a. Conversely, let G be any *po*-group in which a^+ exists for all a. By (2), we have

$$(4) \qquad (a - b)^+ + b = [(a - b) \smile 0] + b = a \smile b \qquad \text{for all } a, b.$$

But $(a - b)^+ + b$ exists by hypothesis; hence $a \smile b$ always exists. Dually, since $x \geqq 0$ implies $0 = x - x \geqq 0 - x = -x$ and conversely, the correspondence $x \to -x$ is a dual automorphism. Hence

$$(5) \qquad -(-a \smile -b) = a \frown b \text{ always exists.}$$

Ex. 1. Prove that the following laws hold in any *po*-groups:[*]

(a) $x \geqq x'$ and $y \geqq y'$ imply $x + y \geqq x' + y'$,

(b) $x \geqq y$ implies $a - x + b \leqq a - y + b$,

(c) $x \frown y = -(-x + (x - y)^+) = -(x - y)^+ + x$.

Ex. 2. Prove in detail the equivalence of (1) and (2) in any group which is also a lattice.

Ex. 3. Show that an *l*-group may be defined as a group, with a second binary operation $\smile$ which is idempotent, commutative, associative, and satisfies (2).

Ex. 4. Show that an *l*-group may be defined as a group with a unary operation $a \to a^*$ (standing for $a \smile 0$), which is invariant under all inner automorphisms and satisfies: (i) $0^* = 0$, (ii) $c = c^* - (-c)^*$, (iii) the binary operation $(a - b)^* + b$ is associative.

Ex. 5. Show that one can dispense with the associative law of addition in Thm. 1, if one assumes that, given $a \in G$ and $x, y \in G^+$, there exists $z \in G$ such that $z + a = x + (y + a)$.

[*] More or less detailed proofs of Exs. 1–4 may be found in G. Birkhoff [6].

2. Examples. We shall now illustrate the wide prevalence of l-groups in mathematics by some simple examples. In all cases, Theorems 1–2 afford the most convenient way of verifying the conditions defining l-groups. We start with commutative or "Abelian" l-groups.

Example 1. G is the additive group of real numbers; G^+ consists of all those which are non-negative.

Example 2. G is the group of all positive rational numbers under multiplication (the integer one is the group identity); G^+ is the set of all positive integers. In this case x^+ is the numerator of x when reduced to lowest terms.

Example 3. G is the group of all vectors $x = (x', x'')$ with two real components, under addition; G^+ contains x if and only if $x' > 0$, or $x' = 0$ and $x'' \geqq 0$.

All of the "vector lattices" discussed in Ch. XV are commutative l-groups. We select two examples.

Example 4. G is the additive group of all continuous real functions defined on the interval $0 \leqq x \leqq 1$; G^+ consists of all those which are non-negative (satisfy $f(x) \geqq 0$ for all x). Here $f^+(x)$ is, for all x, the larger of $f(x)$ and 0.

Example 5. G is the additive group of functions of bounded variation on $0 \leqq x \leqq 1$ with $f(0) = 0$. G^+ consists of all such "non-decreasing" functions (functions for which $x \geqq y$ implies $f(x) \geqq f(y)$). Here $f^+(x)$ is the positive variation of $f(x)$, in the usual sense.

An instructive example of a discrete non-commutative l-group is the following. (Such a group must be infinite, by Thm. 7.)

Example 6. G has three generators a, b, c of infinite order, and defining relations $a + b = c + a$, $a + c = b + a$, $b + c = c + b$. G^+ contains $ma + nb + n'c$ if and only if $m > 0$, or $m = 0$ while $n \geqq 0$ and $n' \geqq 0$.

We give two examples of non-commutative Lie l-groups.[3] We can lexicographically order the two-parameter non-Abelian Lie group, as follows.

Example 7. G consists of all couples (x, y) of real numbers, addition being defined by the formula

$$(x, y) + (x', y') = (x + x', e^{x'}y + y').$$

G^+ consists of those couples with $x > 0$, or $x = 0$, $y \geqq 0$.

Example 8. G consists of all matrices X of the form pictured at the right, under matrix multiplication. $X \geqq 0$ means $a > 0$, or $a = 0$ and $b > 0$, or $a = b = 0$ and $c \geqq 0$.

$$X = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

The following important example of a non-commutative infinite continuous l-group has been discussed in some detail by Everett and Ulam [1]; see also S. S. Batty and A. G. Walker, Quar. Jour. Math. 17 (1946), 145–52.

Example 9. G consists of the order-preserving homeomorphisms of the interval $0 \leqq x \leqq 1$ under substitution. G^+ consists of those satisfying $f(x) \geqq$

---

[3] See G. Birkhoff, *Lattice-ordered Lie groups*, Speiser Festschrift Volume, 209–17, for a discussion of Lie l-groups.

x for all x. As a lattice, G is thus a sublattice of the lattice of Example 4, but the group operation is different. Thus $f^+(x)$ is the larger of x and $f(x)$.

Ex. 1. (a) Prove in detail that Examples 1–5 are Abelian l-groups.

(b) Prove that Examples 6–9 are l-groups.

Ex. 2. Show that the following systems are po-groups or nearly so, but are not in general lattices:

(a) G consists of the integers under addition; G^+ consists of the integers n greater than two.

(b) G is the multiplicative group of all rational numbers not zero; G^+ consists of all integers.

(c) G is the additive group of a field of characteristic infinity, which is "formally real" in the sense that $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ implies $x_1 = x_2 = \cdots = x_n = 0$. G^+ is the subset of all sums of squares.

Ex. 3*. Generalize Example 5 to the additive group of all valuations of bounded variation on any lattice L, satisfying $v[O] = 0$. (Hint: See Ch. V, Thm. 17.)

Ex. 4*. Generalize Example 9 to the group of lattice-automorphisms of any chain, under substitution.

Problem 95. Characterize abstractly, as groups, as lattices, and as l-groups, the l-groups of all lattice-automorphisms of a general chain. (Remark: The automorphisms of a chain C are the same as those of the completion $\bar{C}$ by cuts of C. At least in many cases, the points of $\bar{C}$ correspond to ideals in the l-group, having the given point for fixpoint.)

3. Digression: directed groups as semigroups. By a *directed group*, we mean a po-group having the Moore-Smith property

(6) Given $a, b \in G$, there exists $c \in G$ with $c \geqq a$ and $c \geqq b$.

Evidently any l-group, being a lattice, is a directed group.

LEMMA 1 (Clifford[4]). *In any po-group, the Moore-Smith property is equivalent to the assertion that*

(7) *Every element is a difference of positive elements.*

Proof. Assuming (6) with $b = 0$, we get $a = c - (-a + c)$, where $c \geqq 0$ and $-a + c = -a + (c - a) + a \geqq -a + 0 + a = 0$. Conversely, if $a = a' - a''$ and $b = b' - b''$, where a', a'', b', b'' are positive, then $c = a' + b'$ is an upper bound to a and b.

We shall now show that any directed group is determined to within isomorphism by the semigroup of its positive elements, ordered by the divisibility relation. It follows that l-groups can be regarded as the natural extensions to groups of a well-defined class of semigroups. The construction of the ordered additive group of all integers from the semigroup of positive integers is included as a special case.

First, note that the set S of all positive elements of any directed group G satisfies conditions (i)–(iv) of Thm. 1, and also the cancellation law

(8) $x + a = y + a$ or $b + x = b + y$ implies $x = y$.

[4] A. H. Clifford, Annals of Math. 41 (1940), p. 467.

By (8) and (iv), assumed only for S, we see that

(9) Given $a, x \in S$, exactly one $x_a \in S$ satisfies $x + a = a + x_a$.

We can restate these conditions as follows. S is a semigroup satisfying the cancellation laws. In S, $a \leqq b$ means that b is a left-multiple of a, or equivalently, that b is a right-multiple of a. That is, $a \leqq b$ means $b \in S + a = a + S$.

In any such semigroup, $x + a + b = a + x_a + b = a + b + (x_a)_b$, and $x + y + a = x + a + y_a = a + x_a + y_a$. Therefore we have

(10) $$(x_a)_b = x_{a+b} \text{ and } (x + y)_a = x_a + y_a.$$

These rules are obvious in groups, where $x_a = -a + x + a$. The subtle fact is that they are valid in any semigroup[5] S which satisfies the cancellation law (8) and the weak commutative law $S + a = a + S$ for all $a \in S$. We can construct a group G out of the formal differences $(b, a) = (b - a)$ of elements of S, by letting

(11) $(b - a) = (d - c)$ in G mean $b + c = d + a_c$ in S,

(12) $(b - a) + (d - c)$ in G be $((b + d_a) - (c + a))$,

where $b + d_a$, $c + a$ are in S. Simple calculations show that formulas (11)–(12) always define a group, in which the couples $(b - 0)$ form a semigroup isomorphic with S, and that $(b - a) = (b - 0) - (a - 0)$ in the group G. Using Thm. 1, we conclude

THEOREM 3. *A directed group may be defined as the extension to a group G of a semigroup S in which* (i) *the cancellation law holds*, (ii) $S + a = a + S$ *for all* $a \in S$, (iii) $a + b = 0$ *implies* $a = b = 0$.

COROLLARY 1. *An l-group may be defined as in Theorem* 3, *if one assumes further* (iv) *any two elements of X have a least common multiple in S.*

In fact, (iii) is not really essential, if we are willing to introduce an equivalence relation.

Ex. 1. Show that the negative elements of any l-group form a residuated l-semigroup, with $a:b = (a - b)^-$, but that the positive elements do not.

Ex. 2. Show that a commutative integral l-semigroup A consists of the negative elements of some l-group, if and only if A satisfies the cancellation law.

---

[5] The semigroup extension to a group under these hypotheses is due to A. Malcev, *Über die Einbettung von associativer Systemen in Gruppen*, Mat. Sbornik 6 (1939), p. 331. The application to l-groups is due to von Neumann (see G. Birkhoff [6]).

4. **Basic algebraic rules.** Since the correspondence $x \to -x$ is a dual automorphism, so is the correspondence $x \to a - x + b$, and we have, in any l-group

$$a - (x \frown y) + b = (a - x + b) \smile (a - y + b). \tag{13}$$

Setting $x = a$ and $y = b$ in (13), we get

THEOREM 4. *In any l-group, we have for all a, b,*

$$a - (a \frown b) + b = b \smile a. \tag{13'}$$

COROLLARY 1. *In any commutative l-group, we have*

$$a + b = (a \smile b) + (a \frown b) \text{ for all } a, b.^{6} \tag{13''}$$

In Example 2 of §2, the *modular law* (13″) specializes to the celebrated identity $ab = (a, b)[a, b]$ of number theory.

DEFINITION. *The positive part* a^+ *of an element* a *is* $a \smile 0$; *the negative part* a^- *of* a *is* $a \frown 0$; *the absolute* $|a|$ *of* a *is* $a \smile -a$.

Setting $b = 0$ in Corollary 1, we get

COROLLARY 2. *For any* a, $a = a^+ + a^-$.

In words, every element of an l-group is the sum of its positive and negative parts (so-called Jordan decomposition).

THEOREM 5. *Any l-group is a distributive lattice.*

Proof. By Bergmann's Cor. 1 of Thm. 1, Ch. IX, it is enough to show that $a \frown x = a \frown y$ and $a \smile x = a \smile y$ imply $x = y$. But by (13′), they imply

$$x = (a \frown x) - a + (x \smile a) = (a \frown y) - a + (y \smile a) = y.$$

THEOREM 6. *In any l-group, we have*

$$a \frown b = 0 \text{ and } a \frown c = 0 \text{ imply } a \frown (b + c) = 0, \tag{14}$$

$$a \smile b = 0 \text{ and } a \smile c = 0 \text{ imply } a \smile (b + c) = 0. \tag{14'}$$

Proof. Using duality, this is a special case of Thm. 7 of Ch. XIII. However, we give a fresh proof of (14). Since a, b, c are positive, clearly $a \frown (b + c) \geqq 0$. But by the dual of (2),

$$0 = 0 + 0 = (a \frown b) + (a \frown c) = (a + a \frown c) \frown (b + a \frown c)$$
$$= (a + a) \frown (a + c) \frown (b + a) \frown (b + c) \geqq a \frown (b + c).$$

We can reword Thm. 6 in terms of the important concept of disjointness.

---

[6] Historical note. Cor. 1 was discovered by Dedekind [1, p. 133], and rediscovered by H. Freudenthal [1, p. 642]. The distributive law was also discovered, in the commutative case, by Dedekind [1, p. 135], and rediscovered by Freudenthal, loc. cit. The concept of absolute was introduced by Kantorovitch [1]. The generalizations to non-commutative groups are due to the author [6].

DEFINITION. *Two positive elements a and b will be called disjoint—in symbols, $a \perp b$,—if and only if $a \frown b = 0$.*

In Example 2 of §2, this specializes to the concept of relative primeness. Thm. 6 asserts that the set of positive elements disjoint to any a is closed under addition. Further, if we assume $a \frown b = 0$ in (13′), we get, since $b \smile a = a \smile b$,

LEMMA 1. *Disjoint elements are permutable,*

$$\text{(15)} \qquad \text{If } a \frown b = 0, \text{ then } a + b = b + a.$$

LEMMA 2. *If $b \frown c = 0$, then $(b - c)^+ = b$ and $(b - c)^- = -c$.*

Proof. By our preceding formulas, $(b - c) \smile 0 = (b \smile c) - c = b - (b \frown c) + c - c = b$, and dually.

LEMMA 3. *If $na \geqq 0$, then $a \geqq 0$.*

Proof. Expanding by the dual of (2), $n(a \frown 0) = na \frown (n-1)a \frown (n-2)a \frown \cdots \frown a \frown 0$. But if $na \frown 0 = 0$, this equals $(n-1)a \frown (n-2)a \frown \cdots \frown a \frown 0 = (n-1)(a \frown 0)$. Now cancelling, we get $a \frown 0 = 0$, as desired.

Combining Lemma 3 with its dual, we get

THEOREM 7. *In an l-group, every element except the identity has infinite order.*

Another corollary is the fact that, in any *commutative* l-group, $na \geqq nb$ implies $n(a - b) \geqq 0$, *and so* $a \geqq b$.

LEMMA 4. *The positive and negative parts of any element are disjoint,*

$$\text{(16)} \qquad \text{For any } a, \qquad (a \smile 0) \frown (-a \smile 0) = a^+ \frown (-a^-) = 0.$$

Proof. Clearly $-(a \smile -a) = -a \frown a$. Hence $2(a \smile -a) = (a \smile -a) - (a \frown -a) \geqq 0$. Hence by Lemma 3, $a \smile -a \geqq 0$, so that (dualizing) $a \frown -a \leqq 0$. Using this and Thm. 5, we get $(a \smile 0) \frown (-a \smile 0) = (a \frown -a) \smile 0 = 0$. Incidentally, $|a| = 0$ implies $a \smile -a = a \frown -a$, so that $a = -a$, $2a = 0$, and $a = 0$.

THEOREM 8. *In any l-group, the absolute satisfies*

$$\text{(17)} \qquad \text{If } a \neq 0, \text{ then } |a| > 0, \text{ while } |0| = 0.$$

$$\text{(18)} \qquad |na| = |n| \cdot |a| \text{ for any integer } n,$$

$$\text{(19)} \qquad |a - b| = (a \smile b) - (a \frown b),$$

$$\text{(20)} \qquad |(a \smile b) - (a^* \smile b)| \leqq |a - a^*| \text{ and dually.}$$

Proof. Formula (17) follows from (19) with $b = 0$. This also gives $|a| = a^+ - a^-$, but by Lemmas 1 and 4, a^+ and a^- are disjoint and permutable. Hence $na = n(a^+) - n(a^-)$, and by Thm. 6 and induction, $n(a^+) \frown n(-a^-) = 0$.

Hence by Lemma 2, $(na)^+ = n(a^+)$ and $(na)^- = n(a^-)$. This implies (18) for positive n. The result for negative n now follows since $| -x | = | x |$.

We next prove (19); of course we cannot assume (17) or (18). Justifying the successive equations by Cor. 2 of Thm. 4, group algebra, and (2) and its dual, respectively, we compute

$$| a - b | = (a - b)^+ - (a - b)^- = [(a - b) \smile 0 + b] - [(a - b) \frown 0 + b]$$
$$= (a \smile b) - (a \frown b).$$

Finally, to prove (20), expand the left-hand side by (19) to get $a \smile b \smile a^* - (a \smile b) \frown (a^* \smile b) = a \smile a^* \smile b - (a \frown a^*) \smile b$, using the distributive law (Thm. 5). This reduces to the case $a \geqq a^*$, since by (19) the right-hand side of (20) is $a \smile a^* - a \frown a^*$. In this case, writing $a = t + a^*$ $[t \geqq 0]$, we have

$$a \smile b = (t + a^*) \smile b = t + [a^* \smile (-t + b)] \leqq t + (a^* \smile b).$$

Right-subtracting $a^* \smile b$, we get (20) since $t = | a - a^* |$.

Ex. 1. Show that if $x, y \geqq 0$ in an l-group, then $a \frown (x + y) \leqq (a \frown x) + (a \frown y)$.

Ex. 2. Show that the free l-group with one generator is $J \times J$, where J is the l-group of ordinary integers under addition and the usual order relation.

Ex. 3. Show that in any commutative l-group A, for any positive integer n, the correspondence $x \to nx$ is an isomorphism of A with an l-subgroup of itself.

Ex. 4*. Define a "valuation" from a lattice L to a commutative l-group G as any single-valued function $v[x]$ from L into G which satisfies (12''). Generalize the theory of metric lattices (Ch. V, §7) to this case.[7]

Ex. 5*. Show that in Example 9, $na \geqq nb$ need not imply $a \geqq b$ (Everett and Ulam [1, Thm. 11]).

Ex. 6*. Show that (20)–(20') hold in any po-group in which, if $0 \leqq x \leqq a + b$ $[a, b \geqq 0]$, then $x = s + t$, where $0 \leqq s \leqq a, 0 \leqq t \leqq b$.[8]

Ex. 7*. Define an l-loop as a loop (Ch. VI, §1), which is a lattice, in which every "loop-translation" $x \to (a + x) + b$ is an order-automorphism.

(a) Show that any l-loop is a distributive lattice.

(b) Show that $[b - (a \frown b)] + a = a \smile b = b + [-(a \frown b) + a]$, and $a - (a \frown b) = (a \smile b) - b$. If a, b commute, then (13'') holds.

(c) Show that the positive parts of $a - b$ and $b - a$ are disjoint.

(d) Show that if we define $1 \cdot a = a$ and $(n + 1)a = na + a$, then $na \geqq 0$ implies $a \geqq 0$, and $na = ka$ for even one $k < n$ implies $a = 0$.

Problem 96. Characterize abstractly, to within isomorphism, the free l-group with two generators.

Problem 97. Find a generalization of Thm. 3 which is valid in any l-loop.

---

[7] In virtue of Thm. 13, the only essential generalization is, however, to non-Archimedean, simply ordered groups.

[8] For Ex. 6 and the significance of this condition, see F. Riesz [2] and G. Birkhoff [6, Thms. 49–50]; also Lemma 3 of Ch. XV, §7, and A. Bischof, Schr. Math. Inst. Berlin 5 (1941), 237–62. For Exs. 2–3, see G. Birkhoff [6, Thms. 17–18]. The results of Ex. 7 are due to I. Kaplansky (letter to the author). Some of the results are true more generally for l-quasigroups. See D. Zelinsky, Bull. Am. Math. Soc. 54 (1948), 175–183.

5. Ideals. It is well-known that the congruence relations on any group G are the partitions of G into the cosets of its different normal subgroups N. Therefore, the congruence relations on an l-group are those decompositions into cosets of normal subgroups which have the substitution property for the two lattice operations—or equivalently, by (4)–(5), make $a \equiv b\ (\theta)$ imply $a^+ \equiv b^+\ (\theta)$.

DEFINITION. *By an l-ideal of an l-group G is meant a normal subgroup of G which contains with any a, also all x with $|x| \leqq |a|$.*[9]

Clearly G and 0 are l-ideals of G; they are called improper l-ideals; all other l-ideals of G are called proper l-ideals. Again, let N be any l-ideal of G, and suppose that $a, b \in N$. If $a \frown b \leqq x \leqq a \smile b$, then

$$|x| = x \smile -x \leqq (a \smile b) \smile -(a \frown b) = a \smile b \smile -b \smile -a$$

$$= |a| \smile |b| \leqq |a| + |b|.$$

Hence $x \in N$, and any l-ideal of an l-group is a *convex* l-subgroup.

THEOREM 9. *The congruence relations on any l-group G are the partitions of A into the cosets of its different l-ideals.*

Proof. If N is the set of elements congruent to 0 under a congruence relation, then $a \in N$ and $|x| \leqq |a|$ imply $a \frown -a \leqq x \leqq a \smile -a$; hence $0 \frown 0 \leqq x \leqq 0 \smile 0 \bmod N$, and so $x \in N$. Conversely, if N is an l-ideal, then $x \equiv x^* \bmod N$ implies $|(x \smile y) - (x^* \smile y)| \leqq |x - x^*|$ by (20), and therefore $x \smile y \equiv x^* \smile y \bmod N$. Using left-right symmetry and duality, we see that the partition of G into the cosets of N has the substitution property for both lattice operations, completing the proof.

Again, the congruence relations on any algebra A are a complete sublattice of the lattice of all partitions of the elements of A (Ch. II, Thm. 4). Therefore the congruence relations on any l-group G are a sublattice of the lattice of all congruence relations on G, when the latter is regarded purely as a lattice. Since this is distributive (Ch. II, Thm. 5), we obtain

THEOREM 10. *The l-ideals of any l-group G form a complete distributive lattice; hence so do the congruence relations on G.*

Combining with Ch. VI, §8, Ex. 2(a), or paraphrasing suitably the argument of Ch. II, §8, we get

THEOREM 11. *Any two representations of an l-group G as a direct union (cardinal product) have a common refinement. If the lattice of all congruence relations on G has finite length, then G has a unique representation as the direct union of indecomposable factors.*

---

[9] We follow the terminology of Stone [6]. The concept of l-ideal is due to Kantorovitch [1, p. 155, conditions (α)–(β)]. Thms. 9–11 are due to the author, who called l-ideals "normal subspaces" in [LT]. F. Riesz [2] called them "familles presque complètes." Kakutani has used the term l-ideal slightly differently.

Different proofs of these results may be found in G. Birkhoff [6].

Ex. 1. Prove that any l-ideal of an l-group G is a convex l-subgroup, using the lemma of Ch. II, §5. Prove that conversely, if G is Abelian, all its convex l-subgroups are l-ideals.

Ex. 2. Prove that the congruence relations on any l-group G satisfy the infinite distributive law (9) of Ch. II.

6. Units. The concept of a unit is very useful, especially in the case of commutative l-groups.

DEFINITION. *By a strong unit*[10] *of an l-group G is meant an element $e \in G$ such that, for any $a \in G$, $ne > a$ for some positive integer n. Two elements a and b of G are called disjoint if and only if $|a| \frown |b| = 0$. A positive element $c \in G$ is called a weak unit if the only element disjoint from it is 0.*

LEMMA 1. *Any strong unit is a weak unit.*

Proof. By Lemma 3 of §4, any strong unit is positive. By Thm. 6, for any e, $e \frown a = 0$ implies $ne \frown a = 0$ for all n. But if e is a strong unit, $ne \geqq a$ for some n, and so $e \frown a = 0$ implies $a = ne \frown a = 0$, whence e is a weak unit.

Not all weak units are strong units. For example, the additive l-group of all continuous real functions on the domain $0 \leqq x < +\infty$ has the weak unit $f(x) = 1$, but no strong unit, since for no n and $f(x) \geqq 0$ is $nf(x) \geqq [f(x) + x]^2$, for all x. On the other hand, in the l-group of all bounded real-valued functions on any domain, the function $f(x) = 1$ is a strong unit.

Even in l-groups without weak units, l-ideals may have strong units; such l-ideals are called *principal* l-ideals. In fact, in any commutative l-group, every positive element is a strong unit for an appropriate l-ideal (F. Riesz [2, p. 188]), as we now show.

THEOREM 12. *In any commutative l-group, for any $a > 0$, the set $J(a)$ of all b such that $|b| < na$ for some positive integer n forms an l-ideal having a as strong unit. Moreover $J(a)$ is the smallest l-ideal which contains a.*

Proof. If $|b| < ma$ and $|c| < na$, then clearly $|b \pm c| < (m+n)a$; while if $|b| < ma$ and $|x| \leqq |b|$, then $|x| < ma$; hence $J(a)$ is an l-ideal. Obviously a is a strong unit of $J(a)$. Finally, any l-ideal which contains a must contain every na and so all b with $|b| < na$.

Now let A be any Abelian l-group. Unless A is simply ordered, by the invariance of order under group-translation it will contain an element a such that neither $a \geqq 0$ nor $0 \geqq a$. For this a, $a^+ > 0$ and $-a^- > 0$ will be disjoint, by Lemma 4 of §4. Hence, by Thms. 6 and 12, $J(a^+)$ and $J(-a^-)$ will be disjoint l-ideals. By Thm. 9 of Ch. VI, we infer

[10] The concept of a strong unit goes back to Archimedes; that of weak unit is due to Freudenthal [1]. The useful terms "strong unit" and "weak unit" are due to Bohnenblust; they will be used extensively in Ch. XV.

Lemma 2. *A commutative l-group is either simply ordered or subdirectly reducible.*[11]

Now, by applying Thm. 10 of Ch. VI, we get immediately

Theorem 13. *Any commutative l-group is a subdirect union of simply ordered l-groups.*

Ex. 1. Show that the conclusions of Thm. 12 hold for any element a in the group-theoretic central of a non-commutative l-group.

Ex. 2. Show that, in Example 6 of §2, the set $J(c)$ is not an l-ideal.

Ex. 3. (a) Show that, in any l-group, the set $\{a\}^*$ of all elements disjoint from any fixed element a is a subgroup which contains, with any b, all x satisfying $|x| \leqq |b|$.

(b) Infer that, in any commutative l-group, the set $\{a\}^*$ is always an l-ideal. Show this is false in Example 6 of §2.

Ex. 4. Show that any l-ideal T of an l-ideal S of an Abelian l-group A is itself an l-ideal of A, but that this need not hold in non-commutative l-groups. (Try Example 6 of §2.)

Ex. 5. (a) Show that if the "structure lattice" of all l-ideals of a commutative l-group has finite length, then every l-ideal is principal.

(b) Show that the principal l-ideals of any commutative l-group A form a topologically dense sublattice of the structure lattice of A.[12]

Problem 98. In a Lie l-group, do $na \geqq nb$ imply $a \geqq b$? Are the results of Ex. 3b, Ex. 4, and Ex. 5a above valid in any Lie l-group? Is every Lie l-group simply connected?[13]

Problem 99. Are Ex. 4 and Ex. 5a valid in any l-group having a finite number of generators, in the usual group-theoretic sense?

7. Simply ordered groups; Archimedean case. A *simply ordered group*, or *ordered group*, is usually defined as a *po*-group which satisfies

P4. Given x, y, either $x \geqq y$ or $y \geqq x$.

That is, it is a *po*-group which is a chain in the sense of Ch. III—or equivalently, in which every element is positive, negative, or zero. Being a chain, it is a lattice, and hence an l-group.

We have seen (Thm. 7) that in any l-group, every element except the identity has infinite order. Conversely, one can show[14]

Theorem 14. *Any abstract commutative group A whose elements are all of infinite order can be made into a simply ordered group.*

Proof. In such a group, the equation $nx = ma$ has at most one solution. For $nx = ny$ implies $n(x - y) = 0$, hence $x = y$. If $nx = ma$ has a solution, we denote it $(m/n)a$, and observe that all the laws of vector algebra hold for the multiplication by *rational* scalars so defined.

---

[11] This is Thm. 36 of G. Birkhoff [6]. It is closely related to Satz 14 of P. Lorenzen, *Abstrakte Begrundung der multiplikativen Idealtheorie*, Math. Zeits. 45 (1939), 533–53.

[12] Exs. 3–5 are Thm. 22, the Remark on p. 311, and Thms. 28–29 of G. Birkhoff [6].

[13] For these questions, see G. Birkhoff, *Lattice-ordered Lie groups*, Speiser Festschrift Commentarii Math. Helvetici, 209–17.

[14] This result is due to F. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen*, Rendic. Palermo 35 (1913), 225–36. An interesting algebraic study of Abelian groups without elements of finite order has been made by R. Baer, Duke Jour. 3 (1937), 68–122.

By a well-ordered *rational basis* for A, we mean a well-ordered (finite or infinite) subset of elements a_α of A such that every non-zero element of A is a finite rational combination

$$n_1 a_{\alpha(1)} + \cdots + n_r a_{\alpha(r)} \qquad [\alpha(1) < \cdots < \alpha(r)]$$

of the a_α, while $\sum n_i a_{\alpha(i)} = 0$ implies that every $n_i = 0$—or equivalently, $\sum (m_i/n_i) a_{\alpha(i)} = 0$ implies that every $m_i/n_i = 0$. The existence of well-ordered rational basis can be proved directly, since any maximal well-ordered rationally independent subset is a basis. Finally, relative to such a basis, any element of A not 0 may be called positive or negative according as its first non-zero coefficient m_i/n_i is positive or negative. This "lexicographic" ordering of A clearly defines from it a simply ordered group.

COROLLARY. *A commutative group is the additive group of an l-group if and only if it has no element of finite order except the identity.*

In the logical foundations of analysis, an especially important role is played by ordered groups which are "Archimedean," in the following sense.

DEFINITION. *An element a of a po-group is called incomparably smaller than a second element b (in symbols, $a \ll b$) if and only if $na \leqq b$ for any integer n. A po-group is called Archimedean if and only if $a \ll b$ implies $a = 0$.*

Otherwise stated, $a << b$ means that b is an upper bound for the entire cyclic subgroup generated by a. Thus in Example 3, $(0, 1) \ll (1, 0)$; in the construction of Thm. 14, $a_1 \gg a_2 \gg a_3 \gg \cdots$. It is easily verified that the relation $\ll$ is antisymmetric and transitive, and that any subgroup of an Archimedean l-group is itself Archimedean with respect to the same order relation, whether it is an l-subgroup or not. We note further

LEMMA 1. *An l-group G is Archimedean if and only if*

(*) $\qquad$ *$na \leqq b$ for all $n = 1, 2, 3, \cdots$ implies $a \leqq 0$.*

Proof. If G satisfies (*), and $na \leqq b$ for $n = 0, \pm 1, \pm 2, \cdots$, then $na \leqq b$ and $n(-a) \leqq b$ for $n = 1, 2, 3, \cdots$. Hence by (*), $a \leqq 0$ and $-a \leqq 0$, proving $a = 0$. Thus G is Archimedean; the proof is valid in any *po*-group.

Conversely, suppose G is Archimedean, and $na \leqq b$ for all $n = 1, 2, 3, \cdots$. Then $na^+ = (na)^+ = na \smile 0 \leqq b \smile 0$ as in the proof of Thm. 8, for $n = 1, 2, 3, \cdots$. But $na^+ \leqq 0 \leqq b^+$ for $n = 0, -1, -2, \cdots$; hence $na^+ \leqq b^+$ for $n = 0, \pm 1, \pm 2, \cdots$. Since G is Archimedean, we infer $a^+ = 0$ and $a = a^+ + a^- \leqq 0$, q.e.d.

LEMMA 2. *A simply ordered group G is Archimedean if and only if any $e > 0$ is a strong unit.*

Proof. If any $e > 0$ is a strong unit, then $a \neq 0$ implies $n \mid a \mid > b$ for all b and appropriate n; but $\mid a \mid = \pm a$; hence $(\pm n)a > b$ for some n, whence G is Archimedean. Conversely, if G is Archimedean, then, by Lemma 1, $ne \leqq b$ for all n is impossible; hence some $ne > b$ for any $e > 0$, and so e is a strong unit.

LEMMA 3. *In a simply ordered group, $na \geqq nb$ implies $a \geqq b$, and so $na = nb$ implies $a = b$.*

Proof. Unless $a \geqq b$, we have $a < b$, whence $na < nb$ since addition is order-isomorphic. This is contrary to hypothesis. We note that $na = nb$ does not imply $a = b$ in the l-group of Example 9.

THEOREM 15. *Any simply ordered Archimedean group G is isomorphic to a subgroup of the additive group of all real numbers, and so is commutative.*[15]

Proof. Let $e > 0$ be arbitrary. For any $a \in G$, we can define the set $L(a)$ of all rational fractions m/n $[n > 0]$ such that $me \leqq na$, and the set $U(a)$ of all m/n with $me \geqq na$. By P4, every m/n is in $L(a)$ or $U(a)$, equality occurring only if $me = na$. Again, by the Archimedean property, $-me < a < me$ for some m; hence neither $L(a)$ nor $U(a)$ is void. Further, if $m/n \in U(a)$ and $m'/n' \geqq m/n$, then $m'n \geqq mn'$. Hence $m'ne \geqq mn'e \geqq n'na$ and so, by Lemma 3, $m'e \geqq n'a$, implying $m'/n' \in U(a)$. Hence, using duality, $L(a)$ and $U(a)$ are the two halves of a Dedekind cut in the rationals. Again, no two distinct elements a and b can determine the same cut, or we would have $(a - b) \ll e$. This establishes a one-one correspondence $a \leftrightarrow a'$, $b \leftrightarrow b'$ between G and a class R of real numbers, which clearly preserves order.

It remains to show that $a + b$ in G corresponds to $a' + b'$ in R. This may be shown by choosing, for arbitrarily large n, $me \leqq na \leqq (m + 1)e$ and $m'e \leqq nb \leqq (m' + 1)e$; then $L(a + b)$ contains $(m + m')/n$ and $U(a + b)$ contains $(m + m' + 2)/n$; we leave the remaining details to the reader.

Ex. 1. (a) Show that the l-ideals of any ordered group form a chain.

(b) Show that, if the l-ideals of a commutative l-group G form a chain, then G is simply ordered.

(c) Show that the l-ideals in Example 6 of §2 form a chain, though the group is not simply ordered. Infer that Thm. 13 cannot be extended to non-commutative l-groups.

Ex. 2. (a) Show that any commutative l-group without proper l-ideals (congruence relations) is a subgroup of the additive group of real numbers, and conversely.

(b) Show that a commutative group without elements of finite order can be made into an Archimedean ordered group if and only if its cardinal number is bounded by the power of the continuum.

Ex. 3*. Let G be the additive group of all continuous real-valued functions defined on the interval $[0, +\infty)$; let J be the l-ideal of all functions $f(x)$ such that $f(x) = 0$ for all $x > N(f)$ (i.e., "ultimately identically zero").

(a) Show that G is Archimedean but that G/J is not.

(b) Show that $f \ll g$ in G/J is equivalent to $f = O(g)$ in the usual Bachmann-Hardy-Landau notation.

---

[15] This result is due to O. Hölder, Leipz. Ber. 53 (1901), 1–64, esp. pp. 13–14; see also R. Baer, Jour. f. Math. 160 (1929), 208–26; H. Cartan, Bull. Sci. Math. 63 (1939), 201–5; F. Loonstra, Proc. Ned. Akad. Wet. 49 (1945), 41–6. Lemma 3 is due to F. W. Levi, Proc. Indian Acad. Sci. 16 (1942), 256–63; see also ibid. 17 (1943), 199–201. Four postulate systems for ordered Abelian groups are given by A. Tarski in his *Introduction to logic*. See also L. S. Rieger, Vestn. Kral. Ceske Spol. Nauk. Trida Mat.-Prir. 1946, no. 6, 31 pp., where the idea of a cyclically ordered group is introduced.

(c) Show that, given $f_1 \leqq f_2 \leqq f_3 \leqq \cdots$ countable, one can always construct g such that every $f_i \ll g$ in G/J. (Thm. of duBois-Reymond).

Ex. 4*. Show that if G is an Archimedean l-group, and if the center of G contains the commutator subgroup of G, then G is commutative (Everett and Ulam [1, p. 210]).

Ex. 5*. (a) Show that, in any ordered group, $mx + ny = ny + mx$ implies $x + y = y + x$ (B. Neumann).

(b) Show that, in any ordered group, $-a - b + a + b \ll |a| + |b|$, but that this is not true in Example 9 of §2.

Ex. 6*. Show that the free group with n generators can be made into an ordered group, using the method of Thm. 14 and Ex. 5b as guides (Everett and Ulam [1, §§6-7]).

Problem 100. Are Exs. 5a–5b valid for Lie l-groups?

Problem 101. Determine necessary and sufficient conditions that an abstract group be group-isomorphic with an ordered group.

Problem 102. Determine all ways in which the free group with n generators can be made into an ordered group, resp. an l-group. Same questions for the free Abelian group with n generators, if isomorphic ordered groups are identified.

8. Ordered fields. An *ordered ring* may be defined as a ring which is a simply ordered group under addition, in which

(21) the product of any two positive elements is positive.

Since $a(-b) = -ab$, this guarantees that the product of any positive element with a negative element is negative, and that the product of two negative elements is always positive. An ordered ring which is a field is called an *ordered field*.

Example 10. Let F consist of 0 and ordinary semi-infinite formal *power series* in x, with real coefficients a_k and with (positive or negative) integral exponents

$$\text{(F)} \qquad p(x) = a_n x^n + a_{n+1} x^{n+1} + a_{n+2} x^{n+2} + \cdots \qquad [a_n \neq 0].$$

If we define

$$\sum a_k x^k + \sum b_k x^k = \sum (a_k + b_k) x^k$$

and

$$\left(\sum a_k x^k\right)\left(\sum b_k x^k\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k,$$

we get a well-known field. If we define $f > 0$ to mean that the leading coefficient $a_n > 0$, we get an ordered field.

In Example 10, we could have taken coefficients in any ordered field without affecting the construction. Thus, by induction, we can make an ordered field out of power series in n variables. One can also construct *non-commutative* ordered fields (alias ordered skew fields or ordered division rings) as follows.[16]

Example 11. Let G consist of 0 and the power series

$$\text{(G)} \qquad g(y) = p_m y^m + p_{m+1} y^{m+1} + p_{m+2} y^{m+2} + \cdots \qquad [p_m \neq 0]$$

[16] D. Hilbert, *Grundlagen der Geometrie*, 7th ed.; K. Reidemeister, *Grundlagen der Geometrie*, p. 40. Ordered fields are also discussed by P. Dubreil, *Algèbre*, vol. 1.

with coefficients p_k in the ordered field of Example 10. Let addition and order be defined as in Example 10. But let the definition of multiplication stem from the basic formula $yx = 2xy$, so that if $p = \sum_n^\infty a_k x^k$,

$$yp = y\left(\sum_n^\infty a_k x^k\right) = \left(\sum_n^\infty 2^k a_k x^k\right)y = \tau(p)y,$$

and generally

$$\left(\sum a_{hi} x^h y^i\right)\left(\sum b_{jk} x^j y^k\right) = \sum 2^{ij} a_{hi} b_{jk} x^{h+j} y^{i+k}.$$

Since $p \to \tau(p)$ is an automorphism of the coefficient field, this defines a ring R. (This is like the basic construction of cyclic algebras and "crossed products.") Moreover one can extract inverses in G by successive divisions of leading coefficient by leading coefficient, with remainder of lower degree. We leave to the reader the proof that exact division of any monomial by any other (non-zero) monomial, on either side, is possible.

Generally, let F be any ordered field or skew field. Given positive a, b, F, by definition either $a \ll b$, or $b \ll a$, or $na \leqq b$ and $nb \leqq a$ for sufficiently large n. In the latter case, we write $a \sim b$, and say that a and b have the *same order of magnitude*. Since $\sim$ is an equivalence relation (we omit the proof), this terminology is legitimate; and we can even define an order of magnitude as one of the equivalence classes defined by $\sim$.

THEOREM 16. *The "orders of magnitude" of any ordered field or skew field themselves form an ordered group.*[17]

Proof. Since $nx \leqq b$ if and only if $anx = n(ax) \leqq ab$ and symmetrically, the "ordering" by $\ll$ is preserved under all group translations $x \to axa_1$, and so is the relation of having the same order of magnitude.

Thus in Example 10, this ordered group is the additive group of the integers; the leading exponent of $f(x)$ determines its order of magnitude; this interpretation is closely related to Ex. 3 of §7.

The theory of lattice-ordered rings and fields is not yet even in its infancy. Thus no system of postulates has been developed applicable to the algebra of $n \times x$ matrices $A = \| a_{ij} \|$, lattice-ordered by letting $A \geqq 0$ mean that every $a_{ij} \geqq 0$. Neither has a discussion been given, from the ordered ring point of view, of the Jordan algebra of $n \times n$ symmetric matrices, partly ordered by letting $A \geqq 0$ mean that A is non-negative definite.[18]

[17] See H. Hahn, *Uber die nichtarchimedischen Grossensysteme*, S.-B. Wiener Akad. Math.-Nat. Klasse Abt. IIa, 116 (1907), 601–53. Incidentally, Hilbert, op. cit., has shown that any ordered group can be embedded in the multiplicative group of an ordered field or skew field.

[18] The reader's attention is called to Ex. 2(c), §3; to P. Jordan, J. von Neumann, and E. Wigner, Annals of Math. 35 (1934), 29–64; to S. W. Steen, Proc. Lond. Math. Soc. 41 (1936), 361–92; 43 (1937), 529–43; 44 (1938), 398–411; to A. A. Albert, Bull. Am. Math. Soc. 46 (1940), 521–22; and to W. Prenowitz, Am. Math. Monthly 53 (1946), 439–49. Relevant also are Artin's penetrating papers on "formally real" fields, discussed in van der Waerden [1, Ch. X]. (See Ex. 1b below.) See also J. G. Mikusinski, Comptes Rendus 224 (1947), 1685–7.

Ex. 1. (a) Show that the positive elements of any ordered field, commutative or not, form an ordered group under multiplication.

(b) Show that in any ordered ring, any sum of squares is positive.

Ex. 2. Show that any Archimedean ordered field is isomorphic with a subfield of the ordered field of real numbers.

Ex. 3. Show that Example 10 contains the field of rational functions as a subfield. What power series does $1/(1 + x^2)$ correspond to?

Ex. 4. Show that, in Example 10, n need not be an integer, but might be any real number. (In this way we include irrational algebraic functions.)

Problem 103. Can Example 3 of §2 be made into an ordered ring?

9. Complete l-groups. The real numbers under addition, and many other l-groups of importance in analysis, satisfy the following condition.

DEFINITION. *A po-group G is called complete (σ-complete) if and only if every non-void (resp. countable) bounded set has a g.l.b. and a l.u.b.*

Let x be any element of any po-group G. If s is any upper bound for the set $\{nx\}$, then by invariance of order under group translation, so are $s + x$ and $s - x$. Therefore $\{nx\}$ cannot have a *least* upper bound unless $x \geqq 0$ and $x \leqq 0$, proving

LEMMA 1. *The set of all integral multiples (powers) of a non-zero element of a po-group cannot have a l.u.b.*

Therefore, apart from the trivial case $G = 0$, no po-group can be complete or even σ-complete in the sense of Ch. IV; this is why we have modified our terminology.

THEOREM 17. *Any subgroup of a σ-complete po-group G is Archimedean, and even "integrally closed," in the sense that*

$$(*) \qquad na \leqq b, \textit{ for all } n = 1, 2, 3, \cdots \textit{ and fixed } b, \textit{ implies } a \leqq 0.$$

Conversely, the completion by non-void cuts of any integrally closed po-group A is a complete po-group.[19]

Proof. By definition of σ-completeness, $na \leqq b$ in G for all $n = 1, 2, 3, \cdots$ implies that $c = \bigvee na$ exists. But this implies $c + a = \bigvee (n + 1)a \leqq \bigvee na = c$, since the set of $(n + 1)a$ is a subset of the set of all na. And this implies $a \leqq 0$.

Conversely, let A be any po-group; we form the completion $\bar{A}$ of A by non-void cuts, as follows. Any non-void subset X of A, the set $U(X)$ of whose upper bounds is not void, determines a unique cut[20] $(L(U(X)), U(X))$ in A—

[19] For this result see Arnold, Mat. Sbornik 36 (1929), 401–7; L. Kantorovitch, Doklady IV (1935), 13–16; Krull's v-Gruppensatz, *Idealtheorie*, p. 120; P. Lorenzen, Math. Zeits. 45 (1939), 533–53; A. H. Clifford, Annals of Math. 41 (1940), 465–73; J. Dieudonné, Bull. Soc. Math. France 69 (1941), 133–44; Everett and Ulam [1]. The non-commutative case was first treated by Everett and Ulam; the extension from directed to po-groups is new.

[20] Here $L(Y)$ denotes the set of all lower bounds of the set Y. We assume familiarity with Ch. IV, §7, in which $U(X)$ is denoted X^* and $L(Y)$, Y^+. Note that the two void cuts correspond to elements $\pm\infty$ respectively.

hence a unique element of $\bar{A}$. Moreover X and X_1 determine the same cut if and only if $U(X) = U(X_1)$. Conversely, every element of $\bar{A}$ is determined in this way by one or more X.

We define addition in $\bar{A}$ by letting $X + Y$ denote the set of all $x + y$ [$x \in X$, $y \in Y$]. This is never void; neither is $U(X) + U(Y)$. This addition is evidently associative; moreover the set A^- of $x \leqq 0$ in A can easily be proved to be an identity under addition in $\bar{A}$—i.e., $U(X + A^-) = U(A^- + X) = U(X)$, for all X. Finally, addition is *single-valued*: substitution of equal summands leaves sums equal. For if $U(X) = U(X_1)$, then $u \in U(X + Y)$ means $u \geqq x + y$ for all $x \in X$. This means $u - y \geqq x$, or $u - y \in U(X)$, or $u - y \in U(X_1)$, or $u - y \geqq x_1$ for all $x_1 \in X_1$, $y \in Y$, that is, $u \in U(X_1 + Y)$. Hence $U(X) = U(X_1)$ implies $U(X + Y) = U(X_1 + Y)$; similarly for right-hand summands. Again, $X \leqq X_1$ (interpreted equivalently as set-theoretic or order-inclusion) clearly implies $X + Y \leqq X_1 + Y$; hence addition conserves order. It therefore remains to show that inverses exist. This we now do.

Let $-U$ denote the set of additive inverses of elements of $U(X)$; consider $Z = X + (-U)$. Since $x \leqq u$ for all $u \in U(X)$, $z = x + (-u) \leqq 0$ for all $z \in Z$; hence $0 \in U(Z)$ and $U(Z) \geqq A^+$. To show that Z is the identity, it therefore suffices to show that every $c \in U(Z)$ is positive. Indeed, suppose $c \geqq x + (-u)$, that is, $c + u \geqq x$, for all $x \in X, u \in U$. Fix u_1. Then since $c + u_1 \geqq x$ for all $x \in X$, $u_2 = c + u_1 \in U(X)$. Therefore, for all $x \in X$, $c + u_2 = 2c + u_1 \geqq x$; hence $c + u_2 \in U(X)$. Iterating this process, we get $u_1, u_2, u_3, \cdots$ such that $c + u_n = nc + u_1 \geqq x$ for any $x \in X$. Hence $n(-c) = -nc \leqq -x + u_1$ for u_1, any $x \in X$, and all $n = 1, 2, 3, \cdots$. But by (*), this implies $-c \leqq 0$, or $c \geqq 0$, q.e.d.

COROLLARY. *A directed group is a subgroup of a complete l-group if and only if it is "integrally closed."*

For in a directed group G, every pair x, y has an upper bound, hence a l.u.b. if G is conditionally complete.

Ex. 1. Show that a *po*-group is σ-complete if and only if every finite or countable non-void set of positive elements has a greatest lower bound.

Ex. 2. (a) Show that if the positive elements of an l-group G satisfy the descending chain condition, G is complete.

(b) Show that the additive group of the integers is the only ordered group in which the positive elements satisfy the descending chain condition.

Ex. 3. Show that the partly ordered completion by cuts of any *po*-group G can be made into a semigroup, in which $x \geqq y$ implies $x + a \geqq y + a$ and $b + x \geqq b + y$ for all a, b. Show that if G is directed, this partly ordered semigroup is a conditionally complete lattice.

Ex. 4*. Show that not every Archimedean directed group is integrally closed.

Ex. 5*. Let S be a commutative semigroup under multiplication, in which the cancellation law holds and $ab = 1$ imply $a = b = 1$. Let G be the usual extension of S to a group; define a "v-ideal" of G as a subset V which contains, with any $g \in G$, all sg [$s \in S$].

(a) Show that the v-ideals of G form a complete l-group if and only if S satisfies the condition (**) $a^n \mid b^n c$ for fixed a, b, c and all n implies $a \mid b$.

(b) Extend to the non-commutative case (see Thm. 3).

Ex. 6*. Under what conditions can the completion by cuts of a directed group G be made into an l-semigroup?

10. Infinite distributivity. By definition, any group translation of an l-group is a lattice automorphism. Hence it carries infinite joins and meets into infinite joins and meets, respectively. This fact may be expressed formally in the infinite distributive laws

$$(22)\qquad \begin{aligned} a + \vee x_\alpha &= \vee (a + x_\alpha), \qquad a + \wedge x_\alpha = \wedge (a + x_\alpha), \\ \vee x_\alpha + b &= \vee (x_\alpha + b), \qquad \wedge x_\alpha + b = \wedge (x_\alpha + b). \end{aligned}$$

Similarly, since every correspondence of the form $x \to a - x + b$ is a dual automorphism, we have the law

$$(22') \qquad a - \vee x_\alpha + b = \wedge (a - x_\alpha + b), \qquad \text{and dually.}$$

Now let $v = \vee x_\alpha$. Then, for all a and α,

$$0 \leqq (a \frown v) - (a \frown x_\alpha) \leqq v - x_\alpha \text{ by } (20).$$

But $\wedge (v - x_\alpha) = v - \vee x_\alpha = v - v = 0$ by (22′); and by what we have just seen, $0 = \wedge [(a \frown v) - (a \frown x_\alpha)] \leqq \wedge (v - x_\alpha)$; hence

$$0 = \wedge [(a \frown v) - (a \frown x_\alpha)] = (a \frown v) - \vee (a \frown x_\alpha).$$

Transposing, we get the first of the infinite distributive laws

$$(23) \qquad a \frown \vee x_\alpha = \vee (a \frown x_\alpha) \quad \text{and} \quad a \smile \wedge x_\alpha = \wedge (a \smile x_\alpha);$$

the second follows by duality. Summarizing, we have[21]

Theorem 18. *The infinite distributive laws* (22)–(23) *are valid in any complete l-group.*

Corollary. *Any σ-complete l-group G is a topological group and a topological lattice in its order-topology: $x_n \to x$ and $y_n \to y$ imply $x_n + y_n \to x + y$, $x_n \frown y_n \to x \frown y$, $x_n \smile y_n \to x \smile y$.*

Proof. The case of the group operation is typical. We let $u_n = \vee_{h>n} x_h$ and $v_n = \vee_{k>n} y_k$; then by definition (Ch. IV, §8), $\wedge u_n = x$ and $\wedge v_n = y$. Also by definition,

$$\begin{aligned} \text{Lim sup } \{x_n + y_n\} &= \bigwedge_n \{ \bigvee_{m>n} (x_m + y_m)\} = \bigwedge_n \{ \bigvee_{h,k>n} (x_h + y_k)\} \\ &= \bigwedge_n \{ \bigvee_{h>n} [\bigvee_{k>n} (x_h + y_k)]\} = \bigwedge_n \{ \bigvee_{h>n} [x_h + v_n]\} = \bigwedge_n \{u_n + v_n\}, \end{aligned}$$

[21] This result is due to Kantorovitch [1, Thms. 10–21], who assumed commutativity. As noted in G. Birkhoff [6] (cf. Thm. 19 below), commutativity does not enter into the proof. See also C. J. Everett, Duke Jour. 11 (1944), 109–19, and Everett and Ulam [1, pp. 211–12], for the Ex. below; also [LT, §140].

using (22) twice. Again, given m, n, $u_m + v_n \leqq u_{m+n} + v_{m+n}$; hence, using (22) twice more,

$$\bigwedge_n \{u_n + v_n\} \leqq \bigwedge_{m,n} \{u_m + v_n\} = \bigwedge_m \{ \bigwedge_n (u_m + v_n)\} = \bigwedge_m \{u_m + y\} = x + y.$$

Dually, Lim inf $\{x_n + y_n\} \geqq x + y$, completing the proof. The proof for the lattice operations uses (23) in place of (22); see Thm. 14, Ch. IX.

Ex. 1. In an l-group G, let $x_n \to x$ mean that there exist $t_n \uparrow x$, $u_n \downarrow x$, such that $t_n \leqq x_n \leqq u_n$ for all n. Call $\{x_n\}$ *o-regular* whenever, for some $v_n \downarrow 0$, $| x_n - x_{n+p} | \leqq v_n$ for all positive integers n, p. Prove that if every monotone o-regular sequence converges to a limit, then every o-regular sequence o-converges. Do these imply that G is σ-complete? Note that every convergent sequence is o-regular.

11. Closed l-ideals. Let J be any complemented l-ideal of an l-group G, with complement J'. Then any $a \in G$ has one "component" a' in G/J, and one a'' in G/J'; moreover since $J \frown J' = 0$, a is determined by the pair (a', a''). Further, J consists of the pairs $(0, a'')$, J' of the pairs $(a', 0)$; and, since $J + J' = G$, $(a', 0)$ and $(0, a'')$ exist for any $(a', a'') \in G$. This proves that *complemented l-ideals correspond to direct factors of G.*

We now extend our earlier definition of disjointness, by letting $a \perp b$ (in words, a and b are disjoint) mean $| a | \frown | b | = 0$. Using the terminology and notation of Ch. IV, §5, we then define J^* as the set of all $b = (b', b'') \perp (0, a'')$ for all $a = (0, a'') \in J$. This clearly means $| b'' | \frown | a'' | = 0$ for all a'' (including $a'' = b''$)—hence $b'' = 0$. Conversely, always $(b', 0) \perp (0, a'')$. Therefore if J is complemented, $J' = J^*$ and $J = J'' = J^{**}$.

More generally, let S^* be the "polar" of *any* subset S of a *complete* l-group G. If $\{b_\alpha\}$ is any subset of S^*, meaning that $| b_\alpha | \frown | s | = 0$ for all $s \in S$, and if $\bigvee | b_\alpha |$ exists (i.e., if the set of all b_α is bounded), then by Thm. 18, $\bigvee | b_\alpha | \frown | s | = 0$, whence, since $0 \leqq | \bigvee b_\alpha | \leqq \bigvee | b_\alpha |$, $| \bigvee b_\alpha | \frown | s | = 0$, and so $\bigvee b_\alpha \in S^*$. Further, if $b \in S^*$ and $c \in S^*$, then

$$(24) \qquad | b + c | \leqq | b | + | c | + | b |,$$

since $- | b | - | c | - | b | \leqq b + c \leqq | b | + | c | + | b |$; hence by Thm. 6, $b + c \in S^*$. Also, if $b \in S^*$ and $| c | \leqq | b |$, then $c \in S^*$—and, in particular, $-b \in S^*$. Hence S^* is a *closed absolute subgroup* of G, in the sense that: (i) S^* is a subgroup, (ii) if $b \in S^*$ and $| c | \leqq | b |$, then $c \in S^*$, (iii) if every $b_\alpha \in S^*$ and $\bigvee b_\alpha$ exists in G, then $\bigvee b_\alpha \in S^*$. We now discuss closed absolute subgroups, ultimately showing that they are complemented l-ideals.

Evidently any closed absolute (i.e., convex) subgroup which is a normal subgroup in the group-theoretic sense is a closed l-ideal in the following sense.

DEFINITION. *An l-ideal J of a complete l-group G is called closed*[22] *if and only if it contains, with any bounded subset* $\{x_\alpha\}$, *also* $\bigvee x_\alpha$.

[22] Closed l-ideals are the "familles complètes" of F. Riesz [2]. Riesz proved Thm. 19 for principal l-ideals, assuming commutativity. We avoid this assumption.

Remark. Since the correspondence $x \to -x$ leaves J setwise invariant and inverts order, it follows that J also contains $\bigwedge x_\alpha$. Further, since any l-ideal is convex, closure in the above sense is equivalent to topological closure in the order topology.

For any subset T of a complete l-group G, clearly $T \frown T^* = 0$. We next show that, if T is a closed absolute subgroup, then also $T + T^* = G$. To show this, we define the T-component x_T of any $x \geqq 0$ of G, by $x_T = \sup_{t \in T} x \frown t$; by hypothesis, $x_T \in T$. Clearly $0 \leqq x_T \leqq x$; hence, writing $x = x_T + u$, we have $u \geqq 0$. Moreover for any $t_1 \in T$, since $x_T + |t_1| \in T$, we have

$$x_T \geqq x \frown (x_T + |t_1|) = (x_T + u) \frown (x_T + |t_1|) = x_T + (u \frown |t_1|),$$

whence $u \frown |t_1| = 0$ for all $t_1 \in T$, and so $u \in T^*$. Thus every *positive* $x \in G$ can be written $t + u$ $[t \in T, u \in T^*]$. But now, the positive elements of T and T^*, being disjoint, are permutable (§4, Lemma 1). Hence, for any $x \in G$, we have

$$\begin{aligned} x = x^+ - (-x^-) &= (t + u) - (t_1 + u_1) = t + u - u_1 - t_1 \\ &= (t - t_1) + (u - u_1), \end{aligned}$$

so that $T + T^* = G$. Moreover since the elements $t - t_1$ of T are permutable with those $u - u_1$ of T^*, both T and T^* are *normal* subgroups of $G = T + T^*$; hence both are (closed) l-ideals. Since they are complementary, we conclude

THEOREM 19. *For any l-ideal J of a complete l-group G, the following assertions are equivalent:* (i) *J is complemented*, (ii) $J = J^{**}$, (iii) *J is closed. If they hold, then J^* is the complement of J.*

Since any intersection of closed l-ideals is evidently closed, we obtain the following useful corollary.

COROLLARY. *The closed (i.e., complemented) l-ideals of any complete l-group form a complete Boolean algebra.*

Ex. 1. Show that any positive element a of a complete l-group G is a weak unit for the closed l-ideal a^{**}.

Ex. 2. Show that any l-group is a topological lattice and a topological group in its order topology.

Ex. 3. Let S be any subset of a complete l-group G. Show that G is the direct union of S^* and S^{**}.

Problem 104. Is any *po*-group a topological group and a topological lattice in its interval topology?

Problem 105. Is there a common abstraction which includes Boolean algebras (rings) and l-groups as special cases? (Note that all Boolean rings can be completed, but not all l-groups.)

12. Complete l-groups are commutative. Let G be any complete l-group. For any element $c \in G$, we have $c^- \in (c^+)^*$; hence the decomposition of G into the complementary l-ideals $(c^+)^{**}$ and $(c^+)^*$ allows us to reduce any question regarding any $c \in G$ to the two special cases $c \geqq 0$ and $c \leqq 0$. We shall use this principle several times in establishing the following remarkable result.[23]

THEOREM 20. *Any complete l-group G is commutative.*

LEMMA 1. *If all positive elements of an l-group G are permutable, then G is commutative.*

Proof. $a + b = a^+ + a^- + b^+ + b^-$, $b + a = b^+ + b^- + a^+ + a^-$. If positive elements are permutable, then a^+ and a^- are permutable with b^+ and b^-; hence $a^+ + a^- + b^+ + b^- = b^+ + a^+ + a^- + b^- = b^+ + b^- + a^+ + a^-$, completing the proof.

Hence, in Thm. 20, we need only consider the case of positive a and b. Again, by the remark above, we can confine attention to the cases $a - b \geqq 0$ and $b - a \geqq 0$, and to the cases $-a - b + a + b \geqq 0$ and $-a - b + a + b \leqq 0$. This gives us four cases, of which $a \geqq b \geqq 0$ and (by left-right symmetry) $b + a \geqq a + b$ is typical. We define t by $-a + b + a = b + t$, so that $t \geqq 0$. We further define $b_n = -na + b + na$, $t_n = -na + t + na$, for every integer n; thus the b_n, t_n are the transforms of b, t under the group of inner automorphisms generated by $x \to -a + x + a$. Observe that since $0 \leqq b \leqq a$, the interval $[0, a]$ being invariant under all these inner automorphisms, we have $0 \leqq b_n \leqq a$ for all a. Moreover we can prove $b_{n+1} = b + t + t_1 + \cdots + t_n$ by induction, since

$$-a + (b + t + t_1 + \cdots + t_{n-1}) + a = -a + b + a + \sum_{i=1}^{n-1} (-a + t_i + a)$$

$$= (b + t) + t_1 + t_2 + \cdots + t_n.$$

Now suppose $t_1 = -a + t + a \geqq t$. Then, for any integer n, $t_{n+1} - t_n = -na + (t_1 - t) + na \geqq 0$, since inner automorphisms preserve order. Hence $0 \leqq t \leqq t_1 \leqq t_2 \leqq t_3 \leqq \cdots$, and, for any positive integer n, we have

$$nt \leqq t + t_1 + t_2 + \cdots + t_{n-1} \leqq -b + b_{n+1} \leqq a.$$

Hence, by Thm. 17, $t \leqq 0$; but $t \geqq 0$ by hypothesis; hence $t = 0$.

Similarly, consider the case $t_1 \leqq t$. Then we have as above $0 \leqq t \leqq t_{-1} \leqq t_{-2} \leqq t_{-3} \leqq \cdots$. Also,

$$b = a + (b + t) - a = a + b - a + a + t - a = a + b - a + t_{-1},$$

and so $a + b - a = b - t_{-1}$. By induction on n, we can show that

$$b_{-n-1} = a + (b - t_{-1} - t_{-2} - \cdots - t_{-n}) - a = b - t_{-1} - t_{-2} - \cdots - t_{-n-1}.$$

[23] Known for some time in the simply ordered case; conjectured for l-groups in G. Birkhoff [6]. The first proof for l-groups was given by Iwasawa, Jap. Jour. Math. 18 (1943), 777–89. The present proof follows the lines suggested in G. Birkhoff [6].

Hence, for any positive integer n,

$$nt \leqq t_{-n} + t_{-n-1} + \cdots + t_{-2} + t_{-1} = -a - b_{-n-1} + a + b = -b_n + b \leqq b.$$

Hence if $t_1 \leqq t$, $t \leqq 0$ and so $t = 0$ as before.

But, by use of components, we can reduce the general case to the two cases $t_1 \geqq t$ and $t_1 \leqq t$, projecting onto $(t_1 - t)^{+*}$ and $(t_1 - t)^{+**}$. Hence, in any case, $t = 0$, and $a + b = b + a$, completing the proof.

Corollary. *Any Archimedean directed group is commutative.*

Ex. 1. Prove Lemma 1 in full detail.[24]

Ex. 2. (a) By a *component* of a positive element e of an l-group A is meant an element e' such that $e' \frown (e - e') = 0$. Prove that the components of any positive $e \in A$ form a Boolean algebra.

(b) Show that if A is a complete l-group with weak unit e, then the factors of A in direct decompositions correspond one-one with the components of e.

Ex. 3. Show that e is a weak unit of a complete l-group A if and only if $x \frown ne \to x$ for all $x \in A$.

Ex. 4. Show that any complete l-group is either isomorphic with the ordered group of the integers, or is isomorphic with the ordered group of all real numbers, or is directly decomposable.

Ex. 5*. Show that a complete l-group either satisfies the chain condition, or has at least the cardinal number of the continuum.

Problem 106. Find necessary and sufficient conditions that an abstract group be group-isomorphic with an l-group. (Cf. Problem 101, §7.)

13. Chain condition for elements. We now consider l-groups whose elements satisfy the following *chain condition*

(C) every non-void set of positive elements includes a *minimal* member.

In such an l-group G, any element which covers 0 will be called a *prime*.

It is easy to prove that G is a complete l-group, and so commutative. However, we prefer to give a self-contained discussion from basic principles, assuming only the algebraic formulas of §4.

Lemma 1. *Any two primes are permutable.*

This follows from Lemma 1 of §4. It is a corollary that the primes generate an Abelian subgroup, consisting of all elements which can be expressed as sums $n_1p_1 + \cdots + n_sp_s$ of multiples of a finite number of distinct primes, with positive or negative integers n_i as coefficients.

Now let $a > 0$ be given, and consider all those differences $a - \sum n_ip_i$ which are positive. By the chain condition, one of these must be minimal, and so cannot contain any prime q (or else $a - (\sum n_ip_i + q)$ would be smaller). Again, by the chain condition, every positive element b except 0 contains a prime,

[24] Ex. 1 is due to Freudenthal [1]; Ex. 2 to S. Bochner and R. S. Phillips, Annals of Math. 42 (1941); Exs. 3–4 to G. Birkhoff [6].

namely, some minimal x such that $0 < x \leqq b$. Hence our minimal difference must be 0, so that $a = \sum n_i p_i$.

But every element can be expressed as a difference of positive elements: $c = c^+ - (-c)^+$ for all c, hence

LEMMA 2. *Any element not* 0 *can be expressed as a sum of integral multiples of a finite number of distinct primes, as* $a = n_1 p_1 + \cdots + n_s p_s$.

Putting Lemmas 1–2 together, we infer that G is Abelian. Again, if all n_i are positive, then clearly a is positive. Conversely, distinguishing positive and negative coefficients, if $a = m_1 p_1 + \cdots + m_r p_r - n_1 q_1 - \cdots - n_s q_s \geqq 0$, then $m_1 p_1 + \cdots + m_r p_r \geqq n_s q_s + \cdots + n_1 q_1$; but by Thm. 6, since distinct primes are disjoint, this implies $n_s q_s + \cdots + n_1 q_1 = 0$. Hence

LEMMA 3. *In Lemma* 2, *a is positive if and only if every n_i is positive.*

It is a corollary that a is zero (positive and negative) if and only if every n_i is positive and negative, which is absurd. It is a corollary that the representation of Lemma 1 is unique; for if a had two different representations, their difference would represent 0, whence all coefficients would be zero. We can summarize

THEOREM 21. *Let G be any l-group which satisfies the chain condition. Then G is commutative, and each non-zero element of G can be expressed uniquely as a sum of integral multiples of distinct primes. Such a sum is positive if and only if all coefficients are positive.*[26]

Ex. 1. Show that, in Thm. 21, G is determined to within isomorphism by the cardinal number of the set of its primes.

Ex. 2. Show that the l-ideals of G correspond one-one to the subsets of its primes, and form an atomic Boolean algebra.

14. Structure of non-Archimedean, commutative l-groups. We can obtain an interesting analysis of the structure of any commutative l-group, the (distributive) lattice of whose l-ideals has finite length. Indeed, by Thm. 13, any commutative l-group in which the l-ideal 0 is meet-irreducible is simply ordered. From this (cf. Ex. 1, §7) we conclude

LEMMA 1. *The structure lattice of a commutative l-group in which the l-ideal 0 is meet-irreducible is a chain.*

But now if J is any l-ideal of an l-group A, the l-ideals of A which contain J form a lattice isomorphic with the lattice of all l-ideals (congruence relations) of A/J; indeed, this "Second Isomorphism Theorem" is a principle of universal algebra. Combining this observation with Lemma 1, we get

LEMMA 2. *In the distributive lattice of all l-ideals of a commutative l-group, the elements which contain any meet-irreducible element form a chain.*

---

[26] For the commutative case, see M. Ward, Duke. Jour. 6 (1940), pp. 641–651; also A. Clifford, Bull. Am. Math. Soc. 40 (1934), p. 329, Thm. 2. The result was freed from the hypothesis of commutativity in G. Birkhoff [6, Thm. 37].

Hence the sets of meet-irreducible l-ideals which are contained in the different maximal l-ideals of the l-group are without common elements, and are unrelated by inclusion relations. It follows that either there is only one maximal proper l-ideal, or the partly ordered set of the meet-irreducible l-ideals is a cardinal sum of two or more components. In the latter case, by Thm. 5 of Ch. IX and formula (6) of Ch. I, the lattice of l-ideals is a direct union. Hence it contains two proper complementary l-ideals, and by paragraph one of §11 the l-group is a direct union. We thus reach the following useful conclusion.

THEOREM 22. *Let G be any commutative l-group, the lattice of whose l-ideals has finite length. Then either G is a direct union (i.e., cardinal product), or it contains a maximal l-ideal M which contains every other proper l-ideal.*

Ex. 1. For given *po*-groups G and H, let $G + H$ denote the set of all couples (g, h). In $G + H$, let $(g, h) + (g', h')$ be defined as $(g + g', h + h')$, and let $(g, h) \geqq (g', h')$ mean $g \geqq g'$ and $h \geqq h'$. Show that the direct union (cardinal product) $G + H$ so defined is always a *po*-group, and is an l-group if and only if both G and H are.

Ex. 2. For given *po*-groups G and H, let $G \circ H$ denote the same group as the $G + H$ of Ex. 1, but let $(g, h) \geqq (g', h')$ be defined to mean $g > g'$, or $g = g'$ and $h \geqq h'$. Show that $G \circ H$ is always a *po*-group, and is an l-group if and only if G is simply ordered and H is an l-group, except in the trivial case that H consists of 0 alone. (Cf. Ch. II, §7, Ex. 2.)[38]

Ex. 3. For any l-group G, let $S(G)$ denote the lattice of all l-ideals of G, ordered by set-inclusion. Show that, in the notation of Exs. 1–2 and the generalized arithmetic notation of Ch. I, $S(G + H) = S(G) \cdot S(H)$, whereas $S(G \circ H) = S(H) \oplus S(G)$.

[38] For further results see the Harvard Doctoral Thesis of Murray Mannos (1942); see also H. Shimbireva, Math. Sbornik 20 (1947), 145–78.

CHAPTER XV

VECTOR LATTICES

1. Introduction. Abstract function spaces, unknown forty years ago, have shed so much light on the theory of functions that their study is now recognized as an important branch of mathematics. Usually, as in the case of Hilbert space and Banach spaces, this study has been based on an analysis of the properties of *distance* in vector spaces.[1]

The author believes that an analysis of the properties of *order* in function spaces is equally deserving of attention, and may prove equally fruitful. The present chapter is devoted to this analysis; in addition, all of the material on l-groups and commutative l-groups, deduced in Chapter XIV, is applicable. We begin by defining partly ordered vector spaces and vector lattices.

DEFINITION. *A partly ordered vector space is a vector space V with real scalars, which is a po-group under addition, and in which, for any positive scalar λ, $x \to \lambda x$ is an automorphism. If V is a lattice, it is called a vector lattice; if it is conditionally complete or σ-complete, it is called a complete or σ-complete vector lattice, respectively.*

Thus vector lattices, complete vector lattices, and σ-complete vector lattices are respectively l-groups, complete l-groups, and σ-complete l-groups, in which multiplication by scalars is possible, conforming to the usual rules of vector algebra, and also to the rule that $x \to \lambda x$ preserves order if $\lambda > 0$, and inverts it if $\lambda < 0$. We shall assume below familiarity with the contents of Ch. XIV, in which such l-groups have been discussed. We recall also that any vector space is a *commutative* group under addition.

Vector lattices over ordered fields other than the real field may also be studied.[2]

LEMMA 1. *In a vector lattice, every l-ideal is a subspace, and hence a congruence module for all algebraic operations.*

Proof. Let J be any l-ideal. If $a \in J$, then $a^+ \in J$ and $a^- \in J$. Hence, for any positive integer n, $na^+ \in J$ and $-na^- \in J$. Hence for any positive λ, and so for any λ, $\lambda a^+ \in J$ and $\lambda a^- \in J$. Therefore $\lambda a = \lambda(a^+ + a^-) = \lambda a^+ + \lambda a^- \in J$.

---

[1] See M. H. Stone, *Linear transformations in Hilbert spaces and their applications to analysis*, New York, 1932, and S. Banach [1].

The concept of vector lattice is due to Kantorovitch [1] (and earlier announcements). Freudenthal [1] developed the idea independently, attributing his inspiration to F. Riesz [1].

[2] See A. F. Monna, Nederl. Akad. Wet. 52 (1943), 308–21 and 654–61, and ibid. 53 (1944), 385–99. Postulates for complete vector lattices have been discussed by A. Judin, Uchenye Zapiski Leningrad 83 (1941), 57–61.

In [LT], l-ideals were called "normal subspaces."

Ex. 1. (a) Let G be any l-group which is also a vector space. Show that, for any positive rational scalar λ, $x \to \lambda x$ is a lattice-automorphism.

(b) Show that this need not be true for multiplications by irrational scalars in the vector space of all real numbers, under some orderings. (Hint: Cf. Thm. 14, Ch. XIV.) Show that it need not be true even under orderings making the real numbers into a complete l-group. (Hint: Use group-automorphisms.)

Ex. 2. Show that, in any σ-complete vector lattice, the operation of multiplication by a real scalar λ may be defined in terms of addition and order, and so need not be introduced as an undefined primitive concept.

Ex. 3. In the plane of all vectors (x, y), let $(x, y) \geqq 0$ be defined to mean $x \geqq 0$ and $y \geqq \sqrt{x}$; and let $(x, y) \geqq (x', y')$ mean that $(x - x', y - y') \geqq 0$. Which of the postulates for a vector lattice fails?

2. Examples. The simplest vector lattice, and the prototype for all vector lattices, is of course the real number system R. This is a one-dimensional vector space, having the positive numbers and zero as its non-negative elements. By Lemma 2 of §6, Ch. XIV, combined with Thm. 15 of Ch. XIV, one can show that R is the *only* vector lattice without proper l-ideals (i.e., the only "simple" vector lattice in the sense of universal algebra). Again, we have

LEMMA 2. *Any direct union of vector lattices is a vector lattice.*

The proof is left to the reader. It is also easy to show that if the original vector lattices are complete or σ-complete, then so is their direct union. It is a corollary that the spaces R^n of all vectors $[x_1, \cdots, x_n]$ with n real components, R^d of all infinite sequences $x_1, x_2, x_3, \cdots$ of real numbers, and R^c of all real functions $f(x)$ defined on the interval $0 \leqq x \leqq 1$ are complete vector lattices. These notations are self-explanatory, if one admits the power notation of Ch. I, and imagines d and c as denoting countable infinity resp. the power of the continuum.

It is also clear that any subspace of a vector lattice, which is a sublattice as well, is a vector lattice. That is, if a subset contains with any f and g also $f + g$, $f \smile g, f \frown g$, and every λf, then it is a vector lattice relative to the same operations.

These hypotheses are satisfied by the following sets of functions: the subset B of R^c consisting of all bounded functions; the subset (b) of R^d consisting of all bounded sequences; the subset C of R^c consisting of all continuous functions; the subset (c) of R^d consisting of all convergent sequences; more generally, by the continuous functions $C(X)$ on any topological space X. They are also satisfied by: the set $D(X)$ of functions on any such X which admit only a finite number of discontinuities; the set M of measurable functions (in the sense of Lebesgue) on the real line; the subset M^p having summable pth powers; the set (l^p) in R^d of all sequences with finite $\sum_{k=1}^{\infty} |x_k|^p$.

Finally, let Γ be any (infinite) group of one-one transformations of a space X into itself, and call a function "almost periodic" (in the sense of Bochner) when every infinite sequence of its transforms under Γ contains a uniformly convergent subsequence. Then the real functions on X almost periodic under Γ satisfy our hypotheses.[3]

Most of these examples are discussed as metric or topological vector spaces in Banach [1], whose notation we have adopted whenever convenient.

We can determine all vector lattices of finite dimension, as follows.[4] Any such vector lattice V is either a direct union of vector lattices of lower dimension, or it contains a unique maximal l-ideal M, by Thm. 22 of Ch. XIV. This M will itself be a vector lattice of lower dimension, and may be treated by induction; moreover by paragraph one of the present section, the quotient-algebra V/M is the real number system R. It is now easy to show that $V = R \circ M$, in the sense of Ex. 2 of §14, Ch. XIV. We conclude

THEOREM 1. *Every finite-dimensional vector lattice can be built up from R by direct and lexicographic union.*

COROLLARY. *Every Archimedean finite-dimensional vector lattice is isomorphic to R^n, for some n.*

Infinite-dimensional Archimedean vector lattices need not be even isomorphic to a subalgebra of $R^{\aleph}$, for any cardinal number $\aleph$. As noted by Nakayama (Proc. Imp. Acad. Tokyo 18 (1942), 1–4), a vector lattice V can be represented as such a subalgebra if and only if the intersection of its maximal l-ideals is 0. Kaplansky has noted that the real functions on $0 \leqq x \leqq 1$, continuous except at a finite number of simple poles of second order, $\alpha_1/(x - a_1)^2$, form an Archimedean vector lattice, the intersection of whose maximal l-ideals consists of all continuous functions and so is not 0.

Ex. 1. (a) Show that if S is any vector sublattice (subalgebra) of any power $R^{\aleph}$ of R, then the intersection of its maximal l-ideals is 0.

(b) Using the result of paragraph one of §2, prove that conversely, if the intersection of the maximal ideals M of a vector lattice V is 0, then V is a vector sublattice of some power of R.

Ex. 2. Let V be an n-dimensional vector lattice; let M be a proper l-ideal of V which contains every proper l-ideal, so that $V/M = R$; let e be any positive element not in M.

(a) Show that, for any $x \in M$, we have $x \ll e$. (Hint: Consider the principal l-ideal with strong unit $|x|$.)

(b) Infer that, for any $x \in M$, $\lambda e + x \geqq 0$ if and only if $\lambda > 0$, or $\lambda = 0$ and $x \geqq 0$; that is, infer that $V = R \circ M$.

Ex. 3. Show that there are respectively 1, 2, 3, 8, 18 non-isomorphic vector lattices of dimensions 1, 2, 3, 4, 5.

3. Other examples; completeness. Other vector lattices can be constructed by forming quotient-spaces (i.e., homomorphic images) V/J of known vector lattices V, modulo l-ideals J.

Function theory abounds in examples of l-ideals of vector lattices. For instance, the set of functions equal to zero except on a finite set is an l-ideal in

[3] If $h = f \smile g$, and $h(aT_n)$ is any sequence of transforms of h, then we can choose a subsequence and a subsubsequence on which both f and g converge uniformly, whence so does h.

[4] This is the main result of the Harvard Doctoral Thesis of Murray Mannos (1942).

R^d, R^c, and in their vector sublattices. So is the set B of bounded functions. Moreover if M and M^p are defined as in §2, then every M^p is an l-ideal of M; so is every (l^p) an l-ideal of R^d.

Similarly, the set N of functions vanishing except on a set of Lebesgue measure zero (so-called "null functions") is an l-ideal of R^c and its vector sublattices. It is even a σ-ideal, in the sense that it contains with any countable set f_i, the least upper bound $\vee f_i$.

Furthermore, the quotient-algebras ("vector quotient-lattices") M/N and M^p/N define the usual "spaces" S of measurable functions and L^p, as vector lattices. Another interesting vector lattice is the space $(M \frown B)/(N \frown B)$ of bounded measurable functions modulo null functions.

It is a curious fact that L^2 and (l^2), though equivalent as metric linear spaces (to Hilbert space), are not isomorphic as vector lattices. For there exist in (l^2) positive elements whose positive subelements are simply ordered; L^2 contains no such elements.

We have already observed that R^n, R^d, and R^c are complete vector lattices. Moreover since l-ideals are convex, we know

Theorem 2. *Any l-ideal of a complete (σ-complete) vector lattice is itself complete (resp. σ-complete).*

It is a corollary that the spaces B, (b), (l^p) and N are complete vector lattices.

Now consider the space S of measurable functions $f(x)$, modulo null functions. Let $X(f, a)$ denote the set on which $f(x) \leqq a$. Then $X(f, a)$ is an order-preserving function from the infinite interval R: $(-\infty, +\infty)$ to the complete Boolean algebra $\bar{M}$ of Thm. 15, Ch. X. Moreover if $X(f, a) = X(g, a)$ for all a, then the set on which $|f(x) - g(x)| < 1/n$ for all n is null; hence $f(x) - g(x)$ is a null function and $f = g$. Again, for any $f \in S$, $\inf_a X(f, a) = 0$ and $\sup_a X(f, a) = I$. Conversely, any $X(a)$ having the properties just described is an $X(f, a)$—and $f(x)$ can be constructed through approximating step-functions assuming countably many distinct values. Since, finally, $f \geqq g$ is equivalent to $X(f, a) \leqq X(g, a)$ for all a, we conclude

Lemma 3. *The space S is lattice-isomorphic with the set of functions from R to $\bar{M}$ which are isotone and satisfy* $\inf_a X(a) = 0$ *and* $\sup_a X(a) = I$.

But this is a convex subset of the lattice $\bar{M}^R$, in the notation of Ch. I, §7, and the latter is complete since $\bar{M}$ is. Hence

Theorem 3. *The space S of measurable functions modulo null functions is a complete vector lattice.*

It is a corollary that the vector lattices L^p and SB are complete, since they are l-ideals (convex subsets) of the space S. On the other hand, the space C is not even σ-complete.

Ex. 1. Prove that the space C is not σ-complete.

Ex. 2. (a) Call a vector lattice "σ-full" if, whenever $a_i \frown a_j = 0$ for all $i \neq j$, $\vee a_i$ exists. Show that M is σ-full.

(b) Show that any commutative l-group can be extended to a σ-full l-group, and similarly for vector lattices.

Problem 107. Is every vector lattice a homomorphic image of a subalgebra of a direct union of replicas of R? (Cf. §13.)

4. Order and star topologies. The reader may recall, from Ch. IV, §§8–9, the definitions of order-convergence and star-convergence for sequences in general σ-lattices. We shall now consider special properties of these topologies, true for vector lattices.

We have already shown in §10 of Ch. XIV that the algebraic operations $x + y$, $x \frown y$, $x \smile y$ were continuous in the order topology of any σ-complete l-group. Actually, by taking some care about the existence of limits, the proofs may be extended to arbitrary l-groups. Thus in particular, in any l-group,

$$\text{(1)} \qquad \text{If} \quad f_n \downarrow 0 \text{ and } g_n \downarrow 0, \quad \text{then} \quad (f_n + g_n) \downarrow 0.$$

We shall now prove the continuity of scalar multiplication.

LEMMA 4. *Let V be any σ-complete vector lattice. Then*

$$\text{(2)} \qquad \textit{If} \quad \lambda_n \to 0 \quad \textit{and} \quad f \quad \textit{is fixed, then} \quad \lambda_n f \to 0,$$

$$\text{(3)} \qquad \textit{If} \quad \lambda_n \to \lambda \quad \textit{and} \quad f_n \to f, \quad \textit{then} \quad \lambda_n f_n \to \lambda f.$$

Proof of (2). We shall show that $|\lambda_n f| = |\lambda_n| \cdot |f| \to 0$. But in this case we can show that $\text{Lim sup} |2\lambda_n f| = 2 \text{ Lim sup} |\lambda_n f| = \text{Lim sup} |\lambda_n f| \geqq 0$, whence $\text{Lim sup} |\lambda_n f| = 0$. This shows $|\lambda_n f| \to 0$, implying $\lambda_n f \to 0$.

Proof of (3). $|\lambda_n f_n - \lambda f| \leqq (\sup |\lambda_n|) \cdot |f_n - f| + |\lambda_n - \lambda| \cdot |f|$, and the right-hand side order-converges to zero by (2).

Combining the preceding results, we get

THEOREM 4. *Under its order topology, any σ-complete vector lattice is a topological linear space and topological lattice.*

But it is easy to show that in any case, functions continuous with respect to a convergence topology are ipso facto continuous in the associated star-topology (one need only take successive subsequences from arbitrary sequences). This gives the

COROLLARY. *Under its star topology, any σ-complete vector lattice is a topological linear space and topological lattice.*

Ex. 1. Show that (2) is not true in all vector lattices.

Ex. 2. Show that star-convergence in the space S is equivalent to "convergence in measure," in the usual sense that $f_n \to 0$ means that, given $\epsilon > 0$, N exists so large that for all $n > N$, $|f_n(x)| \geqq \epsilon$ on a set of measure at most ϵ. ([LT, p. 113]; Kantorovitch, Comptes Rendus Paris 201 (1935), p. 1457.) Show that order-convergence is "convergence almost everywhere."

5. Relative uniform convergence. Following a basic idea of E. H. Moore,[5] we shall say that a sequence $\{f_n\}$ of elements of a vector lattice converges "relatively uniformly" to an element f, if and only if, for some u and $\lambda_n \downarrow 0$, $|f_n - f| \leqq \lambda_n u$. First we shall correlate this relative uniform topology with the order topology.

LEMMA 5. *In any σ-complete vector lattice, a sequence $\{f_n\}$ order-converges to f if and only if $|f_n - f| \leqq w_n$ for some $w_n \downarrow 0$.*

Proof. Since $x \to x - f$ is a lattice automorphism which leaves absolutes of differences unchanged, we can assume $f = 0$. In this case, $w_n = \bigvee_{k \geqq n} |f_k|$ provides the desired sequence. The converse is immediate, since $\operatorname{Lim\,sup} |f_n| \leqq \operatorname{Lim} w_n = 0$ and dually.

THEOREM 5. *In any σ-complete vector lattice, relative uniform convergence implies order-convergence. The reverse implication holds, if $u_n \downarrow 0$ implies that some sequence $\{ku_{n(k)}\}$ is bounded.*

Proof. If $|f_n - f| \leqq \lambda_n u$ and $\lambda_n \downarrow 0$, then $\{f_n\}$ order-converges to f by (2) and Lemma 5. Conversely, if $|f_m - f| \leqq u_n$, where $u_n \downarrow 0$, and if u is an upper bound to the $ku_{n(k)}$, then $|f_n - f| \leqq u/k$ for all $n > n(k)$.

The above hypothesis holds in the "regular" case of Kantorovitch.[6] It holds in the space S, since $|u_n(x)| < 1/k^2$ except on a set of measure at most $1/k^2$, for all $n > N(k)$, provided $N(k)$ is large enough. Similarly, it holds in the spaces L^p. It does not hold in the spaces B, (b) (see [LT, p. 114]).

It is easily proved that, with respect to relative uniform convergence of sequences as just defined, formulas (8)–(10) of Ch. IV, §8, are fulfilled. However, condition (11) of Ch. IV, §9, need not hold; neither need every derived set be closed.[7] But, as in §9 of Ch. IV, the first defect can be eliminated by defining *relative uniform star-convergence* to mean relative uniform convergence of some subsubsequence of every subsequence. We shall show in §9 that, in the case of Banach spaces, this relative uniform star-convergence defines the metric topology; hence in this case, the second defect is eliminated also.

---

[5] *The New Haven Mathematical Colloquium*, New Haven, 1914, pp. 31, 39; see also Bull. Am. Math. Soc. 18 (1912), p. 334. A similar definition is given by Kantorovitch [1, p. 142]. For Cor. 1 below see A. Youdine, Doklady URSS 27 (1939), 418–22; [LT, p. 121]; and B. Nagy, Comm. Math. Helv. 17 (1944), 209–13.

[6] [1], see Thm. 26. In his original paper (Doklady URSS IV (1935), pp. 13–16), Kantorovitch used a weaker definition: that if $\lambda_n \downarrow 0$ implies $\lambda_n u_n \to 0$, then $\{u_n\}$ is bounded. This weaker definition apparently is satisfied in the spaces B, (b).

[7] The latter defect was considered by Moore, op. cit., p. 40. Most of the results of §§5–11 are due to the author, [LT, §§141–51]; see also Abstract 43-3-21 (1937) of Bull. Am. Math. Soc.; Proc. Nat. Acad. Sci. 24 (1938), 155–9; and F. Riesz [2]. Bounded functions from partly ordered linear spaces to Banach spaces were considered earlier by L. Kantorovitch and B. Vulich, Compositio Math. 5 (1937), 119–65. See also B. Vulich, Doklady URSS 52 (1946), 475–8.

Ex. 1. Prove that any σ-complete vector lattice satisfies the following "generalized Cauchy condition": $\{f_n\}$ is order-convergent if and only if $|f_m - f_n| \to 0$ as $m, n \to \infty$.

Ex. 2*. Generalize Lemma 5 to arbitrary l-groups.

6. Additive functions between vector lattices. In §§ 6–8 we shall consider the functions $T: f \to fT$ from a vector lattice F to a complete vector lattice X. We shall restrict our attention to "additive" functions—to functions which satisfy the identity $(f + g)T = fT + gT$.

It is well known that the additive functions between any two vector spaces themselves form a vector space, if one defines λT and $T + U$ through the identities $f(\lambda T) = \lambda(fT)$ and $f(T + U) = fT + fU$. In the present case, this new vector space can be partly ordered, as follows.

Definition. *The additive function T is non-negative if and only if it is isotone, in the usual sense that*

$$f \geqq g \text{ in } F \text{ implies } fT \geqq gT \text{ in } X. \tag{4}$$

This is obviously equivalent to requiring that $f - g \geqq 0$ imply $(f - g)T \geqq 0$ —in words, that T carry positive elements into positive elements (or 0, which we call positive).

Theorem 6. *Under the preceding definition, the additive functions from F to X form a partly ordered vector space.*

The proof that they form a *po*-group is a corollary of Thm. 1 of Ch. XIV: condition (iv) follows from commutativity; (i) and (ii) are trivial; we now prove (iii). Suppose $T + U = 0$, $T \geqq 0$, and $U \geqq 0$. Then $g \geqq 0$ implies $gT \geqq 0$ and so $gU = -gT \leqq 0$; but $gU \geqq 0$ by the hypothesis $U \geqq 0$; hence $gU = 0$ for all $g \geqq 0$. But this implies $fU = (f^+ - (-f)^+)U = f^+U - (-f)^+U = 0$, or $U = 0$, completing the proof of (iii). Thm. 6 now follows since clearly, if $\lambda \geqq 0$ and $U \geqq 0$, then $\lambda U \geqq 0$.

On the other hand, they need not form a vector lattice (see Ex. 1 below). To get a vector lattice, we must restrict ourselves to what may properly be called "bounded" additive functions.

Ex. 1. Using a "Hamel basis" with respect to rational scalars, construct an additive function from R to R which is "unbounded" in the sense of §7.

Ex. 2. Show that if condition (iii) is omitted in Thm. 1 of Ch. XIV, we can still get a *po*-group by redefining $a = b$ to mean that both $a - b$ and $b - a$ are in G^+.

Ex. 3. Define the partly ordered vector space of Thm. 6 as X^F, and denote direct unions as products. Which laws of ordinary algebra remain valid in the resulting calculus?

7. Bounded additive functions. Indeed, if an additive function T from F to X lies in any vector lattice, then the set $\{T, 0\}$ must be bounded—i.e., additive functions U and V must exist, such that $V \leqq 0$, $T \leqq U$.

Definition. *An additive function T will be called bounded if and only if the set $\{T, 0\}$ is bounded above and below.*

LEMMA 1. *If T is bounded, then it carries bounded sets (i.e., sets H satisfying $a \leqq H \leqq b$) in F into bounded sets in X.*

Proof. If $a \leqq h \leqq b$, and $V \leqq T, 0 \leqq U$, then

$$hT = aT + (h - a)T \leqq aT + (h - a)U \leqq aT + (b - a)U,$$

and dually, $hT \geqq bT + (b - a)V$. Hence the set of hT $[h \in H]$ is bounded.

LEMMA 2. *If T carries bounded sets into bounded sets, then $T^+ = T \smile 0$ exists. In fact, $fT^+ = \sup_{0 \leqq x \leqq f} xT$ if $f \geqq 0$, and $fT^+ = f^+T^+ - (-f^-)T^+$ in any case.*

LEMMA 3. *In any l-group, if $x \leqq g + h$ $[x \geqq 0, g \geqq 0, h \geqq 0]$, then $x = s + t$, where $0 \leqq s \leqq g$ and $0 \leqq t \leqq h$.*

Proof of Lemma 3. Set $s = x \frown g$; then

$$t = -x \frown g + x = -g + x \smile g \leqq -g + (g + h) = h.$$

Obviously $0 \leqq s \leqq g, 0 \leqq t \leqq h, x = s + t$.

Proof of Lemma 2. Firstly, the T^+ defined is additive. Indeed, by Lemma 3, $\sup xT$ for $0 \leqq x \leqq (f + g)$ is $\sup (y + z)T = \sup (yT + zT)$ for $0 \leqq y \leqq f$, $0 \leqq z \leqq g$. And this is $(\sup yT) + (\sup zT)$, since on one hand the latter is an upper bound to the $yT + zT$, and on the other any upper bound to all $yT + zT$ contains $yT + \sup zT$ for every fixed y, and hence $\sup yT + \sup zT$.

It remains to show that $T^+ = T \smile 0$. But clearly $f \geqq 0$ implies $f(T^+ - T) \geqq fT - fT = 0$ and $f(T^+ - 0) \geqq 0T - f0 = 0$; hence T^+ is an upper bound to 0 and T. Conversely, if U is any (additive) upper bound to 0 and T, then for all x between 0 and f,

$$fU = xU + (f - x)U \geqq xT + (f - x)0 = xT,$$

whence $f(U - T^+) = fU - fT^+ \geqq 0$ for all $f \geqq 0$, and $u \geqq T^+$.

THEOREM 7. *The bounded additive functions from F to X form a vector lattice. This is embedded in the partly ordered vector space of Thm. 6, and contains every vector lattice so embedded.*

Proof. If $V \leqq 0, T \leqq U$, and $V^* \leqq 0, T^* \leqq U^*$, then clearly $V + V^* \leqq 0$, $T + T^* \leqq U + U^*$ and $V \leqq 0, \lambda T \leqq \lambda U$ or the reverse for all λ; hence the bounded additive functions form a subspace of the vector space of Thm. 6. By Thm. 2 of Ch. XIV, this subspace is a vector lattice. And by the first remark of the present section, every vector lattice embedded in the partly ordered vector space of Thm. 6 is contained in this subspace.

THEOREM 8. *Each of the following conditions is equivalent to boundedness:* (i) *T carries bounded sets into bounded sets,* (ii) *T is the difference of non-negative functions.*

Proof. By Lemma 1, boundedness implies (i); by Thm. 7 above and Cor. 2

of Thm. 4 of Ch. XIV, (i) implies (ii). Finally, if $T \geqq 0$ and $U \geqq 0$, then $-T-U \leqq T-U \leqq T+U$; hence (ii) implies boundedness.

Ex. 1. Show that, in case X is the real number system, any additive functional is a valuation. Show that it is "bounded" if and only if it is of "bounded variation" in the sense of Ch. V, §10. Infer that, for X real, the results of §7 are equivalent to those of Ch. V, §10.

Ex. 2*. Generalize the theory of valuations, including Ch. V, §10, to the case of functions with values in a general complete vector lattice—in a general complete l-group.

8. Functionals and conjugate spaces. We now restrict ourselves to the case that X is the real number system, recalling that the analysis of real-valued functions or "functionals" on abstract spaces has attracted especial attention from mathematicians ever since the pioneer work of Volterra and Fréchet (see Banach [1] for modern viewpoints and problems).

We define the *conjugate space* F^* of a vector lattice F as the vector lattice (Thm. 7) of all bounded additive functionals on F. We shall show in Thm. 11 that this definition effectively specializes to the concept of a "conjugate space" as treated in Banach [1], though apparently quite different from it.

Surprisingly, it includes as another special case the notion of a "Dualraum" introduced by Koethe and Toeplitz.[8] Hence it seems destined to play an important role in future functional analysis, especially in view of its simplicity and intrinsic character.

Without attempting profundities, we shall prove the important relation $F \leqq (F^*)^*$. Indeed, every $f \in F$ defines an additive functional ϕ on F^*: $\phi(T) = fT$. Moreover every such ϕ is bounded; since $f = f - (-f^-)$, we need only prove this in the case $f \geqq 0$. But if $f \geqq 0$ and $V \leqq T \leqq U$, then $fV \leqq fT \leqq fU$; and it follows that the $\phi(T)$ on any bounded set (closed interval) are bounded.

The extensibility of positive linear functionals on Banach lattices has been treated by M. Krein, Comm. math. Kharkov 14 (1937), 227–37; see also M. Krein, Doklady URSS 23 (1939), 745–5, 25 (1939), 723–6, and 28 (1940), 18–22; and V. Šmulian, ibid. 30 (1941), 394–8. Additive functionals have further been considered by A. G. Pinsker, Doklady URSS 55 (1947), 299–302.

9. Banach lattices. Every known example of a Banach space (or "espace (B)" in the sense of Banach [1, p. 52]) is also a vector lattice in a natural sense. Moreover, in every case, the ordering $f \leqq g$ and the norm function $\|f\|$ are related by the following condition

(5) $$|f| \leqq |g| \text{ implies } \|f\| \leqq \|g\|.$$

[8] Jour. für Math. 171 (1934), 193–226. To prove our statement, we assume what is true in all the examples cited by these authors: that F contains every $(0, \cdots, 0, 1, 0, \cdots)$ and contains $|x|$ if it contains x. For in this case, every positive functional assumes some non-negative value λ_k on x_k, and sup $\Sigma\, \lambda_k\xi_k$ on $\Sigma\, \xi_k x_k$. Hence every positive functional, and therefore every difference of positive functionals, yields an absolutely convergent $\Sigma\, \lambda_k\, |\xi_k|$, and so is in the Koethe-Toeplitz Dualraum. Conversely, if u is in the Dualraum, then the positive and negative u_k define new monotone additive functionals, whose sum is u.

A vector lattice which is a Banach space and satisfies (5) will be called a *Banach lattice*. One shows easily that, in any Banach lattice,

(6) $$\| f \| = \| \, |f| \, \| \quad \text{for all } f.$$

We shall show next that, in any Banach lattice L, metric convergence is equivalent to relative uniform star-convergence, and that the continuous additive functionals on L are simply the bounded additive functionals. Hence, in all known cases, *metric concepts can be replaced by simple order concepts.*[9]

LEMMA 1. *No vector lattice L which contains a sequence $\{f_n\}$ such that all sequences $\{\lambda_n f_n\}$ are order-bounded, can be made into a Banach lattice.*

Proof. Suppose L were made into a Banach lattice, and set $\lambda_n = n/\| f_n \|$. If u were an upper bound to all $\lambda_n f_n$, then $\| u \|$ would have to exceed every n, since $\| \lambda_n f_n \| = n$.

LEMMA 2. *The operations $f + g$, $f \frown g$, and $f \smile g$ are metrically uniformly continuous, in any Banach lattice.*

Proof. By definition and formula (20) of Ch. XIV, we have

$$| (f \circ g) - (f^* \circ g) | \leqq | f - f^* |,$$

whether $\circ$ denotes $+$, $\frown$, or $\smile$. By (5)–(6), this implies the corresponding metric inequality; hence all three operations are uniformly continuous, with modulus of continuity one, in the usual metric $\| f - g \|$.

COROLLARY. *If $\sum_{n=1}^{\infty} a_n = a$, $\sum_{n=1}^{\infty} b_n = b$, and $\sum_{n=1}^{\infty} x_n = x$ metrically, and $a_n \leqq x_n \leqq b_n$ for all n, then $a \leqq x \leqq b$.*

LEMMA 3. *Any separable Banach lattice has a weak unit e.*

Proof. Let $\{f_n\}$ be any countable, metrically dense subset of L. Define $e = \sum_{n=1}^{\infty} |f_n|/2^n \| f_n \|$. For any $g > 0$ in L, we have $\| g - f_n \| < \| g \|/10$, for some n. Moreover $e \frown g = 0$ would imply $g \frown (|f_n|/2^n \| f_n \|) \leqq g \frown e = 0$, and so $g \frown |f_n| = 0$. But $g \frown |f_n| = g \frown [(f_n \smile 0) - (f_n \frown 0)]$, and substitution of g for f_n in this expression moves it through at most $\| g \|/5$, by Lemma 2. Since $g \frown [(g \smile 0) - (g \frown 0)] = g$, this implies $\| (g \frown |f_n|) - g \| \leqq \| g \|/5$, and so $g \frown |f_n| > 0$. Hence $g \frown e \geqq (g \frown |f_n|)/2^n \| f_n \| > 0$, and e is a weak unit. This result is due to Freudenthal [1], p. 648.

THEOREM 9. *In any Banach lattice, metric convergence is equivalent to relative uniform star-convergence.*

---

[9] Since these order concepts apply also to non-metric topological linear spaces, as in the Dualraum of Koethe and Toeplitz, it would seem worthwhile to parallel the usual theory of metric linear spaces and normed rings by a self-contained complete theory of vector lattices and lattice-ordered rings, with applications to specific cases. Such an analysis has not yet been made. Cf. R. C. James, A. D. Michal, and M. Wyman, Bull. Am. Math. Soc. 53 (1947), 770–4; M. H. Stone, Annals of Math. 48 (1947), 851–6.

Proof. By the homogeneity of both topologies, we need only consider convergence to 0. But if $|f_n| \leqq \lambda_n u$ and $\lambda_n \downarrow 0$, then clearly $\|f_n\| \leqq \|\lambda_n u\| = |\lambda_n| \cdot \|u\| \downarrow 0$. Thus relative uniform star-convergence implies metric star-convergence and so metric convergence. Conversely, if $\|f_n\| \to 0$, we can so choose $n(k)$ that $k^3 \|f_{n(k)}\| \to 0$, and then construct $v = \sum_{k=1}^{\infty} kf_{n(k)}$ with $|f_{n(k)}| \leqq |v|/k$.

Since $a \leqq x \leqq b$ implies $\|x\| \leqq \|a\| + \|b - a\|$, order-boundedness of a subset of a Banach lattice clearly implies metric boundedness. The converse is not however usually true. Thus in L^p and (l^p), there is no upper bound to the elements of norm one—though in the spaces B and (b) there is. But in all cases, we have the following remarkable result.

THEOREM 10. *Metric "boundedness" and order-boundedness (§7) are equivalent, for additive functionals T on a Banach lattice.*

Thus the condition that T should "carry bounded sets into bounded sets" is the same, whether interpreted in terms of metric boundedness or order boundedness.

Proof. If T is bounded metrically, then, for any $a > 0$, $|x| < a$ implies $\|x\| \leqq \|a\|$; hence $|xT| \leqq \|a\| \cdot \|T\|$, and the xT form a bounded set. Conversely, if T is metrically unbounded, then a sequence $\{x_n\}$ exists with $\|x_n\| \leqq 2^{-n}$ yet $|x_nT| \uparrow +\infty$. Hence, by the Cor. of Lemma 3, the elements $a = \sum_{n=1}^{\infty} x_n^-$ and $b = \sum_{n=1}^{\infty} x_n^+$ bound a set of y on which yT is unbounded; that is, T is order-unbounded.

Ex. 1. Show that the spaces S and R^c cannot be made into a Banach lattice. (Hint: Let $f_n(x) = 1$ if $0 < x < 1/n$, and zero elsewhere.)

Ex. 2. Show that no infinite-dimensional "σ-full" vector lattice (cf. Ex. 2, §3) can be made into a Banach lattice.

Ex. 3. (a) Show that if f_n is a decreasing sequence of elements of a Banach lattice which converges metrically to 0, then it order-converges to 0.

(b) Show that, in any Banach lattice, a metrically convergent sequence star-converges to the same limit.

Ex. 4. (a) Let V be any Banach lattice in which $u_n \downarrow 0$ implies that some sequence $\{ku_{n(k)}\}$ is order-bounded. Show that order-convergence in V implies metric convergence; and that star-convergence is equivalent to metric convergence.[10]

(b) In the Banach lattice (b), let u_n be the sequence composed of n zeros followed by all ones. Show that the sequence $\{u_n\}$ order-converges to 0, without converging metrically or relatively uniformly.

10. Uniformly monotone norm. We shall call the norm in a Banach lattice "uniformly monotone" when, given $\epsilon > 0$, one can find $\delta > 0$ so small that if $f \geqq 0$, $g \geqq 0$, and $\|f\| = 1$, then $\|f + g\| \leqq \|f\| + \delta$ implies $\|g\| \leqq \epsilon$. We shall call a Banach lattice with a uniformly monotone norm, a ***UMB-lattice***.

Thus the space L obviously has uniformly monotone norm, since $\|f + g\| = \|f\| + \|g\|$. Similarly, the spaces L^p and (l^p) have uniformly monotone norm, and so they are UMB-lattices. In fact, any metrically closed subspace and sublattice of any UMB-lattice, is clearly itself a UMB-lattice.

[10] For a recent related result, see H. Nakano, Proc. Imp. Acad. Tokyo 19 (1943), 10–11.

On the other hand, the norm in the spaces B, (b), and C is not uniformly monotone.

THEOREM 11. *In a UMB-lattice, any metrically bounded set of elements, which is a "directed set" in the lattice order, converges metrically.*

Proof. We can confine our attention to the successors of a fixed element a, and so, since $f \to f - a$ is an isometric lattice-automorphism, we can assume that all elements f_α of the set are non-negative. Again, by changing the scale, we can assume $\| f_\alpha \| \leqq 1$ for all α. But in this case, if α is so chosen that $\| f_\alpha \| \geqq \sup \| f_\alpha \| - \delta$, we will have $\| f_\beta - f_\alpha \| \leqq \epsilon$ for all $f_\beta > f_\alpha$, proving our result.

COROLLARY. *Any UMB-lattice is a complete vector lattice.*

For if a set has an upper bound, so do the joins of the finite subsets of the set, and these form a metrically bounded directed set.

THEOREM 12. *In a UMB-lattice, order-convergence and relative uniform convergence are equivalent.*

Proof. By Thm. 5, it is sufficient to show that

$$u_n \downarrow 0 \text{ implies } \| u_n \| \downarrow 0 \text{ in any UMB-lattice.} \tag{7}$$

For (7) implies that, for some $n(k)$, $\| u_{n(k)} \| \leqq 1/k2^k$; hence the infinite linear sum $\sum_{k=1}^{\infty} k u_{n(k)}$ exists and is (Lemma 3, §9) an upper bound to the sequence $\{k u_{n(k)}\}$. By Thm. 5, this implies the equivalence of order- and relative uniform convergence.

We now prove (7). By Thm. 11, $\{u_n\}$ converges metrically to some a. By Lemma 3, §9, $a \frown 0 = 0$ and $a \smile u_n = u_n$ for all n; hence $0 \leqq a \leqq u_n$ for all n, and so $a = 0$, as asserted.

COROLLARY. *Star-convergence and metric convergence are equivalent, in any UMB-lattice.*[11]

Finally, we may note that Thm. 10 may be extended to functions T with values in any UMB-lattice. The second half of the proof need not be changed. As regards the first half, note that since any two decompositions of the interval $0 \leqq x \leqq f$ have a common refinement, the xT $[0 \leqq x \leqq f]$ form a directed set. Hence if T is metrically bounded, so are the xT, and by Thm. 11 they converge to a supremum fT^+. Dually, the xT have a lower bound, and so T is order bounded.

Ex. 1. Show that (7) is false in the space (b).

Ex. 2. (a) Prove that the spaces L^p and (l^p) are UMB-spaces.

(b) Show by a direct counterexample that the spaces C and (b) are not UMB-spaces.

[11] This corollary is closely related to results of Kantorovitch (Comptes Rendus, 201 (1935), p. 1457, and [1, p. 154]). The case of AL-spaces is covered in Thm. 15 of Ch. V.

Ex. 3*. A Banach space is called "uniformly convex" (J. W. Clarkson), if there exists a single-valued function $\delta(\epsilon)$, positive if $\epsilon > 0$, such that if $\|f\| = \|g\| = 1$ and $\|f - g\| \geqq \epsilon$, then $\|\frac{1}{2}(f + g)\| \leqq 1 - \delta(\epsilon)$. Show that any uniformly convex Banach lattice is a UMB-lattice.

11. A decomposition theorem. Let L be any UMB-lattice, and $\lambda(f)$ any bounded additive functional on L. We shall show that $\lambda(f)$ decomposes L into components on which $\lambda(f)$ is positive, negative, and zero respectively. First

LEMMA 1. *Let N^+, N^-, and N^0 be defined as the sets of f such that $0 < x \leqq |f|$ implies $\lambda(x) > 0$, $\lambda(x) < 0$, and $\lambda(x) = 0$, respectively. Then N^+, N^-, and N^0 are independent l-ideals.*

Proof. Suppose $f \in N^+$ and $g \in N^+$. Then $0 < x \leqq |f + g|$ implies $0 < x \leqq |f| + |g|$, whence $x = y + z$, where $0 \leqq y \leqq |f|$, $0 \leqq z \leqq |g|$, and $y > 0$ or $z > 0$; hence $\lambda(x) = \lambda(y) + \lambda(z) > 0$. That is, N^+ is closed under addition. Again, if $f \in N$ and $|h| \leqq |f|$, then $0 < x \leqq |h|$ implies $0 < x \leqq |f|$, whence $\lambda(x) > 0$ and $h \in N^+$. We conclude that N^+ is an l-ideal. Similarly, N^- and N^0 are l-ideals.

Now, since l-ideals form a distributive lattice, the l-ideals N^+, N^-, and N^0 must be independent if $N^+ \frown N^- = N^- \frown N^0 = N^0 \frown N^+ = 0$. But this is almost trivial: if $f \neq 0$, then $f \in N^+$ implies $\lambda(|f|) > 0$, $f \in N^-$ implies $\lambda(|f|) < 0$, and $f \in N^0$ implies $\lambda(|f|) = 0$; these conditions are mutually exclusive.

THEOREM 13. *L is the direct union of N^+, N^-, and N^0.*

Proof. By the italicized statement of Ch. XIV, §11, paragraph one, and Lemma 1 above, it is sufficient to show that L is the linear sum of the subspaces (note Lemma 1, §1) N^+, N^-, N^0; that is, that $L = N^+ + N^- + N^0$. To prove this, we first require uniform monotonicity to prove

LEMMA 2. *The functional $\lambda(x)$ attains its supremum M on any interval $0 \leqq x \leqq f$.*

Proof. Choose x_i so that $\lambda(x_i) > M - 3^{-i}$; we shall show that $g = \lim\sup\{x_i\}$—which exists by the Cor. of Thm. 11—satisfies $\lambda(g) = M$. Indeed,

$$\lambda(x_i \smile x_j) = \lambda(x_i) + \lambda(x_j) - \lambda(x_i \frown x_j) > M - 3^{-i} - 3^{-j},$$

whence $\lambda(x_i \smile x_{i+1} \smile \cdots \smile x_{i+n}) > M - (3^{-i} + \cdots + 3^{-i-n})$ exceeds $M - 2\cdot 3^{-i}$. Passing to the limit once, $M \geqq \lambda(\sup_{k \leqq i}\{x_k\}) \geqq M - 2\cdot 3^{-i}$. Passing to the limit similarly again, by continuity in the metric topology, which (Thm. 12, Cor.) implies continuity in the order-topology, we get $\lambda(g) = M$.

The relation $L = N^+ + N^- + N^0$ is now obvious from

LEMMA 3. *In Lemma 2, let u be the infimum of the x between 0 and f such that $\lambda(x) = M$; define v dually; let $w = f - u - v$. Then $u \in N^+$, $v \in N^-$, $w \in N^0$, and $f = u + v + w$.*

Proof. The existence of u and v (and thus of w) follows from the completeness of L. Again, if $\lambda(x) = \lambda(y) = M$, then $\lambda(x \frown y) + \lambda(x \smile y) = 2M$.

But $\lambda(x \frown y) \leqq M$ and $\lambda(x \smile y) \leqq M$, and so $\lambda(x \frown y) = \lambda(x \smile y) = M$. It follows by Theorem 11 and continuity that $\lambda(u) = M$. Moreover $0 < x \leqq u$ implies $\lambda(u - x) < \lambda(u)$ and so $\lambda(x) = \lambda(u) - \lambda(u - x) > 0$; hence $u \in N^+$. Dually, $v \in N^-$. Hence $u \frown v = 0$ by Lemma 1, whence $u + v = u \smile v \leqq f$ and $0 \leqq w \leqq f$. Finally, $0 < x \leqq w$ implies $\lambda(x) + \lambda(u) = \lambda(x + u) \leqq \lambda(u)$, whence $\lambda(x) \leqq 0$. Dually, it implies $\lambda(x) \geqq 0$, and so $\lambda(x) = 0$. Hence $w \in N^0$. But $f = u + v + w$ is obvious, completing the proof.

Ex. Show that Lemma 1 holds in any vector lattice, but that Lemmas 2–3 and Thm. 13 are not true in the space C.

12. Integral representation. Let V be any σ-complete vector lattice with a weak unit e. By a *resolution* of e, we mean a monotone increasing family of components e_λ of e, such that

$$(8) \qquad \lambda < \mu \text{ implies } e_\lambda \leqq e_\mu, \ \operatorname{Lim}_{\lambda \to \infty} e_\lambda = e, \ \operatorname{Lim}_{\lambda \to -\infty} e_\lambda = 0.$$

With respect to any such "resolution of the identity," we can define *integrals* as follows.

For any finite M, and any partition π of the interval $-M \leqq \lambda \leqq M$ into subintervals $\lambda_{i-1} \leqq \lambda \leqq \lambda_i$, we may form $u_\pi = \sum_i \lambda_{i-1}(e_{\lambda_i} - e_{\lambda_{i-1}})$ and $v_\pi = \sum_i \lambda_i(e_{\lambda_i} - e_{\lambda_{i-1}})$, these we regard respectively as *under* and *over* approximations to the integral. If π and π' are any two partitions, then one shows easily that $u_\pi \leqq u_{\pi \frown \pi'} \leqq v_{\pi \frown \pi'} \leqq v_{\pi'}$; moreover $| v_{\pi'} - u_\pi | \leqq 2\epsilon e$, where ϵ is the length of the largest subinterval of π or π'. Hence, since $2\epsilon e \downarrow 0$ as $\epsilon \downarrow 0$ by (2), the u_π and v_π approach the same limit g. We *define* this limit to signify the symbol

$$(9) \qquad g = \int_{-m}^{m} \lambda \, de_\lambda .$$

This defines *bounded* integrals. We define

$$(10) \qquad f = \int_{-\infty}^{\infty} \lambda \, de_\lambda = \operatorname*{Lim}_{n \to \infty} \left\{ \int_{-n}^{n} \lambda \, de_\lambda \right\},$$

in case this limit exists, in the sense of order-convergence.

We have just seen that each resolution of e on a bounded interval defines a bounded integral g; clearly $| g | \leqq Me$ for some finite M. Conversely, let g be any element of V which is *bounded* relative to e in this sense—i.e., for which e is a strong unit. Then we can define e_λ as the component of e in the closed l-ideal having $(\lambda e - g)^+$ for strong unit. It is not hard to show that (9) holds, with respect to this resolution. More generally, we can show

THEOREM 14. *Any element f of a σ-complete vector lattice V with weak unit e can be represented as an integral* (10).

Proof. For any positive integer n, we construct the bounded *truncation* f_n of f, by

$$(11) \qquad f_n = -ne \smile (f \frown ne) = (-ne \smile f) \frown ne \qquad \text{(see L5).}$$

Then the sequence of $f_n^+ = 0 \smile (f \frown ne)$, which is bounded above by f^+, converges to a limit $f^* \leqq f^+$, by σ-completeness. But, as in Ch. XIV, §11, we can show that $(f^+ - f^*) \frown e = 0$, whence $f^+ - f^* = 0$, and so $f_n^+ \uparrow f^+$. Dually, $f_n^- \downarrow f^-$, whence

$$(12) \qquad f_n = f_n^+ + f_n^- \to f^+ + f^- = f,$$

in the sense of order-convergence. Hence (10) holds, where $f_n = \int_{-n}^{n} \lambda \, de_\lambda$ as previously.

The preceding representation was first suggested by Freudenthal [1], who however made many unnecessary assumptions. We can make it unique if we add the requirement[12] that $e_\lambda = \sup_{\mu<\lambda} e_\mu$, for all λ.

But now, we note that the closed l-ideals of V, which form a complete Boolean algebra, can themselves be represented by open-and-closed subsets of a compact Boolean space S (Ch. XI, Thm. 3). Using this representation, Stone [6] has shown that V can be represented by functions which are finite and *continuous* on S, except perhaps on a nowhere dense set; moreover vector and lattice operations have their usual meaning, except that nowhere dense sets are ignored throughout. Von Neumann (unpublished lectures given in April 1940) has obtained essentially identical results. Moreover S. Kakutani and M. and S. Krein[13] have characterized the vector lattice of *all* continuous functions on an arbitrary compact Hausdorff space. The basic fact is that such a vector lattice has a strong unit e (any weak unit is strong), and that it can be made into a Banach lattice if one defines

$$(13) \qquad \|f\| = \inf_{|f| \leqq \lambda e} \lambda.$$

13. Additive set functions and (L)-spaces. Consider the class $L(A)$ of all bounded valuations $f[x]$ (Ch. V, §6), which also satisfy $f[O] = 0$, on a fixed Boolean algebra A. Under any isomorphic representation of A as a field Φ of sets, $L(A)$ may be regarded as the class of all *bounded, additive set-functions* on Φ.

---

[12] This representation of "Lebesgue-Nikodym" type has been developed further by J. Dieudonné, Annals of Math. 42 (1941), 547–55; Bull. Soc. Math. France 72 (1944), 193–239; M. Nakamura and G. Sunouchi, Proc. Imp. Acad. Tokyo 18 (1942), 333–5; C. E. Rickart, Trans. Am. Math. Soc. 56 (1944), 50–66; M. Cotlar and E. Zarantonello, Publ. Inst. Mat. Univ. Nac. Litoral VIII (1948), No. 3.

[13] M. and S. Krein [1], and Doklady URSS 27 (1940), 427–30; S. Kakutani, Proc. Imp. Acad Tokyo 16 (1940), 63–7; Annals of Math. 42 (1941), 994–1024; H. F. Bohnenblust, ibid., 1025–8. Also, J. A. Clarkson, Annals of Math. 48 (1947), 845–50.

LEMMA. *If $v[x]$ is a valuation on any Boolean algebra, then the variation of $f[x]$ on any chain $a = x_0 < x_1 < \cdots < x_n = b$ is equal to that on some chain $a \leqq y \leqq b$ of length two.*

Proof. Let y be the union of a and the differences $x_i - x_{i-1} = x_i \frown x'_{i-1}$ such that $v[x_i] > v[x_{i-1}]$.

It follows that being bounded is equivalent to having bounded variation (Ch. V, §10). We know already (Ch. V, Thm. 17) that the valuations of bounded variation on any lattice form a vector lattice; hence $L(A)$ is a vector lattice. We shall now show that if we define the total variation as norm, $L(A)$ becomes a Banach lattice. But by the lemma, the total variation of $f[x]$ is

$$(14) \qquad \| f \| = \sup \{(f[x] - f[0]) + (f[I] - f[x])\} = \sup \{f(x) - f(x')\}.$$

Moreover since the bigger $f(x)$ is, the smaller is $f[x'] = f[I] - f[x]$, we have further

$$(14') \qquad \| f \| = \sup_x f[x] - \inf_x f[x] = \sup \{2f[x] - f[I]\}.$$

THEOREM 15. *If we define norm in $L(A)$ as total variation (i.e., by (14)), then $L(A)$ becomes a Banach lattice in which*

$$(15) \qquad \text{if } f > 0 \text{ and } g > 0, \text{ then } \| f + g \| = \| f \| + \| g \|.$$

Proof. For relatively complemented lattices, being bounded is equivalent to having bounded variation (Ch. V, §10). But we know (Thm. 17 of Ch. V) that the valuations of bounded variation on *any* lattice form a vector lattice.

Next, $L(A)$ is a Banach space. For clearly $\| cf \| = | c | \cdot \| f \|$. Again,

$$\begin{aligned} \| f + g \| &= \operatorname{Sup}_x \{f[x] - f[x'] + g[x] - g[x']\} \\ &\leqq \operatorname{Sup}_{x,y} \{f[x] - f[x'] + g[y] - g[y']\} = \| f \| + \| g \|. \end{aligned}$$

If $f \neq 0$, then $f[x] \neq 0$ for some x. Hence either $f[x'] = f[x]$, and $\| f \| \geqq f(I) = 2f[x] > 0$, or $f[x] \neq f[x']$, and $\| f \| \geqq \operatorname{Max}\{f[x] - f[x'], f[x'] - f[x'']\} = | f[x] - f[x'] | > 0$. Thus $f \neq 0$ implies $\| f \| > 0$, and $L(A)$ is a metric vector space. Finally, if $\| f_m - f_n \| \to 0$, as $m, n \to \infty$, then, for any x, $\| f_m[x] - f_n[x] \| \to 0$; hence we may define $f(x) = \operatorname{Lim}_{n \to \infty} f_n[x]$. This $f[x]$ is clearly additive, since all f_n are; moreover clearly $f[O] = 0$ and $\| f_n - f \| \to 0$. If $f > 0$, clearly $f[x] - f[x'] \leqq f[I] - f[0]$; hence

$$(14') \qquad \text{if } f > 0, \text{ then } \| f \| = f[I].$$

This immediately implies (15).

It remains to prove that $| f | \leqq | g |$ implies $\| f \| \leqq \| g \|$. But by (15), writing $h = | g | - | f | \geqq 0$, it is sufficient to prove that $\| f \| = \| \, | f | \, \|$. This we now show. By §10 of Ch. V, $f^+(I) = \sup f[x]$ and $f^-(I) = \inf f[x]$. Moreover $f[x'] = f[I] - f[x]$. Hence

$$\text{(16)} \qquad \begin{aligned} \| f \| &= \operatorname{Sup} \{2f[x] - f[I]\} = 2f^+[I] - f[I] \\ &= f^+[I] - f^-[I] = |f|[I] = \| |f| \|, \text{ by } (14'). \end{aligned}$$

Definition. *A Banach lattice which satisfies* (15) *will be called an abstract* (L)*-space.*

Corollary. *The bounded valuations which satisfy* $f[O] = 0$, *on any Boolean algebra, form an abstract* (L)*-space. Any abstract* (L)*-space is a UMB-lattice.*

There is a close connection between abstract (L)-spaces and measure and probability. This we now formulate.

Definition. *By a "distribution" or "probability functional" on a Boolean algebra* A *is meant a positive valuation* $p[x]$ *which satisfies* $p[O] = 0$ *and* $p[I] = 1$. *If* A *is a Boolean* σ*-algebra, and if* $p[\vee_{i=1}^{\infty} x_i] \leqq \sum_{i=1}^{\infty} p[x_i]$, *then* $p[x]$ *is called a "*σ*-distribution."*

The relation of such distributions to probability has been discussed in Ch. XII, §9; see also Ch. X, §12, for the relation to measure theory.

Theorem 16. *The set* $D(A)$ *of distributions on* A *consists of the positive elements of* $L(A)$ *having norm one. It is therefore metrically closed, convex, and has diameter two at most.*

Proof. By definition, $D(A)$ consists of the positive elements satisfying $f[I] = 1$. But if $f > 0$, then $\| f \| = f[I]$, proving the first statement. Again, both the set of $f \geqq 0$ (by Lemma 3 of §9) and the "unit sphere" of f of norm one are metrically closed; hence so is their intersection $D(A)$. While if $p > 0$, $q > 0$, $\lambda > 0$, $\mu > 0$, $\lambda + \mu = 1$, then $\lambda p + \mu q > 0$; and if besides $\| p \| = \| q \| = 1$, then $\| \lambda p + \mu q \| = \lambda \| p \| + \mu \| q \| = 1$. Finally, if $p, q \in D(A)$, then $\| p - q \| \leqq \| p \| + \| -q \| = 2$.

Remark. The distance function $\| p - q \|$ is the "stochastic distance" of Nikodym and Mazurkiewicz.[14]

Ex. 1. Prove that (15) and (16) imply Kakutani's condition,[15] that if $x \frown y = 0$, then $\| x + y \| = \| x - y \|$.

Ex. 2. Extend the lemma of the text to all relatively complemented lattices.

Ex. 3. Prove that a distribution $p[x]$ is a σ-distribution if and only if $x_i \frown x_j = 0$ for all $i \neq j$ implies $p[\vee_{i=1}^{\infty} x_i] = \sum_{i=1}^{\infty} p[x_i]$.

Ex. 4. Show that every $x \in A$ defines an element m_x of the conjugate space of $L(A)$, by $m_x[x] = f[x]$.

---

[14] O. Nikodym, Fund. Math. 15 (1930), 131–79; Mazurkiewicz, Monats. f. Math. u. Phys. 41 (1934), 343–53. The metric for the traditional "convergence in probability" is implied by convergence with respect to this $\| p - q \|$, but fails to yield a Banach space.

[15] S. Kakutani [1, condition IX]. A study of Banach lattices in which, for some real, single-valued function $\phi(\lambda, \mu)$, $x \frown y = 0$ implies $\| x + y \| = \phi(\| x \|, \| y \|)$ has been made by F. H. Bohnenblust, Duke Jour. 6 (1940), 627–40. Exs. 2–5 below are taken from [LT, §§166–8]. Ex. 4 is greatly generalized in S. Kakutani, Annals of Math. 42 (1941), p. 1021, Thm. 15.

Ex. 5. Show that the diameter of $D(A)$ is zero or exactly two.

Ex. 6. Extend the results of §6 to the case that A is a "generalized Boolean algebra" without I.

Problem 108. Can any σ-complete l-group be extended to a full, complete, vector lattice?

14. The σ-distributions. We now consider the subset $L_\sigma(A)$ of σ-additive valuations on a Boolean σ-algebra A, satisfying $f[O] = 0$—and the corresponding subset $D_\sigma(A)$ of σ-distributions.

LEMMA. *Each of the following continuity conditions is equivalent to σ-additivity: (i) $x_n \downarrow O$ implies $f[x_n] \to 0$, and (ii) $x_n \to x$ in the order-topology implies $f[x_n] \to f[x]$.*

Proof. Since $y_n \to y$ if and only if $x_n \downarrow 0$ exists satisfying $| y_n - y | \leqq x_n$, where $| y_n - y |$ denotes the symmetric difference between y_n and y, conditions (i) and (ii) are equivalent. But $\bigvee_{i=1}^{n} x_n \to \bigvee_{i=1}^{\infty} x_n$; hence if f is continuous, $f[\bigvee_{i=1}^{\infty} x_i] = \text{Lim}\, [\bigvee_{i=1}^{n} x_n] \leqq \sum_{i=1}^{\infty} f[x_i]$. Conversely, since $x_n \downarrow 0$ implies $x_1 = \bigvee_{i=1}^{\infty} (x_i - x_{i+1})$, where $(x_i - x_{i+1}) \frown (x_j - x_{j+1}) = 0$ if $i \neq j$, $f[x_1] = \sum_{i=1}^{\infty} f[x_i - x_{i+1}]$ if f is σ-additive. But this clearly implies $f[x_n] = \sum_{i=n}^{\infty} f[x_i - x_{i+1}] \to 0$, completing the proof.

THEOREM 17. *If A is a Boolean σ-algebra, then $L_\sigma(A)$ is a metrically closed l-ideal of $L(A)$.*

Proof. Since $| f[x_n] | \leqq \| f_n - f \| + f_m[x_n]$, if every f_m is continuous and $\| f_m - f \| \to 0$, then $x_n \downarrow 0$ implies $f[x_n] \to 0$; thus $L_\sigma(A)$ is metrically closed. That $L_\sigma(A)$ is a vector subspace of $L(A)$ is trivial; it remains to prove the "normality" condition: that $f \in L_\sigma(A)$ and $0 < g \leqq | f |$ imply $g \in L_\sigma(A)$. But indeed, under these hypotheses $x_n \downarrow 0$ and $0 \leqq y_n \leqq x_n$ imply $y_n \to 0$ and so $f[y_n] \to 0$; hence $\sup_{0 \leqq y_n \leqq x_n} | f[y_n] | \to 0$. But by hypothesis and the Lemma of §13, $| g[x_n] | \leqq | f | [x_n] \leqq 2 \sup_{0 \leqq y_n \leqq x_n} | f[y_n] |$; therefore $g(x_n) \to 0$. By the lemma above, this implies $g \in L_\sigma(A)$, completing the proof.

COROLLARY 1. *For any Boolean σ-algebra A, the set of σ-additive valuations $f[x]$ of A satisfying $f[O] = 0$ is an abstract (L)-space. Hence the σ-additive set-functions on any σ-field of sets form an abstract (L)-space.*

COROLLARY 2. *The σ-distributions on A form a metrically closed, convex subset of $L(A)$.*

Ex. Show that any σ-additive distribution on a Boolean σ-algebra A is necessarily bounded.

15. Representation of separable abstract (L)-spaces. Let L be any separable abstract (L)-space, with a countable, metrically dense subset of elements f_1, $f_2, f_3, \cdots$. We sketch a proof of the fact that L can be embedded in the space (L) defined in § 2.

We define a weak unit, as in Lemma 3 of §9, by

$$e = \sum_{k=1}^{\infty} | f_n |/2^n \, \| f \| > 0. \tag{17}$$

We let A be the complete Boolean algebra of all closed l-ideals of A. If J is any such closed l-ideal, and if J' is its complement, we can form by Thm. 11 and metric completeness the join e_J of all elements $x \leqq e$ such that $x \frown y = 0$ for all $y \in J'$. Likewise, we can form $e_{J'}$; moreover $e_J \frown e_{J'} = 0$, $e_J + e_{J'} = e$. Thus A is isomorphic to the complete Boolean algebra[16] of all components of e. Since this is a separable, metric Boolean algebra, it is isomorphic (Thm. 15, Ch. X and Thm. 10, Ch. XI) with a subalgebra of the measure algebra of all measurable subsets of the interval $0 \leqq x \leqq 1$, modulo sets of measure zero.

Similarly, for any $f \in L$ and any closed l-ideal J, we can form $(f^+)_J$ and $(f^-)_J$; hence $f_J = (f^+)_J + (f^-)_J$. That is, every $f \in L$ has components on every J.

In order to represent f by completely additive valuations, we need one more remark. The functional

$$\lambda(f) = \|f^+\| - \|f^-\| = \|f^+\| - \|(-f)^+\| \tag{18}$$

is a linear functional of norm one on L; the proof is as follows. We wish to prove that $\lambda(f + g) = \lambda(f) + \lambda(g)$, that is, that

$$\|(f + g)^+\| - \|(-f - g)^+\| = \|f^+\| - \|(-f)^+\| + \|g^+\| - \|(-g)^+\|.$$

This follows, transposing, from the following identities

$$\begin{aligned}\mu &= \|(f+g)^+\| + \|(-f)^+\| + \|(-g)^+\| = \|(f+g)^+ + (-f)^+ + (-g)^+\| \\ &= \|(f + g)^+ + (f^+ - f) + (g^+ - g)\| \\ &= \|[(f + g) \smile 0] - (f + g) + f^+ + g^+\| \\ &= \|[0 \smile (-f - g)] + f^+ + g^+\| = \|(-f - g)^+\| + \|f^+\| + \|g^+\|.\end{aligned}$$

Trivially, $\lambda(cf) = c\lambda(f)$. We now associate with each $f \in L$, the following functional on A,

$$f(J) = \lambda(f_J). \tag{19}$$

By Thm. 11, $\lambda(f_J) = f(J)$ is σ-additive. Furthermore, since $(f + g)_J = f_J + g_J$ and $(cf)_J = cf_J$, addition in L corresponds to addition of valuations. We next show that $\|f\|$ is the norm, sup $\|\lambda(f_J) - \lambda(f_{J'})\|$, introduced in Thm. 15, for set-functions. For all J,

$$\begin{aligned}\|\lambda(f_J) - \lambda(f_{J'})\| &\leqq |\,\|f_J^+\| - \|f_J^-\| - \|f_{J'}^+\| + \|f_{J'}^-\|\,| \\ &\leqq \|f_J^+\| + \|f_{J'}^+\| + \|f_J^-\| + \|f_{J'}^-\| = \|f^+\| + \|f^-\| = \|f\|.\end{aligned}$$

[16] The results here and below are mostly due to Kakutani [1]; see also M. and S. Krein [1]; the exposition is new. The results of §§13–14 may be found in [LT] and in Kakutani [1]. A discussion of spaces of continuous functions (conjugates of abstract (L)-spaces) may be found in Kakutani [2], and in M. and S. Krein, Doklady URSS 27 (1940), 427–30 and I. Vernikoff, S. Krein, and A. Tovbin, 30 (1941), 785–7.

But for the particular J generated by f^+ as weak unit, we have

$$f_J = f^+, \quad f_{J'} = f - f_J = f^-, \quad \text{and so} \quad \lambda(f_J) = \|f^+\|,$$

$$\lambda(f_{J'}) = -\|f^-\|, \quad \text{and} \quad \|\lambda(f_J) - \lambda(f_{J'})\| \geqq \|f\|.$$

Combining these inequalities, we get our result. Finally, it remains to show that $f^+(J) = \text{Sup}_{K \leqq J}(K)$, so that lattice operations have the same meaning as for valuations. But since $f(K) \leqq f^+(K) \leqq f^+(J)$ for all $K \leqq J$, the inequality in one direction is obvious. The reverse inequality follows again by projecting on the closed l-ideal H of L generated by f^+, and setting $K = J \frown H$, giving $f(J \frown L) = f^+(J)$.

We note further that, since norm and lattice operations are preserved, and since infinite joins are merely metric limits of finite joins, and since any abstract (L)-space is a complete lattice, the $f(J)$ are a *closed* sublattice of the complete lattice of all σ-additive valuations on A. We summarize.

THEOREM 18. *Any separable abstract (L)-space is isomorphic with a closed sublattice and metrically closed linear subspace of the "concrete" (L)-space of all Lebesgue integrable functions $f(x)$ defined on the unit interval $0 \leqq x \leqq 1$, modulo functions vanishing almost everywhere (i.e., except on a set of measure zero).*

Problem 109. Generalize the results of §15 to arbitrary abstract (L)-spaces, using the Theorem of Loomis to pass from Boolean σ-algebras to sets.

16. Further references. Because of limitations of time and space, I have not included various other results about vector lattices, but shall give only references.

Abstract Lebesgue-Radon-Nikodym Theorems and integration theories have been given by B. Vulich, Uchenye Zapiski Leningrad 83 (1941), 3–29; A. Bischof, Schr. Math. Inst. Univ. Berlin 5 (1941), 237–62; E. Foradori, Deutsche Mat. 4 (1939), 578–82 and 5 (1940), 37–43; J. Dieudonné, Bull. Soc. Math. France 72 (1944), 193–239; and A. Pinsker, Doklady URSS 49 (1945), 8–11 and 168–71. Various interesting properties of l-ideals (alias normal subspaces) have been proved by S. Bochner and R. S. Phillips, Annals of Math. 42 (1941), 316–24. See also S. Bochner, ibid. 48 (1947), 1014–61.

The representation of vector lattices has been treated by K. Yosida, Proc. Imp. Acad. Tokyo 17 (1941), 121–24 and (with M. Fukamiya) 479–82, and 18 (1942), 339–42. See also A. G. Pinsker, Doklady URSS 55 (1947), 379–81 and G. P. Akilov, ibid. 57 (1947), 643–6.

Applications to completely monotone functions have been given by S. Bochner, Duke Jour. 9 (1942), 519–26, and by S. Bochner and Ky Fan, Annals of Math. 48 (1947), 168–79.

Applications to the ordinary theory of differentiation and differential equations have been given by W. M. Whyburn, Am. Math. Monthly 47 (1940), 1–10—the basic definition being due to F. Riesz, Pisa Annali (1937), p. 191. A discussion of abstract differentiation has been given by Anne O'Neill, Duke Jour. 12 (1945), 89–99.

Applications to functional equations have been given by L. Kantorovitch, Doklady URSS 4 (1936), 219–24, and Acta Math. 71 (1939), 63–97.

CHAPTER XVI

ERGODIC THEORY

1. Cyclic semigroups of transition operators. We shall be concerned below with cyclic semigroups of transition operators on (L)-spaces, in the following precise mathematical sense.

DEFINITION. *A "transition operator" on an (abstract) (L)-space L is an additive operator which carries distributions (i.e., positive elements of norm one) into distributions. A "cyclic semigroup" of operators on a space S consists of an operator T and its powers*[1] $T^2, T^3, \cdots$ *(discrete case), or else of a family of operators T^r defined and continuous in r for all positive real r and satisfying $T^r T^s = T^{r+s}$ for all r,s (continuous case).*

The case of transition operators on (L)-spaces is distinguished from the general case[2] of semigroups of linear operators on Banach spaces, by the following useful result.

THEOREM 1. *Transition operators are either isometries or contractions: they satisfy $\| fT - gT \| \leqq \| f - g \|$.*

Proof. Since $fT - gT = (f - g)T$, we need only show that $\| hT \| \leqq \| h \|$. But $\| h^+T \| = \| h^+ \|$ and $\| h^-T \| = \| h^- \|$, since T carries positive (and so negative) elements of norm one into similar elements. Hence

$$\| hT \| = \| h^+T + h^-T \| \leqq \| h^+T \| + \| h^-T \| = \| h^+ \| + \| h^- \| = \| h \|.$$

2. Interpretation: finite-dimensional case. In case L is finite-dimensional, it is easy to determine all possible transition operators. For by Thm. 1 of Ch. XV, L is then the space of all n-vectors $f = [f_1, \cdots, f_n]$ with $f \geqq 0$ if and only if every $f_i \geqq 0$. Hence the transition operators on L are the $n \times n$ matrices $T = \| t_{ij} \|$ such that (i) every $t_{ij} \geqq 0$, and (ii) $t_{i1} + \cdots + t_{in} = 1$ for all i. In other words, in the finite-dimensional case, transition operators are what are usually called "matrices of transition probabilities." These are very well known; it is precisely their behavior which is discussed in the theory of finite "dependent probabilities,[3] alias "Markoff processes."

[1] If T is any transition operator, then all its powers are transition operators; hence the most general discrete cyclic semigroup of transition operators is given by the powers of an arbitrary transition operator T.

[2] For the general case, see E. Hille, *Functional analysis and semi-groups*, Am. Math. Soc. Colloquium Publications, vol. 31, New York, 1948.

[3] See M. Fréchet, *Méthodes des fonctions arbitraires, théorie des événements en chaîne* $\cdots$," Paris, 1938, where further references to the immense literature on this subject may be found.

From the numerous (see Exs. 1–2 below) realizations of such matrices by "stochastic processes," we select one illustration.

Example 1. Let $i = 1, 2, \cdots, 52!$ denote the possible arrangements of a pack of cards. Describe the shuffling habits of a dealer by saying that in one shuffle he transforms the pack from state i to state j with probability t_{ij}. Let S and T be successive shuffles by different dealers. The total transition probability u_{ij} from state i to state j will be the sum of the probabilities $u(i, k, j)$ that the pack will pass from i to j through the different intermediate states k. And if S and T are *independent*, we will have[4] $u(i, k, j) = s_{ik}t_{kj}$, whence u_{ij} is the matrix product ST.

Hence if a single dealer shuffles repeatedly without changing his habits, the effect of n shuffles is T^n, corresponding to a discrete cyclic semigroup of transition operators.

Ex. 1. Show that the transition probabilities of radioactive disintegration can be described by a continuous cyclic semigroup of transition operators between the elements.

Ex. 2. Let T be any $n \times n$ matrix satisfying conditions (i)–(ii) of the text. Using n roulette wheels and suitable rules, invent a "game" corresponding to T.

Ex. 3*. Show that if L is n-dimensional, then the most general continuous semigroup of transition operators on L has the form $T^t = E \exp(tX)$, where (i) E is the most general transition operator satisfying $E^2 = E$, and (ii) X is the most general $n \times n$ matrix having non-negative terms off the principal diagonal, and having the sum of the terms in each row equal to zero.

Ex. 4*. Let Σ be a system with finite or countable discrete "states" $i = 1, 2, 3, \cdots$, and let s, t be fixed times. Let $\mathfrak{A}$ be the Boolean σ-algebra of all propositions of the form: Σ is in X at time s and in Y at time t, where X, Y are arbitrary sets of states. Let $p: p(X, Y)$ be any σ-distribution on $\mathfrak{A}$.

(a) Show that the $p(i, j)$, where i, j are individual states, determine p uniquely.

(b) Define the matrix $\| t_{ij} \|$ as $p(i, j)/p(i, I)$, if $p(i, I) > 0$, and as $\delta_{i,j}$ otherwise (Kronecker delta). Show that this is a matrix of transition probabilities.

(c) Show that, apart from cases where some $p(i, I) = 0$, there is a one-one correspondence between σ-distributions $p(X, Y)$ and matrices of transition probabilities.[5]

Problem 110. Extend the results of Ex. 4 to the case of a continuum of states.

3. Interpretation: general case. Cyclic semigroups of transition operators arise in probability theory under very general conditions, which will now be described.

Probability was defined mathematically in Ch. XII, §9, as a "valuation" (or measure function) $p[X]$ on a Boolean algebra $\mathfrak{A}$, which satisfied $p[X] \geqq 0$ for all $X \in \mathfrak{A}$ and $p[I] = 1$. In Ch. XV, §13, it was shown that the class of all probability functions on any fixed $\mathfrak{A}$ was a closed, convex set P in an abstract (L)-space, and that the diameter of P was two, apart from trivial cases. In Ch. XV, §14, the same was shown to be true of the set of all σ-distributions on any Boolean σ-algebra.

Frequently, the elements $X, Y, \cdots$ of $\mathfrak{A}$ represent properties of a system Σ

[4] J. L. Coolidge, *An introduction to mathematical probability*, Oxford Press, 1925, p. 18.

[5] This correlates our definition of a transition operator with the notion of a "stochastic process" as defined by J. L. Doob.

observable *a posteriori*, while for each $t > 0$, $p_t[X] \in P$ represents our best *a priori* prediction of what the state of $\sum$ will be t units of time from some initial instant. Suppose that the following additional condition is also satisfied:

(*) *If $s < t$, any $p_s \in P$ determines $p_t = p_s T_{s,t}$ uniquely, regardless of the values of p_r for $r < s$.*

We can then argue as follows.

Hypothesis p_s with frequency λ_s and hypothesis q_s with frequency μ_s should yield inference $p_s T_{s,t}$ at time t with frequency λ_s and inference $q_s T_{s,t}$ with frequency μ_s. Hence $(\lambda_s p_s + \mu_s q_s) T_{s,t} = \lambda_s p_s T_{s,t} + \mu_s q_s T_{s,t}$. Since (admissible) distributions must go into admissible distributions, we infer that every $T_{s,t}$ is a transition operator.

Further, if $r < s < t$, then for every admissible p_r,

$$p_r T_{r,t} = p_t = p_s T_{s,t} = (p_r T_{r,s}) T_{s,t} = p_r (T_{r,s} T_{s,t}).$$

Hence $T_{r,s} T_{s,t} = T_{r,t}$. Let T^u denote $T_{0,u}$. If the $T_{r,s}$ are *temporally homogeneous*, in the sense that for all r, u, $T_{0,u} = T_{r,r+u}$, we infer directly $T^u T^v = T^{u+v}$. Hence *we have a continuous cyclic semigroup of transition operators whenever we have temporal homogeneity and* (*) *holds.*[6]

Discrete cyclic semigroups of transition operators arise similarly whenever (as in Example 1) the state of Σ changes through any sequence of transitions due to repetitions of the same cause, provided that Σ has time to "forget" its entire previous history between successive transitions.

Ex. Show that a two-parameter family of transition operators can satisfy $T_{r,s} T_{s,t} = T_{r,t}$ for all $r < s < t$, and also $T^u T^v = T^{u+v}$ for all $u, v > 0$, even though $T_{0,u} \neq T_{r,r+u}$ in general. (Hint: Let $T_{r,s} = E$, where E is idempotent.)

4. Specific illustrations. The following are typical examples of "stochastic processes," represented by cyclic semigroups of transition operators.

Example 2. A Geiger counter records cosmic rays,[7] at an average rate of λ per minute. Let $\mathfrak{A}$ be the Boolean algebra of all sets X, Y, $\cdots$ of integers $n = 0, 1, 2, \cdots$. Let $p_t[X]$ be the *a priori* probability that the total number n of cosmic rays counted in any t minute interval will be in X. This is a stochastic process.

An exact formula can be developed briefly as follows. In a time interval of Δt minutes, the transition probabilities are nearly expressed by the infinite

[6] In this connection, we note a direct relation between the concept of a transition operator and the laws of thermodynamics, quite apart from Fourier's differential equations for heat conduction. Let the thermal energy of each region R of an insulated solid I be $h(R)$; let the thermal energy five minutes later be $h^*(R)$. Then conservation of energy makes $h(I) = 1$ imply $h^*(I) = 1$, and the second law of thermodynamics implies that everywhere positive temperature, relative to any zero, is preserved.

[7] Example 2 typifies the "Poisson case" of A. Khinchine, *Die asymptotische Gesetze der Wahrscheinlichkeitsrechnung*, Berlin, 1933, Ergebnisse series. Khinchine does not stress the semigroup aspect; see also Ex. 1 below. See also A. Khinchine, *Statistical mechanics*, translated by G. Gamow, Dover, 1948.

square matrix $T^{\Delta t} = (I + \lambda\Delta tJ)/(1 + \lambda\Delta t)$, where I is the identity matrix, and J has ones immediately above the main diagonal, and zeros elsewhere—whence J^n has ones n spaces above the main diagonal, and zeros elsewhere. Passing to the limit,

$$T^t = \operatorname*{Lim}_{n\to\infty} (T^{t/n})^n = \operatorname*{Lim}_{n\to\infty} (I + \lambda tJ/n)^n/(1 + \lambda t/n)^n$$
$$= e^{-\lambda t}(I + \lambda tJ + \lambda^2t^2J^2/2! + \cdots \lambda^nt^nJ^n/n! + \cdots).$$

There follows the well-known formula

$$(1) \qquad p_t[X] = e^{-\lambda t} \sum_{n \in X} \lambda^n t^n/n!\,.$$

Example 3. Let Σ be the position of a tiny particle suspended in a liquid, and undergoing "Brownian movement" under random molecular bombardment. Let its position be (a_1, a_2, a_3) at time $t = 0$. Let $\mathfrak{A}$ be the Boolean algebra of all "elementary" subsets (Ch. XI, §1) of space. For each $X \in \mathfrak{A}$ and positive real number t, let $p_t[X]$ be the probability that the particle will be in X at time t, as far as this can be determined from knowing the position at $t = 0$.

The analytical treatment of this case is more difficult. However, Kolmogoroff[8] has shown that if we assume (as in §3) that we have a cyclic semigroup of transition operators,[9] that these can be expressed in the form of integral equations, and the phenomenon is spatially homogeneous and isotropic, then

$$(2) \qquad p_t[X] = \frac{1}{\sqrt{\pi\lambda t}} \iiint_X e^{-\Sigma(x_i - a_i)^2/\lambda t}\, dx_1\, dx_2\, dx_3\,,$$

for a suitable coefficient of diffusion λ.

It is to be noted that in Example 3 the transition operators involved are not powers in the ordinary sense of an infinitesimal transition operator; in fact, they do not even have inverses.[10] Hence the semigroup involved cannot be extended to a group.

Example 4. Let $v(t)$ denote the instantaneous vector velocity of a fluid of known turbulence characteristics at a fixed point P and variable time t; let the mean velocity and $v(0)$ be known. Then for each elementary subset R of

[8] A. Kolmogoroff, *Die analytische Methoden der Wahrscheinlichkeitsrechnung*, Math. Annalen 104 (1931), 414–58, and *Zur Theorie der stetigen zufalligen Prozesse*, ibid., 108 (1933), 149–60. I only indicate his precise assumptions; the final formulas has been obtained earlier by Einstein and Smoluchowski.

[9] The assumption of the independence of successive transition operators is not fulfilled over extremely short intervals of time. If it were, by a well known theorem of Wiener, the particle would have an infinite mean velocity.

[10] That this was true for the transition operators involved in heat conduction (last footnote of §3) was already observed by Kelvin; see J. C. Maxwell, *Theory of Heat*, London, 1872, p. 244. For special ways in which semigroups can be generated by infinitesimal operators, see G. Birkhoff, *Product integration*, M. I. T. Jour. Math. Phys. 16 (1937), p. 123; E. Hille, *Notes on linear transformations* II, Annals of Math. 40 (1939), 1–47, and op. cit. supra.

the velocity or "hodograph" space, let $p_t[R]$ be the probability that $v \in R$ at time t, as far as this is predictable. (This may not be a semigroup.)

Example 5. Consider the n-body problem of Newtonian gravitation theory, mentioned in Ch. XII, §4. If our knowledge of the n-body system Σ at time $t = 0$ is expressed by the probability[11] function $p[X]$, then at time t_1 it is expressed by $p_t[X] = p[X\tau^{-1}]$, where τ is the transformation of phase-space induced in time t_1 by the differential equations of motion.

Ex. 1. Describe analytically the statistically predicted decomposition products of a radioactive element after a time lapse t, in terms of the matrix of transition frequencies of it and the elements into which it is decomposed. Take a specific example, such as radium.

Ex. 2. Show that if the inverse of a transition operator T exists and is a transition operator, then T is an isometry. Infer that if the space L on which it operates is finite-dimensional, T is a permutation matrix.

Ex. 3. Write down specific analytical formulas for τ in the case of the two-body problem, in Example 5.

5. Types of transition operators. In the usual discussions of Markoff processes,[12] it is necessary to give separate formulations for discrete and continuous physical systems, and often a third formulation for the "deterministic" case as well. Our more geometrical approach avoids this multiple formulation, and has the added advantage of giving easily visualized means for distinguishing the essentially different cases. To show this, we first consider cases in which Theorem 1 assumes special forms; we use the notation of §3.

Consider the "tychistic" case of "independent probabilities," in which pT is independent of T, as in the case of successive throws of a pair of dice. This is the case where P is contracted to a point by T, and L projected onto the axis through this point. Again, in the antipodal deterministic case of classical mechanics, we have an *isometry* of L.

It is the intermediate "stochastic" case which is typical of the theory of dependent probabilities: here the set P is contracted somewhat, but not to a point. A case of especial importance is that in which the following condition, first signalized by Markoff, is fulfilled.

Hypothesis of Markoff. For some r, there is a positive lower bound d in L to the transforms pT^r of distributions p. This means that $d > 0$ and that $d \leqq pT^r$ for all $p \in P$.

This is fulfilled in Example 1, since shuffles differing by a transposition are

[11] Our knowledge is not exact, because of limits on instrumental precision; in the theory of errors, it is often assumed to be given by a Gaussian distribution. For a detailed discussion of the relation between differential equations of motion and transformations of phase space, see G. D. Birkhoff, *Dynamical systems*, Am. Math. Soc. Colloquium Publications, vol. 9, New York, 1927; also H. Poincaré, *Méthodes nouvelles de la mécanique céleste*, Paris, 1899.

[12] Kolmogoroff, loc. cit.; J. L. Doob, Trans. Am. Math. Soc. 42 (1937), 107–40; with a useful bibliography. S. Bochner, Annals of Math. 48 (1947), 1014–61, gives an abstract treatment.

always possible in practice, and the symmetric group is generated by transpositions. It is also fulfilled in Example 3, provided the liquid is in a *bounded* container, and in Example 4. It is not fulfilled in Examples 2 or 5. We shall now study its consequences.

6. Stable distributions; Markoff's theorem. We first define a distribution p to be "stable" under a transition operator T, if and only if it is a *fixpoint* of T—that is, if and only if $pT = p$. In this case, by Thm. 1, distributions originally near p stay near p under T and its iterates.

THEOREM 2. *The set of points of any (L)-space left fixed by any transition operator T is metrically closed, a subspace, and a sublattice.*

Proof. Since T is continuous, the set is metrically closed in L. Since T carries upper (lower) bounds into upper (lower) bounds, and is a contraction, it carries the unique upper bound $x = f \cup g$ to f and g, which satisfies $\|f - x\| + \|x - g\| \leqq \|f - g\|$, into itself.

It is a corollary that the "stable distributions" (the intersection of the subspace of Thm. 2 with P) are a closed convex set. Hence the number of stable distributions is either zero, one (the "metrically transitive" case[13]), or infinite. The metrically transitive case is the most interesting, but all three cases are possible. Note the following example.

Example 6. Let T carry $x = [x_1, x_2, x_3, \cdots]$ into $[0, x_1, x_2, \cdots]$, in the (L)-space (l). Then T is an isometric transition operator; yet $xT = x$ only if $x = 0$.

In various cases, stable distributions can be found explicitly by special methods. Considerations of symmetry are often helpful (see Exs. 1, 6* below). Again, if the pT^n are bounded above, then $p^* = \text{Lim sup}_{n\to\infty} pT^n$ is a positive fixpoint of L, and $p^*/\|p^*\|$ is a stable distribution. In the finite-dimensional case, the characteristic polynomial of the matrix $\|t_{ij}\|$ of transition probabilities can of course be used; the existence of a positive characteristic vector[14] follows from the preceding remark and Thm. 1.

We shall now show that if the Hypothesis of Markoff is satisfied, we always have the metrically transitive case.

THEOREM 3. *If Markoff's Hypothesis is satisfied, then there is a unique stable distribution p_0. Moreover the pT^k tend to p_0 uniformly, with the rapidity that the terms of a convergent geometrical progression tend to zero.*

---

[13] In the sense of G. D. Birkhoff and Paul Smith, *Structure analysis of surface transformations*, Jour. de Math. 7 (1928), p. 365.

[14] This result is due to G. Frobenius, *Über Matrizen aus nichtnegativen Elementen*, S.-B. Berlin (1912), 456–77. A more general proof can be based on the fact that, projectively, the non-negative vectors of L form a simplex, and the fixpoint theorem of Brouwer for continuous transformations of simplexes; cf. Alexandroff-Hopf [1, p. 480]. For a recent attempt to extend these ideas to the infinite-dimensional case, see E. Rothe, Am. Jour. Math. 66 (1944), 245–54.

Proof. Let $p, q \in P$ be given. Set $h = p \frown q, f = p - h, g = q - h, \mu = 1 - \|h\|$. Then $f, g \geqq 0$, $\|f\| = \|g\| = \mu$, and $\|p - q\| = \|f\| + \|g\| = 2\mu$, by Ch. XIV, (19), and Ch. XV, (6) and (15). Also, since T is additive, $pT^r - qT^r = fT^r - gT^r$. By the additivity of norm (Ch. XV, (15)),

$$\|fT^r - gT^r\| = \|fT^r\| + \|gT^r\| - 2\|fT^r \frown gT^r\| = 2\mu - 2\|fT^r \frown gT^r\|.$$

Evidently $f = \mu p_1$ for some distribution p_1; hence by Markoff's Hypothesis $fT^r \geqq \mu d$; similarly, $gT^r \geqq \mu d$; hence $fT^r \frown gT^r \geqq \mu d$. By obvious substitutions in preceding equations, we infer

$$\|pT^r - qT^r\| = \|fT^r - gT^r\| \leqq 2\mu - 2\mu\|d\| = (1 - \|d\|)2\mu.$$

Since $2\mu = \|p - q\|$, we conclude the following important

LEMMA. *T^r contracts P uniformly; in symbols*

$$(3) \qquad \|pT^r - qT^r\| \leqq (1 - \|d\|)\|p - q\|.$$

Theorem 3 follows from (3) and simple geometrical considerations.[15] Indeed, if $k > nr$, then $pT^k = (pT^{k-nr})(T^r)^n$ lies in the transform of P under the nth iterate of T^r. These form a nested sequence $P \geqq PT^r \geqq PT^{2r} \geqq \cdots \geqq PT^{nr} \geqq \cdots$, and by (3) the diameter of PT^{nr} is at most $2(1 - \|d\|)^n$. Hence for any $p \in P$, $\|pT^h - pT^k\| \leqq 2(1 - \|d\|)^n$ if $h, k > nr$. Thus the pT^h satisfy Cauchy's convergence test, and, P being a complete metric space, they converge to a limit p_0.

Furthermore, p_0 is *stable*. For since $pT^s \to p_0$ as $s \to \infty$, and T^r is continuous, $pT^sT^r \to p_0T^r$; but $pT^{s+r} \to p_0$ as $s \to \infty$, and so $p_0T^r = p_0$. The *uniqueness* of p_0, and the fact that it is the same for all p, now follow from (3).

COROLLARY 1. *In the case of a discrete semigroup, for any fixed p,* Sup $pT^n \leqq p + \sum_{k=0}^{\infty}(pT - p)T^k$ *is finite. With continuous semigroups,* Sup pT^r *is similarly finite if the pT^r are bounded on $0 \leqq r < r_0$ for some $r_0 > 0$.*

Remark. This follows since T^r is continuous in r.

COROLLARY 2. *Let $T_1, \cdots, T_n$ be any sequence of transition operators, and denote* $\mathrm{Inf}_{p \in P}\, pT_i$ *by d_i. Then*

$$(4) \qquad \|p(T_1T_2 \cdots T_n) - q(T_1T_2 \cdots T_n)\| \leqq \|p - q\| \cdot \prod_{i=1}^{n}(1 - \|d_i\|).$$

---

[15] Historical note. Thm. 3 was first proved for finite matrices by Frobenius, op. cit. The geometrical half of the proof goes back to C. Neumann, who used it to solve Dirichlet's problem for convex regions (cf. Picard's *Traité d'analyse*, 2d ed., vol. 1, p. 170). It was used by Picard (op. cit., vol. 2, p. 301) to prove the existence of solutions of certain nonlinear differential equations. The geometrical approach to the theorem on matrices was sketched by G. Rajchmann (Comptes Rendus 190 (1930), p. 729; cf. J. Hadamard, Atti Congresso Bologna 5 (1928), 133–9). The general case was first treated by the author, Proc. Nat. Acad. Sci. 24 (1938), 154–9.

Ex. 1. Show that in Example 1, the distribution which assigns to each arrangement the probability $1/52!$ is stable.

Ex. 2. Show that if L is finite-dimensional, the conclusion of Thm. 3 implies Markoff's hypothesis, and that so does the inequality (3). Show that these converses need not be true if L is infinite-dimensional.

Ex. 3. Show that if L is finite-dimensional, Thm. 3 holds whenever, given $p, q \in P$, there exists a number r such that $pT^r \frown qT^r > 0$. Show that this is not true in the infinite-dimensional case. Show that (3) implies Thm. 3 in any case.

Ex. 4*. Let $\| t_{ij} \|$ be any matrix of non-negative terms from an ordered field, such that the sum of the terms in each row and in each column is one. Show that it is a weighted mean of permutation matrices.[16]

Ex. 5*. (a) Let $T = \| t_{ij} \|$ be any $n \times n$ matrix of transition probabilities satisfying Markoff's Hypothesis. Show that the components of the unique stable distribution $(p_1, \cdots, p_n)$ are rational functions of the t_{ij}, and obtain explicit formulas if $n = 3$.

(b) Using Bayes' Theorem, show that the equations $p_i t_{ij} = p_j t_{ji}^{\sim}$ define from T a unique "probability of causes" matrix $T^{\sim}$ in case all p_i are positive.

(c) Show that $T^{\sim\sim} = T$ always, and that $T^{\sim} = T$ if and only if[17] $t_{kj}t_{ji}t_{ik} = t_{ki}t_{ij}t_{jk}$ for all i, j, k.

Ex. 6*. In the kinetic theory of gases, consider the problem of n elastic spheres of equal mass. Show that the distribution which assigns in the $(6n - 1)$-dimensional phase-space of all positions and velocities compatible with a given total kinetic energy K, a probability density proportional to the product of volume in the configuration space, by area on the $(3n - 1)$-dimensional sphere of velocity-distributions compatible with K, is invariant under the transformations of phase-space corresponding to the passage of time. Then letting $n \to \infty$, obtain Maxwell's law of velocity distribution.

Problem 111. Extend the result of Ex. 4 to the infinite-dimensional case, under suitable hypotheses.

7. Ergodic elements. It is clear that in the deterministic (isometric) case of classical mechanics, the transforms pT^r of non-stable distributions cannot converge, since $\| pT^{r+1} - pT^r \| = \| pT - p \|$ identically. Nevertheless, as is well-known, their *averages* p_N ($\sum_{k=0}^{N-1} pT^k/N$ in the discrete, $\int_0^N pT^s\, ds/N$ in the continuous case) do frequently converge; theorems proving this conclusion are usually called "ergodic theorems."[18]

Since Markoff's Theorem 3 is much stronger than ergodicity, it seems natural to try to prove ergodic theorems which apply simultaneously to the deter-

[16] G. Birkhoff, Revista Univ. Nac. Tucuman 5 (1946), 147–51.

[17] This simplifies a result of Kolmogoroff, Math. Annalen 112 (1936), 155–61.

[18] Ergodic theorems have a philosopical bearing on statistical mechanics, but the connection between the two is still incomplete. For a historical discussion of the connection, see G. D. Birkhoff and B. O. Koopman, *Recent contributions to ergodic theory*, Proc. Nat. Acad. Sci. 18 (1932), 279–82; also E. Hopf, *Ergodentheorie*, Berlin, 1937, and N. Wiener, *The ergodic theorem*, Duke Jour. 5 (1939), 1–18. Proofs of the ergodic theorem in classical mechanics were first given by J. von Neumann, Proc. Nat. Acad. Sci. 18 (1932), 70–82, and G. D. Birkhoff, ibid. 17 (1931), 650–65. The latter's "pointwise ergodic theorem" is applicable to individual paths, and hence more relevant to dynamics; its proof is, incidentally, combinatory and so lattice-theoretic in spirit. See also Nelson Dunford and D. S. Miller, Trans. Am. Math. Soc. 60 (1946), 538–49; H. R. Pitt, Proc. Camb. Phil. Soc. 38 (1942), 325–43; W. Hurewicz, Annals of Math. 45 (1944), 192–206; P. R. Halmos, Proc. Nat. Acad. Sci. 32 (1946).

ministic, stochastic, and mixed case. This idea has occurred independently to various authors;[19] we shall carry through the details in §§8–10.

First, let $\{T^\tau\}$ be any discrete or continuous cyclic semigroup of linear operators on a Banach space B. We shall call an element $f \in B$ "ergodic" if and only if the *averages* g_s of the fT^τ, defined above, converge metrically to a fixpoint. Example 6 of §6 shows that, even in the case of transition operators on (L)-spaces, there need exist no fixpoints except 0; hence we cannot hope for an ergodic theorem in the real sense of the word, in all cases. We can however prove the following result.

THEOREM 4. *The set E of elements ergodic under any cyclic semigroup $\{T^\tau\}$ of linear isometries or contractions of any Banach space is a metrically closed subspace. It contains all its images and antecedents under $\{T^\tau\}$.*

Proof. If the means g_s of f and g_s^* of f^* converge to a and a^* respectively, then the means $g_s + g_s^*$ resp. λg_s of $f + f^*$ resp. λf converge to $a + a^*$ resp. λa; hence E is a subspace. It is equally easy to show that E is metrically closed. For $\| f - f^* \| < \epsilon$ implies $\| g_s - g_s^* \| < \epsilon$ for all s. Hence if $\| f^{(n)} - f^* \| \to 0$ as $n \to \infty$, and every $f^{(n)}$ is ergodic, the $a^{(n)} = \lim_{s\to\infty} g_s^{(n)}$ converge metrically to a limit a. Moreover

$$\| g_s^* - a \| \leqq \| g_s^* - g_s^{(n)} \| + \| g_s^{(n)} - a^{(n)} \| + \| a^{(n)} - a \| .$$

But the first and third of these terms are bounded by $\| f^* - f^{(n)} \|$ and so are arbitrarily small when n is large. While for fixed n, the second tends to zero as $s \to \infty$. Hence $g_s^* \to a$ as $s \to \infty$, and f^* is ergodic. Finally, that E contains all its images and antecedents under T^τ is obvious, since every fT^τ has the same limit of means (if any) as f.

But any metrically closed subspace of a Banach space is ipso facto weakly closed, hence[20]

COROLLARY. *The set E is closed under the weak topology of the space.*

---

[19] A. Khinchine, op. cit., and J. L. Doob, Trans. Am. Math. Soc. 36 (1934), 759–75 and 44 (1938), 87–150, observed that (in the "tychistic" case) sequences of independent distributions were expressible as a single measure on a product space. Hence if certain other conditions are fulfilled, the classical ergodic theorem of G. D. Birkhoff applies, and yields various results. The finite-dimensional case was treated in another way by M. Fréchet, op. cit. supra, p. 109. The cases in which T is defined by an integral equation was also treated by Fréchet, Bull. Soc. Math. France 62 (1934), 68–83.

The present direct formulation was first treated by the author, Proc. Nat. Acad. Sci. 24 (1938), 154–9, where weak convergence was proved. The improved results given in the text were substantially obtained by F. Riesz, *Some mean ergodic theorems*, Jour. Lond. Math. Soc. 13 (1938), 274–8, and by S. Kakutani and K. Yosida, *Operator theoretical treatment of Markoff's process*, Proc. Imp. Acad. Tokyo 14 (1938), pp. 286, 333, 363. F. Riesz gives an interesting historical review, mentioning his own earlier work, in Commentarii Math. Helv. 17 (1945), 221–39. See also M. Fréchet, Revue Sci. III. 79 (1941), 407–17; W. F. Eberlein, Proc. Nat. Acad. Sci. 34 (1948), 43–7; H. Nakano, Annals of Math. 49 (1948), 538–56.

[20] According to Banach [1, p. 133], $x_i \to x$ "weakly" if and only if for every (bounded) linear functional λ, $\lambda(x_i) \to \lambda(x)$. The result quoted is one of Banach's fundamental theorems; a complete proof is given by Banach [1, pp. 58–8 and 113–4].

8. Ergodic theorem. We now obtain a general sufficient condition for an element of a Banach space to be ergodic.

THEOREM 5 (Ergodic Theorem). *If the means g_s of the fT^r lie in a weakly compact set, then f is ergodic.*

Proof. By hypothesis, some subsequence $\{g_{s(i)}\}$ of $\{g_s\}$ converges weakly to a limit a. But every $f - fT^r$ is ergodic, since if $s > r$,

$$\left\| \frac{1}{s} \sum_{k=0}^{s-1} (f - fT^r)T^k \right\| = \frac{1}{s} \left\| \sum_{k=0}^{r-1} fT^k - \sum_{k=s}^{s+r-1} fT^k \right\| \leqq 2r/s,$$

so that the means of its transforms converge metrically to 0. (A similar formula holds for continuous semigroups.)

Hence every difference $f - g_{s(i)}$, being a mean of $f - fT^r$, is in the set E of ergodic elements. But this set is weakly closed (by the Corollary of Thm. 4); hence $f - a$ is in E. It remains to show that a is in E—whence $f = (f - a) + a$ will be in E. But this is an obvious corollary of the

LEMMA. *If any subsequence $\{g_{s(i)}\}$ of the g_s converges metrically or weakly to the limit a, then a is a fixpoint.*

Proof. One can assume $\| f \| = 1$ without losing generality. But in this case, for any positive integer s and any $k < s$, $s(g_s - g_sT^k)$ is $\sum_{r=0}^{k-1} fT^r - \sum_{r=s-k}^{s-1} fT^r$ resp. $\int_0^k fT^r \, dr - \int_{s-k}^{s} fT^r \, dr$ in the discrete resp. continuous case. In either case,

$$\| g_s - g_sT^k \| \leqq 2k/s. \tag{4}$$

Now with metric convergence, $\| g_{s(i)} - a \| \to 0$ implies $\| g_{s(i)}T^k - aT^k \| \to 0$ for any k. But $\| g_{s(i)} - g_{s(i)}T^k \| \to 0$ by (4); hence $\| a - aT^k \|$ is less than any positive constant, and $a = aT^k$. Similarly, with weak convergence, $\lambda(g_{s(i)} - g_{s(i)}T^k) \to 0$ for every linear functional λ and every k; hence for all λ, $\lambda(a - aT^k)$ is less than any positive constant. Hence $\lambda(a) = \lambda(aT^k)$ for every λ, whence $a = aT^k$.

Whether or not the theorem holds whenever the T^r are continuous linear operators is an undecided question.

9. Corollaries. From Theorem 5, one can infer directly

COROLLARY 1. *Let $\{T^r\}$ be any cyclic semigroup of linear isometries or contractions of a Banach space which is finite-dimensional, a space (L^p), or a space (l^p) $(p > 1)$. Then every element is ergodic under $\{T^r\}$.*

For in the finite-dimensional case the unit sphere is metrically compact, and in the other cases it is weakly compact. A direct proof can also be given for the spaces (L^p) and (l^p) $(p > 1)$, which applies to any "uniformly convex" Banach space.[21]

[21] See the author's *The mean ergodic theorem*, Duke Jour. 5 (1939), 19–20. For the properties of the spaces considered, see Banach [1], pp. 84, 130–1.

Corollary 2. *If $a \leqq fT^r \leqq b$ for all r, and the Banach space is the space (L) or (l), then f is ergodic.*

In words, f is ergodic if its transforms are bounded lattice-theoretically. This follows immediately from the well-known fact that the set $a \leqq f \leqq b$ is weakly compact.

Corollary 3. *If the function $f(x) = 1$ is invariant under transition operators T^r on the space (L), then every element is ergodic.*

For the condition $a \leqq f(x) \leqq b$ for all x is preserved under $\{T^r\}$, since transition operators are linear and order-preserving; hence by Corollary 2, all bounded functions are ergodic elements of the space (L). But bounded functions are topologically dense; hence the argument is completed by Theorem 4.

In particular, Corollary 3 applies to measure-preserving point transformations of any space Ω of finite total measure. But, as noted by Liouville, with any Lagrangian dynamical system, the flows T^t of phase-space corresponding as in Example 5 to lapses of time t are measure-preserving in Hamiltonian coordinates, since[22] under these $\dot{p}_i = \partial H/\partial q_i$ and $\dot{q}_i = -\partial H/\partial p_i$. Hence Cor. 3 applies to any Lagrangian system whose total measure is finite (i.e., usually, whose phase-space is compact).

Now consider the kinetic theory of gases. As in Ex. 6 of §6, we can find a stable distribution. Hence if we could prove that the flow with a given energy was "metrically transitive," we could conclude that the time average of velocity distributions always approached this distribution. But this conjecture has never been proved or disproved.

10. Extensions. We are now ready to extend Corollary 2 to arbitrary (L)-spaces; the extension is due to Kakutani.[23] Let T^n be a discrete semigroup of transition operators on an abstract (L)-space L. For any $f \in L$, the fT^n when combined linearly and lattice-theoretically generate a *separable* closed subspace S of L. By Thm. 18 of Ch. XV, this may be embedded in the ordinary space (L). Hence the fT^n, being bounded by Inf $\{fT^n\}$ and Sup $\{fT^n\}$ in S, lie in a weakly compact set. Hence Cor. 2 applies also to discrete semigroups on abstract (L)-spaces. To pass to the case of continuous semigroups, we need merely restrict our attention to the means of $g = \int_0^1 fT^r\, dr$ under the discrete semigroup $T^1, T^2, T^3, \cdots$. We conclude

Theorem 6. *Any element f of an abstract (L)-space, whose transforms under a cylic semigroup of transition operators are bounded lattice-theoretically, is ergodic.*

Theorem 7. *If an element f of an abstract (L)-space is ergodic under a cyclic semigroup of transition operators, and $0 \leqq x \leqq f$, then x is ergodic.*

[22] An infinitesimal transformation $\dot{x}_i = X_i$ conserves volume if and only if Div $X = \sum \partial X_i/\partial x_i = 0$. In the above case, the divergence is $\sum \partial^2 H/\partial p_i \partial q_i - \sum \partial^2 H/\partial q_i \partial p_i = 0$.

[23] *Mean ergodic theorem in abstract (L)-spaces*, Proc. Imp. Acad. Tokyo 15 (1939), 121–3; see Kakutani [1] for details.

Proof. Let y_s and g_s denote the sth means of x and f respectively; since transition operators are positive, $0 \leqq y_s \leqq g_s$ for all s. But by hypothesis, $\{g_s\}$ converges to a stable distribution a as $s \to \infty$; hence

$$\| y_s - (y_s \frown a) \| \leqq \| g_s - (g_s \frown a) \| \to 0.$$

By Thm. 6, $y_s \frown a$ is ergodic for all s; hence the "ergodic oscillation" $\limsup_{s,s' \to \infty} \| y_s - y_{s'} \|$ of x is bounded by any positive number. For since every $x - y_s$ is ergodic, as in the proof of Thm. 5, it is equal to that of every y_s, and this is bounded by every $\| y_s - y_s \frown a \|$ since $y_s \frown a$ is ergodic. Hence it is zero, and x is ergodic.

It is not however true in general that the ergodic elements of an (L)-space form an l-ideal (normal subspace). To see this, consider Example 6 with $f = [1, -1, 0, 0, \cdots]$. Then f is ergodic, whereas f^+ and f^- are not.

11. Poincaré's recurrence theorem. Closely related to the Ergodic Theorem is Poincaré's well known Recurrence Theorem (Wiederkehrsatz), for deterministic processes in a phase-space of finite total measure. We shall now see how far this result can be extended to stochastic processes.[24] In order to find this out, we first make the relevant hypothesis.

Hypothesis A. For some $e > 0$ and f with $0 \leqq f \leqq e$, we have $eT = T$.

The relation of this hypothesis to that of invariant measure (needed to exclude Example 6), is obvious. In the deterministic case treated by Poincaré, Hypothesis A implies

$$f \frown \limsup_{n \to \infty} \{fT^n\} = f. \tag{5}$$

In the deterministic case, where we are dealing with characteristic functions of sets, (5) is moreover equivalent to

$$\operatorname*{Lim}_{m \to \infty} f \frown m \limsup_{n \to \infty} \{fT^n\} = f. \tag{5'}$$

Our main conclusion is the following.

THEOREM 8. *Hypothesis* A *implies* (5′), *for any transition operator* T.

Proof. Denote $\limsup_{n \to \infty} \{fT^n\}$ by f^*;[25] in the language of Ch. XIV, §11, Theorem 8 asserts that f is in the closed l-ideal $J(f^*)$ generated by f^*. To prove this, let $g = f - \lim_{m \to \infty} f \frown mf^*$ be the component of f in the complement J' of $J(f^*)$, and let $g^* = \limsup_{n \to \infty}\{gT^n\}$. Then since $g \leqq f$, we have $g^* \leqq f^*$. Moreover since $J(f^*)$ and J' are disjoint l-ideals, $g \frown f^* = 0$; hence $g \frown g^* = 0$. The theorem is clearly tantamount to $g = 0$; this we now prove.

[24] This question was raised by M. Kac, *On the notion of recurrence in discrete stochastic processes*, Bull. Am. Math. Soc. 53 (1947), 1002–10. Kac treated the case of countably many discrete states.

[25] See especially Ex. 1, loc. cit., where what we have here denoted $J(f^*)$ would be denoted $(f^*)^{**}$.

Evidently $g \leqq e = g^* + (e - g^*)$, whence

$$g \leqq [g \frown g^*] + [g \frown (e - g^*)] = 0 + g \frown (e - g^*) \leqq e - g^*.$$

By definition of g^*, evidently also $g^*T = g^*$. Therefore Hypothesis A is still satisfied if we substitute $e_1 = e - g^*$ for e and g for f. Further, since $g \leqq e_1$ and $e_1T = e_1$, every $gT \leqq e_1$, and so $g^* \leqq e_1$. Hence we can argue as before, getting $g \leqq e_1 - g^* = e - 2g = e_2$. Repeating the argument k times, we have $e - kg^* \geqq g \geqq 0$ for all k. Hence $g^* = 0$ and $\| g \| \leqq \| g^* \| = 0$, completing the proof.

Ex. 1. Prove that Hypothesis A implies (5) in the deterministic case.

Ex. 2. Prove that for any N, Hypothesis A implies

$$\lim_{k \to \infty} f \frown (fT^N + \cdots + fT^{N+k}) = f, \tag{5'}$$

in the general case.

Ex. 3. Prove that Hypothesis A need not imply (5), or even

$$f \frown \bigvee_{n=1}^{\infty} fT^n = \lim_{N \to \infty} \bigvee_{n=1}^{N} (f \frown fT^n) = f, \tag{5'''}$$

in the general case. (Hint: Try the idempotent case.)

BIBLIOGRAPHY

This partial bibliography comprises only works of especial originality or historical importance. More complete references will be found in the text. For aspects relating to logic, a complete bibliography has been published by the Journal of Symbolic Logic, Vol. 1, Part 4. Since 1940, papers on lattice theory have been indexed under that heading in Mathematical Reviews.

A. A. Albert, [1] *Modern higher algebra*, Chicago, 1937.

P. Alexandroff and H. Hopf, [1] *Topologie*, Berlin, 1935.

S. Banach, [1] *Théorie des opérations linéaires*, Warsaw, 1933.

A. A. Bennett, [1] *Semi-serial order*, Am. Math. Monthly 37 (1930), 418–23.

G. Bergmann, [1] *Zur Axiomatik der Elementargeometrie*, Monatsh. Math. und Phys. 36 (1929), 269–84.

G. Birkhoff, [1] *On the combination of subalgebras*, Proc. Camb. Phil. Soc. 29 (1933), 441–64; [2] *Combinatorial relations in projective geometries*, Annals of Math. 36 (1935), 743–8; [3] *On the structure of abstract algebras*, Proc. Camb. Phil. Soc. 31 (1935), 433–54; [4] *General ergodic theorems* (with L. Alaoglu), Annals of Math. 41 (1940), 293–309; [5] *Generalized arithmetic*, Duke Jour. 9 (1942), 283–302; [6] *Lattice-ordered groups*, Annals of Math. 43 (1942), 298–331.

G. Birkhoff and S. MacLane, [1] *Survey of modern algebra*, New York, 1941.

G. Boole, [1] *The mathematical analysis of logic*, Cambridge, 1847; [2] *An investigation into the laws of thought*, London, 1854 (reprinted by Open Court Publishing Co., Chicago, 1940).

J. Certaine, [1] *Lattice-ordered groupoids and some related problems*, Harvard Doctoral Thesis (unpublished), 1943.

M. M. Day, [1] *Arithmetic of ordered systems*, Trans. Am. Math. Soc. 58 (1945), 1–43.

R. Dedekind, [1] *Über Zerlegungen von Zahlen durch ihre grossten gemeinsamen Teiler*, Festschrift Techn. Hoch. Braunschweig (1897), and Ges. Werke, Vol. 2, pp. 103–48; [2] *Über die von drei Moduln erzeugte Dualgruppe*, Math. Annalen 53 (1900), 371–403, and Ges. Werke, Vol. 2, 236–71.

R. P. Dilworth, [1] *Non-commutative residuated lattices*, Trans. Am. Math. Soc. 46 (1939), 426–44. [2] *Lattices with unique complements*, Trans. Am. Math. Soc. 57 (1945), 123–54.

C. J. Everett and S. Ulam, [1] *On ordered groups*, Trans. Am. Math. Soc. 57 (1945), 208–16.

H. Freudenthal, [1] *Teilweise geordnete Moduln*, Proc. Akad. Wet. Amsterdam 39 (1936), 641–51.

O. Frink, [1] *Topology in lattices*, Trans. Am. Math. Soc. 51 (1942), 569–82; [2] *Complemented modular lattices and projective spaces of infinite dimension*, ibid., 50 (1946).

V. Glivenko, [1] *Géometrie des systèmes de choses normées*, Am. Jour. 58 (1936), 799–828; [2] *Théorie des structures*, Paris, 1938.

M. Hall, [1] *Projective planes*, Trans. Am. Math. Soc. 54 (1943), 229–77.

F. Hausdorff, [1] *Grundzuge der Mengenlehre*, Leipzig, 1914; [2] *Mengenlehre*, Berlin, 1927 (second ed. of [1]).

E. V. Huntington, [1] *Sets of independent postulates for the algebra of logic*, Trans. Am. Math. Soc. 5 (1904), 288–309.

B. Jónsson and A. Tarski, [1] *Direct decompositions of finite algebraic systems*, Notre Dame Mathematical Lectures, No. 5 (1947), 64 pp. (See also Abstract 51-9-149 (1945) of Bull. Am. Math. Soc.).

S. Kakutani, [1] *Concrete representation of abstract (L)-spaces and the mean ergodic theorem*, Annals of Math. 42 (1941), 523–37; [2] *Concrete representation of (M)-spaces*, ibid., pp. 994–1024.

L. KANTOROVITCH, [1] *Lineare halbgeordnete Raume*, Mat. Sbornik 2 (44) (1937), 121–68.

S. KISS, [1] *Transformations on lattices and structures of logic*, privately printed, New York, 1947. For sale by the author at 11 East 92 St.

F. KLEIN, [1] *Einige distributive Systeme in Mathematik und Logik*, Jahr. D. M. V. 38 (1929), 35–40; [2] *Zur Theorie der abstrakten Verknupfungen*, Math. Annalen 105 (1931), 308–23; [3] *Grundzuge der Theorie der Verbande*, (ibid.) 111 (1935), 596–628.

G. KOETHE, [1] *Die Theorie der Verbande, ein neuer Versuch zur Grundlegung der Algebra und der projektiven Geometrie*, Jahr. D. M. V. 47 (1937), 125–44.

M. and S. KREIN, [1] *Sur l'espace des fonctions continues définies sur un bicompact de Hausdorff*, Mat. Sbornik 13 (1943), 1–38.

W. KRULL, [1] *Verallgemeinerte Abelsche Gruppen*, Math. Zeits. 23 (1925), 161–96.

A. KUROSH, [1] *Durchschnittsdarstellungen mit irrededuziblen Komponenten in Ringen und sogenannten Dualgruppen*, Mat. Sbornik 42 (1935), 613–16.

S. LEFSCHETZ, [1] *Algebraic topology*, Am. Math. Soc. Colloquium Publications, vol. 27, 1942.

S. MACLANE, [1] *A lattice formulation for transcendence degrees and p-bases*, Duke Jour. 4 (1938), 455–68.

H. MACNEILLE, [1] Harvard Doctoral Thesis (unpublished), 1935; [2] *Partially ordered sets*, Trans. Am. Math. Soc. 42 (1937), 416–60.

J. C. C. MCKINSEY AND A. TARSKI, [1] *The algebra of topology*, Annals of Math. 45 (1944), 141–91; [2] *On closed elements in closure algebras*, ibid., 47 (1946), 122–62.

K. MENGER, [1] *Ergebnisse eines Kolloquiums*, Vienna, Vol. 1, p. 28; [2] *Bemerkungen zu Grundlagenfragen*, IV, Jahr. D. M. V. 37 (1928), 309–13; [3] *New foundations of projective and affine geometry*, Annals of Math. 37 (1936), 456–82.

GR. C. MOISIL, [1] *Recherches sur l'algèbre de la logique*, Annales Sci. de Jassy, 22 (1936), 1–118.

E. H. MOORE, [1] The New Haven Mathematical Colloquium, *Introduction to a form of general analysis*, Am. Math. Soc. Colloquium Publications, vol. 2, New Haven, 1910.

T. NAKAYAMA, [1] *Algebraic theory of lattices* (in Japanese), Tokyo, 1944.

J. VON NEUMANN, [1] *Continuous geometries*, and *Examples of continuous geometries*, Proc. Nat. Acad. Sci. 22 (1936), 92–110; [2] *Lectures on continuous geometries*, Princeton, 1936–37, 2 vols.; [3] *On regular rings*, Proc. Nat. Acad. Sci. 22 (1936), 707–13.

J. VON NEUMANN AND O. MORGANSTERN, [1] *Theory of economic games and puzzles*, Princeton, 1944.

M. H. A. NEWMAN, [1] *A characterization of Boolean lattices and rings*, J. Lond. Math. Soc. 16 (1941), 256–72.

O. ORE, [1] *On the foundations of abstract algebra*, I, Annals of Math. 36 (1935), 406–37; [2] *On the foundations of abstract algebra*, II, ibid. 37 (1936), 265–92.

C. S. PEIRCE, [1] *On the algebra of logic*, Am. Jour. 3 (1880), 15–57; [2] *On the algebra of logic*, ibid. 7 (1884), 180–202.

FR. RIESZ, [1] *Sur la décomposition des opérations fonctionnelles*, Atti Congresso Bologna 3 (1928), 143–8; [2] *Sur la théorie générale des opérations linéaires*, Annals of Math. 41 (1940), 174–206. (See also Math. Anzeiger Ungar. Akad. Wiss. 56 (1937), 1–46.)

E. SCHRÖDER, [1] *Algebra der Logik*, 3 Vols., Leipzig, 1890–5, with bibliography at end of each volume.

W. SIERPINSKI, [1] *Leçons sur les nombres transfinis*, Paris, 1928.

TH. SKOLEM, [1] *Om konstitutionen av den identiske kalkuls grupper*, Third. Scand. Math. Congr. (1913), 149–63.

M. H. STONE, [1] *Boolean algebras and their relation to topology*, Proc. Nat. Acad. Sci. 20 (1934), 197–202; [2] *Subsumption of Boolean algebras under the theory of rings*, ibid., 21 (1935), 103–5; [3] *The theory of representations for Boolean algebras*, Trans. Am. Math. Soc. 40 (1936), 37–111; [4] *Applications of the theory of Boolean rings to general topology*, ibid. 41 (1937), 375–481; [5] *Topological representations of distributive lattices and Brouwer-*

ian logics, Cas. Mat. Fys. 67 (1937), 1–25; [6] *A general theory of spectra*. II, Proc. Nat. Acad. Sci. 27 (1941), 83–7.

A. Tarski, [1] *Sur les classes closes par rapport à certaines opérations élémentaires*, Fund. Math. 16 (1929), 181–305; [2] *Zur Grundlagung der Booleschen Algebra*, I, ibid., 24 (1935), 177–98; [3] *Gundzuge des systemenkalkuls*, ibid., 25 (1936), 503–26 and 26 (1936), 283–301; [4] *Cardinal algebras*, Oxford Press, 1948.

J. Tukey, [1] *Convergence and uniformity in topology*, Princeton, 1940.

O. Veblen and J. W. Young, [1] *Projective geometry*, Boston, 1910, 2 vols.

B. L. van der Waerden, [1] *Moderne Algebra*, Berlin, 1930–1, 2 vols. (Also second edition.)

H. Wallman, [1] *Lattices and topological spaces*, Annals of Math. 39 (1938), 112–26.

M. Ward and R. P. Dilworth, [1] *Residuated lattices*, Trans. Am. Math. Soc. 45 (1939), 335–54.

A. N. Whitehead and B. Russell, [1] *Principia Mathematica*, 3 vols., Cambridge Press 1925, 1927 (second edition of vols. 1, 2), 1913.

H. Whitney, [1] *The abstract properties of linear dependence*, Am. Jour. 57 (1935), 507–33.

K. Yosida and S. Kakutani, [1] *Operator-theoretical treatment of Markoff's process and mean ergodic theorem*, Annals of Math. 42 (1941), 188–228.

SUBJECT INDEX

AUTHOR INDEX

Colloquium Publications

1. H. S. White, *Linear Systems of Curves on Algebraic Surfaces*;
   F. S. Woods, *Forms of Non-Euclidean Space*;
   E. B. Van Vleck, *Selected Topics in the Theory of Divergent Series and of Continued Fractions*;
   1905, xii, 187 pp. $3.00
2. E. H. Moore, *Introduction to a Form of General Analysis*;
   M. Mason, *Selected Topics in the Theory of Boundary Value Problems of Differential Equations;*
   E. J. Wilczynski, *Projective Differential Geometry*;
   1910, x, 222 pp. out of print

3_1. G. A. Bliss, *Fundamental Existence Theorems*, 1913; reprinted, 1934, iv, 107 pp. out of print

3_2. E. Kasner, *Differential-Geometric Aspects of Dynamics*, 1913; reprinted, 1934; reprinted, 1948, iv, 117 pp. 2.50

4. L. E. Dickson, *On Invariants and the Theory of Numbers*;
   W. F. Osgood, *Topics in the Theory of Functions of Several Complex Variables*;
   1914, xviii, 230 pp. out of print

5_1. G. C. Evans, *Functionals and their Applications. Selected Topics, Including Integral Equations*, 1918, xii, 136 pp. out of print

5_2. O. Veblen, *Analysis Situs*, 1922; second ed., 1931; reprinted, 1946, x, 194 pp. 3.35

6. G. C. Evans, *The Logarithmic Potential. Discontinuous Dirichlet and Neumann Problems*, 1927, viii, 150 pp. out of print
7. E. T. Bell, *Algebraic Arithmetic*, 1927, iv, 180 pp. out of print
8. L. P. Eisenhart, *Non-Riemannian Geometry*, 1927; reprinted, 1934, viii, 184 pp. out of print
9. G. D. Birkhoff, *Dynamical Systems*, 1927; reprinted, 1948, viii, 295 pp. 4.25
10. A. B. Coble, *Algebraic Geometry and Theta Functions*, 1929; reprinted, 1948, viii, 282 pp. 4.00
11. D. Jackson, *The Theory of Approximation*, 1930; reprinted, 1946, viii, 178 pp. 3.35
12. S. Lefschetz, *Topology*, 1930, x, 410 pp. out of print
13. R. L. Moore, *Foundations of Point Set Theory*, 1932, viii, 486 pp. out of print
14. J. F. Ritt, *Differential Equations from the Algebraic Standpoint*, 1932; reprinted, 1948, x, 172 pp. 3.00

15. M. H. Stone, *Linear Transformations in Hilbert Space and their Applications to Analysis*, 1932; reprinted, 1946; reprinted, 1948, viii, 622 pp. 8.00
16. G. A. Bliss, *Algebraic Functions*, 1933; reprinted, 1948, x, 220 pp. 3.75
17. J. H. M. Wedderburn, *Lectures on Matrices*, 1934; reprinted, 1944; reprinted, 1946, x, 205 pp. out of print
18. M. Morse, *The Calculus of Variations in the Large*, 1934; reprinted, 1948, x, 368 pp. 5.35
19. R. E. A. C. Paley and N. Wiener, *Fourier Transforms in the Complex Domain*, 1934, viii, 184 pp. + portrait plate out of print
20. J. L. Walsh, *Interpolation and Approximation by Rational Functions in the Complex Domain*, 1935, x, 382 pp. 6.00
21. J. M. Thomas, *Differential Systems*, 1937, x, 118 pp. 2.00
22. C. N. Moore, *Summable Series and Convergence Factors*, 1938, vi, 105 pp. 2.00
23. G. Szegö, *Orthogonal Polynomials*, 1939; reprinted 1949, x, 403 pp. 6.00
24. A. A. Albert, *Structure of Algebras*, 1939, xii, 210 pp. 4.00
25. G. Birkhoff, *Lattice Theory*, 1940; enlarged and completely revised ed., 1949, xiv, 283 pp. 6.00
26. N. Levinson, *Gap and Density Theorems*, 1940, viii, 246 pp. 4.00
27. S. Lefschetz, *Algebraic Topology*, 1942; reprinted, 1948, vi, 393 pp. 6.00
28. G. T. Whyburn, *Analytic Topology*, 1942; reprinted, 1948, x, 281 pp. 4.75
29. A. Weil, *Foundations of Algebraic Geometry*, 1946, xx, 288 pp. 5.50
30. T. Radó, *Length and Area*, 1948, vi, 572 pp. 6.75
31. E. Hille, *Functional Analysis and Semi-Groups*, 1948, xii, 528 pp. 7.50

AMERICAN MATHEMATICAL SOCIETY
New York 27, N. Y., 531 West 116th Street
Cambridge, England, 1 Trinity Street, Bowes and Bowes