PROCEEDINGS OF THE
Cambridge Philosophical Society

VOL. 31 October, 1935 PART 4

ON THE STRUCTURE OF ABSTRACT ALGEBRAS

BY GARRETT BIRKHOFF, Trinity College

[Communicated by MR P. HALL]

[*Received* 26 April, *read* 3 June 1935]

1. *Introduction.* The following paper is a study of abstract algebras *qua* abstract algebras. As no vocabulary suitable for this purpose is current, I have been forced to use a number of new terms, and extend the meaning of some accepted ones.

An outline of the material will perhaps tell the reader what to expect. In §§ 2–7, the notion of abstract algebra is defined, and relations between abstract algebras of two kinds (groups and "lattices") derived from a fixed abstract algebra are indicated.

In § 8, abstract algebras are divided by a very simple scheme into self-contained "species". Within each species, a perfect duality is found between families of formal laws and the families of algebras satisfying them; this occupies §§ 9–10. After a digression in § 11, some illustrations are discussed in §§ 12–15.

In §§ 16–18, the "lattice" $E(C)$ of the equivalence relations between the objects of a fixed aggregate C is defined; in §§ 20–21 such lattices are shown to be interchangeable with lattices of Boolean subalgebras and lattices of subgroups. Other miscellaneous facts are proved in § 19, § 22, and § 23. In § 24, the interesting truth is established that, if C is an algebra, then the equivalence relations which are homomorphic are a "sublattice" of $E(C)$.

In § 25 an open question is settled, and the paper concludes in §§ 26–31 with some observations on topology. Many incidental results have of course not been mentioned.

The reader will find it easier to follow the exposition if he remembers that operations are considered as fundamental throughout, while algebras and to an even greater extent elements within the same algebra are juggled freely.

2. *Abstract algebras defined.* By an "abstract algebra" is meant, loosely speaking, any system of elements and operations such as a ring, a field, a group, or a Boolean algebra. A tentative formal definition is the following.

Let $\mathfrak{C}$ be any class of "elements", and let F be a class of "operators" $f_1, f_2,$

$f_3, \ldots$. Further, let there be assigned to each f_i of F a set $\mathfrak{D}_i$ of sequences[†] of elements of $\mathfrak{C}$, to be called the "proper domain" of f_i. And, finally, let each f_i be a single-valued function of its proper domain to $\mathfrak{C}$—in other words, let f_i assign to each sequence σ of $\mathfrak{D}_i$ a unique "f_i-value" $f_i(\sigma)$ in $\mathfrak{C}$.

Then the couple $(\mathfrak{C}, F)$ will be called an "abstract algebra" A, or for brevity in this paper, an "algebra". The number of different elements of $\mathfrak{C}$ will be called the "order" of A.

3. *The group of automorphisms of an algebra.* It would be pointless to prove in detail what is already known, that every algebra has a group. It is enough to restate in explicit language the outlines of the usual doctrine.

By an "automorphism" of an algebra $(\mathfrak{C}, F)$ is meant a (1, 1) transformation α of $\mathfrak{C}$ into itself such that

(*a*) $\sigma \epsilon \mathfrak{D}_i$ implies $\alpha(\sigma) \epsilon \mathfrak{D}_i$ and conversely.

(*b*) $f_i(\alpha(\sigma)) = \alpha(f_i(\sigma))$ for any $\sigma \epsilon \mathfrak{D}_i$.

And by a "group" is meant any algebra $(\mathfrak{A}, G)$ satisfying

G 1: To each element α of $\mathfrak{A}$ corresponds a unique "inverse" $\alpha^{-1} = g_1(\alpha)$ in $\mathfrak{A}$.

G 2: To each sequence (α, β) of two elements of $\mathfrak{A}$ there corresponds a unique "product" $\alpha\beta = g_2(\alpha, \beta)$ in $\mathfrak{A}$.

G 3: $(\alpha\alpha^{-1})\beta = \beta$ and $\beta(\alpha\alpha^{-1}) = \beta$ for any α and β in $\mathfrak{A}$.

G 4: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for any α, β, and γ in $\mathfrak{A}$.

THEOREM 1[‡]: *The automorphisms of any algebra form a group, and any group can be realized as the group of the automorphisms of a suitable algebra.*

4. *The lattice of subalgebras of an algebra.* Only recently the object of special research has been what I consider to be a dual notion, that of the "lattice" of the subalgebras of an algebra.

Let $\mathfrak{S}$ be any subclass of $\mathfrak{C}$ (in the notation of § 2) with the property that if σ lies in $\mathfrak{D}_i$ and its elements in $\mathfrak{S}$, then $f_i(\sigma)$ also is in $\mathfrak{S}$. Then the couple $(\mathfrak{S}, F)$ will be called a "subalgebra" of the algebra $(\mathfrak{C}, F)$.

By a "lattice" is meant any system of double composition satisfying the commutative, associative and absorption laws. That is, in the notation of § 2; a lattice is an algebra $(\mathfrak{L}, H)$ satisfying

L 1: Any two elements A and B of $\mathfrak{L}$ have a unique "meet" $A \cap B = h_1(A, B)$ and a unique "join" $A \cup B = h_2(A, B)$ in $\mathfrak{L}$.

L 2: $A \cap B = B \cap A$ and $A \cup B = B \cup A$ for any A and B of $\mathfrak{L}$.

L 3: $A \cap (B \cap C) = (A \cap B) \cap C$ and $A \cup (B \cup C) = (A \cup B) \cup C$ for any A, B, and C of $\mathfrak{L}$.

L 4: $A \cap (A \cup B) = A \cup (A \cap B) = A$ for any A and B of $\mathfrak{L}$.

[†] By a "sequence" we mean a "well-ordered set". We can use the locutions "finite sequence" and "enumerated sequence" to express that the ordinal number of the set is finite, or that of the ordered positive integers.

[‡] The first statement is known; the second will be proved in § 15.

THEOREM 2[†]: *The subalgebras of any algebra form a lattice, and any lattice can be realized as the lattice of the subalgebras of a suitable algebra.*

5. *Some general isomorphisms.* Let A be any abstract algebra. We shall adopt the notation $G(A)$ for the group of the automorphisms of A, $L(A)$ for the lattice of the subalgebras of A. Expressions such as $G(L(A))$ and $L(L(G(A)))$ are then self-explanatory.

We shall also adopt the usual definitions[‡] of isomorphism and homomorphism. We shall supplement these by saying that a (1, 1) correspondence between a lattice L and a lattice $\bar{L}$ is "dually isomorphic" if and only if it inverts the operations of meet and join—i.e. if and only if the hypothesis that a and b of L correspond respectively to $\bar{a}$ and $\bar{b}$ of $\bar{L}$ implies that $a \frown b$ and $a \smile b$ correspond respectively to $\bar{a} \smile \bar{b}$ and $\bar{a} \frown \bar{b}$.

We shall now state some perfectly general operation-preserving correspondences which occur repeatedly in algebra.

(1) Every automorphism α of A induces an automorphism on $G(A)$, $L(A)$, $G(G(A))$, $L(G(A))$, and so on down the line. Moreover, products and inverses are preserved under this correspondence. Therefore a homomorphic correspondence exists between $G(A)$ and a subgroup of any $G^* = G(\ldots(A)\ldots)$.

The special case $G^* = G(G(A))$ gives the important homomorphism between $G(A)$ and the group of the "inner" automorphisms of $G(A)$; this defines an isomorphism between $G(A)$ and $G(G(A))$ if and only if $G(A)$ is complete.

Again, if A is a lattice, and $G^* = G(L(A))$, the homomorphism is an isomorphism, since each element of A is a sublattice.

(2) An automorphism α of A is said to "centralize" a complex C of elements of A if and only if it leaves every element of C fixed—i.e. carries it into itself.

This assigns to every subalgebra S of A the subgroup $\mathfrak{S}(S)$ of $G(A)$ centralizing it, and to every subgroup $\mathfrak{S}$ of $G(A)$ the subalgebra $S(\mathfrak{S})$ of elements of A centralized by $\mathfrak{S}$. And since $S \supset T$ implies $\mathfrak{S}(S) \subset \mathfrak{S}(T)$, while $\mathfrak{S} \supset \mathfrak{T}$ implies $S(\mathfrak{S}) \subset S(\mathfrak{T})$, the correspondence inverts inclusion relations[§].

In any case $S(\mathfrak{S}(S)) \supset S$ and $\mathfrak{S}(S(\mathfrak{S})) \supset \mathfrak{S}$. If for any S (or $\mathfrak{S}$) the correspondence is *reciprocal*—that is, $S(\mathfrak{S}(S)) = S$ (or $\mathfrak{S}(S(\mathfrak{S})) = \mathfrak{S}$)—we shall say that S or $(\mathfrak{S})$ is "replete". Since inclusion is inverted, we can assert

THEOREM 3: *If the replete elements of $L(A)$ and $L(G(A))$ are sublattices L_1 of $L(A)$ and L_2 of $L(G(A))$ respectively, then L_1 and L_2 are dually isomorphic.*

[†] These facts were proved by the author in "On the combination of subalgebras", *Proc. Cambridge Phil. Soc.* 29 (1933), 441–64: $A \frown B$ is the set of elements common to the subalgebras A and B, $A \smile B$ is the meet of the subalgebras containing both A and B. In later citations, the above paper will be referred to for short as "Subalgebras".

[‡] Cf. B. L. van der Waerden's *Moderne Algebra*, 1 (Berlin, 1930–1), 28–32.

[§] The notion of inclusion in an abstract lattice is naturally defined by writing $a \subset b$ if and only if $a \smile b = b$.

It is by proving the hypotheses of Theorem 3, in the case where A is the field of algebraic numbers, that it has been[†] shown that the lattice of finite extensions of the rational domain is dually isomorphic with the lattice of the subgroups of finite index in the group $G(A)$ (relative to the four rational operations).

A similar correspondence exists[‡] between any discrete Abelian group and the group of its characters; consequently

(5·1) If G is any enumerable Abelian group, and X is the group of the characters of G, then $L(G)$ and $L(X)$ are dually isomorphic. Hence if G is any finite Abelian group, then $L(G)$ is dually isomorphic with itself.

(3) We can easily combine the above relations. By (1) each automorphism of A induces an automorphism on $A_1 = L(A)$, $A_2 = G(A)$, etc. Taking the subgroups of $G(A)$ centralizing the various subalgebras of the A_i, and proceeding as in (2), one obtains blurred dual isomorphisms between $L(G(A))$ and the $L(A_i)$.

The special case of A_2 yields an interesting blurred dual isomorphism of $L(G(A))$ with itself.

6. *Lattice graphs.* Lattices lend themselves to graphical representation much more readily than groups. In fact we have

THEOREM 4: *Any finite lattice can be represented by one or more graphs in space, but not every graph represents a lattice.*

In constructing representations, we shall need the notion of "covering". An element a of a lattice L is said to "cover" an element b of L if and only if $a \supset b$ (i.e. $a \cup b = a$), $a \neq b$, and $a \supset c \supset b$ implies either $c = a$ or $c = b$.

Now we can associate with any finite lattice L a graph $\Gamma(L)$ composed of (i) small circles in (1, 1) correspondence with the elements of L, and (ii) non-horizontal line segments drawn between circle-pairs if and only if the element of L which corresponds to the upper circle "covers" the element corresponding to the lower one.

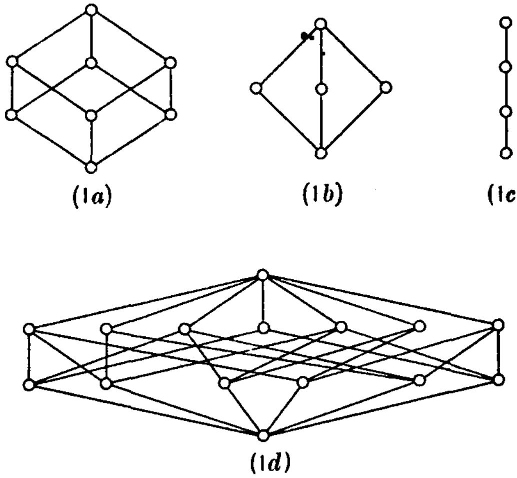
Such a diagram[§] represents inclusion relations, and hence the operations of taking joins and meets. The best way to make this plain is probably to give examples. Accordingly, the reader will find graphed in Fig. 1, (1*a*) the lattice of the Boolean algebra of eight elements, (1*b*) the lattice of *its* Boolean subalgebras (isomorphic with the lattice of the subgroups of the four-group), (1*c*) the lattice of the subrings of the ring of integers modulo p^3, and (1*d*) the symmetrical equivalence lattice of degree four (cf. § 18).

[†] E. Steinitz, *Algebraische Theorie der Körper* (Berlin, 1930), p. 143.

[‡] L. Pontrjagin, "Theory of topological commutative groups", *Ann. of Math.* 35 (1934), 361–88, Theorems 2 and 4. If X is continuous, we admit only closed subgroups. (5·1) was added in revision; the surprising thing is that it has not been explicitly stated before.

[§] This representation dates back at least to H. Vogt, *Résolution algébrique des équations* (Paris, 1895), p. 91.

Incidentally, by the "class of conjugate elements" including any element a of an algebra A is meant the set of a and its images under the group $G(A)$ of the automorphisms of A. Two different classes of conjugate elements are evidently disjoint.


(1a) (1b) (1c)

(1d)

Fig. 1.

THEOREM 5: *Any finite lattice L specifies and is specified by a "geometrico-tactical configuration" $Ta(L)$ in the sense of E. H. Moore*[†]. *The "rank" of $Ta(L)$ is equal to the number of different classes of conjugate elements of L.*

We shall merely give the construction, and leave the proof, which has many details but is not difficult, to the reader.

The elements of $Ta(L)$ are to be the elements of L; the "sets" of $Ta(L)$ are to be the classes of conjugate elements of L; $a \epsilon L$ is to be called "incident" with $b \epsilon L$ if and only if $a \neq b$ and either $a \supset b$ or $a \subset b$; the "sets" are to be ordered in such a way that if the set of a comes before the set of b, and a is incident with b, then $a \subset b$.

7. *Algebraic synthesis*. In this section we shall define three simple ways of building up algebras synthetically from smaller algebras having the same operators.

Let $A_1, \ldots, A_n$ be any well-ordered set of algebras having the same operators f_k. By the "direct product" $A_1 \times ,\ldots \times A_n$ is meant[‡] the algebra A (1) whose elements are the different ennuples $a = [a_1, \ldots, a_n]$ of elements $a_1 \epsilon A_1, \ldots, a_n \epsilon A_n$, (2) whose operators are the f_k, (3) in which the proper domain $\mathfrak{D}_k$ of f_k consists of

[†] E. H. Moore, "Tactical memoranda I–III", *Am. Jour. Math.* 18 (1896), 264. The definition is too long to repeat.

[‡] This definition includes the standard definitions of direct products of groups and topological manifolds, and of the direct sum of linear algebras (of hypercomplex numbers).

those and only those sequences σ of elements $a^j = [a_1^j, \dots, a_n^j]$ of A $(j = 1, \dots, r)$ each of whose "component" sequences σ_i of elements $a_i^1, \dots, a_i^r$ is in the proper domain of f_k in A_i, and (4) whose f_k-values over $\mathfrak{D}_k$ are given by

$$f_k(\sigma) = [f_k(\sigma_1), \dots, f_k(\sigma_n)]. \tag{7·1}$$

In the special case $A_1 = \dots = A_n = B$, we write $A = B^n$.

It is important to observe that $A_1 \times \dots \times A_n$ is determined to within isomorphism by the *aggregate* of the A_i, and that[†]

$$(A_1 \times \dots \times A_m) \times (B_1 \times \dots \times B_n) \sim A_1 \times \dots \times A_m \times B_1 \times \dots \times B_n. \tag{7·2}$$

It is a corollary that the commutative and associative laws hold.

It is often useful to represent an algebra as a subalgebra or a homomorphic image of a direct product. We shall see in § 11 that one can usually put such representations into "canonical" forms having additional properties, which we shall state next.

A subalgebra S of $A \times B$ is called a "meromorphic" product[‡] of A and B (in symbols, $S = A :\cdot B$) if and only if (1) to each $a \epsilon A$ corresponds a $b \epsilon B$ such that $[a, b] \epsilon S$, (2) to some $a \epsilon A$ correspond distinct elements b_1 and b_2 of B such that $[a, b_1] \epsilon S$ and $[a, b_2] \epsilon S$, and (3) the counterparts of (1)–(2) under the inversion $A \rightleftharpoons B$ also hold.

Similarly the image H of $A \times B$ under a homomorphism θ is called a "central" product of A and B (in symbols, $H = A :. B$) if and only if (1) to any two distinct elements a_1 and a_2 of A corresponds an element $b \epsilon B$ such that $[a_1, b]$ and $[a_2, b]$ have distinct images under θ, and (2) the counterpart of (1) under the inversion $A \rightleftharpoons B$ also holds.

The reader should be cautioned that $A :\cdot B$ and $A :. B$ (unlike $A \times B$) are not determined to within isomorphism by A and B. With this in mind, we can assert

(7·3) $S = A :\cdot B$ implies $S = B :\cdot A$ and $H = A :. B$ implies $H = B :. A$.

(7·4) $S = (A :\cdot B) :\cdot C$ implies $S = A :\cdot (B :\cdot C)$. But $H = (A :. B) :. C$ need not[§] imply $H = A :. (B :. C)$.

(7·5) Any $A :\cdot B$ is homomorphic to A and to B.

The proofs, which are uninteresting, are omitted.

A CLASSIFICATION OF UNIFORM ALGEBRAS

8. *Uniform operators and species of algebras.* General classifications of abstract systems are usually characterized by a wealth of terminology and illustration, and a scarcity of consequential deduction. Whatever value is in the following plan

[†] By $A \sim B$ (A and B any algebras), we denote "A and B are isomorphic".

[‡] This definition generalizes a usage in group theory started by R. Remak, *Journal für Math.* 163 (1930), 6.

[§] For a counter-example, cf. 6 of the author's paper "Group synthesis", now in the hands of the editors of the *Trans. Amer. Math. Soc.*

therefore is derived from Theorems 8–10, their corollaries, and the perspective it gives to the results stated in §§ 12–13. But first we shall need several definitions.

Let A be any algebra, k_i any ordinal number, and f_i any operator of A. The operator f_i is called "k_i-ary", or a "uniform" operator of "index" k_i, if and only if (using the terminology of § 2) the proper domain of f_i is the set of all sequences of length k_i. That is, if and only if f_i assigns to each sequence $(x_1, \ldots, x_{k_i})$ of elements of A, a single value $y = f_i(x_1, \ldots, x_{k_i})$ in A.

In the remainder of the paper, every operator will be understood to be uniform.

Definition 1: *Let ρ be any aggregate of ordinal numbers $k_1, \ldots, k_s$. An algebra A will be called "of species Σ_ρ", if and only if its operators $f_1, \ldots, f_s$ are of indices $k_1, \ldots, k_s$.*

Thus groups are (uniform) algebras of species (2, 1), lattices of species (2, 2), and Boolean algebras of species (2, 2, 1).

9. *Functions and laws within a species.* The explicit nature of several implicitly accepted fundamental processes of abstract algebra becomes clear when we take as their proper domain a particular species of (uniform) algebra. The main difficulties are with regard to definition. Therefore we state

Definition 2: *By a "function of rank* 0*" associated with the species Σ_ρ is meant a primitive symbol (which is usually a Latin letter with or without subscripts). By a "function of rank n" is meant any symbolic formula*

$$f_i(\phi_1, \ldots, \phi_{ki}) \tag{9·1}$$

in which the ϕ_j are functions of ranks $< n$, and n is the least ordinal exceeding the ranks of all the ϕ_j.

Thus in a Boolean algebra, the expressions a, $a+b$, and $a+bc$ are functions of rank 0, 1, and 2 respectively, on the primitive symbols a, b, and c.

By simple induction on rank, we can show that any substitution ξ of one element of an algebra $A \epsilon \Sigma_\rho$ for all occurrences of each primitive symbol of a function ϕ of Σ_ρ determines a "value" $\xi(\phi) \epsilon A$ which results when the operations are performed in order of rank.

Definition 3: *By a "law" of an algebra A is meant any equation between two functions ϕ and ϕ' of the species of A such that $\xi(\phi) = \xi(\phi')$ no matter what substitution ξ of elements of A for the primitive symbols (which will usually be the same for ϕ as for ϕ') is made.*

Thus equations G 2–G 4 of § 3 are laws of groups, and equations L 2–L 4 of § 4 are laws of lattices.

By a "law" of a set of algebras (of a given species) is meant of course a law of every algebra of the set. We can assert, as a direct consequence of the definitions, THEOREM 6: *If a law is true of a set $\mathfrak{A}$ of algebras, then it is true of any subalgebra or homomorphic image of any one, and of any direct product of any number of the algebras of $\mathfrak{A}$.*

COROLLARY 1: *If A and B both satisfy a given set of laws, then so do any $A :\cdot B$ and $A :. B$.*

COROLLARY 2: *The set of laws of any aggregate of algebras A_i is the same as that of the direct product A^* of all the A_i.*

For by Theorem 6 all the laws of the set hold for A^*, and by studying separate components we obtain the converse.

THEOREM 7: *Let A be any algebra.* (1) *If, for $h = 1, \ldots, k_i$, $\phi_h = \phi'_h$ is a law of A, and f_i is any operator of A of index k_i, then $f_i(\phi_1, \ldots, \phi_{k_i}) = f_i(\phi'_1, \ldots, \phi'_{k_i})$ is a law of A.* (2) *If $\phi = \phi'$ is a law of A, then any substitution η of one function $\eta(x_j)$ for all occurrences of each primitive symbol x_j in $\phi = \phi'$ yields a law $\eta(\phi) = \eta(\phi')$ of A.*

Conclusion (1) is true since f_i is single-valued. That $\eta(\phi)$ and $\eta(\phi')$ are functions of the species of A follows by induction on type; $\eta(\phi) = \eta(\phi')$ then follows *a fortiori* since each $\eta(x_j) \epsilon A$.

In Theorem 7, A can obviously be replaced by any set of algebras of the same species.

10. *Families of algebras and the dual families of laws.* Theorems 6 and 7 suggest the following definitions:

DEFINITION 4: *Let $\mathfrak{B}$ be any set of algebras of a species Σ. Then the set $\mathfrak{F}(\mathfrak{B})$ of all algebras which can be constructed from algebras of $\mathfrak{B}$ by the taking of subalgebras, homomorphic images, and direct products is called the "family" of algebras generated by $\mathfrak{B}$. Reciprocally $\mathfrak{B}$ is called a "basis" of $\mathfrak{F}(\mathfrak{B})$.*

DEFINITION 5: *Let B be any set of equations between functions of a species Σ. Then the set $\Phi(B)$ of all equations between functions of Σ which can be inferred from B by rules* (1) *and* (2) *of Theorem 7 is called the "family" of equations generated by B, and B is called a "basis" of $\Phi(B)$.*

It is evident that $\mathfrak{F}(\mathfrak{F}(\mathfrak{B})) = \mathfrak{F}(\mathfrak{B})$, and $\Phi(\Phi(B)) = \Phi(B)$; therefore a family of algebras (or equations between functions) of a species Σ is a set which generates itself. From this we see that the set of algebras (or equations between functions) common to any two families of algebras (or equations between functions) of Σ is itself a family of algebras (or equations between functions). So that if we duplicate the definitions of "join" and "meet" of the footnote of § 4, we get

THEOREM 8: *The families of algebras of a species Σ are a lattice $L(\Sigma)$, and the families of equations between functions of Σ are a second lattice $L^*(\Sigma)$.*

Let B be any set of equations between functions of a species Σ. Form the "free"[†] algebras $F(B, m)$, whose elements are the classes of functions on m

primitive symbols equated under $\Phi(B)$. By rule (1) of Definition 5, $F(B,m)$ is an algebra of Σ, and by (2), $F(B,m)$ satisfies all the laws of B. Moreover, by Theorem 7 every algebra of species Σ generated by m elements and of which B is a set of laws is a homomorphic image of $F(B,m)$. Conversely, every law of $F(B,m)$ involving m primitive symbols is by definition an equation of $\Phi(B)$. Hence if we define $\mathfrak{F}(B)$ as the family of algebras generated by the $F(B,m)$, we see

THEOREM 9: *To every set B of equations between functions of a species Σ corresponds a family $\mathfrak{F}(B)$ of algebras such that $\Phi(B)$ is the set of laws of $\mathfrak{F}(B)$. $\mathfrak{F}(B)$ is the family of the homomorphic images of the "free" algebras $F(B,m)$.*

Reciprocally, let $\mathfrak{A}$ be any set of algebras $A_1, \ldots, A_s$ of orders $a_1, \ldots, a_s$ of a species Σ. Let $x_1, \ldots, x_n$ be any set of n primitive symbols, and let $\xi_{i,j}$ denote any of the a_i^n single-valued transformations of the x_k into A_i. The transforms will generate in A_i a subalgebra $S_{i,j}$. Form the direct product S^* of all such $S_{i,j}$, and associate with each x_k that element of S^* each of whose (i,j)th components is the transform of x_k under $\xi_{i,j}$. These elements will generate a subalgebra of S^*, which will be denoted by $F(\mathfrak{A},n)$. By Definition 4, $F(\mathfrak{A},n)\in\mathfrak{F}(\mathfrak{A})$, and so by Theorem 6 every law of $\mathfrak{A}$ is a law of $F(\mathfrak{A},n)$.

But if $\Phi(\mathfrak{A})$ denotes the family of equations between functions of species Σ true of $\mathfrak{A}$, then by Definition 3 the equations in $F(\mathfrak{A},n)$ between the values of functions of the elements corresponding to the x_k constitute precisely the subset of $\Phi(\mathfrak{A})$ involving n primitive symbols. That is,

$$F(\mathfrak{A},n) \sim F(\Phi(\mathfrak{A}),n). \qquad (10\cdot 1)$$

It is a corollary that $\mathfrak{F}(\Phi(\mathfrak{A}))$ is contained in $\mathfrak{F}(\mathfrak{A})$. But by Theorem 6, $\mathfrak{F}(\mathfrak{A})$ is contained in $\mathfrak{F}(\Phi(\mathfrak{A}))$, proving

THEOREM 10: *The correspondence of each family $\mathfrak{F}$ of algebras of a species Σ to the family $\Phi(\mathfrak{F})$ of equations between functions of Σ which are laws of $\mathfrak{F}$, and of each family Φ of equations between functions of Σ to the family $\mathfrak{F}(\Phi)$ of algebras of Σ for which the equations of Φ are laws, is reciprocal—that is, $\mathfrak{F}(\Phi(\mathfrak{F}))=\mathfrak{F}$ and $\Phi(\mathfrak{F}(\Phi))=\Phi$.*

This theorem shows that the laws of formal inference and of algebraic synthesis are both logically complete.

Since this (1, 1) correspondence inverts inclusion, we have

COROLLARY 1: *In Theorem 8, $L(\Sigma)$ and $L^*(\Sigma)$ are dually isomorphic.*

COROLLARY 2: *Let $\mathfrak{A}$ be any set of algebras $A_1, \ldots, A_s$ of orders $a_1, \ldots, a_s$. The order of any algebra generated by m elements and obeying the laws of $\mathfrak{A}$ is at most*

$$\prod_{1}^{s} a_i^{a_i^m}.$$

[†] In case B is the set of equations G 2–G 4 of § 3 on algebras of species (2, 1), we have the so-called "free" groups. Another connection with standard usage is made by calling $F(B,m)$ the "calculus" on m symbols defined by the laws of B.

THEOREM 11: *Let $\mathfrak{A}$ be any finite set of algebras of finite order of a species Σ containing a finite number of operators of finite index. Then the laws of $\mathfrak{A}$ involving a finite number m or fewer primitive symbols have a finite basis.*

Each function on m primitive symbols determines an element of

$$F^* = F(\Phi(\mathfrak{A}), m),$$

and since the order of F^* is finite (by Corollary 2 above), there exists a finite number M such that each element of F^* is determined by a single "representative" function of rank not greater than M. But the (finite) set of equations equating each function on m primitive symbols of rank not greater than $M+1$ to the representative of the corresponding element of F^* defines F^*, and is consequently the basis desired.

11. *Meromorphic and central products.* In § 7 it was stated that meromorphic products and central products were canonical representations of subalgebras and of homomorphic images of direct products, respectively. To this effect we prove

THEOREM 12: *Let A and B be any algebras (of the same species). If S is a subalgebra of $A \times B$, then we can find subalgebras A_S of A and B_S of B, such that either $S \sim A_S$, $S \sim B_S$, or $S \sim A_S :\cdot B_S$.*

Let A_S be the range of the A-components, and B_S that of the B-components of the elements of S. A_S and B_S are clearly subalgebras. Moreover $S \subset A_S \times B_S$, while (1) and its inverse are satisfied. Hence either $S = A_S :\cdot B_S$, or (2) is not satisfied and $S \sim A_S$, or the inverse of (2) is not satisfied and $S \sim B_S$.

THEOREM 13: *If C is a homomorphic image of $A \times B$, and to every element x of A or B corresponds an operation having x for its value, then we can find homomorphic images $\bar{A}$ of A and $\bar{B}$ of B such that either $C \sim \bar{A}$, $C \sim \bar{B}$, or $C = \bar{A} :. \bar{B}$.*

The construction consists in identifying elements a and a' of A if and only if $[a, b]$ and $[a', b]$ have the same homomorphic image for every $b \epsilon B$—and doing the same thing for B. The details are uninteresting.

12. *The family of modular lattices.* Lattices by definition constitute a family within the species of algebras "of double composition"—i.e. of type (2, 2). We have already seen that they are of very general occurrence.

In this section we shall consider the subfamily of "modular" lattices—that is, of the lattices satisfying the following "modular" identity discovered by Dedekind[†],

L 5: $(A \cap B) \cup (C \cap (A \cup B)) = ((A \cap B) \cup C) \cap (A \cup B)$, which is to say, $A \subset B$ implies $A \cup (C \cap B) = (A \cup C) \cap B$ irrespective of C.

[†] *Gesammelte Werke*, 1, p. 121. Cf. also a paper by O. Ore on modular lattices, for which he prefers the term Dedekind structures, *Annals of Math.* 36 (1935), 406–37.

The normal subgroups of any group[†], the ideals of any ring[†], subspaces in abstract vector space[†], and linear sets in projective geometries[‡] constitute modular lattices. Further, so do the modules of any ring, and Galois extensions[§] of the rational domain. Whether all modular lattices can be realized in these ways is an open question.

Closely allied with lattices are those algebras (of species (2, 2, 1)) which satisfy, besides L 1–L 4,

L 7: To any A corresponds a "complement" $\bar{A}$ satisfying $A \cap \bar{A} \cap B = A \cap \bar{A}$ and $A \cup \bar{A} \cup B = A \cup \bar{A}$ irrespective of B.

(12·1)[‡] The algebras A of finite order in the family of algebras satisfying L 1–L 5 and L 7 have the Boolean algebra of order two and the finite projective geometries for a basis, and any such A is the direct product of algebras of the basis.

THEOREM 14: *The free modular lattice generated by three elements is a meromorphic product of modular lattices of orders two and five.*

To prove Theorem 14, we must refer to Tables I–III of "Subalgebras". The 28-lattice described there has (in the notation of Table I) the following homomorphic images:

$$\begin{tikzcd}
X \supset G_k \arrow[dd, dash] & X \supset F_k \arrow[dd, dash] & & X \supset B \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
& & N_1 \subset X \subset M_1 \arrow[dr, dash] & N_2 \subset X \subset M_2 \arrow[d, dash] & N_3 \subset X \subset M_3 \arrow[dl, dash] \\
X \subset H_k & X \subset G_k & & X \subset A &
\end{tikzcd}$$

Moreover, its elements have unique expressions, no two alike, as 7-vectors with components in these images. Hence the 28-lattice is isomorphic with a sublattice of their direct product. Theorem 12 completes the proof.

Since the only homomorphic image of the 5-lattice graphed above is the trivial 1-lattice satisfying, with 2-lattices,

L 6: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

we obtain the

COROLLARY: *Any lattice equation on three primitive symbols is either a consequence of L 5, or else, taken with L 5, it gives L 6.*

[†] "Subalgebras", Theorems 26·1, 27·1, and (essentially) §28. On the other hand, the closed (normal) subgroups of the translations of the line do not satisfy L 5. To show this, let r and s be any two incommensurables, and take the subgroups generated by the translations $x \to x + r$, $x \to x + s$, and $x \to x + 2r$.

[‡] G. Birkhoff, "Combinatorial relations in projective geometries", *Annals of Math.* 36 (1935), 743–8.

[§] "Hausdorff groupoids", *Annals of Math.* 35 (1934), 360.

As a matter of practical curiosity, the author studied the 5-lattice graphed above. By a difficult argument which was submitted to the referee, he proved that the algebras of finite order in the family of algebras satisfying

L 51: $A \cup (X \cap B) \cup (Y \cap B) \supset B \cap (A \cup X) \cap (A \cup Y) \cap (X \cup Y)$

L 52: $A \cup (X \cap B) \cup (Y \cap B) \cup (X \cap Y) \supset B \cap (A \cup X) \cap (A \cup Y)$

coincided with the set of the meromorphic products of the 5-lattice and its subalgebras.

13. *The family of distributive lattices.* At present the most satisfactory illustration of the theory of §§ 8–10 is furnished by the family of "distributive" lattices—that is, the subfamily of modular lattices for which L 6 is a law. But first let us repeat some simple definitions.

By a "ring" of point-sets is meant[†] any system of point-sets containing the sum and the product of any two of its members. By a "σ-ring" is meant one which contains the sum and the product of any enumerable collection of its members. A ring (σ-ring) is called a "field" ("σ-field") if and only if it contains the complement of any one of its members.

(13·1)[‡] Any ring of point-sets is a distributive lattice, and any distributive lattice can be realized as a ring of point-sets.

(13·2)[§] Any field of point-sets is a Boolean algebra, and any Boolean algebra can be realized as a field of point-sets.

(13·3) L 2–L 4 and L 6 are a basis for the laws of the lattice of two elements, and L 2–L 4 and L 6–L 7 are a basis for the laws of the Boolean algebra of two elements.

Thus we see that the algebras defined by rings (or fields) of point-sets are *families* of algebras. Now any subalgebra or direct product of σ-rings (or σ-fields) is itself a σ-ring (σ-field), as can be shown by easy constructions. But

THEOREM 15[||]: *The σ-rings of point-sets are not a family of algebras, and neither are the σ-fields.*

[†] F. Hausdorff, *Mengenlehre* (Berlin, 1927), Chapter v.

[‡] "Subalgebras", Theorem 25·2. Other instances of distributive lattices are listed in F. Klein's "Einige distributive Systeme in Mathematik und Logik", *Jahr. d. D.M.V.* 38 (1929), 35–40.

[§] Proved by M. H. Stone, "Boolean algebras and their application to topology", *Proc. U.S.A. Acad.* 20 (1934), 197–202. The family of Boolean algebras is hence generated by any Boolean algebra containing more than one element. It is a corollary that any family of equations between functions of species (2, 2, 1) which contains an equation not derivable from L 2–L 7 contains the equation $x=y$. Cf. J. Lukasiewicz, "Ein Vollständigkeitsbeweis des zweiwertigen Aussagenkalkuls", *Comptes Rendus de Varsovie*, 24 (1932), 153.

[||] Added in revision.

For we can exhibit homomorphic images of a σ-ring and a σ-field not themselves σ-rings (σ-fields). Take all Borel-measurable sets on the line interval $[0, 1]$; they define a σ-field, and hence a σ-ring. But the homomorphic image M^* formed by neglecting sets of measure zero is not realizable even as a σ-ring, let alone a σ-field, of point-sets.

For this was shown in Theorem 25·3 of "Subalgebras" for the σ-subring of intervals $[0, x]$.

Considering the algebra of intervals $[0, x]$ and $[0, x)$ alone, we see that there exists an algebra of point-sets containing the sum and the product of any sequence of its elements, having a homomorphic image—obtained by setting $[0, x] = [0, x)$—not realizable as a similar ring of point-sets.

On the other hand, A. Tarski[†] has recently shown that the algebras of point-sets containing the complement of any one, and the sum and product of any sequence of its elements, do constitute a family of algebras.

14. *Application to hypercentral groups.* Much of the value of the definition of lattices lies in the theorems which it permits us to state. We shall illustrate by this restating two known facts about "hypercentral" groups—that is, groups all of whose factor-groups have a proper central[‡].

(14·1) If H is a hypercentral group of finite order, and $L_p(H)$ denotes the subset of $L(H)$ formed by the subgroups of H whose orders are powers of the prime p, then
$$L(H) = L_2(H) \times L_3(H) \times L_5(H) \dots.$$

(14·2) The subgroups of any hypercentral group satisfy the condition (1) if C covers A and B, and $A \neq B$, then A and B cover $A \cap B$ (cf. § 6, ¶ 2).

There are innumerable other ways in which groups illustrate the above theory.

15. *Any abstract group is a group of automorphisms.* We shall now prove the result announced in § 3, namely

THEOREM 1: *Let S be any abstract group. Then there exists an algebra A_G, the group of whose automorphisms is isomorphic with S.*

Let the elements of A_G be identified with the single elements a and the couples (a, b) of elements a and b of S. And let the operators of A_G be unary operators f_c associated with the elements c of S, plus one binary operator g, defined by
$$f_c(a) = c, \quad f_c(a, b) = a, \quad g[(a, b), (a', b')] = bb',$$
$$g[a, (a', b')] = g[(a, b), b'] = g[a, a'] = 1.$$

Now let α be any automorphism of A_G. Since $\alpha(f_a) = f_a$ for each $a \epsilon S$, clearly

[†] *Fund. Math.* 24 (1935), 177–98.

[‡] Or equivalently satisfying one of the chain of equations between functions of species (2, 1):
$$ab = ba, \quad (a^{-1}b^{-1}ab)\,c = c\,(a^{-1}b^{-1}ab), \dots.$$
(14·1) is a consequence of a result in Burnside's *Theory of groups of finite order*, 2nd ed. (Cambridge, 1911), p. 163; (14·2) follows from Speiser's *Gruppentheorie*, 2nd ed., Theorem 80.

$\alpha(a)=a$ for each $a\epsilon A_G$; hence $\alpha(a,b)=(a,b')$ for each $(a,b)\epsilon A_G$. But if we denote $\alpha(1,1)$ by $(1,c)$, $(c\epsilon S)$, then

$$\begin{aligned} b=\alpha(b)=\alpha(g[(a,b),(1,1)])&=g[\alpha(a,b),\alpha(1,1)] \\ =g[(a,b'),(1,c)]&=b'c, \end{aligned}$$

whence $\alpha(a,b)=\alpha(a,bc)$ for any $(a,b)\epsilon A_G$.

But for fixed c, each transformation $\alpha(a,b)=(a,bc)$ and $\alpha(a)=a$ is an automorphism of A_G. Since the group of such transformations is isomorphic with S, the theorem is proved.

A more complicated construction was found by the author which permitted A_G to be a distributive lattice.

EQUIVALENCE LATTICES

16. *Equivalence relations defined.* Let C be any class of objects, which for convenience we shall suppose to be letters of the alphabet. The number of objects in C will be noted by $n(C)$.

DEFINITION 6: *By an "equivalence relation" on C is meant any reflexive and "circular" relation—that is, any rule x assigning to each pair (a, b) of objects of C one of the two expressions axb or $a\bar{x}b$, in such a way that* (1) *axa for any object a of C, while* (2) *axb and bxc imply cxa for any objects a, b, and c of C.*

The expression axb is read "a is equivalent to b under x", and $a\bar{x}b$ is read "a is not equivalent to b under x".

The reader should encounter no difficulty in proving that any reflexive and circular relation is reflexive, symmetric, and transitive—and conversely. That is, Definition 6 amounts in effect to the more conventional one of Hasse†.

A well-known argument now yields

THEOREM 16: *There is a* (1, 1) *correspondence between equivalence relations x on C and partitions of the objects of C into non-overlapping "x-categories"‡, under which axb if and only if a and b are in the same x-category.*

The number $H^*(n+1)$ of different equivalence relations on $n+1$ objects can easily be calculated.

For by the usual theory of permutations and combinations, to any fixed object a and any number h $(0\leqslant h\leqslant n)$ corresppond just $\binom{n}{h}$ choices of a category S_a of h

† Hasse, *Höhere Algebra*, 1 (1927), 17. What Hasse (and I) call an "equivalence relation", Carnap calls an "equality relation", and P. A. Macmahon would call a "distribution of $n(C)$ objects of type $(1^{n(C)})$ into classes of type (m)".

‡ "Abstraction class" according to Carnap (*Logische Aufbau der Welt* (Berlin, 1928), p. 102).

objects besides a and equivalent to a. And the remaining $n-h$ objects can be divided into categories in just $H^*(n-h)$ ways. Therefore, by Theorem 16

$$H^*(n+1) = \sum_{h=0}^{n} \binom{n}{h} H^*(n-h). \qquad (16\cdot 1)$$

This recurrence relation has been studied†.

17. *Symbols for equivalence relations.* The handling of equivalence relations is greatly simplified by assigning to each equivalence relation x on C a "special symbol" and a "generic symbol".

To obtain the special symbol for x, first imagine the objects of C written in a certain order, and for this purpose identify them with the numbers $1, 2, 3, \ldots, n(C)$.

Then arrange the objects of each x-category in order, suppress the x-categories containing just one object, and arrange the others in the order of their first objects. The symbol is completed by inserting commas between the different x-categories, and enclosing the entire expression in parentheses.

Thus the special symbols involving the first four integers are (), (12), (13), (14), (23), (24), (34), (12, 34), (13, 24), (14, 23), (123), (124), (134), (234), and (1234).

To obtain the generic symbol for x, count the number of objects in each category, arrange the resulting integers in order of decreasing magnitude, separate them by plus signs, and enclose the whole in parentheses.

Thus the generic symbols for equivalence relations involving four objects are $(1+1+1+1)$, $(2+1+1)$, $(2+2)$, $(3+1)$, (4).

The following proposition is obvious,

THEOREM 17: *The number of generic symbols for equivalence relations on C is equal to the number of partitions of the integer $n(C)$.*

18. *The lattice $E(C)$.* In this section we shall show how one is naturally led to consider the equivalence relations on a class C as the elements of a lattice $E(C)$.

DEFINITION 7: *Let C be any class of objects, and let x and y be equivalence relations on C. By the "meet" $x \frown y$ of x and y is meant the relation u on C defined by the rule‡ (1) aub if and only if axb and ayb; by the "join" $x \smile y$ of x and y is meant the meet v of all equivalence relations z on C such that (2) axb or ayb implies azb.*

It is easy to show that $x \frown y$ is an equivalence relation (i.e. reflexive and circular), and that therefore so is $x \smile y$. It is also easy to verify L2–L4 of §4, whence we have

THEOREM 18: *Under Definition 7, the equivalence relations on C are the elements of a lattice $E(C)$.*

† A. C. Aitken, *Edin. Math. Notes*, 28 (1933), xviii-xxiii.

‡ $x \frown y$ is merely the conventional "logical product" of the relations x and y. The operation of join is, however, new.

$E(C)$ is evidently determined to within isomorphism by $n(C)$; the corresponding abstract lattice may therefore be called "the symmetrical equivalence lattice of degree $n(C)$", and any sublattice of $E(C)$ an "equivalence lattice".

The symmetrical equivalence lattices are the analogues in lattice theory of the symmetrical permutation groups.

19. *Covering and rank conditions.* It is clear that an equivalence relation x *contains* an equivalence relation y—i.e. that $x \cap y = y$—if and only if the x-categories are unions of suitable entire y-categories. Consequently (recurring to the definition of covering made in § 6) x covers y if and only if one x-category is the union of two y-categories, and the other x-categories are the same as the other y-categories. This makes it easy to deduce

THEOREM 19: *If x and y cover z, and $x \neq y$, then $x \cup y$ covers x and y. Again, x covers y if and only if $x \not\subset y$ of type $(2+1+1+\ldots+1)$ exists, satisfying $x = y \cup z$.*

Hence if we define (1) a "chain" connecting $y \in E(C)$ with $x \supset y$ as any sequence of elements $x_0 = y, \ldots, x_n = x$ of $E(C)$ such that x_k covers x_{k-1} for $k = 1, \ldots, n$, and (2) the "rank" $\rho(x)$ of $x \in E(C)$ as the excess of $n(C)$ over the number of x-categories we obtain

THEOREM 20: *x covers y if and only if $x \supset y$ while $\rho(x) = \rho(y) + 1$. Consequently any two chains connecting the same two elements have the same length. Moreover any element of rank m can (by induction and Theorem 19) be represented as the join of m, but not of $m-1$, elements of rank one. Finally*[†]

$$\rho(x \cup y) \leqq \rho(x) + \rho(y) = \rho(x \cup y) + \rho(x \cap y). \qquad (19 \cdot 1)$$

20. *Equivalence lattices and Boolean algebras.* It is well known that any finite Boolean algebra B_n of order 2^n can be identified with the field of all sets of n points.

Let S be any subalgebra of B_n; S is finite and contains the empty set. Therefore the elements of B_n corresponding to the "points" of S will be disjoint subsets whose sum is the complement of the empty set. Conversely, any such choice of disjoint sets of points of B determines a reciprocal subalgebra S of B. And finally this (1, 1) correspondence inverts inclusion, so that we have

THEOREM 21: *If $n(C)$ is finite, then $E(C)$ is dually isomorphic with the lattice of the subalgebras of the Boolean algebra of order $2^{n(C)}$.*

21. *Equivalence lattices and groups.* Let G be any group, and S any subgroup of G. If a and b are any elements of G, we shall write aSb if $ab^{-1} \epsilon S$; $a\bar{S}b$ unless $ab^{-1} \epsilon S$. This is known[‡] to define an equivalence relation on the elements of G.

[†] The first inequality is a consequence of the previous statement; the second requires Theorems 19 and 9·2 of "Subalgebras".

[‡] H. Hasse, *op. cit.* p. 60; the proof is, from the standpoint of group theory, elementary.

Let T be any second subgroup of G. To say that ab^{-1} is in $S \frown T$ is to say that ab^{-1} is in S and in T; hence the ordering of equivalence relations to subgroups preserves meets.

Suppose that ab^{-1} is in $S \smile T$. Then $a = s_1 t_1 \dots s_n t_n b$, where the s_i are in S and the t_i are in T. So that if U is any equivalence relation including S and T, then

$$bU(t_n b), (t_n b) U (s_n t_n b), \dots, (t_1 s_2 \dots b) Ua,$$

whence aUb, and U includes the equivalence relation ordered to $S \smile T$. But the equivalence relation ordered to $S \smile T$ clearly includes those ordered to S and to T; hence by Definition 7 the ordering preserves joins.

It follows that every subgroup lattice is isomorphic with a suitable equivalence lattice. But conversely, if we order to each equivalence relation x on n letters the group G_x of all permutations intransitive on the x-categories, then clearly $G_x \frown G_y = G_{x \frown y}$, while it can be shown* that $G_x \smile G_y = G_{x \smile y}$, whence we have

THEOREM 22: *Every subgroup lattice is isomorphic with an equivalence lattice, and conversely.*

COROLLARY: *Every lattice of subgroups of a finite group is dually isomorphic with a lattice of subalgebras of a finite Boolean algebra, and conversely.*

22. *Automorphisms of* $E(C)$. We now prove a not altogether surprising but by no means trivial result.

THEOREM 23: *The automorphisms of* $E(C)$ *are induced by the permutations of the objects of* C. *If* $n \equiv n(C) > 2$, *they constitute the symmetric group of degree* $n(C)$.

For if $n > 2$, then each element of rank $n-2$ having the generic symbol $([n-k]+k)$ covers exactly $2^{k-1} + 2^{n-k-1} - 2$ elements, $(k \leqslant \frac{1}{2}n)$. Therefore (since rank and covering are invariant under automorphisms) the totality of elements having the generic symbol $([n-1]+1)$ is invariant under any automorphism of $E(C)$. Further, any element of rank one is specified by the elements of genus $([n-1]+1)$ which contain it, and any element at all is specified by the elements of rank one which it contains. Hence any automorphism is completely specified by the permutation it performs on the elements of genus $([n-1]+1)$—corresponding to a permutation of the objects of C. Inspection shows that this is still true if $n \leqslant 2$.

If $n > 2$, the permutations of the objects of C induce precisely the symmetric group on the n elements of $E(C)$ of genus $([n-1]+1)$, completing the proof.

COROLLARY: *Two elements* x *and* y *of* $E(C)$ *are conjugate under the group of the automorphisms of* $E(C)$ *if and only if they have the same generic symbol. Hence*

* The technique consists in passing from G_x to $G_{x \smile y}$ through a finite or transfinite sequence of such intransitive groups, and showing that $G_x \smile G_y$ cannot fail to contain any first one of them.

under the definition of Theorem 5, the geometrico-tactical configuration corresponding to $E\,(C)$ has a "rank" equal to the number of partitions of the integer $n\,(C)$.

For the generic symbols describe precisely the conditions under which the x-categories can be transformed into the y-categories by a suitable permutation of the objects of C.

23. *Homomorphic equivalence relations*†. Consider the equivalence relations on the elements of an *algebra* A. Of especial importance are naturally those which are preserved under the operations of A. These are characterized by

DEFINITION 8: *An equivalence relation x on an algebra A is called "homomorphic" if and only if the x-category of the value of any sequence σ is a single-valued function of the x-categories of the elements of σ—that is, if and only if $a_j x b_j$ ($a_j \epsilon A$; $j = 1, \dots, k_i$; $b_j \epsilon A$) implies*

$$f_i(a_1, \dots, a_{ki})\, x\, f_i(b_1, \dots, b_{ki}). \qquad (23\cdot1)$$

It is obvious that the x-categories of any homomorphic equivalence relation on A are the elements of a homomorphic image of A.

THEOREM 24: *Let A be any algebra whose operators are of finite index. Then the homomorphic equivalence relations on A are a sublattice $H\,(A)$ of the symmetrical lattice $E\,(A)$ of all equivalence relations on A.*

That is, the meet u and the join v (under Definition 7) of any two homomorphic equivalence relations x and y are homomorphic equivalence relations.

If $a_j u b_j$ ($j = 1, \dots, k_i$), then $a_j x b_j$ and $a_j y b_j$; whence, denoting $f_i(a_1, \dots, a_{ki})$ by a and $f_i(b_1, \dots, b_{ki})$ by b, by hypothesis axb and ayb, and consequently aub.

Similarly, if $a_j v b_j$ ($j = 1, \dots, k_i$), then we can form chains‡ $c_1^j = a_j, \dots, c_{2n+1}^j = b_j$ such that $c_{2h-1}^j x c_{2h}^j$ and $c_{2h}^j y c_{2h+1}^j$. Hence, writing $c_h = f_i(c_h^1, \dots, c_h^{ki})$, we obtain $c_{2h-1} x c_{2h}$ and $c_{2h} y c_{2h+1}$, and consequently $c_1 v c_{2n+1}$, which is to say avb. This completes the proof.

The following special results are known:

(23·2) The lattice of the homomorphic equivalence relations on any group or ring is a modular lattice§.

(23·3) The lattice of the homomorphic equivalence relations on any finite modular lattice is a Boolean algebra‖.

† This section was added in revision.

‡ We need k_i to be finite to ensure that n should be finite.

§ "Subalgebras", Theorems 26·1 and 27·1, and Speiser, *op. cit.* Theorem 23. By an abstraction of the same method, we can show that if an algebra A is such that to any homomorphic equivalence $a\,(x \smile y)\,b$ corresponds an element c such that axc and cyb, then the lattice of the homomorphisms of A is a modular lattice. It is the lattice $H\,(A)$ which describes the "structure" of A; hence we may call it the "structure lattice" of A.

‖ This result was implicitly announced by Ore in a lecture at Harvard University, and will presumably appear in his paper already cited.

24. *Simple algebras.* Any algebra A has two homomorphic images—itself and the trivial algebra of one element. These correspond respectively to the equivalence relation o under which aob if and only if $a=b$, and the equivalence relation p under which apb for any a and b of A.

If the lattice of the homomorphic equivalence relations on A contains only these two elements, then A is called "simple"[†]; otherwise A is called "composite".

LEMMA 1: *The 5-lattice (1b) graphed in § 6 is simple.*

The proof is left to the reader.

THEOREM 25: *Any finite symmetrical equivalence lattice $E(C)$ is simple.*

Let x be any homomorphic equivalence relation on $E(C)$ other than o, so that axb $(a \neq b)$. Then $c \epsilon E(C)$ with the special symbol (ii) exists such that $c \frown (a \smile b)=c$, but $c \frown (a \frown b)=o_E$ is the element of $E(C)$ with the special symbol $()$. Naturally cxo_E.

If $d \epsilon E(C)$ has the special symbol (kj), or (jk), $(k \neq j)$, then $e \epsilon E(C)$ with the special symbol (kj), or (jk), generates with c and d a sublattice satisfying Lemma 1; whence $o_E xd$. Repeating this process, we can show that dxf for $f \epsilon E(C)$ with the special symbol (hk), irrespective of h. Hence $o_E xf$ for any f with generic symbol $(2+1+1+\ldots+1)$—and so, by Theorem 20, $o_E xz$ for any $z \epsilon E(C)$ whatever, proving $x=p$. This completes the proof.

A "projective geometry" is a system P of elements called points, lines, planes, etc., having incidence relations of a certain type. Every pair of elements a and b of P intersect in a "meet" element $a \frown b$, and generate a least containing element or "join" $a \smile b$. From the known facts (1) every element is the join of those points which it contains, (2) the join of any two distinct points is a line, (3) every line contains at least three points, and (4) L 2–L 4 are satisfied, it can be proved that

THEOREM 26: *Any projective geometry is simple.*

Let x be any homomorphism of P other than o, so that axb for $a \neq b$; whence $(a \smile b)x(a \frown b)$. By (1), P contains a point q such that $q \frown (a \smile b)=q$, but $q \frown (a \frown b)=o_P$, the empty set. If r is any other point, by (2) and (3) the line $q \smile r$ contains a third point s. But o_E, q, r, s, and $q \smile r$ are a sublattice of P satisfying the hypotheses of Lemma 1, and so $o_E xr$.

That is, $o_E xr$ for any point r, and so by (1) $o_E xt$ for any element t of P, and $x=p$, proving the theorem.

25. *The free lattice generated by three elements.* An open question[‡] of some interest is settled by

THEOREM 27: *The free lattice generated by three elements is of infinite order.*

[†] This is the accepted usage for both groups and linear algebras.

[‡] F. Klein, "Beiträge zur Theorie der Verbände", *Math. Zeitschrift*, 39 (1934), 227–239.

It is sufficient to exhibit an equivalence lattice of infinite order generated by three elements. But let C be the class of the points of 3-space with integral coordinates $(m, 1, m)$, $(1, m+1, m)$, and $(m, m, 1)$. And let e_i be the equivalence relation such that ae_ib $(a, b\epsilon C;\ i=1, 2, 3)$ if and only if a and b have the same x_i-coordinate.

The e_i generate a sequence $t_k\epsilon E(C)$, in which

$$t_1=e_1,\quad t_{6n+2}=t_{6n+1}\cup e_2,\quad t_{6n+3}=t_{6n+2}\cap e_3,\quad t_{6n+4}=t_{6n+3}\cup e_1,\quad t_{6n+5}=t_{6n+4}\cap e_2,$$
$$t_{6(n+1)}=t_{6n+5}\cup e_3,\quad \text{and}\quad t_{6(n+1)+1}=t_{6(n+1)}\cap e_1.$$

Those points which are in the same t_k-category as the point $(1, 1, 1)$ are listed in the following table:

$$\begin{aligned}
t_{6n}&: \sum_{k=1}^{n}(k,1,k)\\
t_{6n+1}&: \sum_{k=1}^{n}(1,k+1,k)+\sum_{k=1}^{n}(k,1,k)+\sum_{i=1}^{\infty}(i,i,1)\\
t_{6n+2}&: (1,1,1)+\sum_{k=1}^{n}(1,k+1,k)\\
t_{6n+3}&: \sum_{k=1}^{n}(1,k+1,k)+\sum_{k=1}^{n+1}(k,k,1)+\sum_{i=1}^{\infty}(i,1,i)\\
t_{6n+4}&: \sum_{k=1}^{n+1}(k,k,1)\\
t_{6n+5}&: \sum_{k=1}^{n+1}(k,k,1)+\sum_{k=1}^{n+1}(k,1,k)+\sum_{i=1}^{\infty}(1,i+1,i).
\end{aligned}$$

Hence the t_k are all different, proving the theorem.

COROLLARY: *Any finite lattice satisfies a law on functions of three symbols which cannot be inferred from* L 2–L 4.

TOPOLOGICAL LATTICES

26. *Topological algebras.* By a "topological algebra" is meant any algebra which contains a "convergence" operator f_L operating only on enumerated sequences, and such that if (1) $f_L(\{x_k^i\})=x_i$ for a sequence of n sequences $\{x_k^i\}$, and (2) $f_i(x_k', \ldots, x_k^n)=y_k$ for fixed i and every positive integer k, then

$$(3)'\quad f_L(\{y_k\})=f_i(x_1, \ldots, x_n).$$

This includes van Dantzig's† definitions of topological groups and topological rings, and automatically defines the notion of "topological lattice".

27. *Transfinite joins and meets.* Let A be any algebra, and σ any well-ordered set of subalgebras of A. By $h_1(\sigma)$ denote the set of elements in every subalgebra of σ, and by $h_2(\sigma)$ the meet of the subalgebras which contain every subalgebra

† "Zur topologische Algebra. I. Komplettierungstheorie", *Math. Annalen*, 107 (1933), 587–626.

of σ. It is easily seen[†] that $h_1(\sigma)$ and $h_2(\sigma)$ are themselves subalgebras of A. Hence the subalgebras of A constitute a "complete" lattice $\bar{L}(A)$ satisfying certain laws resembling L 2–L 4 which have been specified elsewhere[‡], and whose study takes us out of algebra into analysis.

28. *Upper and lower limits.* A convergence operator can be defined in $\bar{L}(A)$ by the analogue of an elementary device of real function theory.

Let a_1, a_2, a_3, ... be any enumerable sequence of elements of $\bar{L}(A)$, and denote by α_k the subsequence $a_k, a_{k+1}, a_{k+2}, \ldots$. Then we can define

$$\operatorname{Inf}\{a_k\}=h_1[h_2(\alpha_1), h_2(\alpha_2), h_2(\alpha_3), \ldots],$$

$$\operatorname{Sup}\{a_k\}=h_2[h_1(\alpha_1), h_1(\alpha_2), h_1(\alpha_3), \ldots].$$

Regardless of j and k, $h_2(\alpha_j) \subset a_{j+k} \subset h_1(\alpha_k)$; hence we have

THEOREM 28: $\operatorname{Inf}\{a_k\} \subset \operatorname{Sup}\{a_k\}$ *identically.*

DEFINITION 9: $f_L(\{a_k\})=a$ *if and only if* $\operatorname{Inf}\{a_k\}=a$ *and* $\operatorname{Sup}\{a_k\}=a$.

29. *Topology.* Consider the topology of the abstract convergence space defined by the operator f_L defined in Definition 9. If $c_k=c$ for every k, then clearly $f_L(\{c_k\})=c$.

Again, $f_L(\{c_k\})=c$ and $f_L(\{c_k\})=c'$ imply $c=\operatorname{Inf}\{c_k\}=c'$. And if $f_L(\{c_k\})=c$ and $k(i)\to\infty$, then

$$c \subset \operatorname{Inf}\{c_k\} \subset \operatorname{Inf}\{c_{k(i)}\} \subset \operatorname{Sup}\{c_{k(i)}\} \subset \operatorname{Sup}\{c_k\} \subset c,$$

and so $f_L(\{c_{k(i)}\})=c$.

Finally, if $f_L(\{c_k\})=c$, then no matter what c_0 is given, the augmented sequence $c_0, c_1, c_2, \ldots$ has certainly the same upper and lower limits as before, and hence converges to c. That is, we have

THEOREM 29: *The space defined by the convergence operator f_L is a Kneser*[§] *"Konvergenzraum" for any complete lattice.*

On the other hand, it need not define the lattice to be a topological lattice. It must in the important case that the lattice is a complete lattice of point-sets. But if the lattice is the complete lattice of closed sets on a line, examples can be given showing that this is no longer the case.

30. *A metric group.* Consider the Boolean algebra $B(\Sigma)$ of the measurable sets in a space Σ having a mass-function[||] in the sense of Carathéodory. Let S and T be any two measurable sets of Σ; we shall use the notation $S+T$ for the

[†] As in "Subalgebras", § 2.

[‡] Stated in "Subalgebras", § 3.

[§] "Die Deformationssätze der einfach zusammenhangenden Flächen", *Math. Zeits.* 25 (1926), 362.

[||] C. Carathéodory, *Vorlesungen über reelle Funktionen* (Berlin, 1927), 2nd ed. p. 238.

sum of S and T, ST for their common part, $\bar{S}$ for the complement of S, and $\mu(S)$ for its measure.

Make a homomorphic image of $B(\Sigma)$ by putting $S=T$ if and only if $\mu(S\bar{T}+\bar{S}T)=0$. Define the "distance" $\rho(S,T)$ from S to T as the smaller of 1 and $\mu(S\bar{T}+\bar{S}T)$. And finally, define the "product" $S.T$ of S and T as $S\bar{T}+\bar{S}T$.

It is easy to show that the equivalence relation is homomorphic, and that $\rho(S,T)$ is metric and makes the image algebra topological in the sense of § 26. Moreover, it is known[†] that the definition of $S.T$ makes $B(\Sigma)$ into an Abelian group. Since finally

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

irrespective of A, B, and C, we have

THEOREM 30: *The homomorphic image of the Boolean algebra of the measurable sets in any space having a regular mass-function, formed by disregarding sets of measure zero, is a metric group*[‡] *under a distance-function which makes the algebra topological.*

31. *Unsolved problems.* The preceding material suggests several interesting questions whose answer is unknown.

Some questions concern equivalence lattices. Is any lattice realizable as a lattice of equivalence relations? Is the dual of any equivalence lattice an equivalence lattice? In particular, is the dual of the symmetrical equivalence lattice of degree four (graphed in § 6) an equivalence lattice? More generally, are equivalence lattices a family in the species of algebras of double composition.

Again, it is known that the free distributive lattice generated by n elements is of finite order $D(n)$, but nothing is known about the function $D(n)$ except its first four terms[§].

Finally, is any finite modular lattice a sublattice of a direct product of finite projective geometries and Boolean algebras of order two?

[†] Proved by P. J. Daniell, "The modular difference of classes", *Bull. Amer. Math. Soc.* 23 (1916), 446–50.

[‡] In the sense of van Dantzig, *op. cit.*

[§] R. Dedekind, *Ges. Werke*, 2, 147, states that $D(1)=1$, $D(2)=4$, $D(3)=18$, $D(4)=166$.