THE THEORY OF REPRESENTATIONS FOR BOOLEAN ALGEBRAS*

BY

M. H. STONE

INTRODUCTION

Boolean algebras are those mathematical systems first developed by George Boole in the treatment of logic by symbolic methods† and since extensively investigated by other students of logic, including Schröder, Whitehead, Sheffer, Bernstein, and Huntington.‡ Since they embody in abstract form the principal algebraic rules governing the manipulation of classes or aggregates, these systems are of technical interest to the mathematician quite as much as to the logician. It is thus natural to suppose that a study of Boolean algebras by the methods of modern algebra will prove fruitful of important and useful results. Indeed, if one reflects upon various algebraic phenomena occurring in group theory, in ideal theory, and even in analysis, one is easily convinced that a systematic investigation of Boolean algebras, together with still more general systems, is probably essential to further progress in these theories.§ The writer's interest in the subject, for example, arose in connection with the spectral theory of symmetric transformations in Hilbert space and certain related properties of abstract integrals. In the actual development of the proposed theory of Boolean algebras, there emerged some extremely close connections with general topology which led at once to results of sufficient importance to confirm our a priori views of the probable value of such a theory.||

In the present paper, which is one of a projected series, we shall be concerned primarily with the problem of determining the representation of a

* Presented to the Society (in part), February 25, 1933; see abstract 39-3-86. Received by the editors October 10, 1935.

† See *The Mathematical Analysis of Logic*, 1847, and *An Investigation of the Laws of Thought*, 1854.

‡ For bibliographical information, see Huntington, these Transactions, vol. 35 (1933), pp. 274–304, especially pp. 274–275.

§ Dedekind's observations and technical contributions, in Mathematische Annalen, vol. 53 (1900), pp. 371–403, relative to the occurrence of such general systems did not immediately provoke general interest. Recently, a considerable amount of work along the general lines laid down by Dedekind has appeared: see, for instance, Fritz Klein, Mathematische Annalen, vol. 105 (1931), pp. 308–323; Garrett Birkhoff, Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), pp. 441–464; O. Ore, Annals of Mathematics, (2), vol. 36 (1935), pp. 406–437.

|| See Stone, Proceedings of the National Academy of Sciences, vol. 20 (1934), pp. 197–202.

given Boolean algebra by algebras of classes, aggregates, or combinations. It is natural to surmise that the problem always has a solution leading to the construction of an algebra of classes isomorphic to the given Boolean algebra. Such a result is a precise analogue of the theorem that every abstract group is represented by an isomorphic group of permutations. Here we shall establish the validity of this surmise and, in addition, shall characterize all possible algebras of classes homomorphic to a given Boolean algebra. It is a curious fact that these results are considerably more recondite than the corresponding theorems for abstract groups: the elements of the representative classes must be taken as certain classes of elements in the given Boolean algebra (in particular, as the prime ideals in the algebra), whereas the elements of the permutations representing an abstract group are taken as elements of the group itself; and the existence of prime ideals, in terms of which the representation is constructed, can apparently be established in general only by an appeal to the Zermelo hypothesis.

The observation that Boolean algebras can be regarded as special instances of the systems known as abstract rings enables us to apply the concepts and results of modern algebraic theory directly to the purposes of the present paper.* Here we shall show in detail that Boolean algebras are identical with those rings with unit in which every element is idempotent.† In this identification, ring addition and multiplication correspond abstractly to the formation of the union (modulo 2) and intersection, respectively, of classes. The union (modulo 2), or symmetric difference, of two classes is the class of objects belonging to one or the other, but not to both, of those classes; and is thus familiar to combinatorial topologists. On algebraic grounds it is convenient to admit rings other than those which possess units. We shall therefore take as the central theme of this paper not merely Boolean algebras, but, more generally, rings in which every element is idempotent, designating the latter systems as Boolean rings or generalized Boolean algebras.

The paper falls naturally into four parts or chapters. The first deals with the formal algebraic properties of Boolean rings; the second with subrings, ideals, and homomorphisms; the third with the structure of Boolean rings with elements which are given as abstract classes; and the fourth with the representation theory. In general we shall limit our investigations to those topics which are essential for an adequate understanding of the algebraic

* For general information concerning modern algebraic developments, we refer to B. L. van der Waerden, *Moderne Algebra*, vol. 1, Berlin, 1930, Chapter 3 of which deals particularly with the definition and basic properties of abstract rings. We shall assume that the reader has a general knowledge of this material.

† See Stone, Proceedings of the National Academy of Sciences, vol. 21 (1935), pp. 103–105; Gegalkin, Matematicheskii Sbornik, vol. 35 (1928), pp. 311–373.

aspects of the representation theory, leaving until another occasion a deeper study of the classification of ideals and the introduction of the concepts of general topology. A more complete survey of the contents of the present paper is the following: Chapter I, Formal algebraic properties of Boolean rings: §1, Direct discussion of Boolean rings; §2, Connections with Boolean algebras; §3, Special Boolean rules; §4, Special elements. Chapter II, Subrings, ideals, and homomorphisms: §1, Subrings and their combinations; §2, Ideals and their combinations; §3, A classification of ideals; §4, Prime ideals; §5, Congruences, ideals and homomorphisms; §6, Direct sums. Chapter III, Algebras of classes: §1, The construction of algebras of classes; §2, Reduction and equivalence; §3, The analysis of algebras of classes; §4, An illustration. Chapter IV, Representation theory: §1, General remarks; §2, Existence and divisibility properties of prime ideals; §3, The perfect representation.

CHAPTER I. FORMAL ALGEBRAIC PROPERTIES OF BOOLEAN RINGS

1. **Direct discussion of Boolean rings.** In this section we shall consider the elementary facts relating to rings in which every element is idempotent, leaving for the remaining sections of the chapter the study of their connections with Boolean algebras and of certain special relations and elements. By a ring we mean a system with double composition, the operations being called addition and multiplication and denoted here by the usual symbols $+$ and $\cdot$ (the latter commonly being suppressed in writing down products), subject to the following laws: addition is commutative and associative, multiplication is associative and both left- and right-distributive with respect to addition, and the equation $x+a=b$ has a solution for arbitrary a and b. We do not assume that multiplication is commutative or that a ring contains more than one element. It is well known that in any ring the solution 0 of the equation $x+a=a$ is independent of a and satisfies the relations $a+0=0+a=0$, $0a=a0=0$; that the solution $-a$ of the equation $x+a=0$ is unique; and that the solution of the equation $x+a=b$ is unique and is given by $x=b+(-a)$, commonly written $b-a$. We now lay down the following formal definition:

DEFINITION 1. *A ring in which every element is idempotent, satisfying the law* $aa=a$, *is called a Boolean ring.*

Our first result is embodied in the following theorem.

THEOREM 1. *A Boolean ring is necessarily commutative; obeys the two equivalent laws* $a+a=0$, $a=-a$; *and necessarily contains divisors of* 0 *if it contains more than two elements. Every Boolean ring A can be imbedded in a Boolean*

ring B which possesses a unit element, in such a manner that B is unique in the following sense: if C is a Boolean ring with unit containing A, then C contains also a Boolean ring B^* isomorphic to B and containing A. A finite Boolean ring necessarily possesses a unit and has a cardinal number which is a power of 2.

In this, as in all subsequent discussions, we may use the familiar rules governing the ring operations without going into complete detail. Using such rules, we see that in a Boolean ring

$$a + b = (a + b)(a + b) = (a + b) + (ba + ab)$$

and hence that $ba+ab=0$. If we put $b=a$ in the latter relation, we find at once that $a+a=0$, or, equivalently, $a=-a$. Using this result, we conclude that $ba=-(ab)=ab$, thus establishing the commutative law for multiplication. The special rules which we have now demonstrated will henceforth be used in our discussions without explicit reference. In a Boolean ring with more than two elements, we can choose a and b so that $a\neq 0$, $b\neq 0$, $a\neq b$. If $ab=0$, then a and b are both divisors of 0. On the other hand, if $ab\neq 0$, then ab and $a+b$ are both divisors of 0: for $a+b=0$ would imply $a=-b=b$, contrary to hypothesis; and $ab(a+b)=aab+abb=ab+ab=0$. A Boolean ring with one or with two elements obviously cannot contain divisors of 0, every product in such a ring either containing 0 as a factor or reducing, by the law of idempotence, to an element other than 0.

In discussing the possibility of imbedding a Boolean ring A in a Boolean ring B with unit, we may disregard the trivial case where A has a unit and B coincides with A. When A has no unit, we construct B by the adjunction of suitable elements. The construction can be carried out even when A has a unit and always produces B as a proper superclass of A. We first provide an abstract element ϵ, distinct from those of A, and define

$$\epsilon\epsilon = \epsilon, \quad \epsilon a = a\epsilon = a, \quad \epsilon + 0 = 0 + \epsilon = \epsilon, \quad \epsilon + \epsilon = 0,$$

observing that the elements 0 and ϵ constitute a two-element Boolean ring. We then consider the ordered pairs (a, α) where a is in A and $\alpha=0$ or $\alpha=\epsilon$, defining the operations of addition and multiplication upon them by the rules

$$(a, \alpha) + (b, \beta) = (a + b, \alpha + \beta),$$
$$(a, \alpha)(b, \beta) = (ab + \alpha b + a\beta, \alpha\beta).$$

It is easily verified that under these operations the class of pairs (a, α) is a Boolean ring with $(0, \epsilon)$ as its unit. Instead of giving all the calculations in detail, we shall discuss only one or two steps. Passing over the commutative

and associative laws for addition and multiplication, we turn to the demonstration of the left-distributive law for multiplication: we have

$$\begin{aligned}(a, \alpha)[(b, \beta) + (c, \gamma)] &= (a, \alpha)(b + c, \beta + \gamma) \\ &= (a(b + c) + \alpha(b + c) + a(\beta + \gamma), \alpha(\beta + \gamma)) \\ &= ((ab + \alpha b + a\beta) + (ac + \alpha c + a\gamma), \alpha\beta + \alpha\gamma) \\ &= (ab + \alpha b + a\beta, \alpha\beta) + (ac + \alpha c + a\gamma, \alpha\gamma) \\ &= (a, \alpha)(b, \beta) + (a, \alpha)(c, \gamma)\end{aligned}$$

by appropriate combination of the properties of A with the easily checked relations $\alpha(b+c)=\alpha b+\alpha c$, $a(\beta+\gamma)=a\beta+a\gamma$, $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$. The right-distributive law then follows from this by the use of the commutative law for multiplication. We now see that the equation $(x, \xi)+(a, \alpha)=(b, \beta)$ has the solution $(x, \xi)=(b+a, \beta+\alpha)$ since

$$(b + a, \beta + \alpha) + (a, \alpha) = (b + a + a, \beta + \alpha + \alpha) = (b, \beta).$$

Thus the pairs (a, α) constitute a commutative ring. The law of idempotence is established as follows:

$$\begin{aligned}(a, \alpha)(a, \alpha) &= (aa + \alpha a + a\alpha, \alpha\alpha) = (a + (\alpha + \alpha)a, \alpha) \\ &= (a + 0a, \alpha) = (a, \alpha).\end{aligned}$$

To show that the Boolean ring thus obtained has $(0, \epsilon)$ as its unit, we note the relations

$$(0, \epsilon)(a, \alpha) = (0a + \epsilon a + 0\alpha, \epsilon\alpha) = (a, \alpha).$$

As in any commutative ring, the unit is unique and is a right- as well as left-unit. The pairs $(a, 0)$ obviously constitute a Boolean ring isomorphic to A in accordance with the equations

$$\begin{aligned}(a, 0) + (b, 0) &= (a + b, 0), \\ (a, 0)(b, 0) &= (ab + 0b + a0, 00) = (ab, 0).\end{aligned}$$

To construct B, we now replace each pair $(a, 0)$ by the corresponding element a without disturbing in any other way the operations defined over the class of pairs (a, α). Evidently B is a Boolean ring with unit isomorphic to the ring of pairs (a, α); and it contains A. If C is a Boolean ring with unit e containing A, we set up an isomorphism between B and a subring B^* of C as follows. The elements of B correspond in a one-to-one manner with the pairs (a, α), by construction. We can easily set up a one-to-one correspondence between the pairs (a, α) and certain elements of C by requiring that $(a, \alpha) \longleftrightarrow a+f(\alpha)$, where a is in A and $f(0)=0$, $f(\epsilon)=e$. The fact that e be-

longs to C but not to A renders the indicated correspondence biunivocal, since $a+f(\alpha)=b+f(\beta)$ implies $f(\alpha)+f(\beta)=a+b\neq e$, $f(\alpha)+f(\beta)=0$, $f(\alpha)=f(\beta)$, $a=b$. In view of the relations $f(\alpha+\beta)=f(\alpha)+f(\beta)$, $f(\alpha\beta)=f(\alpha)f(\beta)$, which are readily checked, the correspondence between the pairs (a, α) and the elements $a+f(\alpha)$ is an isomorphism: for $(a, \alpha)\longleftrightarrow a+f(\alpha)$, $(b, \beta)\longleftrightarrow b+f(\beta)$ imply

$$\begin{aligned}(a, \alpha) + (b, \beta) &= (a + b, \alpha + \beta) \longleftrightarrow (a + b) + f(\alpha + \beta)\\ &= (a + f(\alpha)) + (b + f(\beta)),\\ (a, \alpha)(b, \beta) &= (ab + \alpha b + a\beta, \alpha\beta) \longleftrightarrow ab + \alpha b + a\beta + f(\alpha\beta)\\ &= ab + f(\alpha)b + af(\beta) + f(\alpha)f(\beta)\\ &= (a + f(\alpha))(b + f(\beta)).\end{aligned}$$

The elements $a+f(\alpha)$ thus constitute a Boolean ring B^* isomorphic to B, containing the elements of A (since $a=a+f(0)$), and contained in C.

If A is a finite Boolean ring, we determine its unit explicitly as a symmetric function of its elements. Denoting by $p(a_1, \cdots, a_n)$ the sum of the n elementary symmetric functions of the elements $a_1, \cdots, a_n$, we observe the identity

$$\begin{aligned}p(a_1, \cdots, a_n) = a_k &+ p(a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n)\\ &+ a_k p(a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_n),\end{aligned}$$

valid for any commutative ring. In a Boolean ring A with exactly N elements, we show that $p(a_1, \cdots, a_N)$ is a unit: for, if a_k is one of the elements, the above identity leads, in combination with the peculiar properties of A, to the relation

$$p(a_1, \cdots, a_N)a_k = a_k + 2p(a_1, \cdots, a_{k-1}, a_{k+1}, \cdots, a_N)a_k = a_k.$$

If A is a finite Boolean ring with exactly N elements, we show further that N is a power of 2. Indeed, we shall establish the more general result that an additive abelian group of N elements in which $a+a=0$ has the property that N is a power of 2. For $N=1$, the desired result is obvious. Let us suppose that this result has been extended to those cases where $N\leqq 2^M$. If now $N\leqq 2^{M+1}$ we may suppose also that known cases are excluded by subjecting N to the inequality $N>2^M$. The given group G contains an element a other than 0, the two elements a and 0 constituting a normal subgroup $\mathfrak{g}$ by virtue of the relations $0+0=a+a=0$, $a+0=0+a=a$. The quotient group $G/\mathfrak{g}$ is homomorphic to G and therefore obeys the law $a+a=0$. Since its order is $N/2$ and therefore at most equal to 2^M, we conclude that $N/2=2^m$, $N=2^{m+1}$. The inequalities satisfied by N show that $N=2^{M+1}$. By induction the desired

result holds for all finite groups of the indicated type and hence, in particular, for finite Boolean rings.

2. **Connections with Boolean algebras.** We shall prove in the present section that the fundamental properties of Boolean rings, as stated in Definition 1, in reality constitute a new set of postulates for Boolean algebras and certain simple generalizations thereof, these systems having hitherto been characterized by the postulation of different fundamental properties governing operations among which the ring-addition of the preceding section did not appear. Our task thus consists in setting up suitable relations between the respective operations chosen as fundamental in various sets of postulates, including the set suggested by Definition 1, and in establishing the interdeducibility of the postulates of these different sets. Another task which we might undertake is that of eliminating possible redundancies from the set of ring-postulates, as here extended to include the law of idempotence. We shall not make any serious attempt to carry through the necessary investigations in the present paper, such an enterprise being of secondary importance for our immediate purposes. What is of primary importance here is the identification of the abstract algebras arising from logic and the theory of classes with systems amenable to the methods developed by modern algebraists, namely, with those special rings which we have termed Boolean rings in anticipation of the detailed results of the present section.

We shall first consider a recent set of postulates for Boolean algebras due to Huntington.† The operations in terms of which the postulates are framed are a binary operation, which we shall denote by $\vee$ and which corresponds to logical addition and to the formation of the union for classes, and a unary operation, which is denoted by the prime $'$ and which corresponds to logical negation and to the formation of the complement for classes. These operations are assumed to apply without restriction to elements of the system, yielding elements of the system. Huntington's postulate requiring that the system contain at least two elements plays no part in his deductions and will be suppressed here so as to admit one-element Boolean algebras as well as one-element rings. In stating the connection between Huntington's characterization of Boolean algebras and the properties of Boolean rings, we shall designate several propositions by the numbers attached to them in Huntington's paper, thus facilitating comparison.

THEOREM 2. *If A is a Boolean ring with unit e, the introduction of a binary operation $\vee$ and a unary operation $'$ through the equations*

† Huntington, these Transactions, vol. 35 (1933), pp. 274–304, 557–558. The set in question is discussed on pp. 280–286, 557–558, a serious redundancy in the original set being eliminated on the two pages last cited.

(1) $a \vee b = a + b + ab$, (2) $a' = a + e$

converts A into an algebraic system B in which

(4.3) $a \vee b = b \vee a$, (4.4) $a \vee (b \vee c) = (a \vee b) \vee c$,

(4.6) $(a' \vee b')' \vee (a' \vee b)' = a$,

the old operations being expressed in terms of the new through the equations

(6) $a + b = ab' \vee a'b = (a' \vee b'')' \vee (a'' \vee b')'$,

(7) $ab = (a' \vee b')'$.

On the other hand, if B is an algebraic system obeying the laws (4.3), (4.4) *and* (4.6), *then B is a Boolean algebra; and the introduction of new operations through the equations* (6) *and* (7) *converts B into a Boolean ring A with unit* $e = a \vee a'$ *and zero* $0 = e' = (a \vee a')'$, *the old operations being expressed in terms of the new through the equations* (1) *and* (2) *above.*†

This theorem clearly serves to identify Boolean rings with unit and Boolean algebras, as characterized by Huntington's postulates. In view of Theorem 1, a Boolean ring without unit can be regarded as imbedded in one which has a unit. Hence the present theorem reveals the essential nature of all Boolean rings. In particular, it shows that the operation of addition in a Boolean ring corresponds abstractly to the operation of forming the symmetric difference or union (modulo 2) of classes, as indicated by the relation (6); and it shows similarly that the operation of multiplication corresponds to the operation of forming the intersection of classes, as indicated in the relation (7).

If A is any Boolean ring, either with or without unit, we may write $a \vee b = a + b + ab = p(a, b)$, in terms of the symmetric function introduced in the proof of Theorem 1. We then have

$$a \vee (b \vee c) = p(a, p(b, c)) = a + p(b, c) + ap(b, c) = p(a, b, c)$$
$$= p(p(a, b), c) = (a \vee b) \vee c.$$

Thus the operation introduced in (1) has properties (4.3) and (4.4), expressing the commutative and associative laws. If A has a unit e, we observe that the operation introduced in (2) has the properties

$$a'' = (a + e) + e = a + (e + e) = a + 0 = a,$$
$$(a \vee b)' = (a + b + ab) + e = (a + e)(b + e) = a'b'.$$

With their aid we can establish (4.6), (6), and (7), as follows:

† Stone, Proceedings of the National Academy of Sciences, vol. 21 (1935), pp. 103–105.

$$
\begin{aligned}
(a' \vee b')' \vee (a' \vee b)' &= a''b'' \vee a''b' = ab \vee ab' \\
&= ab + ab' + (ab)(ab') \\
&= ab + a(b + e) + ab(b + e) \\
&= ab + ab + a + ab + ab = a, \\
(a' \vee b'')' \vee (a'' \vee b')' &= (a' \vee b)' \vee (a \vee b')' = a''b' \vee a'b'' = ab' \vee a'b \\
&= a(b + e) + (a + e)b + ab(a + e)(b + e) \\
&= ab + a + ab + b + (a + a)(b + b) = a + b, \\
(a' \vee b')' &= a''b'' = ab.
\end{aligned}
$$

Thus the introduction of the new operations $\vee$ and $'$ converts A into a Boolean algebra B in the sense of Huntington's postulates.

On the other hand, if B is a Boolean algebra in that sense, Huntington has shown that the following propositions are valid in B:

(4.10) $a'' = a$, (4.11) $a \vee a' = b \vee b'$, (4.5) $a \vee a = a$,

(4.16) $ae = a$, (4.22) $a \vee e = e$,

(4.15) $0 \vee a = a$, (4.23) $a0 = 0$,

(4.18) $ab = ba$, (4.19) $(ab)c = a(bc)$, (4.34) $a(b \vee c) = ab \vee ac$,

where e is the element $a \vee a'$, unique in accordance with (4.11), 0 is the element e', and $ab = (a' \vee b')'$ in accordance with (7). On noting that $aa' = (a' \vee a'')' = e' = 0$, we see that

$$
\begin{aligned}
a + b &= ab' \vee a'b = ba' \vee b'a = b + a, \\
a + (b + c) &= a(bc' \vee b'c)' \vee a'(bc' \vee b'c) = a(bc')'(b'c)' \vee a'bc' \vee a'b'c \\
&= a(b' \vee c)(b \vee c') \vee a'bc' \vee a'b'c = ab'c' \vee abc \vee a'bc' \vee a'b'c \\
&= ca'b' \vee cab \vee c'ab' \vee c'a'b = c + (a + b) \\
&= (a + b) + c
\end{aligned}
$$

by virtue of the propositions stated above. We see further that

$$
\begin{aligned}
ab + ac &= ab(ac)' \vee (ab)'(ac) = ab(a' \vee c') \vee (a' \vee b')(ac) \\
&= abc' \vee ab'c = a(bc' \vee b'c) = a(b + c).
\end{aligned}
$$

Thus the operations $+$ and $\cdot$ are both commutative and associative and the second is left- and right-distributive with respect to the first. If we can show that the equation $x + a = b$ has a solution, we can therefore assert that the introduction of these operations converts B into a commutative ring A. Now we evidently have $a + a = aa' \vee a'a = 0$ and $a + 0 = a0' \vee a'0 = a0' = ae = a$. Consequently, we find that $x = b + a$ is a solution in accordance with the rela-

tions $(b+a)+a=b+(a+a)=b+0=b$. Since the indicated solution reduces to $x=0$ when $b=a$, we have also identified 0 as the zero element of the ring A into which B is converted. The proposition (4.16) identifies e as the unit of A. In order to show that A is a Boolean ring, we have only to observe the equations $aa=(a' \vee a')'=a''=a$. To complete the proof of the theorem we must show finally that relations (1) and (2) are valid. Since we have

$$\begin{aligned} a + e &= ae' \vee a'e = a0 \vee a' = a', \\ a \vee b &= (a \vee b)'' = (a'b')' = (a + e)(b + e) + e \\ &= ab + a + b + e + e \\ &= a + b + ab, \end{aligned}$$

the desired results are established.

The postulates of Huntington which have just been discussed are not the only ones in terms of which Boolean algebras may be characterized. Indeed, the sets of postulates which involve only the operations corresponding to the formation of the union and intersection of classes are quite numerous, should one wish to confine himself to those postulates which are perhaps the most natural as well as the most familiar. It may therefore be of some interest if we establish a theorem relating Boolean rings to Boolean algebras as characterized by at least one such set of postulates. In any event, the possibility of extending such a relation so as to obtain a characterization of all Boolean rings, both with and without unit, in terms of union and intersection surely deserves consideration. We shall therefore proceed to discuss two sets of postulates which we have given elsewhere, one set characterizing Boolean algebras, the other slightly more general systems which we have called generalized Boolean algebras and shall now identify with Boolean rings.†

THEOREM 3. *If A is a Boolean ring with unit e, then the replacement of the operation $+$ by a new operation $\vee$ defined by the relation*

$$(1) \qquad a \vee b = a + b + ab$$

converts A into a system B with the properties

$$(1_1) \quad a \vee b = b \vee a;$$

$$(3_1) \quad a(b \vee c) = ab \vee ac; \qquad (3_2) \quad (a \vee b)c = ac \vee bc;$$

(4_1) *there exists an element 0 such that $a \vee 0 = a$ for every a;*

(5) *if there exists an element 0 with the property (4_1), then there exists at least one such element 0 to which corresponds a fixed element e such that the equations $x \vee a = e$, $xa = 0$ have a solution for every element a;*

† Stone, American Journal of Mathematics, vol. 57 (1935), pp. 703–732.

(6_1) $a \vee a = a$; (6_2) $aa = a$;

where the old operation $+$ *is defined in terms of the new by the relation*

(7) $a+b$ *is a solution, necessarily unique, of the simultaneous equations* $x \vee ab = a \vee b$, $x(ab) = 0$.

Conversely, if B *is a system with the indicated properties* (1_1)–(6_2), *the replacement of the operation* $\vee$ *by the new operation* $+$ *defined by the relation* (7) *converts* B *into a Boolean ring* A *with the elements* 0 *and* e *of* (4_1) *and* (5) *as its zero and unit elements respectively, the old operation* $\vee$ *being expressed in terms of the new by the relation* (1).

If A is a Boolean ring with unit e, we verify properties (1_1)–(6_2) as follows: (1_1) is proved as in Theorem 2; (3_1) is proved by the relations $a(b \vee c) = a(b+c+bc) = ab+ac+abc = ab+ac+(ab)(ac) = ab \vee ac$; (3_2) follows from (3_1) by the commutative law for multiplication, already proved in Theorem 1; the element 0 of A has the property (4_1), since $a \vee 0 = a+0+a0 = a$; for the solution x of the equations given in (5) we may take $x = a+e$, where e is the unit in A, since $(a+e) \vee a = (a+e)+a+(a+e)a = a+e+a+a+a = e$, $(a+e)a = a+a = 0$; (6_1) is proved by the relations $a \vee a = a+a+aa = a+a+a = a$; and (6_2) is the characteristic property of Boolean rings. Thus A is converted into a system B in the indicated manner. The relation (7) is verified by virtue of the equations

$$(a + b)ab = ab + ab = 0,$$

$$(a + b) \vee ab = a + b + ab + (a + b)ab = a + b + ab = a \vee b.$$

The converse part of the theorem is proved, though not explicitly stated, in the paper cited above. The properties (1_1)–(6_2) are there shown to be characteristic of Boolean algebras and the solution of the equations (7) is discussed at length, being denoted by $a \Delta b$ instead of $a+b$. The commutative and associative laws for the operation Δ or $+$, and for multiplication, the distributive laws for multiplication, and the existence of a solution of the equation $x+a = b$, are established in Theorems 26, 34, 13, 15, 38, and 33 respectively. Thus the replacement of the operation $\vee$ by the operation $+$ converts B into a commutative ring A. Property (6_2) identifies A as a Boolean ring; and the existence of a unit is established in Theorem 2 of the cited paper, where it is shown that the element e of (5) has the property $ea = a$. The relation $a+0 = a$, proved in Theorem 29, identifies the element 0 of (4_1) as the zero of the ring A. Finally we establish the relation (1) as follows: by (7) we see that $(a+b)+ab$ must satisfy the equation $x \vee (a+b)ab = (a+b) \vee ab$ and hence must be equal to $(a+b) \vee ab$ since $(a+b)ab = ab+ab = 0$; but, by (7) again, $(a+b) \vee ab = a \vee b$.

THEOREM 4. *If A is a Boolean ring, either with or without unit, the replacement of the operation $+$ by the operation $\vee$ defined by the relation*

$$a \vee b = a + b + ab \tag{1}$$

converts A into a system B with the properties

$$a \vee b = b \vee a; \tag{1_1}$$

$$a(bc) = (ab)c; \tag{2_2}$$

$$a(b \vee c) = ab \vee ac; \tag{3_1}$$

(4_1) *there exists an element* 0 *such that* $a \vee 0 = a$ *for every* a;

(5_1) *if* $ba = a$, *there exists an element* 0 *with property* (4_1), *independent of* a *and* b, *such that the equations* $x \vee a = b$, $xa = 0$ *have a solution*;

(5_2) *if* $ab = a$, *there exists an element* 0 *with the property* (4_1), *independent of* a *and* b, *such that the equations* $x \vee a = b$, $ax = 0$ *have a solution*;

$$a \vee a = a; \tag{6_1}$$

$$aa = a; \tag{6_2}$$

where the old operation $+$ is defined in terms of the new by the relation

(7) $a+b$ *is a solution, necessarily unique, of the simultaneous equations* $x \vee ab = a \vee b$, $x(ab) = 0$.

Conversely, if B is a system with the indicated properties (1_1)–(6_2), *the replacement of the operation $\vee$ by the new operation $+$ defined by the relation* (7) *converts B into a Boolean ring A with the element* 0 *of* (4_1) *as its zero element, the old operation $\vee$ being expressed in terms of the new by the relation* (1).

This theorem serves to identify Boolean rings with those systems which we have termed generalized Boolean algebras.

If A is a Boolean ring, we see from the discussion given under Theorem 3 that the operation $\vee$ defined by (1) has properties (1_1), (3_1), (4_1), (6_1), and (6_2). Property (2_2), the associative law for multiplication, holds in A by the definition of a ring. Thus we have only to examine properties (5_1) and (5_2). In view of the commutative law for multiplication in A, these properties are equivalent, and we may confine our attention to the first. We show that $x = a+b$ satisfies the simultaneous equations of (5_1): $x \vee a = (a+b)+a$ $+(a+b)a = a+b+a+a+a = b$, when $ba = a$; and $xa = (a+b)a = a+a = 0$, when $ba = a$. Hence the replacement of the operation $+$ by the operation $\vee$ converts A into a system B of the indicated type. The proof that the relation (7) is valid is the same as that given under Theorem 3.

The converse part of the theorem is proved, but not explicitly stated, in the paper cited above. In fact, Theorem 55 of that paper shows that the argument used in Theorem 3 above applies equally well to the present system B, save for the part relating to the existence of a unit.

3. **Special Boolean rules.** The results of §§1 and 2 show that the various operations $+$, $\vee$, $\cdot$, and $'$ obey all the formal rules peculiar to appropriate corresponding operations upon classes. Many of these special rules, which we may properly designate as Boolean rules, are stated explicitly in the text. Such, for example, are the commutative and associative laws for each of the operations $+$, $\vee$, and $\cdot$, and the distributive laws for $\cdot$ with respect to $+$ and $\vee$. Indeed, the only important rule which is neither stated nor trivially implied by rules given explicitly is the distributive law for $\vee$ with respect to $\cdot$, a rule which we can prove at once in the following manner:

$$\begin{aligned}(a \vee b)(a \vee c) &= (a + b + ab)(a + c + ac) \\ &= a + ac + ac + ba + bc + bac + ab + abc + abc \\ &= a + bc + abc = a \vee bc.\end{aligned}$$

In the sequel, we shall leave the justification for our use of such special Boolean rules to the reader's recollection of the familiar corresponding rules for operations upon classes or to his personal verification of their validity on the basis of Theorem 1 and the relations $a' = a + e$, $a \vee b = a + b + ab$. It is perhaps desirable that we should point out one essential fact at this place: we raise no presumption that every possible law verifiable for the appropriate operations upon classes is also verifiable in the abstract for the associated operations in Boolean rings. Indeed, the proof that such is the case is one of the central features of the representation theory which we propose to build upon the basis of rules already cited or, at least, readily verifiable therefrom.

It is convenient for us to introduce at this point the abstract relation which corresponds to the relation of class-inclusion and to outline its chief properties. More exhaustive investigations of this topic are to be found elsewhere.† We begin with the formal definition of the indicated relation.

DEFINITION 2. *In a Boolean ring A, the element a is said to be less than or to be contained in the element b, in symbols $a < b$, and the element b is said to be greater than or to contain the element a, in symbols $b > a$, whenever any of the equivalent relations*

$$ab = a, \qquad a \vee b = b, \qquad ab' = 0, \qquad a' \vee b = e$$

is satisfied, the last two being significant if and only if A has a unit e.

The equivalence of the indicated relations is evident if we rewrite them in terms of ring addition and multiplication as

† See Huntington, these Transactions, vol. 5 (1904), pp. 288–309; or Stone, American Journal of Mathematics, vol. 57 (1935), pp. 703–732.

$ab = a, \quad a + b + ab = b, \quad ab + a = 0, \quad (a + e) + b + (ab + b) = e,$

respectively.

The chief properties of this relation are given in the following theorem:

THEOREM 5. *The relation* $<$ *of Definition* 2 *obeys the rules*

(1) $a<b$ *and* $b<c$ *imply* $a<c$;

(2) $0<a$ *for every* a, *and* $a<e$ *for every* a *when the Boolean ring* A *has a unit* e;

(3) $a<c$ *and* $b<d$ *imply* $ab<cd$, $a \vee b<c \vee d$;

(4) $bc=0$ *implies* $ac=0$ *if and only if* $a<b$.

The proof of (1) is obtained as follows: $ab=a$ and $bc=b$ together imply $ac=(ab)c=a(bc)=ab=a$. Property (2) results from the equations $0a=0$, $ae=a$. The proof of (3) follows from the relations, valid when $ac=a$ and $bd=d$,

$$\begin{aligned}(ab)(cd) &= (ac)(bd) = ab,\\ (a \vee b)(c \vee d) &= (a + b + ab)(c + d + cd)\\ &= ac + ad + acd + bc + bd + bcd + abc + abd + abcd\\ &= a + ad + ad + bc + b + bc + ab + ab + ab\\ &= a + b + ab = a \vee b.\end{aligned}$$

We verify (4) in two steps: first, if $a<b$, we see that $ab=a$ and $bc=0$ imply $ac=(ab)c=a(bc)=a0=0$; and, secondly, we see that, if $ac=0$ whenever $bc=0$, the fact that $b(a+ab)=ab+ab=0$ enables us to conclude that $a+ab=a(a+ab)=0$, $ab=a$, and $a<b$.

4. **Special elements.** We shall now turn to the study of certain special elements, other than the zero and unit elements, in Boolean rings, namely, those elements which may be briefly described as minimal non-zero elements. It should be observed that we do not assert the existence of such elements in general; we merely consider what occurs when they do exist. We first lay down some formal definitions.

DEFINITION 3. *A non-zero element* a *in a Boolean ring* A *is said to be an atomic element if it has either of the following equivalent properties*:

(1) $a>b$ *implies* $b=a$ *or* $b=0$;

(2) $ab=0$ *or* $ab=a$ *for every* b.

The equivalence of properties (1) and (2) is evident from the fact that $ab=b$ when $a>b$ and that $a>ab$ for every b.

DEFINITION 4. *A class* $\mathfrak{s}$ *of atomic elements is said to be an atomic basis if every non-zero element is the sum of elements in* $\mathfrak{s}$.

DEFINITION 5. *A class $\mathfrak{s}$ of atomic elements is said to be a complete atomic system if $b=0$ is the only element such that $ba=0$ for every a in $\mathfrak{s}$.*

We shall establish several simple theorems concerning systems of atomic elements.

THEOREM 6. *If a and b are atomic elements, then $a=b$ or $ab=0$.*

For $ab\neq 0$ implies both $ab=a$ and $ab=b$ in accordance with Definition 3.

THEOREM 7. *A complete atomic system in a Boolean ring A contains every atomic element in A.*

For an atomic element a, being different from 0, cannot satisfy the relation $ab=0$ for every b in the given system and must therefore be equal to some element b in that system, by virtue of Theorem 6.

THEOREM 8. *If A is a Boolean ring, $\mathfrak{s}$ a complete atomic system in A, and $\mathfrak{s}(b)$ the class of all atomic elements a in $\mathfrak{s}$ such that $ab\neq 0$, then A is isomorphic to the algebra $\mathfrak{R}$ of all classes $\mathfrak{s}(b)$ under the correspondence $b\longleftrightarrow\mathfrak{s}(b)$ in accordance with the properties*

(1) $\mathfrak{s}(b)=\mathfrak{s}(c)$ *if and only if* $b=c$;
(2) $\mathfrak{s}(b+c)=\mathfrak{s}(b)\Delta\mathfrak{s}(c)$;
(3) $\mathfrak{s}(bc)=\mathfrak{s}(b)\mathfrak{s}(c)$;
(4) $\mathfrak{s}(b\vee c)=\mathfrak{s}(b)\cup\mathfrak{s}(c)$.†

If $b=c$, then $ab=ac$ for every a in $\mathfrak{s}$, and hence $\mathfrak{s}(b)=\mathfrak{s}(c)$. On the other hand if $\mathfrak{s}(b)=\mathfrak{s}(c)$, then $ab=ac$ for every a in $\mathfrak{s}$ by virtue of Definition 3; hence $ab+ac=0$, $a(b+c)=0$, $b+c=0$, $b=c$, in accordance with Definition 5. In order that the element a in $\mathfrak{s}$ belong to $\mathfrak{s}(b+c)$ it is necessary and sufficient that $ab+ac=a(b+c)\neq 0$; since $ab+ac=0$ whenever $ab=ac$, we see that the relation $a(b+c)\neq 0$ holds if and only if one, but not both, of the pairs of relations $ab=a$, $ac=0$ and $ab=0$, $ac=a$ is valid; and we therefore conclude that property (2) holds. In similar fashion, we establish properties (3) and (4). We may also deduce (4) from (2) and (3), as follows:

$$\begin{aligned}\mathfrak{s}(b\vee c) &= \mathfrak{s}(b+c+bc) = \mathfrak{s}(b)\Delta\mathfrak{s}(c)\Delta\mathfrak{s}(bc)\\ &= \mathfrak{s}(b)\Delta\mathfrak{s}(c)\Delta\mathfrak{s}(b)\mathfrak{s}(c) = \mathfrak{s}(b)\cup\mathfrak{s}(c).\end{aligned}$$

THEOREM 9. *An atomic basis $\mathfrak{s}$ is a complete atomic system.*

We must show that there is no element b such that $b\neq 0$, $ba=0$ for every element a in $\mathfrak{s}$. Now, if there were, we should have $b=a_1+\cdots+a_n$ for some

† Here, as elsewhere in this paper, we use the symbols $\cup$ and Δ to designate union and union (modulo 2), or symmetric difference, for classes; and we indicate the formation of the intersection by juxtaposition of the symbols for the classes affected.

elements $a_1, \cdots, a_n$ in $\mathfrak{s}$, by Definition 4; we may suppose that these elements are distinct because of the law $a+a=0$. Thus we should obtain the relations $a_1=a_1(a_1+\cdots+a_n)=a_1b=0$ in accordance with Theorem 6 but in contradiction to the fact that $a_1\neq 0$.

THEOREM 10. *The representation of an element b as the sum of elements in a complete atomic system $\mathfrak{s}$ is unique: the summands are precisely the elements of the class $\mathfrak{s}(b)$, $b\neq 0$.*

If $b=a_1+\cdots+a_n$, the elements $a_1, \cdots, a_n$ in $\mathfrak{s}$ being taken as distinct, and if a is an arbitrary element in $\mathfrak{s}$, then $ab=aa_1+\cdots+aa_n$ is different from 0 if and only if one of the relations $a=a_1, \cdots, a=a_n$ is valid, as we see by virtue of Theorem 6. Hence $a_1, \cdots, a_n$ are precisely the elements of the class $\mathfrak{s}(b)$, $b\neq 0$, described in Theorem 8.

From Theorems 8, 9, and 10 we now obtain the following result:

THEOREM 11. *In order that a Boolean ring A contain an atomic basis $\mathfrak{s}$, it is necessary and sufficient that A be isomorphic to the algebra of all finite subclasses of a fixed finite or infinite class Σ, the elements in $\mathfrak{s}$ being in one-to-one correspondence with those of Σ. In particular such a ring A has a unit if and only if the classes $\mathfrak{s}$ and Σ are finite.*

When A has an atomic basis, the theorem follows at once from the preceding results, as we have already indicated. On the other hand, when A is isomorphic to an algebra of classes of the type described, it is evident that the elements of A corresponding to the one-element subclasses of Σ constitute an atomic basis in A. If a Boolean ring A containing an atomic basis $\mathfrak{s}$ has a unit e, then it is evident that $\mathfrak{s}=\mathfrak{s}(e)$ and hence that $\mathfrak{s}$ and the corresponding class Σ must both be finite. The converse result is also obvious.

THEOREM 12. *A finite Boolean ring with at least two elements contains an atomic basis $\mathfrak{s}$ and is therefore isomorphic to the algebra of all subclasses of a finite class Σ in one-to-one correspondence with $\mathfrak{s}$.*

In view of Theorem 11, it is sufficient for us to show that the given Boolean ring A has an atomic basis $\mathfrak{s}$. First we shall show that, if $a\neq 0$ is an arbitrary element in A, then there exists an atomic element contained in a. If a_1 is not an atomic element, there exists an element a such that $a_1a\neq 0$, $a_1a\neq a_1$. We denote a_1a by a_2 and observe that $a_1>a_2$. Let us suppose that there exist in A distinct non-zero elements $a_1, \cdots, a_k$ such that $a_1>a_2>\cdots>a_{k-1}>a_k$. If a_k is not an atomic element, then there exists an element a such that $a_ka\neq 0$, $a_ka\neq a_k$. We denote a_ka by a_{k+1} and observe that $a_k>a_{k+1}$. Thus we see, in view of the finiteness of A, that by virtue of this inductive construction there exist an integer n and elements $a_1, \cdots, a_n$,

where $a_1 > \cdots > a_n$ and a_n is an atomic element. We next designate by $\mathfrak{s}$ the class of all atomic elements in A and prove that $\mathfrak{s}$ is an atomic basis. Since $\mathfrak{s}$ is finite, its elements have a sum a. If b is an arbitrary element in A, we form the element $b+ab$ and apply the result just established: unless $b+ab=0$, there exists an atomic element c contained in $b+ab$. Now such an element c obviously has the properties $ac=c$, $(b+ab)c=c$; but these properties imply that $c=(b+ab)c=bc+bac=bc+bc=0$. We conclude therefore that $b+ab=0$ or, equivalently, $ab=b$. It follows that a is the unit e of the Boolean ring A and that any non-zero element b is expressible as the sum of atomic elements in $\mathfrak{s}$ through the equation $b=ab$. We have thereby shown that $\mathfrak{s}$ is an atomic basis.

We may observe that this theorem yields a new proof of the last part of Theorem 1, according to which every finite Boolean ring has a unit and has a cardinal number of the form 2^M. It shows further that when $M \geqq 1$ this integer is the number of elements in the atomic basis $\mathfrak{s}$.

In order to complete the consideration of finite Boolean rings, we state the following theorem without formal proof:

THEOREM 13. *A finite Boolean ring with exactly one element is isomorphic to the algebra consisting of the void class.*

CHAPTER II. SUBRINGS, IDEALS, AND HOMOMORPHISMS

1. **Subrings and their combinations.** A non-void subclass of an algebraic system is called a subsystem if it is closed under the fundamental operations of the system; that is, if the application of these operations to elements of the subclass yields elements of that class. The subsystems of a Boolean ring A are thus the subclasses of A which contain $a+b$ and ab whenever they contain a and b. The relation $a-b=a+b$, which is an immediate consequence of Theorem 1, therefore serves to identify the subsystems of A with the subrings of A.† Furthermore, the fact that the law of idempotence holds in any subclass of A shows that the subrings of A are Boolean rings in the sense of Definition 1. A few simple properties of the subrings of a Boolean ring A may be noted here without formal proof. Thus a subring $\mathfrak{a}$ has a unit a if and only if it contains an element a such that $ab=b$ or, equivalently, $a>b$ for every element b in $\mathfrak{a}$. Every subring contains the element 0 of A as its zero element. A subclass of a subring $\mathfrak{a}$ is a subring of A if and only if it is a subring of $\mathfrak{a}$. We may also cite the following examples of subrings: the subclass $\mathfrak{o}$ consisting of the element 0 alone; the subclass $\mathfrak{e}$ consisting of all the elements of A; and the subclass $\mathfrak{a}(a)$ consisting of all the elements b such that $ab=b$

† B. L. van der Waerden, *Moderne Algebra*, Berlin, 1930, vol. I, p. 53.

or, equivalently, $b<a$. We observe that $\mathfrak{o}=\mathfrak{a}(0)$; and that $\mathfrak{e}=\mathfrak{a}(e)$ in the case where A has a unit e.

Before passing to the study of combinations of subrings, we pause to consider briefly those non-void subclasses of a Boolean ring which are closed under the operations $\vee$ and $\cdot$ of Theorems 2–4. In view of the relation $a \vee b = a+b+ab$, every subring is such a subclass; but there exist subclasses with the indicated property which are not subrings, as is shown by the example of the subclass consisting of the element a alone, where $a \neq 0$, and by the example of the subclass consisting of the elements 0, a, b, ab, $a \vee b$, where a, b, and 0 are distinct (this subclass consists of three elements when $ab=a$ or when $ab=b$ and of five elements otherwise; Theorem 1 thus shows that it is not a subring). It is easily verified that these subclasses are instances of those algebraic systems variously known as C-lattices, distributive lattices, or arithmetic structures.† More than this is true: for recently MacNeille has proved that every distributive lattice is contained in a Boolean algebra (Boolean ring with unit) as a subclass of the indicated type by virtue of a strictly algebraic construction, of which the imbedding process given in the proof of Theorem 1 above is a special and very much simplified instance.‡

In any algebraic system, the intersection of any class of subsystems is itself a subsystem except, of course, in the case where it is void;§ the intersection is obviously the greatest subsystem contained in all subsystems of the given class. Hence any non-void subclass of an algebraic system generates a least subsystem containing it, namely, the intersection of all subsystems containing it. The subsystem thus generated by a given non-void subclass may be characterized alternatively as the class of all elements which can be constructed as "polynomials" in terms of the elements of the given subclass and of the fundamental operations of the system. It is understood in this statement that certain of the fundamental operations may, in a single application, affect infinitely many elements of the system. If $\mathfrak{A}$ is a non-void class of subsystems $\mathfrak{a}$, we may therefore define the sum and product of the subsystems in $\mathfrak{A}$ as follows: the sum, denoted by $S_{\mathfrak{a}\in\mathfrak{A}}\mathfrak{a}$, is the least subsystem containing every $\mathfrak{a}$ in $\mathfrak{A}$, or, equivalently, is the subsystem generated by the union

† The term C-lattice is used by Garrett Birkhoff, Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), pp. 441–464; distributive lattice by MacNeille, Harvard doctoral dissertation, *The Theory of Partially Ordered Sets*, 1935; arithmetic structure by Ore, Annals of Mathematics, (2), vol. 36 (1935), pp. 406–437.

‡ MacNeille, doctoral dissertation, *The Theory of Partially Ordered Sets*, 1935, not yet published. A summary is given in the Proceedings of the National Academy of Sciences, vol. 22 (1936), pp. 45–50.

§ For some purposes it is convenient to regard the void class as a subsystem, but that is not the case in the present paper.

$\Sigma_{\mathfrak{a}\in\mathfrak{A}}\mathfrak{a}$ of the classes $\mathfrak{a}$ belonging to $\mathfrak{A}$; and the product, denoted by $P_{\mathfrak{a}\in\mathfrak{A}}\mathfrak{a}$, is the intersection $\Pi_{\mathfrak{a}\in\mathfrak{A}}\mathfrak{a}$ of the classes $\mathfrak{a}$ in $\mathfrak{A}$, when it is not void. In the special case where $\mathfrak{A}$ consists of two subsystems $\mathfrak{a}$ and $\mathfrak{b}$, we write the sum as $\mathfrak{a}\vee\mathfrak{b}$ and the product as $\mathfrak{a}\cdot\mathfrak{b}$ or simply $\mathfrak{ab}$. In general, the product of subsystems may fail to exist; but in the case of Boolean rings this difficulty is removed by the fact that the element 0 is common to all subrings. It is important for us to examine the specialization of these general concepts to the case of Boolean rings.

In the first place we shall give more detailed information concerning the subring generated by a given subclass. We have

THEOREM 14. *In order that the subring* $\mathfrak{a}(\mathfrak{s})$ *generated by a non-void subclass* $\mathfrak{s}$ *of a Boolean ring A possess a unit, it is necessary and sufficient that* $\mathfrak{s}$ *contain elements* $a_1, \cdots, a_n$ *such that* $b<a_1\vee\cdots\vee a_n$ *for every element b in* $\mathfrak{s}$. *When this condition is satisfied, the element* $a=a_1\vee\cdots\vee a_n$ *is the unit of* $\mathfrak{a}(\mathfrak{s})$; *and* $\mathfrak{a}(\mathfrak{s})$ *is the class of all elements which can be constructed as polynomials in terms of elements b and* $a+b$, *where b is in* $\mathfrak{s}$, *and of the operations* $\vee$ *and* $\cdot$ *alone. In particular, if A has a unit e and* $\mathfrak{s}$ *contains e, then* $\mathfrak{a}(\mathfrak{s})$ *is the class of all elements which can be constructed as polynomials in terms of elements b and* $b'=b+e$, *where b is in* $\mathfrak{s}$, *and of the operations* $\vee$ *and* $\cdot$ *alone.*

The existence of elements $a_1, \cdots, a_n$ in $\mathfrak{s}$ such that $a_1\vee\cdots\vee a_n>b$ for every element b in $\mathfrak{s}$ leads immediately to the conclusion that $a=a_1\vee\cdots\vee a_n$ is in $\mathfrak{a}(\mathfrak{s})$ and is its unit: for, if c is any element of $\mathfrak{a}(\mathfrak{s})$, then $c=q(b_1, \cdots, b_m)$ where q is a polynomial in terms of elements $b_1, \cdots, b_m$ in $\mathfrak{s}$ and of the operations $+$ and $\cdot$ of the Boolean ring; and, by virtue of the distributive law and the law of idempotence, such an element c satisfies the relations $ac=aq(b_1, \cdots, b_m)=q(ab_1, \cdots, ab_m)=q(b_1, \cdots, b_m)=c$. On the other hand, if $\mathfrak{a}(\mathfrak{s})$ has a unit a, we can express a as a polynomial $r(a_1, \cdots, a_n)$, where $a_1, \cdots, a_n$ are in $\mathfrak{s}$, and have to show, in order to complete the discussion, that a can be expressed as $a_1\vee\cdots\vee a_n$. Since $a_1\vee\cdots\vee a_n$ is in $\mathfrak{a}(\mathfrak{s})$ and since a is the unit in $\mathfrak{a}(\mathfrak{s})$, we have $a_1\vee\cdots\vee a_n<a$. On applying the general relations $b\vee c>b+c$, $b>bc$, $c>bc$ to the polynomial $r(a_1, \cdots, a_n)$ we find that $a_1\vee\cdots\vee a_n>a$. Hence it is true that $a=a_1\vee\cdots\vee a_n$, as we wished to show. In a subring $\mathfrak{a}(\mathfrak{s})$ with unit a, we can apply the relations (1), (2), (6), and (7) of Theorem 2 with appropriate change of letters. Thus if $c=q(b_1, \cdots, b_m)$ where $b_1, \cdots, b_m$ are in $\mathfrak{s}$ we can use these relations to write $q(b_1, \cdots, b_m)=q^*(b_1, \cdots, b_m, b_1', \cdots, b_{m'}')$ where q^* is a polynomial in terms of the operations $\vee$ and $\cdot$ alone, and $b_k'=b_k+a$ for $k=1, \cdots, m$. The final assertions of the present theorem follow at once from this result.

Using the notations for sums and products of subrings introduced above

together with the customary symbol $\subset$ for the relation of class-inclusion, we now state the principle facts concerning the operations upon subsystems. While we phrase them in terms of Boolean rings, they are easily seen to be valid in quite arbitrary algebraic systems.

THEOREM 15. *If A is a Boolean ring, then the class $\mathfrak{A}$ of all subrings of A has the following properties under the operations of addition and multiplication introduced above*:

(1) $\mathfrak{a} \vee \mathfrak{b} = \mathfrak{b} \vee \mathfrak{a}$; (2) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$;

(3) $\mathfrak{a} \vee (\mathfrak{b} \vee \mathfrak{c}) = (\mathfrak{a} \vee \mathfrak{b}) \vee \mathfrak{c}$; (4) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$;

(5) $\mathfrak{a}(\mathfrak{b} \vee \mathfrak{c}) \supset \mathfrak{a}\mathfrak{b} \vee \mathfrak{a}\mathfrak{c}$; (6) $(\mathfrak{a} \vee \mathfrak{b})(\mathfrak{a} \vee \mathfrak{c}) \supset \mathfrak{a} \vee \mathfrak{b}\mathfrak{c}$;

(7) $\mathfrak{a} \vee \mathfrak{a} = \mathfrak{a}$; (8) $\mathfrak{a}\mathfrak{a} = \mathfrak{a}$;

(9) $\mathfrak{a} \subset \mathfrak{b}$ *if and only if* $\mathfrak{a}\mathfrak{b} = \mathfrak{a}$;

(10) *if $\mathfrak{B}$ is a non-void class of non-void classes $\mathfrak{B}$ of subrings $\mathfrak{a}$ of A, and if $\mathfrak{C}$ is the union $\Sigma\mathfrak{B}_{\mathfrak{B}\in\mathfrak{B}}$, then*

$$\sum_{\mathfrak{B}\in\mathfrak{B}} \left(\sum_{\mathfrak{a}\in\mathfrak{B}} \mathfrak{a}\right) = \sum_{\mathfrak{a}\in\mathfrak{C}} \mathfrak{a};$$

(11) *if $\mathfrak{B}$, $\mathfrak{B}$, and $\mathfrak{C}$ have the same significance as in* (10), *then*

$$\prod_{\mathfrak{B}\in\mathfrak{B}} \left(\prod_{\mathfrak{a}\in\mathfrak{B}} \mathfrak{a}\right) = \prod_{\mathfrak{a}\in\mathfrak{C}} \mathfrak{a};$$

(12) *if $\mathfrak{b}$ is any subring of A and $\mathfrak{B}$ is any non-void class of subrings $\mathfrak{a}$ of A, then*

$$\mathfrak{b}\left(\sum_{\mathfrak{a}\in\mathfrak{B}} \mathfrak{a}\right) \supset \sum_{\mathfrak{a}\in\mathfrak{B}} (\mathfrak{b}\mathfrak{a});$$

(13) *if $\mathfrak{b}$ and $\mathfrak{B}$ have the same significance as in* (12), *then*

$$\prod_{\mathfrak{a}\in\mathfrak{B}} (\mathfrak{b} \vee \mathfrak{a}) \supset \mathfrak{b} \vee \prod_{\mathfrak{a}\in\mathfrak{B}} \mathfrak{a}.$$

The special subrings $\mathfrak{o}$ and $\mathfrak{e}$ have the following properties:

(14) $\mathfrak{o}\mathfrak{a} = \mathfrak{o}, \quad \mathfrak{a} \vee \mathfrak{o} = \mathfrak{a}$;

(15) $\mathfrak{e}\mathfrak{a} = \mathfrak{a}, \quad \mathfrak{a} \vee \mathfrak{e} = \mathfrak{e}$.

Except for properties (5), (6), (12), and (13), all these properties are easily verified by quite trivial arguments; and properties (5) and (6) are special cases of (12) and (13) respectively. We shall therefore confine our discussion to the two latter properties. To establish (12) we proceed as follows: an element belongs to the subring on the right of (12) if and only if it is a polynomial in terms of elements simultaneously in the subring $\mathfrak{b}$ and in the sub-

rings $\mathfrak{a}$; on the other hand, an element belongs to the subring on the left of (12) if and only if it is simultaneously a polynomial in terms of elements in $\mathfrak{b}$ and a polynomial in terms of elements in the subrings $\mathfrak{a}$; from these algebraic descriptions, the inclusion-relation (12) is evident. We prove (13) in a similar manner: an element belongs to the subring on the right of (13) if and only if it is a polynomial in terms of elements in the subring $\mathfrak{b}$ and common to all the subrings $\mathfrak{a}$; and an element belongs to the subring on the left of (13) if and only if it is, simultaneously for all subrings $\mathfrak{a}$, a polynomial in terms of elements of the subring $\mathfrak{b}$ and of a subring $\mathfrak{a}$. It is of interest to show that the relations (5) and (6), and hence also the relations (12) and (13), cannot be strengthened. In a Boolean ring with unit and with four or more elements, let a be an element distinct from 0 and from e; let $\mathfrak{a}$ be the subring consisting of the elements 0, a; let $\mathfrak{b}$ be the subring consisting of the elements 0, e; let $\mathfrak{c}$ be the subring consisting of the elements 0, a', where $a'=a+e$; and let $\mathfrak{d}$ be the subring consisting of the elements 0, a, a', e. We then see that $\mathfrak{a}(\mathfrak{b}\vee\mathfrak{c})=\mathfrak{a}$, $\mathfrak{a}\mathfrak{b}\vee\mathfrak{a}\mathfrak{c}=\mathfrak{o}$, $(\mathfrak{a}\vee\mathfrak{b})(\mathfrak{a}\vee\mathfrak{c})=\mathfrak{b}$, $\mathfrak{a}\vee\mathfrak{b}\mathfrak{c}=\mathfrak{a}$, $\mathfrak{o}\neq\mathfrak{a}\neq\mathfrak{b}$.

2. **Ideals and their combinations.** We shall now turn to the study of those special subrings known as invariant subrings or ideals, characterized by the property of containing a and ab together whatever the element b. Thus a non-void subclass of a Boolean ring is an ideal if and only if it contains $a+b$ together with a and b, and c together with a whenever $c<a$. Since ideals are special subrings, the discussion of the preceding section applies to them at once; but, as we shall see below, is capable of being made considerably more precise by virtue of the restriction to ideals. We shall note a few simple properties of ideals without formal proof. Thus, an ideal $\mathfrak{a}$ in a Boolean ring A has a unit a if and only if it consists of all elements c such that $c<a$; in other words, if and only if it is identical with the subring $\mathfrak{a}(a)$ introduced above and seen now to be an ideal. Moreover an ideal $\mathfrak{a}$ which contains the element a necessarily contains the ideal $\mathfrak{a}(a)$. A subclass $\mathfrak{b}$ of an ideal $\mathfrak{a}$ in a Boolean ring A is an ideal in $\mathfrak{a}$, regarded as a Boolean ring, if and only if it is an ideal in A. If $\mathfrak{a}$ is an ideal and $\mathfrak{b}$ a subring, then $\mathfrak{a}$ is an ideal in the subring $\mathfrak{a}\vee\mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ is an ideal in the subring $\mathfrak{b}$. The subrings $\mathfrak{o}$, $\mathfrak{a}(a)$, $\mathfrak{e}$, previously introduced, are all ideals. It is important for us to recall the arithmetical terminology used to describe the inclusion relation $\mathfrak{a}\subset\mathfrak{b}$ between ideals: if $\mathfrak{a}$ is contained in $\mathfrak{b}$, then $\mathfrak{b}$ is said to divide $\mathfrak{a}$ or to be a divisor of $\mathfrak{a}$, and $\mathfrak{a}$ is said to be divisible by $\mathfrak{b}$. Thus the product $\mathfrak{a}\mathfrak{b}$ of ideals $\mathfrak{a}$ and $\mathfrak{b}$ is divisible by its factors $\mathfrak{a}$ and $\mathfrak{b}$, the product being itself an ideal in accordance with a result established below.

The distinction which it was necessary to draw between subsystems of a Boolean ring defined in terms of the operations $+$ and $\cdot$ and those defined in

terms of $\vee$ and $\cdot$ vanishes in the case of multiplicatively invariant subsystems, as indicated in the following theorem:

THEOREM 16. *In order that a non-void subclass* $\mathfrak{a}$ *of a Boolean ring* A *be an ideal it is necessary and sufficient that*

(1) $\mathfrak{a}$ *contain* $a \vee b$ *together with* a *and* b,

(2) $\mathfrak{a}$ *contain* ab *whenever it contains* a;

or, equivalently, that

(1) $\mathfrak{a}$ *contain* $a \vee b$ *together with* a *and* b,

(2′) $\mathfrak{a}$ *contain* c *together with* a *whenever* $c < a$.

Since the conditions (2) and (2′) are equivalent, we need consider only conditions (1) and (2). The necessity of the latter conditions is evident. To establish their sufficiency, it is enough to show that they imply that $\mathfrak{a}$ contains $a+b$ together with a and b. Now if a and b are in $\mathfrak{a}$, so are $a \vee b$ and $(a \vee b)(a+b)$ by virtue of (1) and (2); but the relation

$$(a \vee b)(a + b) = [(a + b) + ab](a + b) = (a + b) + (ab + ab) = a + b$$

shows that $a+b$ is also in $\mathfrak{a}$, as we wished to prove.

Before considering the specialization of Theorem 15 to the case of ideals, it is necessary for us to indicate some particular results analogous to those presented in Theorem 14.

THEOREM 17. *If* $\mathfrak{s}$ *is an arbitrary non-void subclass of a Boolean ring* A *and if* $\mathfrak{a}(\mathfrak{s})$ *is the class of all elements* a *such that* $a < a_1 \vee \cdots \vee a_n$ *for appropriate elements* $a_1, \cdots, a_n$ *in* $\mathfrak{s}$, *then* $\mathfrak{a}(\mathfrak{s})$ *is an ideal; and every ideal containing* $\mathfrak{s}$ *contains* $\mathfrak{a}(\mathfrak{s})$. *The ideal* $\mathfrak{a}(\mathfrak{s})$ *may be characterized alternatively as the class of all elements* a *such that* $a = a_1b_1 \vee \cdots \vee a_nb_n$ *where* $a_1, \cdots, a_n$ *are in* $\mathfrak{s}$ *and* $b_1, \cdots, b_n$ *are in* A. *If* $\mathfrak{s}$ *is the union of the ideals* $\mathfrak{a}$ *in a given class* $\mathfrak{B}$, *then* $\mathfrak{a}(\mathfrak{s})$ *is the class of all elements* a *such that* $a = a_1 \vee \cdots \vee a_n$ *where* a_k *is in* $\mathfrak{a}_k$ *and* $\mathfrak{a}_k$ *in* $\mathfrak{B}$ *for* $k = 1, \cdots, n$.

From Theorem 16, it is evident that an ideal containing the class $\mathfrak{s}$ must contain every element $a_1 \vee \cdots \vee a_n$ where $a_1, \cdots, a_n$ are in $\mathfrak{s}$, and hence every element a such that $a < a_1 \vee \cdots \vee a_n$. Thus $\mathfrak{a}(\mathfrak{s})$ is contained in every ideal which contains $\mathfrak{s}$. To show that $\mathfrak{a}(\mathfrak{s})$ is itself an ideal, we appeal again to Theorem 16. It is evident that condition (2′) of that theorem is satisfied in the present instance. It is easily verified that condition (1) also holds: for, if $a < a_1 \vee \cdots \vee a_n$ and $b < b_1 \vee \cdots \vee b_p$ where $a_1, \cdots, a_n, b_1, \cdots, b_p$ are in $\mathfrak{s}$, then $a \vee b < a_1 \vee \cdots \vee a_n \vee b_1 \vee \cdots \vee b_p$. The equivalent characterization of $\mathfrak{a}(\mathfrak{s})$ is established as follows: if $a < a_1 \vee \cdots \vee a_n$, then $a = a_1b_1 \vee \cdots \vee a_nb_n$ with $b_1 = \cdots = b_n = a$; and, if $a = a_1b_1 \vee \cdots \vee a_nb_n$, then $a < a_1 \vee \cdots \vee a_n$. Finally, to establish the characterization of $\mathfrak{a}(\mathfrak{s})$ when $\mathfrak{s}$ is the union of ideals $\mathfrak{a}$,

we first express the element a in $\mathfrak{a}(\mathfrak{s})$ in the form $a = a_1 b_1 \vee \cdots \vee a_n b_n$ where $a_1, \cdots, a_n$ are in $\mathfrak{s}$. We then observe that there must exist ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ of the given class $\mathfrak{B}$ which contain $a_1, \cdots, a_n$ respectively. It follows that $a_k b_k$ is an element of the ideal $\mathfrak{a}_k$. Thus an obvious change of notation permits us to write $a = a_1 \vee \cdots \vee a_n$ where a_k is in $\mathfrak{a}_k$ and $\mathfrak{a}_k$ in $\mathfrak{B}$, for $k = 1, \cdots, n$. Conversely, every such element is in the ideal $\mathfrak{a}(\mathfrak{s})$, as we have already seen.

With the help of Theorem 17, we can now obtain the desired counterpart of Theorem 15.

THEOREM 18. *In a Boolean ring A, the subrings obtained as sums or as products of ideals are themselves ideals; in other words, the class $\mathfrak{J}$ of all ideals in A is a subsystem of the system $\mathfrak{A}$ of all subrings of A under the unrestricted operations of addition and multiplication. The properties of these operations which hold in $\mathfrak{A}$ hold also in $\mathfrak{J}$, with the refinement that properties* (5), (6), *and* (12) *of Theorem* 15 *are to be replaced respectively by the following sharper properties, to which we give the corresponding numbers*:

(5) $\mathfrak{a}(\mathfrak{b} \vee \mathfrak{c}) = \mathfrak{a}\mathfrak{b} \vee \mathfrak{a}\mathfrak{c}$; (6) $(\mathfrak{a} \vee \mathfrak{b})(\mathfrak{a} \vee \mathfrak{c}) = \mathfrak{a} \vee \mathfrak{b}\mathfrak{c}$;

(12) *if $\mathfrak{b}$ is an ideal and $\mathfrak{B}$ a non-void class of ideals $\mathfrak{a}$, then*

$$\mathfrak{b} \sum_{\mathfrak{a} \in \mathfrak{B}} \mathfrak{a} = \sum_{\mathfrak{a} \in \mathfrak{B}} \mathfrak{b}\mathfrak{a}.$$

The ideal $\mathfrak{a}\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, is the class of elements c where $c = ab$, a in $\mathfrak{a}$ and b in $\mathfrak{b}$. The ideal $\mathfrak{a}(\mathfrak{s})$ of Theorem 17 *is the product of all ideals containing $\mathfrak{s}$; and, in the particular case where $\mathfrak{s}$ is the union of a class of ideals, $\mathfrak{a}(\mathfrak{s})$ is the sum of the ideals in that class.*

If a is any element in the intersection of ideals $\mathfrak{a}$, then ab is also in their intersection whatever the element b. Thus the subring which is the product of the ideals $\mathfrak{a}$ is an ideal. In particular the product $\mathfrak{a}\mathfrak{b}$ of ideals $\mathfrak{a}$ and $\mathfrak{b}$ is an ideal and consists of those elements c such that $c = ab$ where a is in $\mathfrak{a}$ and b in $\mathfrak{b}$: for any such element is common to $\mathfrak{a}$ and $\mathfrak{b}$; and, if c is common to $\mathfrak{a}$ and $\mathfrak{b}$, then $c = ab$ where $a = c$ and $b = c$. Theorem 17 now shows that the ideal $\mathfrak{a}(\mathfrak{s})$ is the product, or, equivalently, the intersection, of all the ideals containing $\mathfrak{s}$, the ideals $\mathfrak{e}$ and $\mathfrak{a}(\mathfrak{s})$ both having the latter property. Now, if $\mathfrak{s}$ is the union of ideals $\mathfrak{a}$, we see from Theorem 17 that $\mathfrak{a}(\mathfrak{s})$ is contained in the subring which is the sum of the ideals $\mathfrak{a}$; but, since $\mathfrak{a}(\mathfrak{s})$ is a subring containing $\mathfrak{s}$, it must contain also the sum in question. It follows that any sum of ideals is identical with the ideal $\mathfrak{a}(\mathfrak{s})$, where $\mathfrak{s}$ is the union of those ideals. The preceding results evidently serve to establish the assertion that $\mathfrak{J}$ is a subsystem of $\mathfrak{A}$. It remains for us to establish the sharper forms of (5), (6), and (12). Since (12) implies (5), we confine our discussion to (6) and (12). In view of Theorem 15,

it is sufficient for us to show that $\mathfrak{b}S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a} \subset S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{b}\mathfrak{a}$, $(\mathfrak{a}\vee\mathfrak{b})(\mathfrak{a}\vee\mathfrak{c}) \subset \mathfrak{a}\vee\mathfrak{b}\mathfrak{c}$. Using the results of Theorem 17 together with those just proved, we see that every element in $\mathfrak{b}S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$ is expressible in the form $b(a_1\vee\cdots\vee a_n)=ba_1\vee\cdots\vee ba_n$ where b is in $\mathfrak{b}$ and a_k in an ideal $\mathfrak{a}_k$ of the class $\mathfrak{B}$. Since ba_k is in the ideal $\mathfrak{b}\mathfrak{a}_k$, we conclude that every element of the indicated form is in the ideal $S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{b}\mathfrak{a}$, thus establishing (12). Similarly, we see that every element in $(\mathfrak{a}\vee\mathfrak{b})(\mathfrak{a}\vee\mathfrak{c})$ can be expressed in the form $(a_1\vee b)(a_2\vee c)$ where a_1 and a_2 are in $\mathfrak{a}$, b is in $\mathfrak{b}$, and c is in $\mathfrak{c}$; and, since $(a_1\vee b)(a_2\vee c)=(a_1a_2\vee a_1c\vee a_2b)\vee bc$ where $a_1a_2\vee a_1c\vee a_2b$ is in $\mathfrak{a}$ and bc is in $\mathfrak{b}\mathfrak{c}$, we see that every such element is in $\mathfrak{a}\vee\mathfrak{b}\mathfrak{c}$, thus establishing (6).

It is of interest to remark that property (13) of Theorem 15 cannot be similarly sharpened. This we shall show by examples to be given in a later paper. It is also of interest to remark that in the case of a general abstract ring the properties (5), (6), and (12) of Theorem 15 cannot be replaced by the sharper ones which have just been established in the case of Boolean rings. We note that under the finite operations, namely, the operations of forming the finite sum $\mathfrak{a}\vee\mathfrak{b}$ and the finite product $\mathfrak{a}\mathfrak{b}$, the system $\mathfrak{J}$ is a distributive lattice by virtue of the sharpened properties (5) and (6). The Boolean rings are thus special instances of those rings in which the ideals constitute a distributive lattice.†

We shall now introduce in the class $\mathfrak{J}$ of ideals a unary operation in many respects analogous to the operation $'$ defined in a Boolean ring with unit. Such an operation can be defined in any commutative ring and can be suitably generalized even in the case of a non-commutative ring. We shall investigate its properties only in the case immediately before us. It will be helpful to make use of the following terminology:

DEFINITION 6. *Two elements a and b in a Boolean ring are said to be orthogonal if $ab=0$; and two non-void subclasses of a Boolean ring are said to be orthogonal if every element of one is orthogonal to every element of the other.*

As a basis for our definition of the desired operation, we first establish the following result:

THEOREM 19. *If $\mathfrak{s}$ is any non-void subclass of a Boolean ring A, then the class $\mathfrak{s}'$ of all elements orthogonal to every element of $\mathfrak{s}$ is an ideal in A which is orthogonal to $\mathfrak{s}$ and contains every subclass of A orthogonal to $\mathfrak{s}$. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are orthogonal if and only if $\mathfrak{a}\mathfrak{b}=\mathfrak{o}$.*

It is obvious that $\mathfrak{s}'$ contains the element 0, that it is orthogonal to $\mathfrak{s}$, and that it contains every subclass of A orthogonal to $\mathfrak{s}$. If a and b are in $\mathfrak{s}'$,

† The indicated class of rings has been discussed by Garrett Birkhoff, under certain strong restrictions, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 613–619.

then $a+b$ is in $\mathfrak{s}'$: for we have $(a+b)c=ac+bc=0+0=0$ for every element c in $\mathfrak{s}$. Similarly, if a is in $\mathfrak{s}'$ and b is in A, then ab is in $\mathfrak{s}'$: for we have $(ab)c=(ac)b=0b=0$ for every element c in $\mathfrak{s}$. We see therefore that $\mathfrak{s}'$ is an ideal. The characterization of the ideal product $\mathfrak{ab}$ given in Theorem 18 shows at once that $\mathfrak{a}$ and $\mathfrak{b}$ are orthogonal if and only if $\mathfrak{ab}=\mathfrak{o}$.

We can now state our fundamental definition.

DEFINITION 7. *The ideal $\mathfrak{s}'$ associated with an arbitrary non-void subclass $\mathfrak{s}$ of a Boolean ring A in the manner indicated in Theorem* 19 *is called the orthogonal complement, or, more briefly, the orthocomplement of $\mathfrak{s}$; and the operation of forming the ideal $\mathfrak{s}'$ is called orthogonal complementation, or, more briefly, orthocomplementation. The orthocomplement of $\mathfrak{s}'$ is denoted by $\mathfrak{s}''$, that of $\mathfrak{s}''$ by $\mathfrak{s}'''$; and, more generally, the symbol $\mathfrak{s}^{(n)}$ is defined recursively for $n\geqq 1$ by the relations $\mathfrak{s}^{(1)}=\mathfrak{s}'$, $\mathfrak{s}^{(n+1)}=(\mathfrak{s}^{(n)})'$.*

The chief properties of the operation so defined are given in the three theorems which follow.

THEOREM 20. *The operation of orthocomplementation has the following general properties*:

(1) $\mathfrak{s}\subset\mathfrak{t}$ *implies* $\mathfrak{s}'\supset\mathfrak{t}'$;

(2) $\mathfrak{s}\subset\mathfrak{a}(\mathfrak{s})\subset\mathfrak{s}''$, *where* $\mathfrak{a}(\mathfrak{s})$ *is the ideal generated by* $\mathfrak{s}$;

(3) $\mathfrak{s}^{(m)}=\mathfrak{s}^{(n)}$ *when* m *and* n *are congruent* (mod 2), $\mathfrak{s}^{(m)}\mathfrak{s}^{(n)}=\mathfrak{o}$ *when* m *and* n *are not congruent* (mod 2); *in particular*, $\mathfrak{s}'''=\mathfrak{s}'$.

If $\mathfrak{s}$ is contained in $\mathfrak{t}$, then $\mathfrak{t}'$ is orthogonal to $\mathfrak{s}$ as well as to $\mathfrak{t}$ and must therefore be contained in $\mathfrak{s}'$ in accordance with Theorem 19. Since $\mathfrak{s}$ is orthogonal to $\mathfrak{s}'$ by definition, $\mathfrak{s}$ is contained in the ideal $\mathfrak{s}''$; and by Theorem 17 we have $\mathfrak{s}\subset\mathfrak{a}(\mathfrak{s})\subset\mathfrak{s}''$. The relation $\mathfrak{s}\subset\mathfrak{s}''$ implies $\mathfrak{s}'\supset\mathfrak{s}'''$; but we also have $\mathfrak{s}'''=(\mathfrak{s}')''\supset\mathfrak{s}'$ and therefore conclude that $\mathfrak{s}'''=\mathfrak{s}'$. By an obvious induction we now see that $\mathfrak{s}^{(n+2)}=\mathfrak{s}^{(n)}$, $\mathfrak{s}^{(n+1)}\mathfrak{s}^{(n)}=\mathfrak{o}$. A further induction leads to the general proposition (3).

THEOREM 21. *Within the class $\mathfrak{Z}$ of all ideals in a Boolean ring A, the operation of orthocomplementation has the following special properties*:

(1) $\mathfrak{a}\subset\mathfrak{a}''$; (2) $\mathfrak{a}\mathfrak{a}'=\mathfrak{o}$; (3) $\mathfrak{o}'=\mathfrak{e}$, $\mathfrak{e}'=\mathfrak{o}$;

(4) *the orthocomplement of a sum is equal to the product of the orthocomplements of the summands; in particular*, $(\mathfrak{a}\vee\mathfrak{b})'=\mathfrak{a}'\mathfrak{b}'$;

(5) *the orthocomplement of a product contains the sum of the orthocomplements of the multiplicands; in particular*, $(\mathfrak{ab})'\supset\mathfrak{a}'\vee\mathfrak{b}'$.

The properties (1), (2), (3) follow at once from Theorems 19 and 20. To prove (4), we observed that, by virtue of Theorems 17 and 18, an element b is in $(S_{\alpha\in\mathfrak{B}}\mathfrak{a})'$ if and only if $b(a_1\vee\cdots\vee a_n)=0$ for every set of elements

$a_1, \cdots, a_n$ belonging respectively to ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ in the class $\mathfrak{B}$. Now $b(a_1 \vee \cdots \vee a_n) = ba_1 \vee \cdots \vee ba_n = 0$ if and only if $ba_1 = \cdots = ba_n = 0$, as is easily verified. The latter condition obviously holds for the indicated elements $a_1, \cdots, a_n$ if and only if b is in every ideal $\mathfrak{a}'$, where $\mathfrak{a}$ is in the class $\mathfrak{B}$. This result serves to establish (4). To prove (5), we observe that by virtue of Theorems 17 and 18 an element b in $S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}'$ is expressible in the form $b = a_1 \vee \cdots \vee a_n$ where a_k is in $\mathfrak{a}_k'$ and $\mathfrak{a}_k$ in $\mathfrak{B}$ for $k = 1, \cdots, n$; hence we see that, if c is an arbitrary element in the product of the ideals $\mathfrak{a}$, then $bc = (a_1 \vee \cdots \vee a_n)c = a_1c \vee \cdots \vee a_nc = 0$; and we conclude that b is in $(P_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a})'$, thus establishing (5).

The properties (1) and (5) of this theorem cannot be sharpened within the class $\mathfrak{F}$, save in the case of Boolean rings of very special type. We shall give relevant examples in another paper.

Since the product $\mathfrak{ab}$ of an ideal $\mathfrak{a}$ and a subring $\mathfrak{b}$ is an ideal in $\mathfrak{b}$, we may seek to determine the orthocomplement of $\mathfrak{ab}$ relative to $\mathfrak{b}$. This determination is possible when $\mathfrak{b}$ is an ideal, and proves to be important in subsequent developments.

THEOREM 22. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in a Boolean ring* A, *the orthocomplement* $\mathfrak{c}$ *of the ideal* $\mathfrak{ab}$ *in the subring* $\mathfrak{b}$ *satisfies the relation* $\mathfrak{c} = \mathfrak{a}'\mathfrak{b}$.

Since $\mathfrak{ab}$ and $\mathfrak{a}'\mathfrak{b}$ are ideals in $\mathfrak{b}$ such that $(\mathfrak{ab})(\mathfrak{a}'\mathfrak{b}) = (\mathfrak{aa}')\mathfrak{b} = \mathfrak{o}$, we see from Theorem 19 that $\mathfrak{c} \supset \mathfrak{a}'\mathfrak{b}$. On the other hand, we obviously have $\mathfrak{c} \subset \mathfrak{b}$, we can prove that $\mathfrak{c} \subset \mathfrak{a}'$, and we can therefore conclude that $\mathfrak{c} \subset \mathfrak{a}'\mathfrak{b}$ and hence $\mathfrak{c} = \mathfrak{a}'\mathfrak{b}$: for, if c is any element in $\mathfrak{c}$, the element ac is in $\mathfrak{ab}$ for every element a in $\mathfrak{a}$ and thus has the property $ac = (ac)c = 0$; but this property implies the relation $\mathfrak{c} \subset \mathfrak{a}'$.

In case $\mathfrak{b}$ is a subring but not an ideal, the relation $\mathfrak{c} \supset \mathfrak{a}'\mathfrak{b}$ is valid but cannot in general be replaced by the stronger relation $\mathfrak{c} = \mathfrak{a}'\mathfrak{b}$. To show this, we use the fact that in general the ideal $\mathfrak{a}$ can be chosen so that $\mathfrak{a} \vee \mathfrak{a}' \neq \mathfrak{e}$. If we then take b as an element not in $\mathfrak{a} \vee \mathfrak{a}'$ and let $\mathfrak{b}$ be the subring consisting of the elements 0, b, we see that $\mathfrak{ab} = \mathfrak{a}'\mathfrak{b} = \mathfrak{o}$, $\mathfrak{c} = \mathfrak{b} \neq \mathfrak{o}$.

3. **A classification of ideals.** The operation of orthocomplementation introduced at the end of the preceding section leads to an important classification of the ideals in a Boolean ring. While an exhaustive study of this classification would take us too far afield, some detailed knowledge of the behavior of ideals under the operation of orthocomplementation is essential in Chapter III. We shall therefore give only a partial investigation of this subject here, leaving for another paper the presentation of the complete theory. It is proper to point out in advance that the proposed classification degenerates only in a few very special types of Boolean ring, too simple to be of very great

interest in any other connection. We shall accordingly have no need to concern ourselves in the present section with the possibility of degeneracies. Our fundamental definition is the following:

DEFINITION 8. *In a Boolean ring A, an ideal $\mathfrak{a}$ is said to be*

(1) *principal if $\mathfrak{a}=\mathfrak{a}(a)$ for some element a;*

(2) *semiprincipal if $\mathfrak{a}=\mathfrak{a}(a)$ or $\mathfrak{a}=\mathfrak{a}'(a)$ for some element a;*

(3) *simple if $\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$;* (4) *normal if $\mathfrak{a}=\mathfrak{a}''$.*

The classes of principal, semiprincipal, simple, and normal ideals are denoted by the letters $\mathfrak{P}$, $\mathfrak{P}^*$, $\mathfrak{S}$, and $\mathfrak{N}$ respectively.

We may observe that the term "principal ideal" is here used with its ordinary significance: for Theorem 17 shows that the ideal $\mathfrak{a}(a)$ is the ideal generated by the class $\mathfrak{s}$ consisting of the element a alone.

The elementary relations between the classes of ideals thus introduced are given in the three following theorems.

THEOREM 23. *The classes defined in Definition* 8 *satisfy the following inclusion relations*:

(1) $\qquad \mathfrak{P}\subset\mathfrak{P}^*\subset\mathfrak{S}\subset\mathfrak{N}\subset\mathfrak{J}$;

(2) $\mathfrak{P}$ *contains* $\mathfrak{o}$; (3) $\mathfrak{P}^*$ *contains* $\mathfrak{e}$.

The relations (2) and (3) are obvious. Of the inclusions in (1), the first and last are obvious. Hence we need discuss in detail only the relations $\mathfrak{P}^*\subset\mathfrak{S}$, $\mathfrak{S}\subset\mathfrak{N}$. Now if the ideal $\mathfrak{a}$ is semiprincipal, we have either $\mathfrak{a}=\mathfrak{a}(a)$ or $\mathfrak{a}=\mathfrak{a}'(a)$ for some element a. In the first case, we let b be an arbitrary element in A and write $b=ab+(b+ab)$. Since ab is in $\mathfrak{a}$, a proof that $b+ab$ is in $\mathfrak{a}'$ will lead to the result that b is in $\mathfrak{a}\vee\mathfrak{a}'$. If c is an arbitrary element in $\mathfrak{a}=\mathfrak{a}(a)$, we have $c(b+ab)=cb+(ca)b=cb+cb=0$ and thus conclude that $b+ab$ is in $\mathfrak{a}'$. Since b is arbitrary, we must have $\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$, so that $\mathfrak{a}$ is a simple ideal. In the second case we apply the result just obtained to write $\mathfrak{e}=\mathfrak{a}(a)\vee\mathfrak{a}'(a)\subset\mathfrak{a}''(a)\vee\mathfrak{a}'(a)=\mathfrak{a}'\vee\mathfrak{a}=\mathfrak{a}\vee\mathfrak{a}'$. It is then evident that $\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$ and that $\mathfrak{a}$ is simple. The proof of the relation $\mathfrak{P}^*\subset\mathfrak{S}$ is thus completed. If now $\mathfrak{a}$ is a simple ideal, we have $\mathfrak{a}''=\mathfrak{a}''\mathfrak{e}=\mathfrak{a}''(\mathfrak{a}\vee\mathfrak{a}')=\mathfrak{a}''\mathfrak{a}\vee\mathfrak{a}''\mathfrak{a}'=\mathfrak{a}\vee\mathfrak{o}=\mathfrak{a}$ in accordance with Theorems 18 and 21; and we conclude that $\mathfrak{a}$ is normal. The relation $\mathfrak{S}\subset\mathfrak{N}$ is thus established.

THEOREM 24. *The relation $\mathfrak{J}\neq\mathfrak{S}$ implies the relation $\mathfrak{J}\neq\mathfrak{N}$; in particular, if the ideal $\mathfrak{a}$ is not simple, the ideal $\mathfrak{a}\vee\mathfrak{a}'$ is not normal. In consequence, the relation $\mathfrak{J}=\mathfrak{N}$ implies the relation $\mathfrak{J}=\mathfrak{S}$.*

Since $(\mathfrak{a}\vee\mathfrak{a}')'=\mathfrak{a}'\mathfrak{a}''=\mathfrak{o}$ by Theorem 21, and since therefore $(\mathfrak{a}\vee\mathfrak{a}')''=\mathfrak{e}$, we see that $\mathfrak{a}\vee\mathfrak{a}'\neq\mathfrak{e}$ implies $\mathfrak{a}\vee\mathfrak{a}'\neq(\mathfrak{a}\vee\mathfrak{a}')''$.

THEOREM 25. *The relation* $\mathfrak{P}=\mathfrak{P}^*$ *implies the relation* $\mathfrak{P}=\mathfrak{S}$ *and hence also the relation* $\mathfrak{P}^*=\mathfrak{S}$. *In fact, the following assertions concerning a Boolean ring A are equivalent*:

(1) $\mathfrak{P}=\mathfrak{S}$; (2) $\mathfrak{P}=\mathfrak{P}^*$;

(3) *there exists an ideal* $\mathfrak{a}$ *such that* $\mathfrak{a}$ *and* $\mathfrak{a}'$ *are in* $\mathfrak{P}$;

(4) *the Boolean ring A has a unit e.*

It is evident that (1) implies (2), and also that (2) implies (3). We show that (3) implies (4). If $\mathfrak{a}=\mathfrak{a}(a)$ and $\mathfrak{a}'=\mathfrak{a}(b)$, then $\mathfrak{a}(a)\vee\mathfrak{a}(b)=\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$ in accordance with the relation $\mathfrak{P}\equiv\mathfrak{S}$. Hence an arbitrary element c is expressible in the form $c=a_1\vee b_1$ where $a_1<a$ and $b_1<b$, as we see by reference to Theorem 17. It follows that $c<a\vee b$. Since c is arbitrary, this relation identifies $a\vee b$ as the unit in A. We now complete the proof by showing that (4) implies (1). If $\mathfrak{a}$ is a simple ideal in a Boolean ring with unit e, the relation $\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$ shows that $e=a\vee b$ where a is in $\mathfrak{a}$ and b in $\mathfrak{b}$, in accordance with Theorem 17. If c is an arbitrary element in $\mathfrak{a}$, we obviously have $cb=0$ and hence $c=ce=c(a\vee b)=ca\vee cb=ca$, or, equivalently, $c<a$. Thus we see that $\mathfrak{a}\subset\mathfrak{a}(a)$. On the other hand it is evident that $\mathfrak{a}(a)\subset\mathfrak{a}$. We therefore conclude that $\mathfrak{a}=\mathfrak{a}(a)$, as we wished to do.

We may remark that in a Boolean ring without unit we have, in general, $\mathfrak{P}\neq\mathfrak{P}^*\neq\mathfrak{S}\neq\mathfrak{N}\neq\mathfrak{J}$; and that in a Boolean ring with unit we have, in general, $\mathfrak{P}=\mathfrak{P}^*=\mathfrak{S}\neq\mathfrak{N}\neq\mathfrak{J}$. When $\mathfrak{J}\neq\mathfrak{N}$ we may have either $\mathfrak{N}\neq\mathfrak{S}$ or $\mathfrak{N}=\mathfrak{S}$; but we have not been able to determine whether the relations $\mathfrak{P}\neq\mathfrak{P}^*$, $\mathfrak{P}^*=\mathfrak{S}$ are compatible or not. The various possibilities will be analyzed more fully on another occasion.

The conditions that an ideal be principal or semiprincipal, as given in Definition 8, are adequate for our purposes; but it is important for us to obtain conditions, other than those given in the definition, for an ideal to be simple or normal. The two theorems which follow present information on this topic.

THEOREM 26. *In order that an ideal* $\mathfrak{a}$ *in a Boolean ring A be simple, it is necessary and sufficient that the product* $\mathfrak{a}\mathfrak{a}(a)$ *be a principal ideal for every element a in A.*

We shall consider $\mathfrak{a}\mathfrak{a}(a)$ as an ideal in the subring $\mathfrak{a}(a)$ with unit a, recalling that the orthocomplement of $\mathfrak{a}\mathfrak{a}(a)$ relative to $\mathfrak{a}(a)$ is the ideal $\mathfrak{a}'\mathfrak{a}(a)$ in accordance with Theorem 22. If $\mathfrak{a}$ is simple relative to A, we have $\mathfrak{a}\mathfrak{a}(a)\vee\mathfrak{a}'\mathfrak{a}(a)=(\mathfrak{a}\vee\mathfrak{a}')\mathfrak{a}(a)=\mathfrak{e}\mathfrak{a}(a)=\mathfrak{a}(a)$ so that $\mathfrak{a}\mathfrak{a}(a)$ is simple relative to $\mathfrak{a}(a)$. By virtue of Theorem 25 we see that $\mathfrak{a}\mathfrak{a}(a)$ is principal relative to $\mathfrak{a}(a)$. Since $\mathfrak{a}\mathfrak{a}(a)$ is an ideal in A and since, considered as a Boolean ring, it has a unit by virtue of its character in $\mathfrak{a}(a)$, we conclude that there exists an element b such that

$\mathfrak{a}\mathfrak{a}(a)=\mathfrak{a}(b)$. Thus, when $\mathfrak{a}$ is simple, $\mathfrak{a}\mathfrak{a}(a)$ is principal. On the other hand, if $\mathfrak{a}\mathfrak{a}(a)$ is principal for every a in A, we write $\mathfrak{a}\mathfrak{a}(a)=\mathfrak{a}(b)\subset\mathfrak{a}(a)$. It follows that $\mathfrak{a}\mathfrak{a}(a)$ is principal, and hence simple, relative to $\mathfrak{a}(a)$. Thus we see that $\mathfrak{a}(a)=\mathfrak{a}\mathfrak{a}(a)\vee\mathfrak{a}'\mathfrak{a}(a)=(\mathfrak{a}\vee\mathfrak{a}')\mathfrak{a}(a)\subset\mathfrak{a}\vee\mathfrak{a}'$; in other words, that $\mathfrak{a}\vee\mathfrak{a}'$ contains a. Since a is arbitrary, we conclude that $\mathfrak{a}\vee\mathfrak{a}'=\mathfrak{e}$, or, in other words, that $\mathfrak{a}$ is simple, as we wished to prove.

THEOREM 27. *The following assertions concerning an ideal* $\mathfrak{a}$ *in a Boolean ring* A *are equivalent*:

(1) $\mathfrak{a}$ *is a normal ideal*;

(2) $\mathfrak{a}$ *is the orthocomplement of some ideal in* A;

(3) $\mathfrak{a}$ *is a product of semiprincipal ideals.*

In general, if $\mathfrak{a}$ *is an arbitrary ideal, then* $\mathfrak{a}''$ *is the product of all the semiprincipal ideal divisors of* $\mathfrak{a}$; *and, in particular, a normal ideal is the product of all its semiprincipal ideal divisors. In the case of a Boolean ring with unit, the term "principal ideal" is to replace the term "semiprincipal ideal" in the preceding statements.*

The equivalence of (1) and (2) is easily proved as follows: if $\mathfrak{a}$ is normal, then $\mathfrak{a}=\mathfrak{b}'$ for $\mathfrak{b}=\mathfrak{a}'$; and, if $\mathfrak{a}=\mathfrak{b}'$, then $\mathfrak{a}=\mathfrak{b}'=\mathfrak{b}'''=\mathfrak{a}''$. If $\mathfrak{a}$ is an arbitrary ideal, it has at least one semiprincipal ideal divisor, the ideal $\mathfrak{e}$. Hence the product of all the semiprincipal ideal divisors of $\mathfrak{a}$ exists and is an ideal $\mathfrak{b}$ which divides $\mathfrak{a}$. Now if $\mathfrak{c}$ is a semiprincipal ideal divisor of $\mathfrak{a}$, we have $\mathfrak{c}'\subset\mathfrak{a}'$, $\mathfrak{c}=\mathfrak{c}''\supset\mathfrak{a}''$, so that $\mathfrak{c}$ is also a semiprincipal ideal divisor of $\mathfrak{a}''$. It follows that $\mathfrak{b}\supset\mathfrak{a}''$. On the other hand, if a is an arbitrary element in $\mathfrak{a}'$, we see that $\mathfrak{a}(a)\subset\mathfrak{a}'$, that $\mathfrak{a}'(a)\supset\mathfrak{a}''\supset\mathfrak{a}$, and hence that $\mathfrak{a}'(a)\supset\mathfrak{b}$. The latter relation implies that $\mathfrak{a}(a)\mathfrak{b}=\mathfrak{o}$. Since a is arbitrary, we see that $\mathfrak{a}'\mathfrak{b}=\mathfrak{o}$ and hence that $\mathfrak{b}\subset\mathfrak{a}''$. It follows from this and the earlier inclusion relation that $\mathfrak{b}=\mathfrak{a}''$; in other words, that $\mathfrak{a}''$ is the product of all the semiprincipal ideal divisors of $\mathfrak{a}$. The special case where $\mathfrak{a}$ is normal, that is, where $\mathfrak{a}=\mathfrak{a}''$, is now obvious. If an ideal $\mathfrak{a}$ is the product of semiprincipal ideals, then we must have $\mathfrak{a}\supset\mathfrak{a}''$ since $\mathfrak{a}''$ is the product of *all* the semiprincipal ideal divisors of $\mathfrak{a}$; we now conclude by virtue of the relation $\mathfrak{a}\subset\mathfrak{a}''$ that $\mathfrak{a}=\mathfrak{a}''$ and hence that $\mathfrak{a}$ is normal. The preceding results show the equivalence of (1) and (3). The final statement of the theorem follows immediately from Theorem 25.

We shall turn now to an examination of the behavior of the various classes of ideals under the operations of addition and multiplication. As a preliminary to our first theorem in this connection, we must make a few remarks concerning congruences in arbitrary algebraic systems. In any algebraic system, the fundamental relation of equality has to be taken as one of the undefined concepts and must be connected with the operations of the

system by suitable postulates. It is sufficient to assume, first, that the relation of equality is a reflexive, symmetric, and transitive dyadic relation, and, second, that in terms of this relation the following law of substitution holds: for each of the operations of the system, the substitution of equal operands for given operands respectively replaces the element resulting from the application of that operation by an equal element. Now any dyadic relation which has these same properties and which holds whenever the fundamental relation of equality holds may be called a congruence in the given algebraic system. The fundamental equality is itself a congruence. By simple inductive arguments it can be shown that, for any given relation of congruence, the following general rule of substitution is valid: if an element a is obtained as a polynomial in terms of elements of the system, then the substitution of respectively congruent elements in this polynomial yields an element congruent to a. Evidently, any relation of congruence in an algebraic system may be used to replace the fundamental relation of equality; if this be done, the system is converted into a new system which is easily seen to be homomorphic to the old. Conversely, any system homomorphic to the given one is isomorphic to a system obtained in this way by the use of an appropriate congruence: when the homomorphism is given, the associated congruence is obtained by defining two elements to be congruent if and only if they are carried by the homomorphism into equal elements of the homomorphic system. The following theorem is stated with these general remarks as a background.

THEOREM 28. *The dyadic relation C defined between the elements of the class $\mathfrak{J}$ of all ideals in a Boolean ring A by setting $\mathfrak{a} \equiv \mathfrak{b}$ if $\mathfrak{a}' = \mathfrak{b}'$, is a congruence in the algebraic system consisting of the class $\mathfrak{J}$ and the operations of unrestricted addition and finite multiplication. Each class of mutually congruent elements in $\mathfrak{J}$ contains one and only one normal ideal as an element, in the following sense: if $\mathfrak{a}$ is any ideal, then $\mathfrak{a}''$ is a normal ideal such that $\mathfrak{a} \equiv \mathfrak{a}''$; and, if $\mathfrak{a}$ and $\mathfrak{b}$ are normal ideals such that $\mathfrak{a} \equiv \mathfrak{b}$, then $\mathfrak{a} = \mathfrak{b}$. The algebraic system $\mathfrak{J}^C$ consisting of the class $\mathfrak{J}$ with the congruence C as the fundamental relation of equality and the operations of finite addition and finite multiplication is a Boolean algebra with unit in accordance with Theorem 3.*†

Most of the properties of the relation C asserted in the theorem are easily verified. Thus $\mathfrak{a} = \mathfrak{b}$ implies $\mathfrak{a}' = \mathfrak{b}'$ and hence $\mathfrak{a} \equiv \mathfrak{b}$; in particular, $\mathfrak{a} \equiv \mathfrak{a}$. We see that $\mathfrak{a} \equiv \mathfrak{b}$ implies $\mathfrak{b} \equiv \mathfrak{a}$, since $\mathfrak{a}' = \mathfrak{b}'$ implies $\mathfrak{b}' = \mathfrak{a}'$; and that $\mathfrak{a} \equiv \mathfrak{b}$ and $\mathfrak{b} \equiv \mathfrak{c}$

† This theorem bears a close formal or structural relation to a general proposition about the logic of Brouwer in the symbolic statement of Heyting, Sitzungsberichte der Preussischen Akademie der Wissenschaften, 1930, pp. 42–56. The proposition in question was given by Glivenko, Académie Royale de Belgique, Bulletins des Sciences, (5), vol. 15 (1929), pp. 183–188.

imply $\mathfrak{a} \equiv \mathfrak{c}$, since $\mathfrak{a}' = \mathfrak{b}'$ and $\mathfrak{b}' = \mathfrak{c}'$ imply $\mathfrak{a}' = \mathfrak{c}'$. If $\mathfrak{A}$ and $\mathfrak{B}$ are subclasses of $\mathfrak{Z}$ in one-to-one correspondence in such a manner that corresponding elements $\mathfrak{a}$ and $\mathfrak{b}$ are in the relation $\mathfrak{a} \equiv \mathfrak{b}$, we see that

$$(\underset{\mathfrak{a}\in\mathfrak{A}}{S}\,\mathfrak{a})' = \underset{\mathfrak{a}\in\mathfrak{A}}{P}\,\mathfrak{a}' = \underset{\mathfrak{b}\in\mathfrak{B}}{P}\,\mathfrak{b}' = (\underset{\mathfrak{b}\in\mathfrak{B}}{S}\,\mathfrak{b})'$$

in accordance with Theorem 21, and hence that

$$\underset{\mathfrak{a}\in\mathfrak{A}}{S}\,\mathfrak{a} \equiv \underset{\mathfrak{b}\in\mathfrak{B}}{S}\,\mathfrak{b}.$$

In particular, we note that $\mathfrak{a} \equiv \mathfrak{c}$ and $\mathfrak{b} \equiv \mathfrak{d}$ imply $\mathfrak{a} \vee \mathfrak{b} \equiv \mathfrak{c} \vee \mathfrak{d}$.

The proof that $\mathfrak{a} \equiv \mathfrak{c}$ and $\mathfrak{b} \equiv \mathfrak{d}$ imply $\mathfrak{ab} \equiv \mathfrak{cd}$ is more difficult. We shall first prove that $\mathfrak{a} \equiv \mathfrak{e}$ and $\mathfrak{b} \equiv \mathfrak{e}$ imply $\mathfrak{ab} \equiv \mathfrak{e}$, or, equivalently, that $\mathfrak{a}' = \mathfrak{o}$ and $\mathfrak{b}' = \mathfrak{o}$ imply $(\mathfrak{ab})' = \mathfrak{o}$. Let a be an arbitrary element in $(\mathfrak{ab})'$, b an arbitrary element in $\mathfrak{a}(a)\mathfrak{a}$, and c an arbitrary element in $\mathfrak{a}(b)\mathfrak{b}$. It is then clear that $\mathfrak{a}(c) \subset \mathfrak{a}(b)\mathfrak{b} \subset \mathfrak{a}(a)\mathfrak{ab} \subset (\mathfrak{ab})'\mathfrak{ab} = \mathfrak{o}$ and hence that $c = 0$. Since c was an arbitrary element in $\mathfrak{a}(b)\mathfrak{b}$, we conclude that $\mathfrak{a}(b)\mathfrak{b} = \mathfrak{o}$ and hence that $\mathfrak{a}(b) \subset \mathfrak{b}' = \mathfrak{o}$, $b = 0$. Since b was an arbitrary element in $\mathfrak{a}(a)\mathfrak{a}$, we conclude that $\mathfrak{a}(a)\mathfrak{a} = \mathfrak{o}$ and hence that $\mathfrak{a}(a) \subset \mathfrak{a}' = \mathfrak{o}$, $a = 0$. Since a was an arbitrary element in $(\mathfrak{ab})'$, we conclude that $(\mathfrak{ab})' = \mathfrak{o}$, as we wished to prove. We next prove that $\mathfrak{a}''\mathfrak{b}''(\mathfrak{ab})' = \mathfrak{o}$. We begin by writing $\mathfrak{a}''\mathfrak{b}''(\mathfrak{ab})' = (\mathfrak{a}' \vee \mathfrak{b}')'(\mathfrak{ab})' = (\mathfrak{a}' \vee \mathfrak{b}' \vee \mathfrak{ab})'$ in accordance with Theorem 21. We then observe that $\mathfrak{a}' \vee \mathfrak{b}' \vee \mathfrak{ab} \supset \mathfrak{a}'(\mathfrak{b} \vee \mathfrak{b}') \vee \mathfrak{ab}' \vee \mathfrak{ab} = (\mathfrak{a} \vee \mathfrak{a}')(\mathfrak{b} \vee \mathfrak{b}')$ and hence that $(\mathfrak{a}' \vee \mathfrak{b}' \vee \mathfrak{ab})' \subset [(\mathfrak{a} \vee \mathfrak{a}')(\mathfrak{b} \vee \mathfrak{b}')]'$. In view of the relations $(\mathfrak{a} \vee \mathfrak{a}')' = \mathfrak{a}'\mathfrak{a}'' = \mathfrak{o}$, $(\mathfrak{b} \vee \mathfrak{b}')' = \mathfrak{b}'\mathfrak{b}'' = \mathfrak{o}$, we can conclude that $\mathfrak{a}''\mathfrak{b}''(\mathfrak{ab})' = \mathfrak{o}$ by virtue of the preceding results. We now observe that $(\mathfrak{a}''\mathfrak{b}'')' \supset (\mathfrak{ab})'$ as a consequence of the relation just established; and that $(\mathfrak{a}''\mathfrak{b}'')' \subset (\mathfrak{ab})'$ in consequence of the relation $\mathfrak{a}''\mathfrak{b}'' \supset \mathfrak{ab}$. We thus see that $(\mathfrak{a}''\mathfrak{b}'')' = (\mathfrak{ab})'$, or, equivalently, that $\mathfrak{a}''\mathfrak{b}'' \equiv \mathfrak{ab}$. The final step of the proof is simple. If $\mathfrak{a} \equiv \mathfrak{c}$ and $\mathfrak{b} \equiv \mathfrak{d}$, then we have $\mathfrak{a}' = \mathfrak{c}'$, $\mathfrak{a}'' = \mathfrak{c}''$ and $\mathfrak{b}' = \mathfrak{d}'$, $\mathfrak{b}'' = \mathfrak{d}''$; hence we have $\mathfrak{a}''\mathfrak{b}'' = \mathfrak{c}''\mathfrak{b}''$ and $\mathfrak{a}''\mathfrak{b}'' \equiv \mathfrak{c}''\mathfrak{b}''$; and finally, from the relations $\mathfrak{a}''\mathfrak{b}'' \equiv \mathfrak{ab}$ and $\mathfrak{c}''\mathfrak{b}'' \equiv \mathfrak{cd}$ we conclude that $\mathfrak{ab} \equiv \mathfrak{cd}$. We can show by examples that this result cannot be extended to the case of unrestricted multiplication.

The assertion concerning the classes of mutually congruent elements is obvious.

Having shown that the relation C is a congruence in the indicated sense, we may use it to replace the fundamental equality in $\mathfrak{Z}$ in accordance with the general remarks above. When we restrict consideration to the finite operations $\vee$ and $\cdot$ alone, we obtain the system $\mathfrak{Z}^C$. We wish to identify this system as a Boolean algebra with $\mathfrak{e}$ as unit, by showing that it has the properties (1_1), (3_1), (3_2), (4_1), (5), (6_1) and (6_2) of Theorem 3. By combining the properties of the congruence C with the results given in Theorem 18, we establish

all the desired properties, except (5), without any difficulty. To prove (5), we show that the relations $\mathfrak{x} \vee \mathfrak{a} \equiv \mathfrak{e}$, $\mathfrak{x}\mathfrak{a} \equiv \mathfrak{o}$ have a solution $\mathfrak{x} \equiv \mathfrak{a}'$. To this end we have merely to note that $(\mathfrak{a}' \vee \mathfrak{a})' = \mathfrak{a}''\mathfrak{a}' = \mathfrak{o} = \mathfrak{e}'$, $\mathfrak{a}'\mathfrak{a} = \mathfrak{o}$, and hence that $\mathfrak{a}' \vee \mathfrak{a} \equiv \mathfrak{e}$, $\mathfrak{a}'\mathfrak{a} \equiv \mathfrak{o}$. To convert $\mathfrak{J}^C$ into a Boolean ring we must replace the operation $\vee$ by an operation $+$ such that $\mathfrak{a}+\mathfrak{b} \equiv \mathfrak{a}\mathfrak{b}' \vee \mathfrak{a}'\mathfrak{b}$, in accordance with Theorem 2. Evidently, it is most convenient to take $\mathfrak{a}+\mathfrak{b}$ as the ideal $\mathfrak{a}\mathfrak{b}' \vee \mathfrak{a}'\mathfrak{b}$, rather than as some other ideal congruent to the latter.

In discussing the class of all normal ideals, it will be necessary to replace addition by a new operation. We therefore give the following formal definition:

DEFINITION 9. *If $\mathfrak{B}$ is a non-void class of ideals $\mathfrak{a}$, the ideal $(S_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a})''$ is called the normalized sum of the ideals $\mathfrak{a}$ in $\mathfrak{B}$ and is denoted by $S''_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$; the normalized sum of ideals $\mathfrak{a}$ and $\mathfrak{b}$ is denoted by $\mathfrak{a} \nabla \mathfrak{b}$. The operation of forming the normalized sum is called normalized addition.*

In terms of this definition, we have

THEOREM 29. *The normalized sum and the product of normal ideals are normal ideals; but a finite sum of normal ideals is not necessarily normal. The normalized sum of arbitrary ideals is the least normal ideal containing all the summands. Within the class $\mathfrak{N}$ of all normal ideals the operations of normalized addition and multiplication have the following properties:*

(1) *if $\mathcal{B}$ is a non-void class of non-void subclasses $\mathfrak{B}$ of $\mathfrak{N}$, then*

$$\underset{\mathfrak{B}\in\mathcal{B}}{S''}\ (\underset{\mathfrak{a}\in\mathfrak{B}}{S''}\mathfrak{a}) = \underset{\mathfrak{a}\in\mathfrak{C}}{S''}\mathfrak{a},$$

where $\mathfrak{C}$ is the union $\Sigma_{\mathfrak{B}\in\mathcal{B}}\mathfrak{B}$;

(2) *if $\mathcal{B}$, $\mathfrak{B}$, and $\mathfrak{C}$ have the same significance as in* (1), *then*

$$\underset{\mathfrak{B}\in\mathcal{B}}{P}\ (\underset{\mathfrak{a}\in\mathfrak{B}}{P}\mathfrak{a}) = \underset{\mathfrak{a}\in\mathfrak{C}}{P}\mathfrak{a};$$

(3) *if $\mathfrak{b}$ is any normal ideal and $\mathfrak{B}$ is any non-void subclass of $\mathfrak{N}$, then*

$$\mathfrak{b}(\underset{\mathfrak{a}\in\mathfrak{B}}{S''}\mathfrak{a}) = \underset{\mathfrak{a}\in\mathfrak{B}}{S''}(\mathfrak{b}\mathfrak{a});$$

(4) *if $\mathfrak{b}$ and $\mathfrak{B}$ have the same significance as in* (3), *then*

$$\underset{\mathfrak{a}\in\mathfrak{B}}{P}\ (\mathfrak{b} \nabla \mathfrak{a}) = \mathfrak{b} \nabla \underset{\mathfrak{a}\in\mathfrak{B}}{P}\mathfrak{a};$$

(5) *if $\mathfrak{B}$ is any non-void subclass of $\mathfrak{N}$, then*

$$(\underset{\mathfrak{a}\in\mathfrak{B}}{S''}\mathfrak{a})' = \underset{\mathfrak{a}\in\mathfrak{B}}{P}\mathfrak{a}';$$

(6) *if* $\mathfrak{B}$ *has the same significance as in* (5), *then*

$$(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\,\mathfrak{a})' = \underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''\mathfrak{a}'.$$

Under the finite operations $\vee$ *and* $\cdot$ *alone, the system* $\mathfrak{N}$ *is a Boolean algebra isomorphic to the system* $\mathfrak{Z}^c$ *of Theorem* 28 *by virtue of the correspondence* $\mathfrak{a}\longleftrightarrow\mathfrak{a}''$. *This algebra has the property that its normal ideals are all principal.*

In view of Theorem 27(2) and Definition 9, it is evident that the normalized sum of ideals is always a normal ideal. In view of Theorem 27(3), it is likewise evident that the product of normal ideals is a normal ideal: since each factor is a product of semiprincipal ideals, the product is also a product of semiprincipal ideals by Theorem 15(11) and Theorem 18. On the other hand, if $\mathfrak{a}$ is a normal ideal which is not simple, the sum $\mathfrak{a}\vee\mathfrak{a}'$ is not normal, as we showed in Theorem 24, in spite of the fact that $\mathfrak{a}$ and $\mathfrak{a}'$ are both normal.

If $\mathfrak{a}$ is an arbitrary ideal, then $\mathfrak{a}''$ is a normal ideal containing $\mathfrak{a}$. If $\mathfrak{b}$ is a normal ideal containing $\mathfrak{a}$, then $\mathfrak{b}$ is the product of semiprincipal ideal divisors of $\mathfrak{a}$ and thus contains $\mathfrak{a}''$, in accordance with Theorem 27. Thus $\mathfrak{a}''$ is the least normal ideal containing $\mathfrak{a}$. By comparing this result with Definition 9, we see that the normalized sum of ideals is the least normal ideal containing all the summands.

Some of the properties (1)–(6) have already been established. Thus (2) has been proved in Theorem 15 (11) and Theorem 18, and (5) follows from Theorem 21(4) and Definition 9 by the use of the relation $\mathfrak{a}'''=\mathfrak{a}'$, since we have

$$(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''\mathfrak{a})' = (\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}\,\mathfrak{a})''' = (\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}\,\mathfrak{a})' = \underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\,\mathfrak{a}'.$$

We can now deduce (6) from (5) by virtue of the relations

$$(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\,\mathfrak{a})' = (\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\,\mathfrak{a}'')' = (\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''\mathfrak{a}')'' = \underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''\mathfrak{a}',$$

since the ideals in $\mathfrak{B}$ and all normalized sums are normal ideals. We can establish (1) from the corresponding property of ordinary sums already established in Theorem 15(10) and Theorem 18 by using the results of Theorem 28 concerning the congruence C: from Definition 9 it is evident that any normalized sum is congruent to the corresponding ordinary sum; in consequence, the two members of (1) above are congruent, the corresponding ordinary sums being equal; and finally, since the members are both normal ideals, their congruence implies their equality. In a similar way, we establish (3) from the corresponding relation for ordinary sums, already proved in Theorem 18(12): the two members of (3) are congruent and, being normal ideals,

are therefore equal. With the help of (5) and (6) it is now easy to deduce (4) from (3), as follows:

$$\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}(\mathfrak{b}\nabla\mathfrak{a}) = \underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}(\mathfrak{b}''\nabla\mathfrak{a}'') = \underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}(\mathfrak{b}'\mathfrak{a}') = (\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''(\mathfrak{b}'\mathfrak{a}'))' = (\mathfrak{b}'(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{S}}''\mathfrak{a}'))'$$

$$= (\mathfrak{b}'(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\mathfrak{a})')' = \mathfrak{b}''\nabla(\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\mathfrak{a})'' = \mathfrak{b}\nabla\underset{\mathfrak{a}\in\mathfrak{B}}{\mathrm{P}}\mathfrak{a},$$

the ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathrm{P}_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$ being normal.

In order to show that under the finite operations ∇ and the system $\mathfrak{N}$ is a Boolean algebra, we must verify properties (1_1), (3_1), (3_2), (4_1), (5), (6_1), (6_2) of Theorem 3. Now (1_1), (4_1), (6_1), and (6_2) are evident from the known properties of the operation $\vee$ and the relation $\mathfrak{a}\nabla\mathfrak{b} = (\mathfrak{a}\vee\mathfrak{b})''$. Properties (3_1) and (3_2) follow at once from (3) above and the commutative law for multiplication. To establish (5) we show that the equations $\mathfrak{x}\nabla\mathfrak{a} = \mathfrak{e}$, $\mathfrak{x}\mathfrak{a} = \mathfrak{o}$, where $\mathfrak{o}$ and $\mathfrak{e}$ are known to be normal ideals and $\mathfrak{a}$ is assumed to be a normal ideal, have as a solution the normal ideal $\mathfrak{x} = \mathfrak{a}'$: we have only to note the relations $\mathfrak{a}'\nabla\mathfrak{a} = (\mathfrak{a}'\vee\mathfrak{a})'' = (\mathfrak{a}''\mathfrak{a}')' = \mathfrak{o}' = \mathfrak{e}$, $\mathfrak{a}'\mathfrak{a} = \mathfrak{o}$. In order to convert this Boolean algebra into a Boolean ring, we have only to introduce the operation $+$ defined by the equation $\mathfrak{a}+\mathfrak{b} = \mathfrak{a}\mathfrak{b}'\nabla\mathfrak{a}'\mathfrak{b}$, in accordance with Theorem 2. It is now easily verified that the correspondence $\mathfrak{a}\longleftrightarrow\mathfrak{a}''$ sets up an isomorphism between the Boolean algebras $\mathfrak{Z}^c$ and $\mathfrak{N}$. This correspondence is biunivocal on account of Theorem 28, which shows that $\mathfrak{a}''$ is a normal ideal congruent to $\mathfrak{a}$ and that $\mathfrak{a}\equiv\mathfrak{b}$ if and only if $\mathfrak{a}'' = \mathfrak{b}''$. The correspondent of $\mathfrak{a}\vee\mathfrak{b}$ is given by $(\mathfrak{a}\vee\mathfrak{b})''$ $= (\mathfrak{a}'\mathfrak{b}')' = \mathfrak{a}''\nabla\mathfrak{b}''$ in accordance with Theorem 21(4) and (6) above. The correspondent of $\mathfrak{a}\mathfrak{b}$ is found to be $(\mathfrak{a}\mathfrak{b})'' = \mathfrak{a}''\mathfrak{b}''$, by the following reasoning: the normal ideal $(\mathfrak{a}\mathfrak{b})''$ is congruent to $\mathfrak{a}\mathfrak{b}$ and hence also to $\mathfrak{a}''\mathfrak{b}''$; since $\mathfrak{a}''\mathfrak{b}''$ is normal, we must have $(\mathfrak{a}\mathfrak{b})'' = \mathfrak{a}''\mathfrak{b}''$ in accordance with Theorem 28. These results establish the indicated isomorphism.

It remains for us to prove that the Boolean algebra $\mathfrak{N}$ has the special property that its normal ideals are all principal. Since $\mathfrak{N}$ has the ideal $\mathfrak{e}$ as its unit, all simple ideals of the algebra $\mathfrak{N}$ are principal; in other words, a simple ideal of $\mathfrak{N}$ is characterized by an element $\mathfrak{a}$ in $\mathfrak{N}$ such that $\mathfrak{b}$ in $\mathfrak{N}$ belongs to the ideal if and only if $\mathfrak{b}\subset\mathfrak{a}$. This result follows from Theorem 25 and applies in particular to semiprincipal ideals of $\mathfrak{N}$. Now a normal ideal of $\mathfrak{N}$ is by virtue of Theorem 27 the product of semiprincipal ideals and hence, by virtue of the result just noted, the product of principal ideals. If $\mathfrak{B}$ is the class of elements $\mathfrak{a}$ generating the various factors in a product of principal ideals, the element $\mathrm{P}_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$ belongs to $\mathfrak{N}$ and is contained in every element $\mathfrak{a}$ in $\mathfrak{B}$; and any element of $\mathfrak{N}$ belonging to the product is contained in every element $\mathfrak{a}$, and hence also in the element $\mathrm{P}_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$. Thus the product of principal ideals in the

algebra $\mathfrak{N}$ is itself the principal ideal generated by the indicated element $P_{\mathfrak{a}\in\mathfrak{B}}\mathfrak{a}$. It follows that every normal ideal of $\mathfrak{N}$ is principal.

Theorem 29 can be summarized briefly by pointing out that under the operations S'', P, and ' the class $\mathfrak{N}$ has *some* of the chief formal properties of an algebra of classes with the corresponding operations of forming *unrestricted* unions, products, and complements respectively. That it does not have *all* the formal properties of such an algebra we shall see later in the present paper.

THEOREM 30. *The class $\mathfrak{S}$ of all simple ideals in a Boolean ring A is a Boolean subring, with* e *as its unit, of the Boolean algebras $\mathfrak{J}^c$ and $\mathfrak{N}$ of Theorems 28 and 29 respectively. The application of the operations of finite addition, finite normalized addition, finite multiplication, and orthocomplementation to simple ideals yields simple ideals; in particular, if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are simple ideals,* $\mathfrak{a}\vee\mathfrak{b}=\mathfrak{a}\vee\mathfrak{b}$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are simple ideals, then $\mathfrak{a}\vee\mathfrak{b}$ is a simple ideal: for $(\mathfrak{a}\vee\mathfrak{b})\vee(\mathfrak{a}\vee\mathfrak{b})'=\mathfrak{a}\vee\mathfrak{b}\vee\mathfrak{a}'\mathfrak{b}'\supset\mathfrak{a}(\mathfrak{b}\vee\mathfrak{b}')\vee\mathfrak{a}'\mathfrak{b}\vee\mathfrak{a}'\mathfrak{b}'=(\mathfrak{a}\vee\mathfrak{a}')(\mathfrak{b}\vee\mathfrak{b}')=\mathfrak{e}\mathfrak{e}=\mathfrak{e}$ and hence $(\mathfrak{a}\vee\mathfrak{b})\vee(\mathfrak{a}\vee\mathfrak{b})'=\mathfrak{e}$. It follows also that $\mathfrak{a}\vee\mathfrak{b}$ is normal and that $\mathfrak{a}\vee\mathfrak{b}=(\mathfrak{a}\vee\mathfrak{b})''=\mathfrak{a}\vee\mathfrak{b}$. If $\mathfrak{a}$ is a simple ideal, then $\mathfrak{a}'$ is a simple ideal: for $\mathfrak{a}'\vee\mathfrak{a}''\supset\mathfrak{a}'\vee\mathfrak{a}=\mathfrak{e}$ and hence $\mathfrak{a}'\vee\mathfrak{a}''=\mathfrak{e}$. The results just proved show that $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}+\mathfrak{b}=\mathfrak{a}\mathfrak{b}'\vee\mathfrak{a}'\mathfrak{b}=\mathfrak{a}\mathfrak{b}'\vee\mathfrak{a}'\mathfrak{b}$ are simple ideals whenever $\mathfrak{a}$ and $\mathfrak{b}$ are simple ideals: for $\mathfrak{a}\mathfrak{b}=\mathfrak{a}''\mathfrak{b}''=(\mathfrak{a}'\vee\mathfrak{b}')'$; and $\mathfrak{a}\mathfrak{b}'\vee\mathfrak{a}'\mathfrak{b}=\mathfrak{a}\mathfrak{b}'\vee\mathfrak{a}'\mathfrak{b}$ whenever $\mathfrak{a}\mathfrak{b}'$ and $\mathfrak{a}'\mathfrak{b}$ are simple. Hence $\mathfrak{S}$ is a subring of $\mathfrak{J}^c$ and also of $\mathfrak{N}$. The ideal e is in $\mathfrak{S}$ and is obviously its unit.

THEOREM 31. *The class $\mathfrak{P}$ of all principal ideals in a Boolean ring A is a Boolean subring of $\mathfrak{N}$ and an ideal in $\mathfrak{S}$; it is isomorphic to the Boolean ring A in accordance with the following relations.*

(1) $\mathfrak{a}(a)=\mathfrak{a}(b)$ *if and only if* $a=b$;

(2) $\mathfrak{a}(a+b)=\mathfrak{a}(a)+\mathfrak{a}(b)=\mathfrak{a}(a)\,\mathfrak{a}'(b)\vee\mathfrak{a}'(a)\mathfrak{a}(b)$;

(3) $\mathfrak{a}(a\vee b)=\mathfrak{a}(a)\vee\mathfrak{a}(b)$; (4) $\mathfrak{a}(ab)=\mathfrak{a}(a)\mathfrak{a}(b)$.

If the Boolean ring A has a unit e, then $\mathfrak{S}=\mathfrak{P}$ and $\mathfrak{a}(a')=\mathfrak{a}'(a)$.

The class $\mathfrak{P}$ is evidently non-void since it contains $\mathfrak{o}=\mathfrak{a}(0)$. In showing that it is an ideal in the Boolean algebra $\mathfrak{S}$, we shall establish properties (3) and (4) above. Theorem 14 shows that the element $a\vee b$ is contained in the ideal $\mathfrak{a}(a)\vee\mathfrak{a}(b)$ and hence that $\mathfrak{a}(a\vee b)\subset\mathfrak{a}(a)\vee\mathfrak{a}(b)$. On the other hand the relations $a<a\vee b$ and $b<a\vee b$ imply that $\mathfrak{a}(a)\subset\mathfrak{a}(a\vee b)$, $\mathfrak{a}(b)\subset\mathfrak{a}(a\vee b)$ and hence that $\mathfrak{a}(a)\vee\mathfrak{a}(b)\subset\mathfrak{a}(a\vee b)$. It follows that (3) is valid. Theorem 26 shows immediately that the ideal $\mathfrak{a}(a)\mathfrak{a}$ is principal, whatever the simple ideal $\mathfrak{a}$. In particular, $\mathfrak{a}(a)\mathfrak{a}(b)$ is principal. Theorem 16 thus shows that $\mathfrak{P}$ is an ideal in $\mathfrak{S}$ and hence a subring in $\mathfrak{N}$. Theorem 18 shows that ab is in the ideal $\mathfrak{a}(a)\mathfrak{a}(b)$ and hence that $\mathfrak{a}(ab)\subset\mathfrak{a}(a)\mathfrak{a}(b)$. On the other hand, the relations $c<a$

and $d<b$ imply $cd<ab$ and hence $\mathfrak{a}(a)\mathfrak{a}(b) \subset \mathfrak{a}(ab)$. It follows that (4) is valid. To prove (1), we note that $a=b$ obviously implies $\mathfrak{a}(a)=\mathfrak{a}(b)$; and that $\mathfrak{a}(a)=\mathfrak{a}(b)$ implies $a<b$, $b<a$ and hence $a=b$. The relations (1), (3), and (4) imply that the correspondence $a \longleftrightarrow \mathfrak{a}(a)$ sets up an isomorphism between A and $\mathfrak{P}$ with respect to the operations $\vee$ and given in these systems. In order to extend this isomorphism to the operation $+$, we use (3) and (4) to prove (2). When $ab=0$ we have $a+b=a \vee b$ and $\mathfrak{a}(a)\mathfrak{a}(b)=\mathfrak{a}(ab)=\mathfrak{a}(0)=\mathfrak{o}$; and we therefore see that $\mathfrak{a}(a+b)=\mathfrak{a}(a \vee b)=\mathfrak{a}(a) \vee \mathfrak{a}(b)=\mathfrak{a}(a)+\mathfrak{a}(b)$. When a and b are arbitrary we apply this result to the elements $a+b$ and ab, which have the property $(a+b)ab=0$, to write $\mathfrak{a}(a+b)+\mathfrak{a}(ab)=\mathfrak{a}(a+b+ab)=\mathfrak{a}(a \vee b)$ $=\mathfrak{a}(a) \vee \mathfrak{a}(b)=\mathfrak{a}(a)+\mathfrak{a}(b)+\mathfrak{a}(a)\mathfrak{a}(b)=\mathfrak{a}(a)+\mathfrak{a}(b)+\mathfrak{a}(ab)$; and we conclude that $\mathfrak{a}(a+b)=\mathfrak{a}(a)+\mathfrak{a}(b)$, as we wished to show. In case A has a unit e, we know that $\mathfrak{P}$ coincides with $\mathfrak{S}$. By simple calculations, we find that $\mathfrak{a}(a')=\mathfrak{a}(a+e)=\mathfrak{a}(a)+\mathfrak{a}(e)=\mathfrak{a}(a)+\mathfrak{e}=\mathfrak{a}(a)\mathfrak{e}' \vee \mathfrak{a}'(a)\mathfrak{e}=\mathfrak{a}'(a)$, as stated in the theorem.

THEOREM 32. *The class $\mathfrak{P}^*$ of all semiprincipal ideals in a Boolean ring A is a subring of $\mathfrak{S}$, with $\mathfrak{e}$ as its unit, isomorphic to the Boolean ring B of Theorem 1; $\mathfrak{P}$ and A are ideals in $\mathfrak{P}^*$ and B respectively. The operations $\vee$, $\cdot$, $+$, and $'$ in the system $\mathfrak{S}$ apply to elements of $\mathfrak{P}^*$ in the manner indicated by the following rules:*

$$(1_1)\quad \mathfrak{a}(a) \vee \mathfrak{a}(b) = \mathfrak{a}(a \vee b); \qquad (1_2)\quad \mathfrak{a}(a) \vee \mathfrak{a}'(b) = \mathfrak{a}'(b + ab);$$

$$(1_3)\quad \mathfrak{a}'(a) \vee \mathfrak{a}'(b) = \mathfrak{a}'(ab);$$

$$(2_1)\quad \mathfrak{a}(a)\mathfrak{a}(b) = \mathfrak{a}(ab); \qquad (2_2)\quad \mathfrak{a}(a)\mathfrak{a}'(b) = \mathfrak{a}(a + ab);$$

$$(2_3)\quad \mathfrak{a}'(a)\mathfrak{a}'(b) = \mathfrak{a}'(a \vee b);$$

$$(3_1)\quad \mathfrak{a}(a) + \mathfrak{a}(b) = \mathfrak{a}(a + b); \qquad (3_2)\quad \mathfrak{a}(a) + \mathfrak{a}'(b) = \mathfrak{a}'(a + b);$$

$$(3_3)\quad \mathfrak{a}'(a) + \mathfrak{a}'(b) = \mathfrak{a}(a + b);$$

$$(4_1)\quad \mathfrak{a}'(a) \text{ is in } \mathfrak{P}^*; \qquad (4_2)\quad (\mathfrak{a}'(a))' = \mathfrak{a}(a).$$

In the case where $\mathfrak{P} \neq \mathfrak{P}^*$, $\mathfrak{P}$ is not a normal ideal in $\mathfrak{P}^*$.

Before giving proofs of the various numbered relations, we shall discuss their consequences. The class $\mathfrak{P}^*$ is non-void since it contains the ideals $\mathfrak{o}$ and $\mathfrak{e}$; it is a subring of $\mathfrak{S}$ by virtue of relations (2_1), (2_2), (2_3), (3_1), (3_2), and (3_3); and it obviously has $\mathfrak{e}$ as its unit. Since $\mathfrak{P}$ is an ideal in $\mathfrak{S}$ by Theorem 31, it is also an ideal in the subring $\mathfrak{P}^*$. When A has a unit, $\mathfrak{P}=\mathfrak{P}^*$ in accordance with Theorem 25, and the Boolean ring B of Theorem 1 coincides with A; the isomorphism between $\mathfrak{P}^*$ and B is thus a consequence of the isomorphism between $\mathfrak{P}$ and A established in Theorem 31. When A has no unit, $\mathfrak{P} \neq \mathfrak{P}^*$

and $A \neq B$. In this case we set up an isomorphism between $\mathfrak{P}^*$ and the Boolean ring of pairs (a, α) described in the proof of Theorem 1, and hence between $\mathfrak{P}^*$ and B. The necessary correspondence is indicated in the relations $\mathfrak{a}(a) \longleftrightarrow (a, 0)$, $\mathfrak{a}'(a) \longleftrightarrow (a, \epsilon)$. With the help of the relations (2_1), (2_2), (2_3), (3_1), (3_2), and (3_3), it is easily seen that this correspondence yields the desired isomorphism. It should be observed that the isomorphism between $\mathfrak{P}^*$ and B preserves the isomorphism between $\mathfrak{P}$ and A already set up in Theorem 31. Since $\mathfrak{P}$ is an ideal in $\mathfrak{P}^*$, it follows that A is an ideal in B; this statement can also be confirmed by virtue of the relations $(a, 0)(b, \beta) = (ab + a\beta + 0b, 0\beta) = (ab + a\beta, 0)$. In order to show that $\mathfrak{P}$ is not normal in $\mathfrak{P}^*$, we shall determine its orthocomplement relative to $\mathfrak{P}^*$. If $\mathfrak{a}$ is any semiprincipal ideal, or, more generally, a quite arbitrary ideal, we see that $\mathfrak{a}\mathfrak{a}(a) = \mathfrak{o}$ implies $\mathfrak{a}(a) = \mathfrak{a}\mathfrak{a}(a) = \mathfrak{o}$ and $a = 0$ whenever a is in $\mathfrak{a}$; and hence that, whenever $\mathfrak{a}\mathfrak{a}(a) = \mathfrak{o}$ for every a, the ideal $\mathfrak{a}$ coincides with $\mathfrak{o}$. Thus the orthocomplement of $\mathfrak{P}$ relative to $\mathfrak{P}^*$ or relative to $\mathfrak{S}$ consists of the ideal $\mathfrak{o}$ alone. Since $\mathfrak{P} \neq \mathfrak{P}^*$ and $\mathfrak{P} \neq \mathfrak{S}$ in the case under consideration, $\mathfrak{P}$ is not normal in $\mathfrak{P}^*$ or in $\mathfrak{S}$.

We turn now to the proof of the various numbered relations stated in the theorem. Of these certain ones have been established previously. Relations (1_1), (2_1), and (3_1) were proved in Theorem 31; (4_1) is part of Definition 8; and (4_2) follows at once from Theorem 23. By using the relation $\mathfrak{a}'(a) = \mathfrak{e} + \mathfrak{a}(a)$ which holds in $\mathfrak{S}$ by virtue of Theorem 30, we see at once that relations (3_2) and (3_3) follow from (3_1) and the known properties of the operation $+$. In a similar way, we deduce (2_2) from (2_1) and (3_1), writing

$$\mathfrak{a}(a)\mathfrak{a}'(b) = \mathfrak{a}(a)(\mathfrak{e} + \mathfrak{a}(b)) = \mathfrak{a}(a) + \mathfrak{a}(a)\mathfrak{a}(b) = \mathfrak{a}(a) + \mathfrak{a}(ab) = \mathfrak{a}(a + ab).$$

We obtain (1_1) from (2_2) by virtue of the relation $\mathfrak{a}(a) \vee \mathfrak{a}'(b) = (\mathfrak{a}'(a)\mathfrak{a}(b))'$. Similarly, we use (2_1) and (1_1) to establish (1_3) and (2_3) respectively with the help of the relations

$$\mathfrak{a}'(a) \vee \mathfrak{a}'(b) = (\mathfrak{a}(a)\mathfrak{a}(b))', \qquad \mathfrak{a}'(a)\mathfrak{a}'(b) = (\mathfrak{a}(a) \vee \mathfrak{a}(b))'.$$

With the results established in Theorems 23–32 we have covered the most important algebraic properties of the classes of ideals introduced in Definition 8. We call particular attention to the fact that Theorems 29–32 may be regarded as propositions concerning the imbedding of a Boolean ring A and its isomorph $\mathfrak{P}$ in Boolean rings of special type. Theorems 31 and 32 together give a new proof of the result of Theorem 1, as we have already observed. Theorems 30 and 31 give a similar imbedding theorem. Theorems 29 and 31 yield the result most interesting from the point of view of the present paper. They show that any Boolean ring A can be imbedded in a Boolean ring B which has a unit, which has the property that its normal ideals are all

principal, and which has under the unrestricted operations of (logical) addition and multiplication many of the formal properties of an algebra consisting of all the subclasses of a fixed abstract class under the operations of forming unrestricted unions and intersections; the Boolean ring B is isomorphic to the system of normal ideals in A. Evidently, B coincides with A when every normal ideal in A is principal, so that we can obtain nothing new when we apply this imbedding theorem to the Boolean ring B. If B had *all* the properties of an algebra of classes of the indicated type, in other words, if B were isomorphic to such an algebra, the representation problem would be solved by means of this imbedding theorem. In fact, this result fails to provide a solution; and, moreover, the considerations upon which it is based do not permit us to go beyond the Boolean ring B.†

4. **Prime ideals.** The ideals in a commutative ring may also be classified in terms of the relation of inclusion or divisibility. The three important types of ideal to be considered here are divisorless ideals, prime ideals, and primary ideals. An ideal $\mathfrak{a}$ is said to be divisorless if it is distinct from the ideal $\mathfrak{e}$ consisting of all the elements of the ring and has no ideal divisors other than $\mathfrak{a}$ and $\mathfrak{e}$. An ideal $\mathfrak{a}$ is said to be prime if it is distinct from $\mathfrak{e}$ and if, whenever it contains the product ab, it contains at least one of the factors a and b. Finally, an ideal $\mathfrak{a}$ is said to be primary if it is distinct from $\mathfrak{e}$ and if, whenever it contains the product ab but not the factor a, it contains some power, b^n, of the other factor b. One of the chief problems of ideal theory is the investigation of the properties of ideal products, the factors of which belong to one or another of the three classes just described. It is important to consider when an arbitrary ideal can be represented as such a product; when such a representation is unique; and when there exist divisorless, prime, or primary ideals at all. The answers to such questions serve to develop, and also to delimit, the generalization of the familiar arithmetic theory of prime numbers to abstract rings.

In the case of Boolean rings, we shall see that the arithmetic theory of prime ideals is equivalent to the theory of representations which is our major concern. It is therefore important that we study the properties of prime ideals in considerable detail. We shall begin with a series of conditions that an ideal be prime.

THEOREM 33. *The following assertions concerning an ideal* $\mathfrak{a}$ *in a Boolean ring* A *are equivalent*: $\mathfrak{a}$ *is divisorless,* $\mathfrak{a}$ *is prime,* $\mathfrak{a}$ *is primary.*

---

† Further light is shed on these remarks by the work of MacNeille, *The Theory of Partially Ordered Sets*, Harvard doctoral dissertation (1935), and Tarski, Fundamenta Mathematicae, vol. 24 (1935), pp. 177–198. See also the end of Chapter III, §3.

The last two assertions are obviously equivalent since $b^n = b$ in accordance with Definition 1. If $\mathfrak{a}$ is a divisorless ideal and a an element not in $\mathfrak{a}$, the ideal $\mathfrak{a} \vee \mathfrak{a}(a)$ must coincide with $\mathfrak{e}$ since it is a divisor of $\mathfrak{a}$ containing an element a not in $\mathfrak{a}$. Theorem 17 and the relation $\mathfrak{a} \vee \mathfrak{a}(a) = \mathfrak{e}$ show that an arbitrary element b can be expressed in the form $b = c \vee d$ where c and d are in $\mathfrak{a}$ and $\mathfrak{a}(a)$ respectively. Since $ad = d$, we have $d + c(a+d) = ad + ac + (ac)(ad) = ac \vee ad = ab$ and hence $d = ab + c(a+d)$, where $c(a+d)$ is in $\mathfrak{a}$. It therefore follows that, when ab is in $\mathfrak{a}$, the element d, and hence also the element $b = c \vee d$, is in $\mathfrak{a}$. Thus $\mathfrak{a}$ must contain b whenever it contains ab but not a; in other words, $\mathfrak{a}$ is a prime ideal. If $\mathfrak{a}$ is a prime ideal and $\mathfrak{b}$ an ideal divisor of $\mathfrak{a}$ not coincident with $\mathfrak{a}$, we select an element a in $\mathfrak{b}$ but not in $\mathfrak{a}$ and form the ideal $\mathfrak{a} \vee \mathfrak{a}(a)$; clearly we have $\mathfrak{a} \subset \mathfrak{a} \vee \mathfrak{a}(a) \subset \mathfrak{b}$. If b is an arbitrary element we write $b = (b + ab) + ab$ where $a(b+ab) = ab + ab = 0$ is in $\mathfrak{a}$ and ab is in $\mathfrak{a}(a)$. Since a is not in $\mathfrak{a}$ while the product $a(b+ab)$ is in $\mathfrak{a}$, the prime ideal $\mathfrak{a}$ must contain $b+ab$. It follows that b is in $\mathfrak{a} \vee \mathfrak{a}(a)$. Since b was arbitrary, we have $\mathfrak{a} \vee \mathfrak{a}(a) = \mathfrak{e}$ and hence $\mathfrak{b} = \mathfrak{e}$. Thus the ideal $\mathfrak{a}$ is divisorless, as we wished to prove.

In view of this theorem we need introduce only one symbol to denote the coincident classes of divisorless, prime, and primary ideals in a Boolean ring A; we shall use the letter $\mathfrak{E}$ for this purpose.

It is now convenient to restate the definition of a prime ideal in a Boolean ring in the following equivalent form, reposing in part upon Theorem 16:

THEOREM 34. *If the elements of a Boolean ring A be distributed between two non-void disjoint classes $\mathfrak{a}$ and $\mathfrak{b}$, then in order that $\mathfrak{a}$ be a prime ideal in A the following set of conditions is necessary and sufficient*:

(1) $a \in \mathfrak{a}$ *and* $b \in \mathfrak{a}$ *imply* $a \vee b \in \mathfrak{a}$;

(2) $a \in \mathfrak{a}$ *and* $b \in A$ *imply* $ab \in \mathfrak{a}$;

(3) $a \in \mathfrak{b}$ *and* $b \in \mathfrak{b}$ *imply* $ab \in \mathfrak{b}$.

We now have the following variation of this result:

THEOREM 35. *In Theorem* 34, *the condition* (2) *may be replaced by*

(2′) $a \in \mathfrak{b}$ *and* $b \in A$ *imply* $a \vee b \in \mathfrak{b}$.

We have to prove that (2) and (2′) are equivalent in the presence of (1) and (3). To prove (2′) from (1), (2), and (3), we proceed as follows: if a is in $\mathfrak{b}$ and b is arbitrary, the assumption that $a \vee b$ is in $\mathfrak{a}$ leads through (2) and the relation $a = a \vee ba = (a \vee b)a$ to the contradiction that a is in $\mathfrak{a}$. To prove (2) from (1), (2′), and (3), we argue as follows: if a is in $\mathfrak{a}$ and b is arbitrary, the assumption that ab is in $\mathfrak{b}$ leads through (2′) and the relation $a = a \vee ab$ to the contradiction that a is in $\mathfrak{b}$.

THEOREM 36. *If the Boolean ring A has a unit, the condition* (3) *of the set* (1), (2′), (3) *of Theorem* 35 *may be replaced by*†

(3′) $a \epsilon \mathfrak{b}$ *implies* $a' \epsilon \mathfrak{a}$.

The prime ideal $\mathfrak{a}$ *contains one, but not both, of the elements* a *and* a'.

We have to prove the equivalence of (3) and (3′) in the presence of (1) and (2′). To prove (3′) from (1), (2′), (3), we proceed as follows: if a is in $\mathfrak{b}$, then the assumption that a' is in $\mathfrak{b}$ leads through (3) and the relation $0 = a'a$ to the result that 0 is in $\mathfrak{b}$ and hence through (2′) and the relation $c = c \vee 0$ to the contradiction that $\mathfrak{b}$ contains every element c. To prove (3) from (1), (2′), (3′), we argue as follows: if a and b are in $\mathfrak{b}$, the assumption that ab is in $\mathfrak{a}$ leads through (1) and (3′) to the result that $a' \vee ab$ is in $\mathfrak{a}$ and hence through (2′) and the relation $a' \vee ab = a' \vee b$ to the contradiction that $a' \vee ab$ is also in $\mathfrak{b}$. Since the class $\mathfrak{a}$ is a prime ideal under conditions (1), (2′), (3′), it contains the product $a'a = 0$ and hence contains at least one of the factors a and a'. Since $\mathfrak{a}$ cannot contain $e = a' \vee a$ without coinciding with $\mathfrak{e}$ against hypothesis, we see that $\mathfrak{a}$ cannot contain both the elements a and a'.

As an application of the criteria given in Theorems 34–36 we have the following result:

THEOREM 37. *The Boolean ring B of Theorem* 1 *contains A as a prime ideal when A has no unit; and the system* $\mathfrak{P}$ *is a prime ideal in* $\mathfrak{P}^*$ *when* $\mathfrak{P} \neq \mathfrak{P}^*$.

In Theorem 32 we have already proved that A and $\mathfrak{P}$ are ideals. In order to show that they are prime ideals it is sufficient to establish condition (3) of Theorem 34. If we consider the Boolean ring of pairs (a, α) introduced in Theorem 1, we see that $(a, \epsilon)(b, \epsilon) = (ab + a + b, \epsilon)$ and hence that the elements of B which are not in A have the property demanded by (3). Similarly, the ideals in $\mathfrak{P}^*$ but not in $\mathfrak{P}$ have by virtue of the relation $\mathfrak{a}'(a)\mathfrak{a}'(b) = \mathfrak{a}'(a \vee b)$ of Theorem 32 (2) the property demanded by (3).

We next investigate the connections between the classification of the present section and that of §3. They are indicated in the following theorem:

THEOREM 38. *In a Boolean ring A, the classes* $\mathfrak{E}$, $\mathfrak{N}$, *and* $\mathfrak{P}^*$ *satisfy the inclusion relation* $\mathfrak{E}\mathfrak{N} \subset \mathfrak{P}^*$. *More precisely, an ideal* $\mathfrak{p}$ *is both prime and normal if and only if* $\mathfrak{p} = \mathfrak{a}'(a)$ *where a is an atomic element; and a prime ideal* $\mathfrak{p}$ *fails to be normal if and only if* $\mathfrak{p}' = \mathfrak{o}$.

† This theorem should be compared with recent work of Huntington, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 127–136 and pp. 137–142. It is easily seen that a Boolean ring with unit together with two subclasses $\mathfrak{a}$ and $\mathfrak{b}$ possessing properties (1), (2′), and (3′) is a system satisfying Huntington's postulates P1–P11 (on pp. 139–140); and, conversely, that any system satisfying those postulates is a Boolean ring with unit together with such subclasses $\mathfrak{a}$ and $\mathfrak{b}$. Huntington's postulates may therefore be regarded as postulates for a Boolean ring with unit together with a prime ideal.

If $\mathfrak{p}$ is any prime ideal, the fact that $\mathfrak{p}$ is divisorless taken together with the fact that $\mathfrak{p}'' \supset \mathfrak{p}$ shows that one of the relations $\mathfrak{p}'' = \mathfrak{p}$, $\mathfrak{p}'' = \mathfrak{e}$ must be true. If $\mathfrak{p}'' = \mathfrak{e}$, then $\mathfrak{p}$ is not normal and the relation $\mathfrak{p}' = \mathfrak{o}$ is valid. If $\mathfrak{p}'' = \mathfrak{p}$, then $\mathfrak{p}$ is normal and $\mathfrak{p}' \neq \mathfrak{o}$. When $\mathfrak{p}' \neq \mathfrak{o}$, we let a be an *arbitrary* element in $\mathfrak{p}'$ such that $a \neq 0$. Since $\mathfrak{p}' \supset \mathfrak{a}(a)$ and $\mathfrak{a}'(a) \neq \mathfrak{e}$, we see that $\mathfrak{p} = \mathfrak{p}'' \subset \mathfrak{a}'(a)$ and hence that $\mathfrak{p} = \mathfrak{a}'(a)$. This result shows that $\mathfrak{p}' = \mathfrak{a}(a)$ contains just one element a distinct from 0; in other words, that $b < a$ implies $b = 0$ or $b = a$. The element a is therefore atomic in accordance with Definition 3. To complete our proof, we must show that any ideal $\mathfrak{a}'(a)$, where a is an atomic element, is both prime and normal. Theorem 23 shows that $\mathfrak{a}'(a)$ is normal. To show that $\mathfrak{a}'(a)$ is prime we proceed as follows: if b and c are elements not belonging to $\mathfrak{a}'(a)$, we have $ab \neq 0$, $ac \neq 0$, and hence, by virtue of the fact that a is an atomic element, $ab = a$, $ac = a$; in consequence, we have $a(bc) = (ab)(ac) = aa = a \neq 0$ and conclude that bc is not in $\mathfrak{a}'(a)$; with the help of Theorem 34 (3), we thus find that $\mathfrak{p} = \mathfrak{a}'(a)$ is a prime ideal.

We shall now turn to the consideration of prime ideals in connection with operations upon ideals and the inclusion or divisibility relation between ideals. We first have

THEOREM 39. *If $\mathfrak{p}$ is a prime ideal in a Boolean ring A and $\mathfrak{a}$ is an arbitrary ideal, then*

(1) *the relations $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a}\mathfrak{p} = \mathfrak{p}$, $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{p}$ are equivalent;*

(2) *the relations $\mathfrak{a} \not\subset \mathfrak{p}$, $\mathfrak{a}\mathfrak{p} \neq \mathfrak{p}$, $\mathfrak{a} \vee \mathfrak{p} \neq \mathfrak{p}$ are equivalent;*

(3) *one and only one of these two sets of mutually equivalent relations is valid. In case $\mathfrak{p}$ is normal, the relations $\mathfrak{a}\mathfrak{p}' = \mathfrak{o}$ and $\mathfrak{a}\mathfrak{p}' = \mathfrak{p}'$, where $\mathfrak{p}' \neq \mathfrak{o}$, are respectively equivalent to the relations in* (1) *and* (2) *respectively.*

We first prove the equivalence of the relations (1): $\mathfrak{a} \subset \mathfrak{p}$ obviously implies $\mathfrak{a}\mathfrak{p} = \mathfrak{a}$; $\mathfrak{a}\mathfrak{p} = \mathfrak{a}$ implies $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{a}\mathfrak{p} \vee \mathfrak{p} = \mathfrak{p}$; and $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{p}$ obviously implies $\mathfrak{a} \subset \mathfrak{p}$. We next observe that one and only one of the relations $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{p}$, $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{e}$ is valid, since $\mathfrak{p}$ is divisorless and $\mathfrak{a} \vee \mathfrak{p}$ is a divisor of $\mathfrak{p}$. Consequently, the relations (2) are simply the negations of the mutually equivalent relations in (1). Thus (2) and (3) both follow from (1). In case $\mathfrak{p}$ is normal, we know from Theorem 38 that $\mathfrak{p}$ is semiprincipal and that $\mathfrak{p}' \neq \mathfrak{o}$. Thus $\mathfrak{a}\mathfrak{p}' = \mathfrak{o}$ implies $\mathfrak{a} = \mathfrak{a}\mathfrak{e} = \mathfrak{a}(\mathfrak{p} \vee \mathfrak{p}') = \mathfrak{a}\mathfrak{p}$; and $\mathfrak{a}\mathfrak{p}' \neq \mathfrak{o}$ implies $\mathfrak{p} \subset \mathfrak{p} \vee \mathfrak{a}\mathfrak{p}' \neq \mathfrak{p}$, $\mathfrak{p} \vee \mathfrak{a}\mathfrak{p}' = \mathfrak{e}$, $\mathfrak{p} \vee \mathfrak{a} = \mathfrak{p} \vee \mathfrak{a}(\mathfrak{p} \vee \mathfrak{p}') = (\mathfrak{p} \vee \mathfrak{a}\mathfrak{p}) \vee \mathfrak{a}\mathfrak{p}' = \mathfrak{p} \vee \mathfrak{a}\mathfrak{p}' = \mathfrak{e}$, and $\mathfrak{a}\mathfrak{p}' = (\mathfrak{p} \vee \mathfrak{a}\mathfrak{p}')\mathfrak{p}' = \mathfrak{e}\mathfrak{p}' = \mathfrak{p}'$. The final statement of the theorem is thus evident.

THEOREM 40. *If $\mathfrak{p}$ is a prime ideal divisor of the ideal product $\mathfrak{a}\mathfrak{b}$ in a Boolean ring A, then $\mathfrak{p}$ is a divisor of at least one of the factors $\mathfrak{a}$ and $\mathfrak{b}$; in other words, $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b}$ implies $\mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \mathfrak{b}$.*

If $\mathfrak{p}$ divides neither $\mathfrak{a}$ nor $\mathfrak{b}$, we have $\mathfrak{a} \vee \mathfrak{p} = \mathfrak{b} \vee \mathfrak{p} = e$, in accordance with the preceding theorem. By Theorem 18 (6), we see that the relation $\mathfrak{ab} \subset \mathfrak{p}$ leads to the absurd result $\mathfrak{p} = \mathfrak{ab} \vee \mathfrak{p} = (\mathfrak{a} \vee \mathfrak{p})(\mathfrak{b} \vee \mathfrak{p}) = ee = e$. Hence $\mathfrak{p}$ must divide $\mathfrak{a}$ or $\mathfrak{b}$. We point out that a corresponding result does not hold for infinite ideal products, as will be seen later. The failure to generalize Theorem 18 (6) to infinite products accounts for the distinction which we have to make here.

THEOREM 41. *If $\mathfrak{p}$ is a prime ideal in a Boolean ring A and $\mathfrak{a}$ is an arbitrary ideal, then at least one of the relations $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a}' \subset \mathfrak{p}$ is valid; if $\mathfrak{a}$ is simple, then only one is valid.*

Since $\mathfrak{p} \supset \mathfrak{o} = \mathfrak{a}'\mathfrak{a}$, at least one of the relations must hold by virtue of Theorem 40. If $\mathfrak{a}$ is simple and if both relations were to hold, we should have $\mathfrak{p} \supset \mathfrak{a} \vee \mathfrak{a}' = e$, $\mathfrak{p} = e$, against hypothesis.

In accordance with the introductory remarks of the present section and the result reached in Theorem 40, we may formulate for consideration the following statement:

FUNDAMENTAL PROPOSITION OF IDEAL ARITHMETIC. *In a Boolean ring A, every ideal other than $\mathfrak{e}$ is the product of all its prime ideal divisors.*

Our comments upon Theorem 40 indicate the possibility that an ideal may be expressible as the product merely of some, rather than of all, of its prime ideal divisors; and we shall see later that this possibility is realized in general. Now it is clear that the Fundamental Proposition of Ideal Arithmetic, and, indeed, all the preceding theorems concerning prime ideals, lack either meaning or content unless we can establish the following result:

FUNDAMENTAL EXISTENCE PROPOSITION. *In a Boolean ring A containing at least two elements, there exists at least one prime ideal.*

The exclusion of one-element Boolean rings is essential here since such a ring contains only the ideal $\mathfrak{o} = \mathfrak{e}$, which is not prime. We shall prove this proposition in Chapter IV, by means of transfinite methods; and we shall show that, if this proposition be true for every A, then the Fundamental Proposition of Ideal Arithmetic is true also for every A. The relation of these two central propositions to the theory of representations will be treated in Chapter IV.

5. **Congruences, ideals, and homomorphisms.** We must now consider the specialization of the general properties of ring-homomorphisms to the case of Boolean rings. We may first recall the principal results for arbitrary commutative rings. We denote a homomorphism from A to B by $A \rightarrow B$, referring to B as homomorphic to A or as a homomorph of A; and similarly we denote

an isomorphism from A to B by $A \longleftrightarrow B$, referring to B as isomorphic to A or as an isomorph of A. Any system with double composition homomorphic to a ring (or to a commutative ring) is itself a ring (or commutative ring). Here we confine our attention to the case of commutative rings. As we have previously remarked the determination of the homomorphs of an arbitrary algebraic system reduces essentially to the determination of all the congruences in the system. In the case of commutative rings, it is found that every congruence is a modular congruence. The modular congruences in a ring A are those defined in terms of the ideals of A by setting $a \equiv b$ if and only if $a-b$ is an element of a specified ideal $\mathfrak{a}$; in order to exhibit the ideal $\mathfrak{a}$ in our notation, we write $a \equiv b \pmod{\mathfrak{a}}$. It is easily verified that the modular congruences in a ring are congruences in the sense previously indicated. The proof that an arbitrary congruence is modular is easily given: the class $\mathfrak{a}$ of all elements a such that $a \equiv 0$ is an ideal since, if it contains a and b, it contains $a-b$ by virtue of the relations $a-b \equiv 0-0 \equiv 0$, and since, if it contains a, it contains ac by virtue of the relations $ac \equiv 0c \equiv 0$; and the relation $a \equiv b$ is equivalent to the relation $a-b \equiv 0$ and hence to the relation $a-b \in \mathfrak{a}$. If C is a congruence with the ideal $\mathfrak{a}$ as its modulus, we can introduce C as the fundamental equality in the given ring A so as to obtain the homomorph A^C, as previously indicated; we can also group the elements of A in classes of mutually congruent elements (mod $\mathfrak{a}$) and define the operations $+$ and for these classes in the usual way so as to obtain the quotient ring $A/\mathfrak{a}$; and we see at once that A^C and $A/\mathfrak{a}$ are isomorphic. The chief theorem concerning the homomorphs of a ring A now asserts that every such homomorph is an isomorph of A^C and of $A/\mathfrak{a}$, where C is the congruence (mod $\mathfrak{a}$) and $\mathfrak{a}$ is the ideal consisting of all the elements of A which are carried into the zero element of the given homomorph.

We begin the consideration of Boolean rings with the following result:

THEOREM 42. *If the algebraic system B is homomorphic to a Boolean ring A with respect to the pair of operations $+$ and $\cdot$ or with respect to the pair of operations $\vee$ and $\cdot$, then B is homomorphic to A with respect to all three of the operations $+$, $\vee$, and $\cdot$; and B is a Boolean ring. If the algebraic system B is homomorphic to a Boolean ring A with unit with respect to the pair of operations $+$ and $\cdot$, with respect to the pair of operations $\vee$ and $'$, or with respect to the pair of operations $\vee$ and $\cdot$, then B is homomorphic to A with respect to all four of the operations $+$, $\vee$, $\cdot$, and $'$; and B is a Boolean ring with unit. The homomorphism $A \rightarrow B$ carries the zero element of A into the zero element of B, and the unit element of A, if any exists, into the unit element of B.*

The first statement of the theorem evidently refers to the two character-

izations of Boolean rings presented in Theorem 4. If B is a system with double composition homomorphic to a Boolean ring A under the operations $+$ and $\cdot$, then B is certainly a ring under the corresponding operations $+$ and $\cdot$ respectively. The law of idempotence is carried over from A to B by the given homomorphism, so that B is a Boolean ring. If the operation $\vee$ is now introduced in A and in B through the equation $a \vee b = a+b+ab$, the behavior of the homomorphism relative to the operations $+$ and $\cdot$ governs its behavior relative to the operation $\vee$; we thus see that the given homomorphism can be extended to cover the operation $\vee$ as well as the operations $+$ and $\cdot$, since the image in B of the element $a \vee b$ in A is evidently equal to the result of applying the operation $\vee$ to the images in B of the elements a and b respectively. On the other hand, if B is homomorphic to A under the operations $\vee$ and $\cdot$, we can show that the properties (1_1), (2_2), (3_1), (4_1), (5_1), (5_2), (6_1) and (6_2) hold in B as well as in A. All of these properties except (5_1) and (5_2) are identities in A and are therefore carried over by the homomorphism as identities in B. For example, if a^* is an arbitrary element of B and 0^* is the image in B of the zero element 0 in A, we can show that $a^* \vee 0^* = a^*$ in B: for there exists an element a in A which has a^* as its image in B, and the relation $a \vee 0 = a$ is carried by the given homomorphism into the relation to be proved. We may thus confine our attention to properties (5_1) and (5_2). If a^* and b^* are arbitrary elements in B satisfying the relation $b^*a^* = a^*$, we have to show that the system $x^* \vee a^* = b^*$, $x^*a^* = 0^*$ has a solution in B. There exist elements c and b in A which have a^* and b^* as their respective images in B under the given homomorphism. If we put $a = bc$, then $ba = b(bc) = bc = a$; and the image of a is $b^*a^* = a^*$. Consequently, the equations $x \vee a = b$, $xa = 0$ have a solution x. If we now take x^* as the image in B of the element x, we see that the equations satisfied by x in A are carried by the given homomorphism into the equations under consideration in B, and that x^* is the desired solution of these equations. Thus B is a generalized Boolean algebra and hence a Boolean ring in terms of the operations $+$ and $\cdot$, as shown in Theorem 4. We have to show that the image of the element $a+b$ in A is equal to the element a^*+b^* in B, where a^* and b^* are the images of a and b respectively. Since $a+b$ is the unique solution of the system $x \vee ab = a \vee b$, $x(ab) = 0$, we see that its image is a solution of the equations $x^* \vee a^*b^* = a^* \vee b^*$, $x^*(a^*b^*) = 0^*$; and since the latter equations have a^*+b^* as their unique solution in B, the desired result follows immediately. The homomorphism $A \rightarrow B$ can thus be extended to cover the operation $+$ as well as the operations $\vee$ and with respect to which it was originally assumed to hold. The remaining statements of the theorem refer in a similar way to the characterizations of Boolean rings with unit presented in Theorems 2 and 4;

they can be established by similar, and slightly simpler, arguments. If A and B are Boolean rings, the homomorphism $A \rightarrow B$ carries the element 0 in A into an element 0^* in B which has the characteristic property of the zero element of B: for if a^* is any element of B and a an element of A with a^* as its image, the relation $a+0=a$ is carried by the homomorphism into the relation $a^*+0^*=a^*$. Similarly if A has a unit e, the homomorphism $A \rightarrow B$ carries e into an element e^* in B which has the characteristic property of a unit element in B: for if a^* is any element of B and a an element of A with a^* as its image, the relation $ea=a$ is carried by the homomorphism into the relation $e^*a^*=a^*$.

We next state the result which determines all the homomorphs of a Boolean ring; the proof has already been sketched above.

THEOREM 43. *In order that a Boolean ring B be homomorphic to a given Boolean ring A, it is necessary and sufficient that B be isomorphic to some quotient ring $A/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in A; in particular, the homomorphism $A \rightarrow B$ determines $\mathfrak{a}$ as the class of all elements in A which have the zero element in B as their image.*

We may consider also the characterization of all congruences in a Boolean ring. We have the following result:

THEOREM 44. *The only congruences in a Boolean ring A are the modular congruences. In order that $a \equiv b \pmod{\mathfrak{a}}$, where $\mathfrak{a}$ is an ideal in A, it is necessary and sufficient that $a+b$ belong to $\mathfrak{a}$, or that there exist elements c and d in $\mathfrak{a}$ for which $a \vee c = b \vee d$.*

That the only congruences in a commutative ring, and hence in a Boolean ring, are modular congruences, we have already proved in our introductory remarks. The relation $a+b=a-b$, which holds by virtue of Theorem 1, shows that $a \equiv b \pmod{\mathfrak{a}}$ if and only if $a+b$ belongs to $\mathfrak{a}$. Thus, if $a \equiv b \pmod{\mathfrak{a}}$, we have $a \vee (a+b) = a+(a+b)+a(a+b) = a+b+ab = a \vee b = b \vee (a+b)$ and hence $a \vee c = b \vee d$ where $c=d=a+b$ and $a+b$ is in $\mathfrak{a}$. On the other hand, if $a \vee c = b \vee d$ where c and d are in $\mathfrak{a}$, we have $a+(c+ac)=b+(d+bd)$ where $c+ac$ and $d+bd$ are in $\mathfrak{a}$ and hence $a+b=(c+ac)+(d+bd)$ where the element on the right is in $\mathfrak{a}$; and we conclude that $a \equiv b \pmod{\mathfrak{a}}$.

We shall next consider the behavior of subrings and ideals of a Boolean ring under an arbitrary homomorphism.

THEOREM 45. *If A_1 and A_2 are Boolean rings, if $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are the classes of all subrings of A_1 and of A_2 respectively, and if the homomorphism $A_1 \rightarrow A_2$ determines the ideal $\mathfrak{a}_1$ in A, then the indicated homomorphism induces a homomorphism $\mathfrak{A}_1 \rightarrow \mathfrak{A}_2$ with respect to the operation of unrestricted addition. In par-*

ticular, the correspondences $A_1 \to A_2$, $\mathfrak{A}_1 \to \mathfrak{A}_2$ *have the following properties*:

(1) *if* $\mathfrak{b}_1$ *is a subring of* A_1, *the images of its elements under the homomorphism* $A_1 \to A_2$ *constitute a subring* $\mathfrak{b}_2$ *of* A_2 *corresponding to it under the homomorphism* $\mathfrak{A}_1 \to \mathfrak{A}_2$;

(2) *if* $\mathfrak{b}_1$ *is the subring generated by a non-void subclass* $\mathfrak{s}_1$ *of* A_1, *then its image* $\mathfrak{b}_2$ *under the homomorphisms* $A_1 \to A_2$ *and* $\mathfrak{A}_1 \to \mathfrak{A}_2$ *is the subring generated by the class* $\mathfrak{s}_2$ *of all images of elements of* $\mathfrak{s}_1$;

(3) *if* $\mathfrak{b}_2$ *is a subring of* A_2, *the class* $\mathfrak{b}_1$ *of all elements of* A_1 *with images in* $\mathfrak{b}_2$ *is a subring of* A_1 *with* $\mathfrak{b}_2$ *as its image under the homomorphisms* $A_1 \to A_2$ *and* $\mathfrak{A}_1 \to \mathfrak{A}_2$;

(4) *if* $\mathfrak{b}_1$ *and* $\mathfrak{c}_1$ *are subrings of* A_1 *with respective images* $\mathfrak{b}_2$ *and* $\mathfrak{c}_2$ *in* A_2, *then the relations* $\mathfrak{b}_1 \vee \mathfrak{a}_1 = \mathfrak{c}_1 \vee \mathfrak{a}_1$ *and* $\mathfrak{b}_2 = \mathfrak{c}_2$ *are equivalent.*

The proof is outlined essentially in (1), (2), and (3). The homomorphism $A_1 \to A_2$ takes the subring $\mathfrak{b}_1$ into a subclass $\mathfrak{b}_2$ of A_2. If a_2 and b_2 are in $\mathfrak{b}_2$, they are images respectively of elements a_1 and b_1 in $\mathfrak{b}_1$. It follows that a_2+b_2 and a_2b_2 are the images respectively of a_1+b_1 and a_1b_1 in $\mathfrak{b}_1$ and hence belong to $\mathfrak{b}_2$. Thus $\mathfrak{b}_2$ is a subring of A_2. The correspondence from $\mathfrak{A}_1$ to part of $\mathfrak{A}_2$ thus set up proves to be the desired homomorphism $\mathfrak{A}_1 \to \mathfrak{A}_2$. By the part of (1) now established, we see that the subring $\mathfrak{b}_1$ generated by a non-void subclass $\mathfrak{s}_1$ of A_1 is carried into a subring $\mathfrak{c}_2$ of A_2 containing the image of $\mathfrak{s}_1$, which we have denoted by $\mathfrak{s}_2$. Hence $\mathfrak{c}_2$ contains the subring $\mathfrak{b}_2$ generated by $\mathfrak{s}_2$. On the other hand, every element of $\mathfrak{c}_2$ is equal to a polynomial in terms of elements of $\mathfrak{s}_2$, by virtue of the construction of $\mathfrak{b}_1$ in terms of $\mathfrak{s}_1$. Hence $\mathfrak{c}_2$ is contained in $\mathfrak{b}_2$. We see therefore that $\mathfrak{b}_2 = \mathfrak{c}_2$, as we wished to prove. By the parts of (1) and (2) now established, we see that the class $\mathfrak{b}_1$ of all elements in A_1 with images in a given subring $\mathfrak{b}_2$ of A_2 generates a subring $\mathfrak{c}_1$ whose image in A_2 is the subring generated by $\mathfrak{b}_2$ and is thus $\mathfrak{b}_2$ itself. By definition, $\mathfrak{b}_1$ contains $\mathfrak{c}_1$. Hence $\mathfrak{b}_1$ coincides with $\mathfrak{c}_1$ and is therefore a subring of A_1 with $\mathfrak{b}_2$ as its image. By the part of (3) thus established, we see that the correspondence $\mathfrak{A}_1 \to \mathfrak{A}_2$ previously set up is a univocal correspondence taking the entire class $\mathfrak{A}_1$ into the entire class $\mathfrak{A}_2$. In view of the part of (2) already proved and in view of the definition of the sum of subrings as the least subring containing all the summands, we now see that the correspondence $\mathfrak{A}_1 \to \mathfrak{A}_2$ is a homomorphism with respect to the operation of unrestricted addition. All parts of the theorem, except (4), are thus proved. To establish (4), we first note that the image of the ideal $\mathfrak{a}_1$ under the correspondence $\mathfrak{A}_1 \to \mathfrak{A}_2$ is the ideal $\mathfrak{o}_2$ consisting of the zero element in A_2 alone. If $\mathfrak{b}_1$ and $\mathfrak{c}_1$ have the respective images $\mathfrak{b}_2$ and $\mathfrak{c}_2$ under the homomorphism $\mathfrak{A}_1 \to \mathfrak{A}_2$, then $\mathfrak{b}_1 \vee \mathfrak{a}_1$ and $\mathfrak{c}_1 \vee \mathfrak{a}_1$ have the respective images $\mathfrak{b}_2 \vee \mathfrak{o}_2 = \mathfrak{b}_2$, and $\mathfrak{c}_2 \vee \mathfrak{o}_2 = \mathfrak{c}_2$. It fol-

lows that $\mathfrak{b}_1 \vee \mathfrak{a}_1 = \mathfrak{c}_1 \vee \mathfrak{a}_1$ implies $\mathfrak{b}_2 = \mathfrak{c}_2$. Furthermore if a_1 is any element with image b_2 in $\mathfrak{b}_2$, then there exists an element b in $\mathfrak{b}_1$ which also has b_2 as its image. The fact that a_1 and b_1 have the same image implies that $a_1 \equiv b_1 \pmod{\mathfrak{a}_1}$, and hence that $a_1 = b_1 + (a_1 + b_1)$ belongs to $\mathfrak{b}_1 \vee \mathfrak{a}_1$. Thus $\mathfrak{b}_1 \vee \mathfrak{a}_1$ is the class of all elements in A_1 with images in $\mathfrak{b}_2$. Similarly, $\mathfrak{c}_1 \vee \mathfrak{a}_1$ is the class of all elements in A_1 with images in $\mathfrak{c}_2$. In consequence, $\mathfrak{b}_2 = \mathfrak{c}_2$ implies $\mathfrak{b}_1 \vee \mathfrak{a}_1 = \mathfrak{c}_1 \vee \mathfrak{a}_1$. This completes the proof of (4). Evidently the homomorphism $\mathfrak{A}_1 \to \mathfrak{A}_2$ determines a relation of congruence which is explicitly characterized by (4). We point out that the homomorphism $\mathfrak{A}_1 \to \mathfrak{A}_2$ cannot in general be extended to hold with respect to the multiplication of subrings. If $\mathfrak{a}_1$ is an ideal other than $\mathfrak{o}_1$ or $\mathfrak{e}_1$, we may determine elements b_1 and c_1 in A_1 such that $b_1 \neq c_1$, $b_1 \not\equiv 0_1 \pmod{\mathfrak{a}_1}$, $c_1 \not\equiv 0_1 \pmod{\mathfrak{a}_1}$, $b_1 \equiv c_1 \pmod{\mathfrak{a}_1}$. If A_2 is isomorphic to $A_1/\mathfrak{a}_1$, then the homomorphism $A_1 \to A_2$ takes b_1 and c_1 into the same element $b_2 \neq 0_2$. If now $\mathfrak{b}_1$ and $\mathfrak{c}_1$ are the subrings consisting of 0_1, b_1 and of 0_1, c_1 respectively, and if $\mathfrak{b}_2$ is the subring consisting of 0_2 and b_2, we see that $\mathfrak{b}_1\mathfrak{c}_1 = \mathfrak{o}_1$, $\mathfrak{b}_1 \to \mathfrak{b}_2$, $\mathfrak{c}_2 \to \mathfrak{b}_2$, $\mathfrak{b}_1\mathfrak{c}_1 \to \mathfrak{o}_2 \neq \mathfrak{b}_2 = \mathfrak{b}_2\mathfrak{b}_2$. This example indicates the impossibility of so extending the homomorphism.

THEOREM 46. *If A_1 and A_2 are Boolean rings, if $\mathfrak{J}_1$ and $\mathfrak{J}_2$ are the classes of all ideals in A_1 and in A_2 respectively, and if the homomorphism $A_1 \to A_2$ determines the ideal $\mathfrak{a}_1$ in A_1, then the indicated homomorphism induces a homomorphism $\mathfrak{J}_1 \to \mathfrak{J}_2$ with respect to the operations of unrestricted addition and finite multiplication. In particular, the correspondences $A_1 \to A_2$ and $\mathfrak{J}_1 \to \mathfrak{J}_2$ have properties* (1)–(4) *of Theorem* 45 *with the term "subring" everywhere replaced by the term "ideal."*

Since ideals are subrings and since the sum of ideals is an ideal in accordance with Theorem 18, we can prove all assertions of the present theorem, except (2) and those dealing with ideal multiplication, by showing that the correspondence $\mathfrak{A}_1 \to \mathfrak{A}_2$ takes $\mathfrak{J}_1$ into $\mathfrak{J}_2$ and then specializing Theorem 45 in the obvious way. Now, if $\mathfrak{b}_1$ is an ideal in A_1, its image $\mathfrak{b}_2$ in A_2 is a subring. Furthermore, if b_2 and c_2 are elements of $\mathfrak{b}_2$ and A_2 respectively, there exist elements b_1 and c_1 in $\mathfrak{b}_1$ and A_1 respectively with b_2 and c_2 as their respective images; and hence b_2c_2 is the image of b_1c_1, an element in $\mathfrak{b}_1$, and accordingly belongs to $\mathfrak{b}_2$. Thus $\mathfrak{b}_2$ is an ideal. On the other hand, if $\mathfrak{b}_2$ is an ideal in A_2, the class $\mathfrak{b}_1$ of all elements in A_1 with images in $\mathfrak{b}_2$ is a subring. Also, if b_1 and c_1 are in $\mathfrak{b}_1$ and A_1 respectively, their respective images b_2 and c_2 belong to $\mathfrak{b}_2$ and A_2 respectively; and hence b_1c_1 has the image b_2c_2 in $\mathfrak{b}_2$ and accordingly belongs to $\mathfrak{b}_1$. Thus $\mathfrak{b}_1$ is an ideal. The correspondence $\mathfrak{A}_1 \to \mathfrak{A}_2$ takes $\mathfrak{J}_1$ into $\mathfrak{J}_2$, as we wished to prove. We next discuss (2). The ideal $\mathfrak{a}_1(\mathfrak{s}_1)$ generated by a non-void subclass $\mathfrak{s}_1$ of A_1 has as its image an ideal $\mathfrak{b}_2$ which contains $\mathfrak{s}_2$, the

image of $\mathfrak{s}_1$. It follows that $\mathfrak{b}_2$ contains the ideal $\mathfrak{a}_2(\mathfrak{s}_2)$ generated by $\mathfrak{s}_2$. On the other hand, the class $\mathfrak{b}_1$ of all elements in A_1 with images in $\mathfrak{a}_2(\mathfrak{s}_2)$ is an ideal which contains $\mathfrak{s}_1$ and hence also $\mathfrak{a}_1(\mathfrak{s}_1)$. It follows that $\mathfrak{a}_2(\mathfrak{s}_2)$ contains $\mathfrak{b}_2$. We therefore conclude that $\mathfrak{a}_2(\mathfrak{s}_2)$ is the image of $\mathfrak{a}_1(\mathfrak{s}_1)$, as we wished to prove. We still have to establish the assertion that the correspondence $\mathfrak{J}_1 \rightarrow \mathfrak{J}_2$ is a homomorphism with respect to finite multiplication. Since it is evident that the image of the product $\mathfrak{b}_1\mathfrak{c}_1$ of ideals $\mathfrak{b}_1$ and $\mathfrak{c}_1$ in A_1 is an ideal contained in the images $\mathfrak{b}_2$ and $\mathfrak{c}_2$ of $\mathfrak{b}_1$ and $\mathfrak{c}_1$ respectively, we see that the image is contained also in the product $\mathfrak{b}_2\mathfrak{c}_2$. On the other hand, if a_2 is an arbitrary element of $\mathfrak{b}_2\mathfrak{c}_2$, it is expressible in the form $a_2 = b_2c_2$, where b_2 is in $\mathfrak{b}_2$ and c_2 in $\mathfrak{c}_2$, as we have proved in Theorem 18; and the elements b_2 and c_2 are the images of elements b_1 and c_1 respectively in $\mathfrak{b}_1$ and $\mathfrak{c}_1$ respectively. Thus a_2 is the image of the element b_1c_1 in $\mathfrak{b}_1\mathfrak{c}_1$ and hence belongs to the image of $\mathfrak{b}_1\mathfrak{c}_1$. We conclude therefore that the image of $\mathfrak{b}_1\mathfrak{c}_1$ coincides with the product $\mathfrak{b}_2\mathfrak{c}_2$ of the images of $\mathfrak{b}_1$ and $\mathfrak{c}_1$ respectively, and thereby bring the proof to a close.

We may point out that the homomorphism $\mathfrak{J}_1 \rightarrow \mathfrak{J}_2$ cannot be extended to the operation of orthocomplementation. This we shall show by examples cited in connection with the following theorem.

Our next result deals with the behavior of ideals relative to the classification of §3. We have

THEOREM 47. *If A_1 and A_2 are Boolean rings, the homomorphism $A_1 \rightarrow A_2$ carries every principal (semiprincipal, simple) ideal in A_1 into a principal (semiprincipal, simple) ideal in A_2; but it may carry a normal ideal in A_1 into a non-normal ideal in A_2.*

If $\mathfrak{b}_1$ is a principal ideal in A_1, its image in A_2 is an ideal which, considered as a Boolean ring, is homomorphic to $\mathfrak{b}_1$ and hence has a unit in accordance with Theorem 42. It follows that $\mathfrak{b}_2$ is a principal ideal in A_2. We pass next to the case of a simple ideal $\mathfrak{b}_1$ in A_1. The images of $\mathfrak{b}_1$ and $\mathfrak{b}_1'$ in A_2 are ideals $\mathfrak{b}_2$ and $\mathfrak{c}_2$ respectively. The relation $\mathfrak{b}_1\mathfrak{b}_1' = \mathfrak{o}_1$ implies the relation $\mathfrak{b}_2\mathfrak{c}_2 = \mathfrak{o}_2$ in accordance with Theorem 46 and hence the relation $\mathfrak{c}_2 \subset \mathfrak{b}_2'$. The relation $\mathfrak{b}_1 \vee \mathfrak{b}_1' = \mathfrak{e}_1$ similarly implies the relation $\mathfrak{b}_2 \vee \mathfrak{c}_2 = \mathfrak{e}_2$. Thus we have $\mathfrak{b}_2 \vee \mathfrak{b}_2' \supset \mathfrak{b}_2 \vee \mathfrak{c}_2 = \mathfrak{e}_2$, $\mathfrak{b}_2 \vee \mathfrak{b}_2' = \mathfrak{e}_2$. It follows that $\mathfrak{b}_2$ is a simple ideal. In case $\mathfrak{b}_1$ is semiprincipal but not principal, $\mathfrak{b}_1'$ is principal. The image $\mathfrak{b}_2$ of $\mathfrak{b}_1$ is simple by the result just established; and the image $\mathfrak{c}_2$ of $\mathfrak{b}_1'$ is principal. Thus $\mathfrak{b}_2' = \mathfrak{b}_2'\mathfrak{e}_2 = \mathfrak{b}_2'(\mathfrak{b}_2 \vee \mathfrak{c}_2) = \mathfrak{b}_2'\mathfrak{c}_2 = \mathfrak{c}_2$ by virtue of the relations noted above. Since $\mathfrak{b}_2$ is simple and $\mathfrak{b}_2'$ is principal, it follows that $\mathfrak{b}_2 = \mathfrak{b}_2''$ is semiprincipal, as we wished to prove. In order to show that similar results do not hold in the case of normal ideals, let us consider the case where the homomorphism $A_1 \rightarrow A_2$ determines an ideal $\mathfrak{a}_1$ which is normal but not simple, with a view to

showing that the normal ideal $\mathfrak{a}_1'$ is carried into a non-normal ideal $\mathfrak{b}_2$. The homomorphism carries $\mathfrak{a}_1$ into $\mathfrak{o}_2$, $\mathfrak{a}_1 \vee \mathfrak{a}_1'$ into $\mathfrak{b}_2$. We shall show that $\mathfrak{b}_2 \neq \mathfrak{e}_2$, $\mathfrak{b}_2' = \mathfrak{o}_2$, so that the relation $\mathfrak{b}_2'' = \mathfrak{b}_2$ is impossible. It is then clear that $\mathfrak{b}_2$ is not normal. Since $\mathfrak{a}_1 \vee \mathfrak{a}_1' \neq \mathfrak{e}_1$, we see with the aid of Theorem 46 (4) that $\mathfrak{b}_2 \neq \mathfrak{e}_2$. Now let $\mathfrak{c}_1$ be the class of all elements in A_1 with images in $\mathfrak{b}_2'$. By virtue of Theorem 46, the image of the ideal $\mathfrak{c}_1(\mathfrak{a}_1 \vee \mathfrak{a}_1')$ is $\mathfrak{b}_2'(\mathfrak{o}_2 \vee \mathfrak{b}_2) = \mathfrak{o}_2$. Hence we have $\mathfrak{c}_1(\mathfrak{a}_1 \vee \mathfrak{a}_1') \subset \mathfrak{a}_1$, $\mathfrak{c}_1\mathfrak{a}_1' = \mathfrak{c}_1(\mathfrak{a}_1 \vee \mathfrak{a}_1')\mathfrak{a}_1' \subset \mathfrak{a}_1\mathfrak{a}_1' = \mathfrak{o}_1$, $\mathfrak{c}_1\mathfrak{a}_1' = \mathfrak{o}_1$, $\mathfrak{c}_1 \subset \mathfrak{a}_1'' = \mathfrak{a}_1$, and $\mathfrak{b}_2' = \mathfrak{o}_2$, as we wished to show. The fact that the homomorphism $A_1 \rightarrow A_2$ does not always carry normal ideals into normal ideals shows that the induced homomorphism $\mathfrak{Z}_1 \rightarrow \mathfrak{Z}_2$ does not always hold relative to the operation of orthocomplementation, since an ideal $\mathfrak{b}_1$ in A_1 may satisfy the relation $\mathfrak{b}_1'' = \mathfrak{b}_1$ and yet have an image $\mathfrak{b}_2$ for which $\mathfrak{b}_2'' \neq \mathfrak{b}_2$.

We shall also consider the behavior of prime ideals under a homomorphism, obtaining the following result:

THEOREM 48. *If A_1 and A_2 are Boolean rings and if $\mathfrak{a}_1$ is the ideal determined in A_1 by the homomorphism $A_1 \rightarrow A_2$, then the indicated homomorphism carries a prime ideal $\mathfrak{p}_1$ in A_1 into an ideal $\mathfrak{p}_2$ in A_2 which is prime or coincides with $\mathfrak{e}_2$ according as $\mathfrak{p}_1$ contains $\mathfrak{a}_1$ or not. If $\mathfrak{p}_2$ is a prime ideal in A_2, the class $\mathfrak{p}_1$ of all elements in A_1 with images in $\mathfrak{p}_2$ is a prime ideal in A_1.*

If $\mathfrak{p}_1$ is prime, then $\mathfrak{p}_1 \vee \mathfrak{a}_1 = \mathfrak{p}_1$ or $\mathfrak{p}_1 \vee \mathfrak{a}_1 = \mathfrak{e}_1$, according as $\mathfrak{p}_1$ contains $\mathfrak{a}_1$ or not, as we have proved in Theorem 39. Since $\mathfrak{p}_1$ and $\mathfrak{p}_1 \vee \mathfrak{a}_1$ have a common image $\mathfrak{p}_2$ in A_2, we see that $\mathfrak{p}_2 \neq \mathfrak{e}_2$ or $\mathfrak{p}_2 = \mathfrak{e}_2$ according as $\mathfrak{p}_1$ contains $\mathfrak{a}_1$ or not. In case $\mathfrak{p}_2 \neq \mathfrak{e}_2$, let $\mathfrak{b}_2$ be an ideal which contains $\mathfrak{p}_2$, and let $\mathfrak{b}_1$ be the ideal consisting of all elements in A_1 with images in $\mathfrak{b}_2$. Since $\mathfrak{b}_1$ evidently contains $\mathfrak{p}_1$, we must have either $\mathfrak{b}_1 = \mathfrak{p}_1$ or $\mathfrak{b}_1 = \mathfrak{e}_1$ and hence either $\mathfrak{b}_2 = \mathfrak{p}_2$ or $\mathfrak{b}_2 = \mathfrak{e}_2$. It follows that $\mathfrak{p}_2$ is divisorless and therefore prime, by virtue of Theorem 33. If $\mathfrak{p}_2$ is a prime ideal in A_2, the ideal $\mathfrak{p}_1$ consisting of all elements in A_1 with images in $\mathfrak{p}_2$ evidently contains $\mathfrak{a}_1$. Since $\mathfrak{p}_2 \neq \mathfrak{e}_2$, we have $\mathfrak{p}_1 \neq \mathfrak{e}_1$ likewise. If $\mathfrak{b}_1$ is an ideal containing $\mathfrak{p}_1$, its image $\mathfrak{b}_2$ contains $\mathfrak{p}_2$ and must therefore coincide with $\mathfrak{p}_2$ or with $\mathfrak{e}_2$. When $\mathfrak{b}_2 = \mathfrak{p}_2$, we must have $\mathfrak{b}_1 \vee \mathfrak{a}_1 = \mathfrak{p}_1 \vee \mathfrak{a}_1$ by Theorem 46 (4); but since $\mathfrak{b}_1 \supset \mathfrak{p}_1 \supset \mathfrak{a}_1$, this relation implies $\mathfrak{b}_1 = \mathfrak{p}_1$. Similarly, when $\mathfrak{b}_2 = \mathfrak{e}_2$, we must have $\mathfrak{b}_1 \vee \mathfrak{a}_1 = \mathfrak{e}_1 \vee \mathfrak{a}_1$ and hence $\mathfrak{b}_1 = \mathfrak{e}_1$. It follows that $\mathfrak{p}_1$ is divisorless and therefore prime.

The final theorem concerning homomorphisms offers a new criterion to determine whether an ideal is prime or not.

THEOREM 49. *In order that an ideal $\mathfrak{p}$ in a Boolean ring A be prime, it is necessary and sufficient that $A/\mathfrak{p}$ be a two-element Boolean ring.*

If $A/\mathfrak{p}$ is a two-element Boolean ring, it consists of a zero element 0^* and

a unit element e^*. An element a in A belongs to $\mathfrak{p}$ or not according as its image under the homomorphism $A \to A/\mathfrak{p}$ is 0^* or e^*. The homomorphism cannot take the product ab into 0^* if it takes a and b both into e^*; in other words, if $\mathfrak{p}$ contains ab, it contains at least one of the elements a and b, and is therefore prime. If $\mathfrak{p}$ is prime, then $A/\mathfrak{p}$ contains no divisors of zero. For if a^* and b^* are elements of $A/\mathfrak{p}$ such that $a^*b^* = 0^*$, they are images of elements a and b in A such that ab is in $\mathfrak{p}$; since $\mathfrak{p}$ is prime, at least one of these elements is in $\mathfrak{p}$, and at least one of the elements a^* and b^* is equal to 0^*. By Theorem 1, the Boolean ring $A/\mathfrak{p}$ cannot have more than two elements. On the other hand, the relation $\mathfrak{p} \neq \mathfrak{e}$ shows that $A/\mathfrak{p}$ has at least two elements. The proof is thus completed.

6. **Direct sums.** In the case of Boolean rings, the theory of representations has a very close connection with the concept of the direct sum and the problem of representing a given Boolean ring as a direct sum. We shall therefor close the present chapter with a brief section devoted to this topic. The direct sum of Boolean rings A_α where the index α ranges over an arbitrary finite or infinite class A is the algebraic system $S_{\alpha \in A} A_\alpha$ described as follows: the elements of the system are all the functions f defined over A with values $f(\alpha)$ in A_α; the relation of equality in the system is defined by putting $f = g$ if and only if $f(\alpha) = g(\alpha)$ for every α; the fundamental operations of the system are addition and multiplication, the sum $f+g$ being defined as the function h such that $h(\alpha) = f(\alpha) + g(\alpha)$ in A_α for every α and the product fg being defined as the function k such that $k(\alpha) = f(\alpha)g(\alpha)$ in A_α for every α. In case the class A consists of the integers 1 and 2, we denote the direct sum of the Boolean rings A_α by $A_1 \vee A_2$; this direct sum may evidently be described as the class of all ordered pairs (a_1, a_2) where a_1 and a_2 are elements of A_1 and of A_2 respectively, with $(a_1, a_2) = (b_1, b_2)$ if and only if $a_1 = b_1$ and $a_2 = b_2$ and with $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$, $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$. The following properties of the direct sum may be stated without formal proof:

THEOREM 50. *The direct sum $S_{\alpha \in A} A_\alpha$ of Boolean rings A_α where α ranges over the class A is a Boolean ring. Its zero element is the function 0 which for each α has as its value $0(\alpha)$ the zero element of A_α. It has a unit if and only if every A_α has a unit; if A_α has a unit e_α for every α, then the function e which for each α has the value $e(\alpha) = e_\alpha$ is the unit of the direct sum.*

It is an important problem to determine when a Boolean ring is isomorphic to a direct sum of Boolean rings in a non-trivial manner. Since the direct sum of a Boolean ring A with a one-element Boolean ring is isomorphic to A, we must evidently exclude one-element summands as trivial. A Boolean ring which is representable as the direct sum of two or more Boolean rings, each

with at least two elements, is said to be reducible; and a Boolean ring which is not so representable is said to be irreducible. The reducibility of a Boolean ring is correlated with its ideal structure by virtue of the following result:

THEOREM 51. *If* $\mathfrak{a}$ *is a simple ideal in a Boolean ring* A, *then* $A \longleftrightarrow (A/\mathfrak{a}) \vee (A/\mathfrak{a}')$, $\mathfrak{a} \longleftrightarrow A/\mathfrak{a}'$, $\mathfrak{a}' \longleftrightarrow A/\mathfrak{a}$. *Conversely, if* A, A_1, *and* A_2 *are Boolean rings such that* $A \longleftrightarrow A_1 \vee A_2$, *then there exists a simple ideal* $\mathfrak{a}$ *in* A *such that* $A_1 \longleftrightarrow A/\mathfrak{a}$, $A_2 \longleftrightarrow A/\mathfrak{a}'$.

If $\mathfrak{a}$ is a simple ideal in A, then every element a in A can be represented in a unique manner as the sum a_1+a_2 of elements a_1 and a_2 in $\mathfrak{a}$ and $\mathfrak{a}'$ respectively. To establish the representation, we note that $\mathfrak{a}$ and $\mathfrak{a}'$ are simple by Theorem 30 and hence that $\mathfrak{a}(a)\mathfrak{a}$ and $\mathfrak{a}(a)\mathfrak{a}'$ are principal ideals $\mathfrak{a}(a_1)$ and $\mathfrak{a}(a_2)$ by Theorem 26. The relations $\mathfrak{a}(a_1) \subset \mathfrak{a}$, $\mathfrak{a}(a_2) \subset \mathfrak{a}'$, $\mathfrak{a}(a_1+a_2) = \mathfrak{a}(a_1)+\mathfrak{a}(a_2) = \mathfrak{a}(a)\mathfrak{a}+\mathfrak{a}(a)\mathfrak{a}' = \mathfrak{a}(a)(\mathfrak{a}+\mathfrak{a}') = \mathfrak{a}(a)(\mathfrak{a}+\mathfrak{a}'+\mathfrak{a}\mathfrak{a}') = \mathfrak{a}(a)(\mathfrak{a} \vee \mathfrak{a}') = \mathfrak{a}(a)\mathfrak{e} = \mathfrak{a}(a)$ show that a_1 is in $\mathfrak{a}$, that a_2 is in $\mathfrak{a}'$, and that $a_1+a_2=a$. If a has a second representation $a=b_1+b_2$ where b_1 and b_2 are in $\mathfrak{a}$ and $\mathfrak{a}'$ respectively, the relation $a_1+a_2=b_1+b_2$ implies the relation $a_1+b_1=a_2+b_2$, which shows that a_1+b_1 and a_2+b_2 belong both to $\mathfrak{a}$ and to $\mathfrak{a}'$. Hence we have $a_1+b_1=a_2+b_2=0$, $a_1=b_1$, $a_2=b_2$. The representation is therefore unique. In terms of this representation we set up a biunivocal correspondence from A to the class of ordered pairs (a_1, a_2) where a_1 is in $\mathfrak{a}$ and a_2 in $\mathfrak{a}'$: we put $a \longleftrightarrow (a_1, a_2)$ if and only if $a=a_1+a_2$. It is evident that this correspondence has the property that $a \longleftrightarrow (a_1, a_2)$ and $b \longleftrightarrow (b_1, b_2)$ imply $a+b \longleftrightarrow (a_1+b_1, a_2+b_2)$, $ab \longleftrightarrow (a_1b_1, a_2b_2)$. Consequently, we see that, if we regard $\mathfrak{a}$ and $\mathfrak{a}'$ as Boolean rings, their direct sum is isomorphic to A. Furthermore, if $a=a_1+a_2$ and $b=b_1+b_2$, we see that $a \equiv a_2 \pmod{\mathfrak{a}}$, $b \equiv b_2 \pmod{\mathfrak{a}}$, $a+b \equiv a_2+b_2 \pmod{\mathfrak{a}}$, and $ab \equiv a_2b_2 \pmod{\mathfrak{a}}$. We conclude at once that, if we regard $\mathfrak{a}'$ as a Boolean ring, then $\mathfrak{a}'$ is isomorphic to $A/\mathfrak{a}$. Since $\mathfrak{a}'$ is simple and $(\mathfrak{a}')' = \mathfrak{a}$, the isomorphism $\mathfrak{a} \longleftrightarrow A/\mathfrak{a}'$ is also valid. The fact that A is isomorphic to the direct sum of $\mathfrak{a}$ and $\mathfrak{a}'$ shows that A is also isomorphic to the direct sum of their isomorphs $A/\mathfrak{a}$ and $A/\mathfrak{a}'$, taken in inverted order.

If $A \longleftrightarrow A_1 \vee A_2$, we see that the class $\mathfrak{a}_1$ of all pairs $(a_1, 0_2)$ in $A_1 \vee A_2$ is an ideal; and similarly that the class $\mathfrak{a}_2$ of all pairs $(0_1, a_2)$ is an ideal. If the ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are regarded as Boolean rings they are isomorphic to A_1 and to A_2 respectively. It is furthermore evident that $\mathfrak{a}_1\mathfrak{a}_2$ consists of the zero element $(0_1, 0_2)$ in $A_1 \vee A_2$ and that $\mathfrak{a}_1 \vee \mathfrak{a}_2$ consists of all elements (a_1, a_2) in $A_1 \vee A_2$. Thus if we pass to the Boolean ring A by means of the isomorphism $A \longleftrightarrow A_1 \vee A_2$, we see that A contains ideals $\mathfrak{b}$ and $\mathfrak{a}$ isomorphic to $\mathfrak{a}_1$ and $\mathfrak{a}_2$ respectively and hence also to A_1 and A_2 respectively, these ideals satisfying the relations $\mathfrak{a}\mathfrak{b}=\mathfrak{o}$, $\mathfrak{a} \vee \mathfrak{b}=\mathfrak{e}$. Since $\mathfrak{a}\mathfrak{b}=\mathfrak{o}$ implies $\mathfrak{a}' \supset \mathfrak{b}$, we see that

$\mathfrak{a} \vee \mathfrak{a}' \supset \mathfrak{a} \vee \mathfrak{b} = \mathfrak{e}$ and hence that $\mathfrak{a}$ is simple. Similarly $\mathfrak{b}$ is simple. Since $\mathfrak{a}' = \mathfrak{a}'\mathfrak{e} = \mathfrak{a}'(\mathfrak{a} \vee \mathfrak{b}) = \mathfrak{a}'\mathfrak{b}$, we have $\mathfrak{a}' \subset \mathfrak{b}$ and hence $\mathfrak{a}' = \mathfrak{b}$, $\mathfrak{b}' = \mathfrak{a}$. The isomorphisms $A_1 \longleftrightarrow \mathfrak{b}$, $\mathfrak{b} \longleftrightarrow A/\mathfrak{b}'$ thus lead to the isomorphism $A_1 \longleftrightarrow A/\mathfrak{a}$. The isomorphisms $A_2 \longleftrightarrow \mathfrak{a}$, $\mathfrak{a} \longleftrightarrow A/\mathfrak{a}'$ lead similarly to the isomorphism $A_2 \longleftrightarrow A/\mathfrak{a}'$.

An immediate consequence of Theorem 51 is the following proposition about reducibility:

THEOREM 52. *A Boolean ring A is reducible if and only if it has more than two elements.*

From the preceding theorem we see that A is reducible if and only if the class $\mathfrak{S}$ of all simple ideals contains an ideal $\mathfrak{a}$ other than $\mathfrak{o}$ or $\mathfrak{e}$, the relations $\mathfrak{a}' \neq \mathfrak{e}$, $\mathfrak{a}' \neq \mathfrak{o}$ being equivalent to the relations $\mathfrak{a} \neq \mathfrak{o}$, $\mathfrak{a} \neq \mathfrak{e}$ respectively. Since the class $\mathfrak{P}$ of all principal ideals is contained in $\mathfrak{S}$ and has the same cardinal number as A, we see that, whenever A contains more than two elements, $\mathfrak{S}$ contains more than the two ideals $\mathfrak{o}$ and $\mathfrak{e}$ and A is reducible. If A has one or two elements, then A has a unit by Theorem 1 and $\mathfrak{S}$ coincides with $\mathfrak{P}$ by Theorem 25. Thus $\mathfrak{S}$ contains only the ideals $\mathfrak{o}$ and $\mathfrak{e}$, and A is irreducible.

We conclude with the consideration of the direct sums of two-element Boolean rings, that is, of non-trivial irreducible Boolean rings. We have

THEOREM 53. *A Boolean ring A is isomorphic to the direct sum of two-element Boolean rings A_α, where α ranges over the class* A, *if and only if it is isomorphic to the algebra of all subclasses of* A.

It is evidently sufficient for us to prove that the direct sum of *identical* two-element Boolean rings A_α, where α is in A, is isomorphic to the algebra of all subclasses of A. To a function f in the direct sum we order the class A_f of all elements α such that $f(\alpha) = e$. It is then evident that $\mathrm{A}_f = \mathrm{A}_g$ if and only if $f = g$, that $\mathrm{A}_{f+g} = \mathrm{A}_f \Delta \mathrm{A}_g$, and that $\mathrm{A}_{fg} = \mathrm{A}_f \mathrm{A}_g$. It follows that the correspondence $f \longleftrightarrow \mathrm{A}_f$ determines an isomorphism between A and an algebra of subclasses of A. That the latter algebra is the algebra of *all* subclasses of A we see as follows: if B is an arbitrary subclass of A, the function f which is equal to e or to 0 according as α is in B or not is an element of the direct sum and has the property that $\mathrm{A}_f = \mathrm{B}$.

This theorem is significant from two points of view. In the first place, it shows that, although every Boolean ring of more than two elements is reducible, such a ring need not be completely reducible in the sense that it is representable as the direct sum of irreducible summands or components. The complete reduction of finite Boolean rings is possible in accordance with Theorem 12; but that of infinite Boolean rings is in general impossible. In the second place, the theorem shows the existence of a connection between

the theory of direct sums and that of the representation of Boolean rings by algebras of classes.

CHAPTER III. ALGEBRAS OF CLASSES

1. **The construction of algebras of classes.** By an algebra of classes or concrete Boolean ring we shall mean a Boolean ring which has as elements certain subclasses of a fixed finite or infinite class and as operations those of forming the union (modulo 2) (or symmetric difference) and the intersection of classes. It is easily verified that the class of all subclasses of a fixed class is such a concrete Boolean ring, in accordance with Definition 1. Furthermore, this algebra of classes contains as a subring every concrete Boolean ring with elements which are subclasses of the same fixed class. The object of the present chapter is to discuss the structure of concrete Boolean rings in terms of the general theory developed in the preceding pages.

While the explicit construction of algebras of classes is not of primary concern to us here, some brief remarks upon this subject will permit us to review briefly a few of the points of contact between the present abstract theory and other branches of mathematics, and also to illustrate some of the concepts which we have had occasion to introduce. The methods available for constructing concrete Boolean rings on the basis of an entirely abstract class are essentially those indicated in Chapter II, §§1–2. To them we may add the use of cardinal numbers in forming rings and ideals: thus the countable subclasses of a non-countable class, the finite subclasses of an infinite class afford examples of Boolean rings which are ideals in the algebras of all subclasses of the respective basic classes. Since the union of classes corresponds in the case of a concrete Boolean ring to the abstract element $a \vee b$, we have been at some pains, particularly in Theorems 14, 16, and 17, to show how the operation $\vee$ can be used in place of the operation $+$ in carrying out such constructions. It is only in the case of a class in which there are given relations, operations, and properties other than those of the pure logic of classes that other methods of construction can be applied to obtain algebras of classes. For example, in the theory of measure in euclidean space of n dimensions, it is the combination of the geometrical and topological properties of the space with the operations of the logic of classes which leads to the study of the various concrete Boolean rings consisting respectively of the subclasses described as follows: Lebesgue measurable sets, Borel measurable sets, Lebesgue measurable sets of finite measure, Borel measurable sets of finite measure, and sets of zero measure. It will be noted that the last-named algebra of classes is an ideal in the algebra of all subsets of the given space. Again, in general topology, analogous circumstances lead to the study of

Boolean rings consisting of the subclasses variously described as follows: Borel sets, nowhere dense sets, and sets of the first category. It will be noted that the two last named algebras of classes are ideals in the algebra of all subclasses of the basic topological space. Similar ideals are of such frequent occurrence and of such real importance in topology that they have been given the special designation "additive hereditary classes" by Kuratowski.†

We may point out that some of the algebras of classes cited above are Boolean rings without unit. For instance, the finite subclasses of an infinite class and the Lebesgue measurable sets of finite measure constitute such rings. It is likewise possible to use these and similar concrete Boolean rings to illustrate other points raised in the development of the general theory. At the end of the present chapter we shall discuss the Boolean ring of Lebesgue measurable sets of finite measure in sufficient detail to uncover a number of such illustrative properties.

2. **Reduction and equivalence.** Before proceeding with the study of concrete Boolean rings, we shall describe a canonical form for such rings, and show how any algebra of classes can be reduced to canonical form; that is, how it can be replaced by an isomorphic algebra of classes in that form.

DEFINITION 10. *If A is a Boolean ring with elements $a, b, c, \cdots$ which are subclasses of a fixed class $\mathrm{E} = \mathrm{E}(A)$ with elements $\alpha, \beta, \gamma, \cdots$, then A is said to be a reduced algebra of classes when it has the following property: every elemen α in E is contained in some element of A and is the only element of E common to all the elements of A containing it.*

We can now prove the following result:

THEOREM 54. *Every algebra of classes with more than one element is isomorphic to a reduced algebra of classes, by virtue of an element-to-element correspondence of the basic classes.*

The case of a one-element algebra of classes is trivial, since it is isomorphic to the algebra of all subclasses of a void class E. In case A is an algebra of two or more subclasses of a class E, we construct an isomorphic reduced algebra of classes B with elements which are classes of subclasses of E. We observe that the zero element 0 of A must be the void class: for if a is any element of A, the equation $a+a=0$ identifies 0 as the symmetric difference of the class a with itself. We observe also that the union of all subclasses of E belonging to A is a non-void subclass H of E. If α is any element of H, the intersection of all those classes a in A which contain α is a non-void class $\mathrm{E}(\alpha)$ contained

† Kuratowski, *Topologie*, vol. 1, Warsaw-Lwow, 1933, p. 29.

in H and containing α. We shall now show that two such classes $E(\alpha)$ and $E(\beta)$ have an element γ in common if and only if they coincide. Let a and b be arbitrary classes belonging to A and containing α and β respectively. If $E(\alpha)E(\beta)$ contains γ then ab also contains γ. Since $ab(a+b)=0$, where 0 is the void class, the symmetric difference $a+b$ cannot contain γ; furthermore it cannot contain α or β without containing $E(\alpha)$ or $E(\beta)$ and hence γ. Since α and β belong to a and to b respectively but not to $a+b$, they must belong to ab and hence to both a and b. It thus follows that $E(\alpha)=E(\beta)$. In consequence of this result, we see that a class a belonging to A has a non-void intersection with a class $E(\alpha)$ if and only if a contains $E(\alpha)$: for if β is common to a and $E(\alpha)$, then β is common to $E(\beta)$, which is contained in a, and $E(\alpha)$; and $E(\alpha)=E(\beta)$. We denote by $\mathfrak{H}$ the class of all classes $E(\alpha)$ and by $\mathfrak{H}(a)$ the class of all classes $E(\alpha)$ which are contained in the class a belonging to A. It is evident that the correspondence $a\rightarrow\mathfrak{H}(a)$ has the following properties: $\mathfrak{H}(a)=\mathfrak{H}(b)$ if and only if $a=b$; $\mathfrak{H}(a+b)=\mathfrak{H}(a)\Delta\mathfrak{H}(b)$; $\mathfrak{H}(ab)=\mathfrak{H}(a)\mathfrak{H}(b)$. Thus the class of all classes $\mathfrak{H}(a)$ is an algebra of classes B isomorphic to A. The correspondence $a\rightarrow\mathfrak{H}(a)$ may evidently be regarded as induced by the correspondence $\alpha\rightarrow E(\alpha)$ carrying H into $\mathfrak{H}$. We still have to show that B is a reduced algebra of classes. Since every α in H is contained in some class a belonging to A, it is clear that every $E(\alpha)$ in H is contained in some class $\mathfrak{H}(a)$ belonging to B. The classes $\mathfrak{H}(a)$ containing an arbitrary $E(\alpha)$ in $\mathfrak{H}$ are those for which a is a class containing α; and hence, for any β such that $E(\beta)\neq E(\alpha)$, there is some such a with the property that a does not contain $E(\beta)$, $\mathfrak{H}(a)$ does not contain $E(\beta)$. It follows that $E(\alpha)$ is the sole element common to the classes $\mathfrak{H}(a)$ containing it. Thus B is a reduced algebra of classes in accordance with Definition 10.

Obviously, if A is any reduced algebra of classes we can construct isomorphic algebras of classes which are not reduced: we have only to replace single elements of the basic class E by two or more elements and to adjoin superfluous elements, in a reversal of the process of reduction described in the proof of Theorem 54.

We shall consider also a relation of equivalence between algebras of classes, defined as follows:

DEFINITION 11. *If A and B are algebras of subclasses of classes E_A and E_B respectively and if there exists a biunivocal correspondence between E_A and E_B which induces an isomorphism $A\longleftrightarrow B$, then the algebras A and B are said to be equivalent.*

Concerning this relation of equivalence, we may state the following theorem without formal proof:

THEOREM 55. *If A, B, and C are algebras of classes, then the relation of equivalence introduced in Definition* 11 *has the following properties*:

(1) *A is equivalent to A*;

(2) *if A is equivalent to B, then B is equivalent to A*;

(3) *if A is equivalent to B and B to C, then A is equivalent to C*;

(4) *if A is a reduced algebra of classes and B is equivalent to A, then B is a reduced algebra of classes.*

It is not true that two isomorphic reduced algebras of classes are necessarily equivalent. Illustrative examples are easily constructed on the basis of the following result:

THEOREM 56. *If A is a reduced algebra of subclasses a of a class* E *and if* H *is any subclass of* E, *then the classes* Ha *constitute a reduced algebra B of subclasses of* H *homomorphic to A under the correspondence $a \rightarrow$ Ha. This homomorphism is an isomorphism if and only if the intersection* Ha *is non-void for every non-void a in A.*

The relations $\mathrm{H}(a+b) = (\mathrm{H}a)+(\mathrm{H}b)$, $\mathrm{H}(ab) = (\mathrm{H}a)(\mathrm{H}b)$ hold in the algebra of all subclasses of E and show that the correspondence $a \rightarrow \mathrm{H}a$ determines a homomorphism $A \rightarrow B$. It is evident that B is a reduced algebra of classes. If the indicated homomorphism is an isomorphism, then $\mathrm{H}a = \mathrm{H}b$ implies $a = b$; in particular, for $b = 0$, we must have $a = 0$ whenever $\mathrm{H}a = 0$. On the other hand, if $\mathrm{H}(a+b) = 0$ implies $a+b = 0$, we see that $\mathrm{H}a = \mathrm{H}b$ implies $\mathrm{H}(a+b) = \mathrm{H}a + \mathrm{H}b = 0$ and hence $a+b = 0$, or, equivalently, $a = b$; and the indicated homomorphism is therefore an isomorphism.

In view of Theorems 54 and 55, we may properly confine our attention to reduced algebras of classes; and we may regard equivalent algebras of classes as abstractly identical. We shall therefore assume in the remainder of the present chapter that we are dealing with reduced algebras of classes exclusively.

3. **The analysis of algebras of classes.** If A is an algebra of subclasses of a class E and if $\mathfrak{a}$ is an ideal in A, we can form the union $\mathrm{E}(\mathfrak{a})$ of all those subclasses of E which belong to the ideal $\mathfrak{a}$. On the other hand, if H is an arbitrary subclass of E, we can form the ideal $\mathfrak{a}(\mathrm{H})$ in A consisting of all those classes which belong to A and are contained in H. The chief task of the present section is to study the two correspondences thus defined between ideals in A and subclasses of E.

We commence with the following theorem:

THEOREM 57. *Let A be an algebra of subclasses a of a class* E; *let $\mathfrak{a}$ be an arbitrary ideal in A; and let* $\mathrm{E}(\mathfrak{a})$ *be the union of all those subclasses of* E *which are elements of the ideal $\mathfrak{a}$. Then the following relations are valid*:

(1) *if* $\mathfrak{B}$ *is any non-void class of ideals in* A, *then*

$$\sum_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) = E(S_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a}), \qquad \prod_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \supset E(P_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a});$$

(2) *if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in* A, *then* $E(\mathfrak{ab}) = E(\mathfrak{a})E(\mathfrak{b})$;

(3) *if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in* A, *then* $\mathfrak{a} \subset \mathfrak{b}$ *implies* $E(\mathfrak{a}) \subset E(\mathfrak{b})$;

(4) *if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in* A, *then* $E(\mathfrak{a}) = E(\mathfrak{b})$ *implies* $\mathfrak{a}' = \mathfrak{b}'$;

(5) *the ideal* $\mathfrak{a}'$ *consists of those and only those subclasses of* E *which belong to* A *and are contained in* $E'(\mathfrak{a})$; *and* $E(\mathfrak{a}') \subset E'(\mathfrak{a})$.

The correspondence $\mathfrak{a}\to E(\mathfrak{a})$ *defines a homomorphism from the system* $\mathfrak{J}$ *of all ideals in* A (*with unrestricted addition and finite multiplication as operations*) *to the system of all classes* $E(\mathfrak{a})$ (*with the operations of forming arbitrary unions and finite intersections*), *in accordance with* (1) *and* (2) *above. This correspondence has the following special properties*:

(6) *if* $\mathfrak{a}$ *is a principal ideal* $\mathfrak{a}(a)$, *then* $E(\mathfrak{a}(a)) = a$;

(7) *if* $\mathfrak{a}$ *is a simple ideal, then* $E(\mathfrak{a}') = E'(\mathfrak{a})$;

(8) *if* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are normal ideals, then* $E(\mathfrak{a}) = E(\mathfrak{b})$ *implies* $\mathfrak{a} = \mathfrak{b}$;

(9) *if* $\mathfrak{p}$ *is a prime ideal, then* $E'(\mathfrak{p})$ *contains at most one element.*

If the correspondence $\mathfrak{a}\to E(\mathfrak{a})$ *is restricted to normal ideals it is biunivocal; if it is restricted to simple, semiprincipal, or principal ideals, it defines an isomorphism and the corresponding classes* $E(\mathfrak{a})$ *constitute an algebra of classes.*

Properties (3) and (6) are evident from the definition of the class $E(\mathfrak{a})$. From (3), we have

$$\sum_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \subset E(S_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a}), \qquad \prod_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \supset E(P_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a}).$$

To complete the proof of (1) we must therefore show that

$$\sum_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \supset E(S_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a})$$

or, equivalently, that

$$\sum_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \supset a \text{ for every } a \text{ in } S_{\mathfrak{a}\in\mathfrak{B}}\,\mathfrak{a}.$$

Now by Theorem 17 such an element a can be expressed in the form $a = a_1 \vee \cdots \vee a_n$ where $a_1, \cdots, a_n$ belong respectively to ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ in $\mathfrak{B}$; and we thus have

$$\sum_{\mathfrak{a}\in\mathfrak{B}} E(\mathfrak{a}) \supset E(\mathfrak{a}_1) \cup \cdots \cup E(\mathfrak{a}_n) \supset a_1 \vee \cdots \vee a_n = a,$$

as we wished to prove. In order to prove (2), it is now sufficient to show that $E(\mathfrak{a})E(\mathfrak{b}) \subset E(\mathfrak{ab})$. We have

$$\mathrm{E}(\mathfrak{a})\mathrm{E}(\mathfrak{b}) = \sum_{a\in\mathfrak{a}} a \sum_{b\in\mathfrak{b}} b = \sum_{\substack{a\in\mathfrak{a}\\ b\in\mathfrak{b}}} ab \subset \mathrm{E}(\mathfrak{ab})$$

since ab evidently belongs to the ideal $\mathfrak{ab}$. We next prove (5). In order that the class a be an element of the ideal $\mathfrak{a}'$ it is necessary and sufficient that $\mathfrak{a}(a)\mathfrak{a}=\mathfrak{o}$. By (2) and (6), the latter relation holds if and only if $a\mathrm{E}(\mathfrak{a}) = \mathrm{E}(\mathfrak{a}(a))\mathrm{E}(\mathfrak{a}) = \mathrm{E}(\mathfrak{a}(a)\mathfrak{a}) = \mathrm{E}(\mathfrak{o}) = 0$, where 0 is the void class and the zero element of A. We thus conclude that $a \subset \mathrm{E}'(\mathfrak{a})$ and that $\mathrm{E}(\mathfrak{a}') \subset \mathrm{E}'(\mathfrak{a})$. The first part of (5) obviously implies (4). If we combine (4) with a result noted in Theorem 28, we obtain (8). To prove (7), we apply (1) and (2) to the relations $\mathfrak{a} \vee \mathfrak{a}' = \mathfrak{e}$, $\mathfrak{a}\mathfrak{a}' = \mathfrak{o}$, which hold when $\mathfrak{a}$ is simple, finding that $\mathrm{E}(\mathfrak{a}) \cup \mathrm{E}(\mathfrak{a}') = \mathrm{E}(\mathfrak{a} \vee \mathfrak{a}') = \mathrm{E}(\mathfrak{e}) = \mathrm{E}$, $\mathrm{E}(\mathfrak{a})\mathrm{E}(\mathfrak{a}') = \mathrm{E}(\mathfrak{a}\mathfrak{a}') = \mathrm{E}(\mathfrak{o}) = 0$ and hence that $\mathrm{E}(\mathfrak{a}') = \mathrm{E}'(\mathfrak{a})$. Finally, we consider (9). If $\mathrm{E}'(\mathfrak{p})$ contains elements α and β where $\alpha \neq \beta$, the fact that A is a reduced algebra of classes shows that there exists a class a in A which contains α but not β. Since a does not belong to $\mathfrak{p}$, we have $\mathfrak{p} \vee \mathfrak{a}(a) = \mathfrak{e}$ in accordance with Theorem 39. Thus we see that $\mathrm{E}(\mathfrak{p}) \cup a = \mathrm{E}(\mathfrak{p}) \cup \mathrm{E}(\mathfrak{a}(a)) = \mathrm{E}(\mathfrak{p} \vee \mathfrak{a}(a)) = \mathrm{E}(\mathfrak{e}) = \mathrm{E}$. Since β is not an element of $\mathrm{E}(\mathfrak{p})$, it must be an element of a, contrary to hypothesis. Hence (9) is established. It is now evident that the correspondence $\mathfrak{a} \to \mathrm{E}(\mathfrak{a})$ sets up a homomorphism as stated in the theorem. We note that the congruence determined in $\mathfrak{F}$ by this homomorphism, namely, the relation $\mathfrak{a} \equiv \mathfrak{b}$ equivalent to $\mathrm{E}(\mathfrak{a}) = \mathrm{E}(\mathfrak{b})$, has by (4) the property that it implies the congruence C of Theorem 38. It follows that the system of classes $\mathrm{E}(\mathfrak{a})$ has the system $\mathfrak{F}^C$ of Theorem 28 as a homomorph. The specialization of this correspondence to the various special classes of ideals now follows at once from Theorems 28–32 and Theorem 42.

THEOREM 58. *Let A be an algebra of subclasses a of a class* E; *let* H *be an arbitrary subclass of* E; *and let* $\mathfrak{a}$(H) *be the class of all elements a in A which are subclasses of* H. *Then* $\mathfrak{a}$(H) *is an ideal in A with the following properties*:

(1) $\mathfrak{a}(\mathrm{H}_1) \vee \mathfrak{a}(\mathrm{H}_2) \subset \mathfrak{a}(\mathrm{H}_1 \cup \mathrm{H}_2)$;

(2) $\mathfrak{a}(\mathrm{H}_1)\mathfrak{a}(\mathrm{H}_2) = \mathfrak{a}(\mathrm{H}_1\mathrm{H}_2)$;

(3) $\mathrm{H}_1 \subset \mathrm{H}_2$ *implies* $\mathfrak{a}(\mathrm{H}_1) \subset \mathfrak{a}(\mathrm{H}_2)$;

(4) $\mathfrak{a}$(H) *is prime if and only if* H′ *has exactly one element.*

In connection with Theorem 57, *the following relations are found to hold*:

(5) $\mathfrak{a}(\mathrm{E}(\mathfrak{b})) \supset \mathfrak{b}$; (6) $\mathrm{E}(\mathfrak{a}(\mathrm{H})) \subset \mathrm{H}$; (7) $\mathfrak{b}' = \mathfrak{a}(\mathrm{E}'(\mathfrak{b}))$.

It is easily verified that $\mathfrak{a}$(H), which always contains the void class 0, that is, the zero element in A, is an ideal in A. Properties (1), (3), (5), and (6) are evident; and (7) is a restatement of Theorem 57 (5). Since the relation

$\mathfrak{a}(H_1)\mathfrak{a}(H_2) \supset \mathfrak{a}(H_1H_2)$ follows from (3), we can prove (2) by showing that $\mathfrak{a}(H_1)\mathfrak{a}(H_2)$ is contained in $\mathfrak{a}(H_1H_2)$. If a is in the ideal $\mathfrak{a}(H_1)\mathfrak{a}(H_2)$, Theorem 18 shows that $a=bc$, where b and c are in $\mathfrak{a}(H_1)$ and $\mathfrak{a}(H_2)$ respectively. It is thus clear that a is contained in H_1H_2 and hence that $\mathfrak{a}(H_1)\mathfrak{a}(H_2) \subset \mathfrak{a}(H_1H_2)$, as we wished to prove. Finally, we consider (4). If $\mathfrak{a}(H)$ is prime, then $E'(\mathfrak{a}(H))$ contains at most one element by Theorem 57 (9). Hence H' contains at most one element by (6) above. It is clear, however, that H' must contain at least one element, since $H'=0$ would imply $\mathfrak{a}(H)=\mathfrak{a}(E)=\mathfrak{e}$, contrary to hypothesis. On the other hand, if H' contains exactly one element α, $\mathfrak{a}(H)$ consists of those classes in A which do not contain α; and the remaining classes in A all contain α and constitute a class $\mathfrak{b}$, which cannot be void since A is a reduced algebra of classes. It is evident that the classes $\mathfrak{a}(H)$ and $\mathfrak{b}$ have the properties enumerated in Theorem 34, and hence that $\mathfrak{a}(H)$ is a prime ideal.

It is now desirable that we consider in greater detail two special cases corresponding to the possible extremes under Theorem 57 (4): the cases where the relation $E(\mathfrak{a})=E(\mathfrak{b})$ is equivalent to the relations $\mathfrak{a}=\mathfrak{b}$, and $\mathfrak{a}'=\mathfrak{b}'$ respectively. For subsequent considerations, it is helpful to introduce the following terminology in the first case:

DEFINITION 12. *An algebra A of subclasses of a class E is said to be perfect if* $E(\mathfrak{a})=E(\mathfrak{b})$ *implies* $\mathfrak{a}=\mathfrak{b}$; *that is, if the homomorphism of Theorem* 57 *is an isomorphism.*

The characterization of perfect algebras of classes involves the following connection with the closing remarks of Chapter II, §4:

THEOREM 59. *In order that an algebra A of subclasses of a class E be perfect, it is necessary and sufficient that*

(1) *the Fundamental Proposition of Ideal Arithmetic hold in A;*

(2) $E'(\mathfrak{p})$ *be a one-element class whenever* $\mathfrak{p}$ *is a prime ideal.*

If the algebra A is perfect then $E(\mathfrak{a})=E=E(\mathfrak{e})$ implies $\mathfrak{a}=\mathfrak{e}$. Theorem 57 (9) therefore shows, by virtue of the relation $E(\mathfrak{p})\neq\mathfrak{e}$, that $E'(\mathfrak{p})$ is a one-element class whenever $\mathfrak{p}$ is a prime ideal. If $\mathfrak{a}$ is an arbitrary ideal not equal to $\mathfrak{e}$, then the prime ideal $\mathfrak{p}$ is a divisor of $\mathfrak{a}$ if and only if $\mathfrak{p}\mathfrak{a}=\mathfrak{a}$; the latter relation is equivalent to $E(\mathfrak{p}\mathfrak{a})=E(\mathfrak{a})$, since A is perfect, and hence to the relations $E(\mathfrak{p})E(\mathfrak{a})=E(\mathfrak{p}\mathfrak{a})=E(\mathfrak{a})$, $E(\mathfrak{a}) \subset E(\mathfrak{p})$. If α is an element not contained in $E(\mathfrak{a})\neq E$, the class H of all elements in E not equal to α determines a prime ideal $\mathfrak{p}=\mathfrak{a}(H)$ in accordance with Theorem 58 (4). By Theorem 58 (6), $E(\mathfrak{p}) \subset H$; since $E'(\mathfrak{p})$ is a one-element class by the preceding results, it follows that $E(\mathfrak{p})=H \supset E(\mathfrak{a})$ and hence that $\mathfrak{p} \supset \mathfrak{a}$. Thus the class $\mathfrak{B}$ of all prime ideal divisors of $\mathfrak{a}$ is non-void and consists of the ideals $\mathfrak{p}=\mathfrak{a}(H)$ where $H \supset E(\mathfrak{a})$ and

H' is a one-element class. We can now show that $\mathfrak{a} = P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}$. By Theorem 57 (1) and the relation $E(\mathfrak{p}) = H$, we have $E(P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}) \subset \Pi_{\mathfrak{p} \in \mathfrak{B}} E(\mathfrak{p}) = E(\mathfrak{a})$. On the other hand, the relation $\mathfrak{a} \subset P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}$ shows that $E(\mathfrak{a}) \subset E(P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p})$. It follows that $E(\mathfrak{a}) = E(P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p})$ and, since A is perfect, that $\mathfrak{a} = P_{\mathfrak{p} \in \mathfrak{B}} \mathfrak{p}$, as we wished to prove.

Now let us suppose that A is an algebra of classes in which conditions (1) and (2) are satisfied. If $\mathfrak{a}$ and $\mathfrak{b}$ are distinct ideals, there must exist a prime ideal $\mathfrak{p}$ containing one but not both of these ideals, in accordance with (1). Let us suppose that our notation is so chosen that $\mathfrak{p}$ contains $\mathfrak{a}$ but not $\mathfrak{b}$. By Theorem 57 (3) we have $E(\mathfrak{p}) \supset E(\mathfrak{a})$. On the other hand, (2) shows that $E'(\mathfrak{p})$ is a one-element class and hence that $\mathfrak{a}(E(\mathfrak{p}))$ is a prime ideal divisor of $\mathfrak{p}$ in accordance with Theorem 58, (4) and (5). It follows that $\mathfrak{p} = \mathfrak{a}(E(\mathfrak{p}))$. If the relation $E(\mathfrak{p}) \supset E(\mathfrak{b})$ were true, we should have $\mathfrak{b} \subset \mathfrak{a}(E(\mathfrak{b})) \subset \mathfrak{a}(E(\mathfrak{p})) = \mathfrak{p}$, contrary to hypothesis. Thus $E(\mathfrak{p})$ contains $E(\mathfrak{a})$ but not $E(\mathfrak{b})$, so that $E(\mathfrak{a}) \neq E(\mathfrak{b})$. We therefore conclude that A is perfect.

We now turn to the second case, that in which $E(\mathfrak{a}) = E(\mathfrak{b})$ and $\mathfrak{a}' = \mathfrak{b}'$ are equivalent relations. In view of Theorem 57 (4), we have merely to ascertain the conditions under which $\mathfrak{a}' = \mathfrak{b}'$ implies $E(\mathfrak{a}) = E(\mathfrak{b})$.

THEOREM 60. *The following assertions concerning an algebra A of subclasses of a class* E *are equivalent*:

(1) $\mathfrak{a}' = \mathfrak{b}'$ *implies* $E(\mathfrak{a}) = E(\mathfrak{b})$;

(2) *every one-element subclass of* E *is an element of* A;

(3) $\mathfrak{a}(H_1) = \mathfrak{a}(H_2)$ *implies* $H_1 = H_2$;

(4) $E(\mathfrak{a}(H)) = H$ *for every subclass* H *of* E;

(5) $E(\mathfrak{a}') = E'(\mathfrak{a})$ *for every ideal* $\mathfrak{a}$ *in* A;

(6) $\mathfrak{a}(H)$ *is a normal ideal for every* H;

(7) $\mathfrak{a}(E(\mathfrak{b})) = \mathfrak{b}''$ *for every ideal* $\mathfrak{b}$ *in* A;

(8) $\mathfrak{a}(H_1) \nabla \mathfrak{a}(H_2) = \mathfrak{a}(H_1 \cup H_2)$ *for all* H_1 *and* H_2.

When these conditions are satisfied, the Boolean ring $\mathfrak{N}$ *of all normal ideals in* A *described in Theorem* 29 *is isomorphic to the algebra of all subclasses of* E. *Conversely, if the Boolean ring* $\mathfrak{N}$ *of all normal ideals in an abstract Boolean ring* B *is isomorphic to the algebra of all subclasses of a class* E, *then* B *is isomorphic to a reduced algebra* A *of subclasses of* E *in which these conditions are satisfied.*

We begin by establishing the implications $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 7 \to 1$, $4 \to 8$, and $8 \to 6$. If (1) holds and H is a one-element subclass of E, then $\mathfrak{a}(H')$ is prime by Theorem 58 (4), $E(\mathfrak{a}(H')) = H'$ by Theorem 57 (9) and Theorem 58 (6), and $\mathfrak{a}'(H') \neq 0$ since (1) and $\mathfrak{a}'(H') = e'$ would imply $H' = E(\mathfrak{a}(H')) = E(e) = E$; and it is therefore evident that H, as the only subclass of H distinct from 0, must be an element of A. If (2) holds, the ideal $\mathfrak{a}(H)$ contains those and only those one-element classes which are subclasses of H; it is thus clear that

$\mathfrak{a}(H_1)=\mathfrak{a}(H_2)$ implies $H_1=H_2$. If (3) holds, we have $\mathfrak{a}(E(\mathfrak{a}(H)))=\mathfrak{a}(H)$ by Theorem 58, (3), (5), and (6), and hence $E(\mathfrak{a}(H))=H$ for every H. If (4) holds, we have $\mathfrak{a}'=\mathfrak{a}(E'(\mathfrak{a}))$ by Theorem 58 (7), and hence $E(\mathfrak{a}')=E(\mathfrak{a}(E'(\mathfrak{a})))$, so that $E(\mathfrak{a}')=E'(\mathfrak{a})$. If (5) holds, we have $E(\mathfrak{a}''(H))=E'(\mathfrak{a}'(H))=E''(\mathfrak{a}(H))=E(\mathfrak{a}(H))$ and hence $\mathfrak{a}''(H)\subset\mathfrak{a}(E(\mathfrak{a}''(H)))=\mathfrak{a}(E(\mathfrak{a}(H)))=\mathfrak{a}(H)\subset\mathfrak{a}''(H)$ by Theorem 58, (3), (5), and (6), so that $\mathfrak{a}(H)=\mathfrak{a}''(H)$ and $\mathfrak{a}(H)$ is normal for every H. If (6) holds, we have $\mathfrak{a}(E(\mathfrak{b}))\mathfrak{b}'=\mathfrak{a}(E(\mathfrak{b}))\mathfrak{a}(E'(\mathfrak{b}))=\mathfrak{a}(E(\mathfrak{b})E'(\mathfrak{b}))=\mathfrak{a}(0)=\mathfrak{o}$, $\mathfrak{a}(E(\mathfrak{b}))\supset\mathfrak{b}$ by Theorem 58, (2), (5), and (7), and hence $\mathfrak{b}''\supset\mathfrak{a}(E(\mathfrak{b}))=\mathfrak{a}''(E(\mathfrak{b}))\supset\mathfrak{b}''$, so that $\mathfrak{a}(E(\mathfrak{b}))=\mathfrak{b}''$. If (7) holds, then $E(\mathfrak{b})=E(\mathfrak{a}(E(\mathfrak{b})))=E(\mathfrak{b}'')$ by Theorem 57 (3) and Theorem 58, (5) and (6), so that $\mathfrak{a}'=\mathfrak{b}'$ implies $\mathfrak{a}''=\mathfrak{b}''$ and $E(\mathfrak{a})=E(\mathfrak{a}'')=E(\mathfrak{b}'')=E(\mathfrak{b})$. If (4) holds, we have $E(\mathfrak{a}(H_1\cup H_2))=H_1\cup H_2=E(\mathfrak{a}(H_1))\cup E(\mathfrak{a}(H_2))$ by Theorem 57 (1) and hence $\mathfrak{a}'(H_1\cup H_2)=(\mathfrak{a}(H_1)\vee\mathfrak{a}(H_2))'$ by Theorem 57 (4); and, since (4) implies (6), we have $\mathfrak{a}(H_1)\nabla\mathfrak{a}(H_2)=(\mathfrak{a}(H_1)\vee\mathfrak{a}(H_2))''=\mathfrak{a}''(H_1\cup H_2)=\mathfrak{a}(H_1\cup H_2)$, in accordance with Definition 9. If (8) holds, we have $\mathfrak{a}''(H)=\mathfrak{a}(H)\nabla\mathfrak{a}(0)=\mathfrak{a}(H\cup 0)=\mathfrak{a}(H)$. The equivalence of assertions (1)–(8) is thus established.

The correspondence $H\to\mathfrak{a}(H)$ takes the class of all subclasses of E into a subclass of the Boolean ring $\mathfrak{N}$ of all normal ideals in A by virtue of (6); and does so in a biunivocal manner in accordance with (3). If $\mathfrak{b}$ is any normal ideal, and $H=E(\mathfrak{b})$, then $\mathfrak{a}(H)=\mathfrak{a}(E(\mathfrak{b}))=\mathfrak{b}''=\mathfrak{b}$ by (7), so that the correspondence takes the class of all subclasses of E into the entire class $\mathfrak{N}$. By Theorem 58 (2) and (8) above, this correspondence determines the isomorphism described in the statement of the theorem. Let us suppose conversely that the Boolean ring $\mathfrak{N}$ associated with an abstract Boolean ring B is isomorphic to the algebra of all subclasses of a class E. Since B is isomorphic to the subring of principal ideals $\mathfrak{P}$, it is evident that B is also isomorphic to an algebra A of subclasses of E. If H is an arbitrary one-element subclass of E, it corresponds in the isomorphism to a normal ideal $\mathfrak{a}$ distinct from 0. Since every element of B which belongs to the ideal $\mathfrak{a}$ corresponds to a subclass of H, we see that $\mathfrak{a}$ must consist of exactly two elements corresponding respectively to H and to the void class. It follows that H is an element of the algebra A. Since A has property (2) of the present theorem by the result just proved, A is evidently a reduced algebra of classes in accordance with Definition 10; and it has all the other properties (1)–(8).

We see that Theorem 60 can be made to yield information about abstract Boolean rings by virtue of the following result:

THEOREM 61. *In order that an abstract Boolean ring B be isomorphic to an algebra A of subclasses of a class* E *with the property* (2) *of Theorem* 60, *it is necessary and sufficient that B contain a complete atomic system.*

The sufficiency of the condition is evident from Theorem 8. The necessity follows at once from the observation that the one-element subclasses of E constitute a complete atomic system in A in accordance with Definition 5: for the image of this system in B under the isomorphism $A \longleftrightarrow B$ is also a complete atomic system.

We have on the basis of Theorems 60 and 61 the following proposition:

THEOREM 62. *In order that an abstract Boolean ring B be isomorphic to the algebra A of all subclasses of a class* E *it is necessary and sufficient that every normal ideal in B be principal and that B contain a complete atomic system.*

The existence of a complete atomic system in B is necessary and sufficient for the existence of an isomorphism $B \longleftrightarrow A$, where A is an algebra of classes with property (2) of Theorem 60, as we have just proved in Theorem 61. In order that every subclass of the basic class belong to such an isomorphic algebra A, it is necessary and sufficient, by virtue of Theorem 60, that every normal ideal in A be principal: for the normal ideals in A are precisely the ideals $\mathfrak{a}(H)$; and such an ideal is principal if and only if the generating class H is an element of A. The isomorphism $A \longleftrightarrow B$ shows that A has the indicated property if and only if every normal ideal in B is principal. The proof is thus completed.

We may remark that Theorems 60 and 61 furnish the basis for our comments concerning the class $\mathfrak{N}$ of normal ideals at the end of Chapter II, §3. Since a Boolean ring does not necessarily contain any atomic element, let alone a complete atomic system, $\mathfrak{N}$ cannot in general be isomorphic to an algebra of all subclasses of an appropriate fixed class.

4. **An illustration.** We shall now consider, by way of illustration, the application of the results of §3 to the algebra A of all Lebesgue measurable subsets of finite measure in the euclidean plane E. Since every one-element set belongs to A, we see that A has property (2) of Theorem 60. Hence the normal ideals in A are precisely the ideals $\mathfrak{a}(H)$, consisting of all sets belonging to A and contained in the arbitrary set H. In order that an ideal be principal, it must be normal and hence must be expressible in the form $\mathfrak{a}(H)$ where H is an element of A. We can now determine the simple ideals in A on the basis of Theorem 26 as follows: every simple ideal is normal and can therefore be expressed as $\mathfrak{a}(H)$; in order that $\mathfrak{a}(H)$ be simple, the product $\mathfrak{a}(H)\mathfrak{a}(H_1) = \mathfrak{a}(HH_1)$ must be principal whenever $\mathfrak{a}(H_1)$ is principal, and conversely; in other words $\mathfrak{a}(H)$ is simple if and only if H has the characteristic property of Lebesgue measurable sets, that HH_1 is in A whenever H_1 is in A. The semiprincipal ideals which are not principal are now seen to be the ideals $\mathfrak{a}(H)$ where the complement of H belongs to A. From these characterizations of the ideals in A, we

see that the classes $\mathfrak{P}$, $\mathfrak{P}^*$, $\mathfrak{S}$, and $\mathfrak{N}$ are distinct. Furthermore, since the sets of zero measure constitute an ideal in A which obviously cannot be put in the form $\mathfrak{a}(H)$, the classes $\mathfrak{N}$ and $\mathfrak{I}$ are also distinct. The prime ideals belonging to $\mathfrak{N}$ are evidently given by $\mathfrak{a}(H)$ where the complement of H is a one-element class. Hence no normal prime ideal in A can contain every set of zero measure; and, if the ideal of sets of zero measure has a prime ideal divisor in A, the latter ideal cannot be normal. This familiar example therefore shows that the classifications discussed in Chapter II, §§3 and 4, are not degenerate except in special Boolean rings.

Chapter IV. Representation theory

1. **General remarks.** We come now to the problem of constructing an algebra of classes isomorphic to a given abstract Boolean ring. Indeed, we shall consider the broader problem of determining all algebras of classes homomorphic to a given Boolean ring. In view of the results of Chapter III, §2, we may confine our attention to reduced algebras of classes and we may regard representations by equivalent algebras of classes as abstractly identical. Thus the general problem of representation theory can be formulated in the following precise terms: if A is any Boolean ring, it is required to construct a family of reduced algebras of classes homomorphic to A so that any algebra of classes homomorphic to A is equivalent, after the reduction described in Theorem 54, to an algebra belonging to this family. We shall be able to solve this problem completely in the present chapter.

The results of Chapter III, §3, are sufficient to indicate that the representation problem is closely bound up with the theory of ideals, particularly the prime ideals. Suppose that the Boolean ring A has a homomorph B with elements which are subclasses of a fixed class E. Then each element of E is associated by Theorem 58 (4) with a prime ideal in B and hence, by virtue of Theorem 48, with a prime ideal in A. We may therefore suppose that each element of E is replaced by the associated prime ideal, so that A is represented by an algebra of classes of its own prime ideals. If this representation be further analyzed, it becomes clear that a given element a in A must be represented by the class of those prime ideals which are thus determined by the given basic class E and do not contain a as an element. Thus any attempt to solve the representation problem must be based upon a preliminary theory of the existence and divisibility properties of prime ideals. In particular, in order to show that A has an isomorphic representation, it is evidently necessary to prove that whenever a and b are unequal elements of A there exists a prime ideal containing one, but not both, of these elements. It is not difficult to see that the existence theorem thus suggested is equivalent to the Funda-

mental Proposition of Ideal Arithmetic, stated at the close of Chapter II, §4.

Our program for solving the representation problem is thus prescribed: we first prove the Fundamental Existence Proposition and the Fundamental Proposition of Ideal Arithmetic, as previously stated; we then determine a representation by subclasses of the class $\mathfrak{S}$ of all prime ideals, noting that this algebra of classes must be perfect in accordance with Definition 12 and Theorem 59; and we then show that all other representations can be constructed from this perfect representation by the process discussed in Theorem 56. It will be observed that the indicated perfect representation also affords an isomorphic representation of the class of all ideals under the operations of unrestricted addition and finite multiplication, in accordance with Theorem 57 and Definition 12.†

It will be evident from a closer inspection of our solution of the representation problem, that the relations thereby revealed are of such a nature that they can appropriately be stated in topological terms. Once such a statement has been made, a number of interesting topological connections are suggested. The further development of the theory in the indicated direction will be carried out in another paper.‡

2. **Existence and divisibility properties of prime ideals.** In view of the remarks made in the preceding section, we shall now resume the study of prime ideals at the point where we broke off in Chapter II, §4. We first establish the Fundamental Existence Proposition.

THEOREM 63. *In a Boolean ring A containing at least two elements, there exists at least one prime ideal.*

We shall give two proofs, both based upon the principle of transfinite induction.§ In view of Theorems 34–36 and 39, we see that the construction of a prime ideal, or, alternatively, the construction of a homomorphism $A \rightarrow B$

† The construction of this perfect representation was described in a communication to the Society, abstracted in its Bulletin, abstract 39-3-86, received January 24, 1933, and also in Proceedings of the National Academy of Sciences, vol. 20 (1934), pp. 197–202. A more general representation theorem (for C-lattices or distributive lattices) was discovered independently and only slightly later by Garrett Birkhoff, see Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), pp. 441–464, Theorem 25.2. Since MacNeille has shown in his doctoral dissertation *The Theory of Partially Ordered Sets* (1935), not yet published, that every distributive lattice can be algebraically imbedded in a Boolean algebra, or Boolean ring, Birkhoff's result may now be regarded as included in those given here.

‡ See Stone, Proceedings of the National Academy of Sciences, vol. 20 (1934), pp. 197–202.

§ Still another proof is given by von Neumann and Stone, Fundamenta Mathematicae, vol. 25 (1935), pp. 353–378; a paper by Tarski, Fundamenta Mathematicae, vol. 15 (1930), pp. 42–50, although couched in the language of the theory of measure, also gives a proof which could be adapted to the present situation.

where B is a two-element Boolean ring necessitates the distribution of the elements of A between two subclasses according to certain prescribed rules, and hence requires the examination and allocation of those elements to subclasses in some orderly fashion. In general, therefore, we can hardly expect to devise a method of construction which does not involve the well-ordering hypothesis.

In our first proof, we work with the class $\mathfrak{J}$ of all ideals in A. We choose an ordinal number ω so that the ideals in A can be put in biunivocal correspondence with the ordinals γ such that $\gamma<\omega$; and we may even suppose that ω is the first ordinal number available for this purpose. Since A has more than one element, we can select an element a not equal to 0. We now define a prime ideal $\mathfrak{p}$ by transfinite induction, first forming ideals $\mathfrak{b}_\alpha$ for all $\alpha<\omega$ and then putting $\mathfrak{p}=S_{\alpha<\omega}\mathfrak{b}_\alpha$. If $\mathfrak{a}_1$ is the first ideal in $\mathfrak{J}$, we define $\mathfrak{b}_1$ as equal to $\mathfrak{o}$ or to $\mathfrak{a}_1$, according as a belongs to $\mathfrak{a}_1$ or not; and, if $\mathfrak{b}_\alpha$ has been defined for all ordinals α such that $\alpha<\beta$ where $\beta<\omega$, we define $\mathfrak{b}_\beta$ as the ideal $S_{\alpha<\beta}\mathfrak{b}_\alpha$ or as the ideal $\mathfrak{a}_\beta \vee S_{\alpha<\beta}\mathfrak{b}_\alpha$ according as a belongs to the latter ideal or not. By the principle of transfinite induction, $\mathfrak{p}$ exists and is an ideal in A. We shall now show that $\mathfrak{p}$ is divisorless and hence prime in accordance with Theorem 33. We first prove that $\mathfrak{p}\neq\mathfrak{e}$; in particular, that $\mathfrak{p}$ does not contain the element a. Since $\alpha<\beta$ implies $\mathfrak{b}_\alpha \subset \mathfrak{b}_\beta$ by construction, we see that, if $\mathfrak{p}$ contained a, Theorem 17 would establish the existence of ordinals $\beta_1<\cdots<\beta_n<\omega$ such that a belongs to $\mathfrak{b}_{\beta_n}=\mathfrak{b}_{\beta_1}\vee\cdots\vee\mathfrak{b}_{\beta_n}$. Similarly, if $\mathfrak{b}_\beta$ contained the element a for $\beta>1$, Theorem 17 would establish the existence of an ordinal $\alpha<\beta$ such that $\mathfrak{b}_\alpha$ contains a: for the fact that $\mathfrak{b}_\beta$ is assumed to contain a excludes the relation $\mathfrak{b}_\beta=\mathfrak{a}_\beta\vee S_{\alpha<\beta}\mathfrak{b}_\alpha$ and thus implies $\mathfrak{b}_\beta=S_{\alpha<\beta}\mathfrak{b}_\alpha$. We see therefore that, if $\mathfrak{p}$ contained a, there would be a first ordinal α such that $\mathfrak{b}_\alpha$ contains a and this ordinal would necessarily be $\alpha=1$. By construction, however, $\mathfrak{b}_1$ does not contain a. Next we prove that if $\mathfrak{a}$ is an ideal divisor of $\mathfrak{p}$, then $\mathfrak{a}=\mathfrak{p}$ or $\mathfrak{a}=\mathfrak{e}$. In the first place let us suppose that $\mathfrak{a}$ does not contain a. If γ is the ordinal assigned to $\mathfrak{a}$, we then have $\mathfrak{a}=\mathfrak{a}_\gamma\supset\mathfrak{p}\supset S_{\alpha<\gamma}\mathfrak{b}_\alpha$ and hence $\mathfrak{p}\supset\mathfrak{b}_\gamma=\mathfrak{a}_\gamma\vee S_{\alpha<\gamma}\mathfrak{b}_\alpha=\mathfrak{a}_\gamma$, since $\mathfrak{a}_\gamma$ does not contain a. Thus in this case we have $\mathfrak{a}=\mathfrak{a}_\gamma=\mathfrak{p}$. In the second place we suppose that $\mathfrak{a}$ contains a and hence that $\mathfrak{a}\supset\mathfrak{p}\vee\mathfrak{a}(a)$. Since the ideal $\mathfrak{a}'(a)$ is equal to $\mathfrak{a}_\delta$ for an appropriate ordinal number δ, and since $\mathfrak{a}(a)\subset\mathfrak{a}_\delta\vee S_{\alpha<\delta}\mathfrak{b}_\alpha$ would imply

$$\mathfrak{a}(a)=\mathfrak{a}(a)\mathfrak{a}_\delta\vee\mathfrak{a}(a)\sum_{\alpha<\delta}\mathfrak{b}_\alpha=\mathfrak{a}(a)\sum_{\alpha<\delta}\mathfrak{b}_\alpha\subset\sum_{\alpha<\delta}\mathfrak{b}_\alpha\subset\mathfrak{p},$$

contrary to the fact that $\mathfrak{p}$ does not contain a, we have

$$\mathfrak{a}'(a)=\mathfrak{a}_\delta\subset\mathfrak{a}_\delta\vee\sum_{\alpha<\delta}\mathfrak{b}_\alpha=\mathfrak{b}_\delta\subset\mathfrak{p}$$

and hence

$$\mathfrak{a} \supset \mathfrak{p} \vee \mathfrak{a}(a) \supset \mathfrak{a}'(a) \vee \mathfrak{a}(a) = \mathfrak{e}, \qquad \mathfrak{a} = \mathfrak{e}.$$

The proof that $\mathfrak{p}$ is a prime ideal is thus completed. It is of interest to indicate a slight modification of the foregoing construction. The hypothesis that A has two or more elements is equivalent to the hypothesis that A contains two or more ideals. If, then, $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals such that $\mathfrak{b}$ is not divisible by $\mathfrak{a}$, we may suppose that the numbering of $\mathfrak{F}$ is arranged so that $\mathfrak{a}_1 = \mathfrak{a}$ and we may choose a as an element which is in $\mathfrak{b}$ but not in $\mathfrak{a}$ and hence is different from 0. The construction given above then yields a prime ideal $\mathfrak{p}$ which is a divisor of $\mathfrak{a}$ but not of $\mathfrak{b}$. We note also that, when A has a unit e, the proof that $\mathfrak{p}$ is a prime ideal given above assumes a slightly simpler form if one takes $a = e$ at the outset.

In our second proof, which is reminiscent of the discussion of simple extensions of a commutative field, we begin by considering the case of a Boolean ring A with unit e. Let the elements of A be placed in biunivocal correspondence with the ordinal numbers γ less than an appropriately chosen ordinal number ω, the element a corresponding to γ being denoted by a_γ. We may suppose that in this correspondence $a_1 = e$, and that a_2 is different from 0 and e when A has more than two elements and is chosen at pleasure as any element a subject to this restriction. We denote by $\mathfrak{a}_\beta$ the subring of A generated by the class of all elements a_α, $\alpha \leqq \beta$, $1 \leqq \beta < \omega$; and by $\mathfrak{b}_\beta$ the subring of A generated by the class of all elements a_α, $\alpha < \beta$, $1 < \beta < \omega$. It is then evident that $\mathfrak{b}_\alpha \subset \mathfrak{a}_\alpha \subset \mathfrak{b}_\beta \subset \mathfrak{a}_\beta$ for $\alpha < \beta$; that $\mathfrak{a}_\beta = \mathfrak{b}_\beta \vee \{a_\beta\}$, $\beta > 1$, where $\{a_\beta\}$ is the subring generated by the element a_β; and that $\mathfrak{b}_\beta = S_{\alpha<\beta}\mathfrak{a}_\alpha$, $\beta > 1$. We shall now show with the help of the principle of transfinite induction that there exists a homomorphism $A \to B$ where B is a two-element Boolean ring. The subring $\mathfrak{a}_1 = \mathfrak{b}_2$ generated by $a_1 = e \neq 0$ consists of the two elements 0 and e so that we can define a homomorphism (indeed, an isomorphism) from $\mathfrak{a}_1$ to B in just one way. Let us suppose that homomorphisms $\mathfrak{a}_\alpha \to B$ have been defined for all ordinals $\alpha < \beta$ in such a way that the correspondent in B of an element in $\mathfrak{a}_\alpha$ is independent of α. Since $\mathfrak{b}_\beta = S_{\alpha<\beta}\mathfrak{a}_\alpha$, it is then evident that the homomorphisms $\mathfrak{a}_\alpha \to B$ together determine a homomorphism $\mathfrak{b}_\beta \to B$: for, if b and c are elements of $\mathfrak{b}_\beta$, there exists an ordinal $\alpha < \beta$ such that b and c are elements of $\mathfrak{a}_\alpha$, as we see by reference to the properties of the subrings $\mathfrak{a}_\alpha$ noted above; and the homomorphism $\mathfrak{a}_\alpha \to B$ implies that the elements $b+c$, bc have the correspondents b^*+c^*, b^*c^* respectively, where b^* and c^* are the fixed correspondents in B of b and c respectively. Now the subring $\mathfrak{b}_\beta$ evidently contains the element $a_1 = e$. Theorem 14 therefore shows that the subring $\alpha_\beta = \mathfrak{b}_\beta \vee \{a_\beta\}$ consists of those and only those elements of A which are expressible in the

form $xa_\beta + ya'_\beta = xa_\beta \vee ya'_\beta$ where x and y are elements of $\mathfrak{b}_\beta$. Since we have $(x_1a_\beta + y_1a'_\beta) + (x_2a_\beta + y_2a'_\beta) = (x_1+x_2)a_\beta + (y_1+y_2)a'_\beta$, $(x_1a_\beta + y_1a'_\beta)(x_2a_\beta + y_2a'_\beta) = (x_1x_2)a_\beta + (y_1y_2)a'_\beta$, we see that $\mathfrak{a}_\beta$ is a homomorph of the Boolean ring $\mathfrak{B}_\beta$ obtained as the direct sum of $\mathfrak{b}_\beta$ with itself, this homomorphism being given explicitly by the correspondence $(x, y) \to xa_\beta + ya'_\beta$. The ideal $\mathfrak{c}_\beta$ determined by this correspondence consists of those and only those elements (x, y) in $\mathfrak{B}_\beta$ such that $xa_\beta + ya'_\beta = 0$, or, equivalently, $xa_\beta = ya'_\beta = 0$; and $\mathfrak{a}_\beta$ is isomorphic to the quotient ring $\mathfrak{B}_\beta/\mathfrak{c}_\beta$ in accordance with Theorem 43. We note that, if (x, y) is in $\mathfrak{c}_\beta$, then $xy = 0$ since $xy = xye = xy(a_\beta \vee a'_\beta) = xya_\beta \vee xya'_\beta = 0 \vee 0 = 0$. Now the homomorphism $\mathfrak{b}_\beta \to B$ evidently induces a homomorphism $\mathfrak{B}_\beta \to C$, where C is a four-element Boolean ring obtained as the direct sum of B with itself. The image of the ideal $\mathfrak{c}_\beta$ under the latter homomorphism is an ideal $\mathfrak{c}$ in C, by virtue of Theorem 46. The ideal $\mathfrak{c}$ cannot contain the unit element (e^*, e^*) in C since, if an element (x, y) in $\mathfrak{c}_\beta$ has the correspondent (x^*, y^*) in C, then $xy = 0$ implies $x^*y^* = 0^*$ (the unit and zero elements in B being denoted by e^* and 0^* respectively). The four elements of C are $(0^*, 0^*)$, $(0^*, e^*)$, $(e^*, 0^*)$, (e^*, e^*); and the ideal $\mathfrak{c}$ must clearly be a principal ideal generated by one of the three elements $(0^*, 0^*)$, $(0^*, e^*)$, $(e^*, 0^*)$. It is easily verified that the quotient ring $C/\mathfrak{c}$ is homomorphic to $\mathfrak{B}_\beta/\mathfrak{c}_\beta$ and hence also to $\mathfrak{a}_\beta$. We now have three cases to consider, according to the nature of the ideal $\mathfrak{c}$. First, if $\mathfrak{c}$ is the principal ideal generated by the element $(e^*, 0^*)$, $C/\mathfrak{c}$ is a two-element ring which is isomorphic to B in one and only one way. Now, if x is an element of $\mathfrak{b}_\beta$ with correspondent x^* in B under the homomorphism $\mathfrak{b}_\beta \to B$, the homomorphism $\mathfrak{B}_\beta \to C$ takes (x, x) into (x^*, x^*); the homomorphism $\mathfrak{a}_\beta \to C/\mathfrak{c}$ therefore takes $x = xa_\beta + xa'_\beta$ into the class of elements congruent (mod $\mathfrak{c}$) to (x^*, x^*); and the isomorphism $C/\mathfrak{c} \to B$ takes this class, which consists of the two elements (e^*, x^*), $(0^*, x^*)$, into the element x^* in B. Hence the induced homomorphism $\mathfrak{a}_\beta \to B$ takes each element of $\mathfrak{b}_\beta \subset \mathfrak{a}_\beta$ into its correspondent under the homomorphism $\mathfrak{b}_\beta \to B$. A similar result obtains in case $\mathfrak{c}$ is the principal ideal generated by the element $(0^*, e^*)$. Finally, if $\mathfrak{c}$ is the principal ideal generated by the element $(0^*, 0^*)$, the quotient ring $C/\mathfrak{c}$ is isomorphic to C. In this case, we can define a homomorphism $C \to C/\mathfrak{d} \longleftrightarrow B$ by choosing the ideal $\mathfrak{d}$ as the principal ideal generated by $(e^*, 0^*)$ or by $(0^*, e^*)$, thus obtaining, as in the two preceding cases, a homomorphism $\mathfrak{a}_\beta \to B$ which takes each element of $\mathfrak{b}_\beta \subset \mathfrak{a}_\beta$ into its correspondent under the homomorphism $\mathfrak{b}_\beta \to B$. From the hypothesis that there exist homomorphisms $\mathfrak{a}_\alpha \to B$ for all $\alpha < \beta$ we therefore conclude that there exists a homomorphism $\mathfrak{a}_\beta \to B$, with the precise properties indicated above. The principle of transfinite induction thus establishes the existence of a homomorphism $\mathfrak{a}_\beta \to B$ for $\beta < \omega$, such that, when $\alpha < \beta$,

this homomorphism takes each element of $\mathfrak{a}_\alpha$ into its correspondent under the homomorphism $\mathfrak{a}_\alpha \to B$. Since we have $A = S_{\beta<\omega}\mathfrak{a}_\beta$, we conclude finally that there exists a homomorphism $A \to B$ which carries each element of $\mathfrak{a}_\beta$ into its correspondent under the homomorphism $\mathfrak{a}_\beta \to B$. By Theorem 49 the ideal $\mathfrak{p}$ determined in A by this homomorphism is a prime ideal. If A contains an element a not equal to 0 or to e, we may suppose that a does not belong to $\mathfrak{p}$. For, if we take $a_2 = a$, we see that the subring $\mathfrak{a}_2$ consists of the four elements $0, a, a', e$, and hence that we can define the homomorphism $\mathfrak{a}_2 \to B$ by the relations $0 \to 0^*$, $a' \to 0^*$, $a \to e^*$, $e \to e^*$. It is now possible to treat the case of a Boolean ring without unit: we have only to imbed the given ring A in a ring with unit in accordance with Theorem 1 and to construct a homomorphism from the imbedding ring to a two-element Boolean ring B in such a manner that an element $a \neq 0$ in A has as its correspondent in B the element e^*. This homomorphism evidently determines a homomorphism $A \to B$ and hence a prime ideal $\mathfrak{p}$ in A; and we may in particular require that $\mathfrak{p}$ shall not contain a specified element $a \neq 0$. It should be noted that the foregoing construction of a prime ideal consists essentially in the assignment, step-by-step, of the correspondents in B of the elements of A; and that at each step the construction reveals automatically whether the assignment is determined by the preceding steps or not. By particularizing the initial steps of the construction a little more, we can obtain a slightly sharper result. Let A be a Boolean ring with more than two elements and unit e; and let a and b be elements such that $a \neq e$, $b \neq e$, $ab \neq a$. We may then carry out the construction of the homomorphism $A \to B$ as before, setting $a_1 = e$, $a_2 = a$, $a_3 = b$ and determining the homomorphism $\mathfrak{a}_3 \to B$ as the correspondence which takes $0, b, a', a' \vee b, ab, a'b, a'b'$, and $ab \vee a'b'$ into 0^* and takes $a, e, b', a \vee b, a \vee b', a' \vee b', ab'$, and $a'b \vee ab'$ into e^*. We leave the details to the reader, noting that $\mathfrak{a}_3$ is in general a ring of sixteen elements which may reduce to one of eight or of four elements by virtue of equalities, such as $a' = b$, not incompatible with the relations $a \neq e$, $b \neq e$, $ab \neq a$. We then see that the homomorphism $A \to B$ takes a into e^* and b into 0^*, so that the resulting prime ideal $\mathfrak{p}$ contains b but not a. In the case of a Boolean ring A without unit, we obtain a similar result by imbedding A in a ring with unit, constructing a homomorphism from the imbedding ring to the two-element Boolean ring B so that the elements a and b in A with $ab \neq a$ are carried into e^* and 0^* respectively, and then determining $\mathfrak{p}$ from the restricted homomorphism $A \to B$.

In proving Theorem 63, we have obtained certain additional information concerning prime ideals. We now formulate this information as a separate theorem.

THEOREM 64. *If A is a Boolean ring containing elements a and b such that $ab \neq a$ or, equivalently, such that $a < b$ is false, then there exists a prime ideal $\mathfrak{p}$ in A which contains b and not a; and, if A is a Boolean ring containing ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{b}$ is not a divisor of $\mathfrak{a}$, then there exists a prime ideal $\mathfrak{p}$ in A which is divisor of $\mathfrak{a}$ but not of $\mathfrak{b}$.*

We may restrict our reliance upon transfinite methods, however, by proving the following result:

THEOREM 65. *Theorem 64 follows from Theorem 63 without the intervention of transfinite methods or of the well-ordering hypothesis.*

We are now to assume that every Boolean ring containing two unequal elements contains a prime ideal. Let A be a Boolean ring containing elements a and b such that $ab \neq a$. Then the ideal $\mathfrak{c} = \mathfrak{a}(b) \vee \mathfrak{a}'(a)$ cannot contain $\mathfrak{a}(a)$, and, in particular, cannot coincide with the ideal $\mathfrak{e}$: for the relation $\mathfrak{a}(a) \subset \mathfrak{c}$ would imply $\mathfrak{a}(a) = \mathfrak{a}(a)\mathfrak{c} = \mathfrak{a}(a)\mathfrak{a}(b) \subset \mathfrak{a}(b)$ and hence $a = ab$, contrary to hypothesis. Since $\mathfrak{c} \neq \mathfrak{e}$, the quotient ring $A/\mathfrak{c}$ contains two or more elements and hence contains a prime ideal $\mathfrak{q}$. The elements of A which are carried by the homomorphism $A \rightarrow A/\mathfrak{c}$ into elements of $\mathfrak{q}$ constitute a prime ideal $\mathfrak{p}$ in accordance with Theorem 46. It is evident that $\mathfrak{p}$ is a divisor of $\mathfrak{c}$ and hence also of $\mathfrak{a}(b)$. On the other hand, $\mathfrak{p}$ is not a divisor of $\mathfrak{a}(a)$: for, if $\mathfrak{p} \supset \mathfrak{a}(a)$, we should have $\mathfrak{p} \supset \mathfrak{a}(a) \vee \mathfrak{c} = \mathfrak{a}(a) \vee \mathfrak{a}(b) \vee \mathfrak{a}'(a) = \mathfrak{e}$, $\mathfrak{p} = \mathfrak{e}$. Thus $\mathfrak{p}$ contains b but not a. Now let A be a Boolean ring containing ideals $\mathfrak{a}$ and $\mathfrak{b}$ where $\mathfrak{b}$ is not a divisor of $\mathfrak{a}$. The quotient ring $A/\mathfrak{b}$ contains an ideal $\mathfrak{c}$ consisting of all the images of elements of $\mathfrak{a}$ under the homomorphism $A \rightarrow A/\mathfrak{b}$, as we showed in Theorem 46. Since $\mathfrak{b}$ is not a divisor of $\mathfrak{a}$, the ideal $\mathfrak{c}$ contains an element other than the zero element. If we apply the first part of the theorem to the Boolean ring $A/\mathfrak{b}$, its zero element, and the indicated element of $\mathfrak{c}$, we see that $A/\mathfrak{b}$ contains a prime ideal $\mathfrak{q}$ which does not contain the specified element of $\mathfrak{c}$ and hence does not contain $\mathfrak{c}$. The elements of A which have images in $\mathfrak{q}$ under the homomorphism $A \rightarrow A/\mathfrak{b}$ thus constitute a prime ideal $\mathfrak{p}$ which contains $\mathfrak{b}$ but not $\mathfrak{a}$, in accordance with Theorem 46.

It is now easy to establish the Fundamental Proposition of Ideal Arithmetic for Boolean rings.

THEOREM 66. *In a Boolean ring A, every ideal other than $\mathfrak{e}$ is the product of all its prime ideal divisors. This result follows from Theorem 64 without the intervention of transfinite methods or of the well-ordering hypothesis.*

If $\mathfrak{a}$ is an ideal in a Boolean ring A such that $\mathfrak{a} \neq \mathfrak{e}$, then Theorem 64 shows that there exists a prime ideal which is a divisor of $\mathfrak{a}$ (but not of $\mathfrak{e}$), since $\mathfrak{e} \not\subset \mathfrak{a}$.

Hence the product of all the prime ideal divisors of $\mathfrak{a}$ exists and is an ideal divisor $\mathfrak{b}$ of $\mathfrak{a}$. If $\mathfrak{a}$ were not also a divisor of $\mathfrak{b}$, Theorem 64 would establish the existence of a prime ideal containing $\mathfrak{a}$ but not $\mathfrak{b}$, contrary to the definition of $\mathfrak{b}$. The relations $\mathfrak{a} \subset \mathfrak{b}$, $\mathfrak{b} \subset \mathfrak{a}$ together imply that $\mathfrak{a} = \mathfrak{b}$, as we wished to prove.

3. **The perfect representation.** We shall now turn to the study of the representation problem. We can give the fundamental theorem of the theory without any further preliminaries.

THEOREM 67. *Let A be a Boolean ring, $\mathfrak{a}$ an arbitrary ideal in A, $\mathfrak{E}$ the class of all prime ideals in A, $\mathfrak{I}$ the algebraic system of all ideals in A under the operations of unrestricted addition and finite multiplication, $\mathfrak{E}(\mathfrak{a})$ the class of all prime ideals which are not divisors of $\mathfrak{a}$, and $I(A)$ the algebraic system with the classes $\mathfrak{E}(\mathfrak{a})$ as elements and with the operations of forming unrestricted unions and finite intersections. Then the correspondence $\mathfrak{a} \rightarrow \mathfrak{E}(\mathfrak{a})$ determines an isomorphism $\mathfrak{I} \longleftrightarrow I(A)$ in accordance with the relations*

(1) $\mathfrak{E}(\mathfrak{a}) = \mathfrak{E}(\mathfrak{b})$ *if and only if* $\mathfrak{a} = \mathfrak{b}$;

(2) *if $\mathfrak{B}$ is any non-void class of ideals, then*

$$\mathfrak{E}\left(\sum_{\mathfrak{a} \in \mathfrak{B}} \mathfrak{a}\right) = \sum_{\mathfrak{a} \in \mathfrak{B}} \mathfrak{E}(\mathfrak{a});$$

(3) $\mathfrak{E}(\mathfrak{a}\mathfrak{b}) = \mathfrak{E}(\mathfrak{a})\mathfrak{E}(\mathfrak{b})$.

Let $\mathfrak{E}(a)$ denote the class $\mathfrak{E}(\mathfrak{a}(a))$ corresponding to the principal ideal $\mathfrak{a}(a)$; and let $B(A)$ be the algebraic system with the classes $\mathfrak{E}(a)$ as elements and with the operations of forming finite unions, symmetric differences (unions modulo 2), and finite intersections. Then $B(A)$ is a concrete Boolean ring or algebra of classes isomorphic to A by virtue of the correspondence $a \rightarrow \mathfrak{E}(a)$ in accordance with the relations

$$\mathfrak{E}(a) = \mathfrak{E}(b) \text{ if and only if } a = b; \tag{4}$$

$$\mathfrak{E}(a + b) = \mathfrak{E}(a) \,\Delta\, \mathfrak{E}(b); \tag{5}$$

$$\mathfrak{E}(a \vee b) = \mathfrak{E}(a) \subset \mathfrak{E}(b); \tag{6}$$

$$\mathfrak{E}(ab) = \mathfrak{E}(a)\mathfrak{E}(b). \tag{7}$$

The system $B(A)$ is a perfect reduced algebra of classes.

We first establish the numbered relations. Theorem 66 shows at once that (1) is valid. The relation (2) is equivalent to the assertion, obviously true, that a prime ideal fails to contain $S_{\mathfrak{a} \in \mathfrak{B}} \mathfrak{a}$ if and only if it fails to contain at least one of the ideals $\mathfrak{a}$ in $\mathfrak{B}$. Relation (3) is equivalent to the assertion that a prime ideal fails to contain $\mathfrak{a}\mathfrak{b}$ if and only if it contains neither $\mathfrak{a}$ nor $\mathfrak{b}$, and hence to the assertion, already proved in Theorem 40, that a prime ideal contains $\mathfrak{a}\mathfrak{b}$ if and only if it contains at least one of the ideals $\mathfrak{a}$ and $\mathfrak{b}$. The relations (4), (6), and (7) then follow immediately from (1), (2), and (3) respec-

tively by virtue of the respective relations (1), (3), and (4) of Theorem 31. The relation (5) is then an immediate consequence of (6) and (7) through the relations

$$\mathfrak{E}(a+b)\cup\mathfrak{E}(a)\mathfrak{E}(b) = \mathfrak{E}((a+b)\vee ab) = \mathfrak{E}(a\vee b) = \mathfrak{E}(a)\cup\mathfrak{E}(b),$$
$$\mathfrak{E}(a+b)\mathfrak{E}(a)\mathfrak{E}(b) = \mathfrak{E}((a+b)ab) = \mathfrak{E}(0) = \mathfrak{O},$$

where $\mathfrak{O}$ is the void subclass of $\mathfrak{E}$. The fact that the correspondences $\mathfrak{a}\rightarrow\mathfrak{E}(\mathfrak{a})$, $a\rightarrow\mathfrak{E}(a)$ set up isomorphisms $\mathfrak{I}\longleftrightarrow I(A)$, $A\longleftrightarrow B(A)$ respectively is now evident from the numbered relations. It remains to show that $B(A)$ is a perfect reduced algebra of classes. If $\mathfrak{p}$ is any prime ideal in A, then the classes $\mathfrak{E}(a)$ where a is in $\mathfrak{p}$ constitute a prime ideal in $B(A)$; and

$$\sum_{a\in\mathfrak{p}}\mathfrak{E}(a) = \mathfrak{E}(\sum_{a\in\mathfrak{p}}\mathfrak{a}(a)) = \mathfrak{E}(\mathfrak{p})$$

in accordance with the relations (2); and, conversely, if the classes $\mathfrak{E}(a)$ constitute a prime ideal in $B(A)$, the corresponding elements a in A constitute a prime ideal $\mathfrak{p}$ in A. The class $\mathfrak{E}(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal, clearly consists of all prime ideals other than $\mathfrak{p}$; and its complement $\mathfrak{E}'(\mathfrak{p})$ thus consists of $\mathfrak{p}$ alone. The classes $\mathfrak{E}(b)$ where b is not in $\mathfrak{p}$ obviously have the ideal $\mathfrak{p}$ in common. If b is any such element and a is an arbitrary element in $\mathfrak{p}$, then $b+ab$ cannot belong to $\mathfrak{p}$ since it is congruent (mod $\mathfrak{p}$) to b; hence $\mathfrak{E}(b+ab)$ contains $\mathfrak{p}$ and, by virtue of the relations $\mathfrak{E}(a)\mathfrak{E}(b+ab)=\mathfrak{E}(a(b+ab))=\mathfrak{E}(0)=\mathfrak{O}$, is contained in the complement of $\mathfrak{E}(a)$. Thus we see that the intersection of the classes $\mathfrak{E}(b)$ where b is not in $\mathfrak{p}$ is contained in the class

$$\prod_{a\in\mathfrak{p}}\mathfrak{E}'(a) = (\sum_{a\in\mathfrak{p}}\mathfrak{E}(a))' = \mathfrak{E}'(\mathfrak{p}),$$

and thus consists of the ideal $\mathfrak{p}$ alone. These facts show that $B(A)$ is a reduced algebra of classes in accordance with Definition 10; and a perfect algebra of classes in accordance with Definition 12, Theorem 59 and Theorem 66.

We shall now introduce the following definition, justified by the result just established:

DEFINITION 13. *The algebra of classes $B(A)$ associated with a Boolean ring A by Theorem 67 is called the perfect representation of A.*

We call particular attention to the fact that, if A is a Boolean ring of just one element, the class $\mathfrak{E}$ is void and $B(A)$ is an algebra consisting of the void class alone.

The application of Theorem 56 to the perfect representation opens the way to the determination of all representations of a given Boolean ring. We obtain the following result:

THEOREM 68. *Let* A, $\mathfrak{E}$, $\mathfrak{E}(\mathfrak{a})$, $I(A)$, $\mathfrak{E}(a)$, *and* $B(A)$ *have the meanings specified in Theorem* 67. *Let* $\mathfrak{H}$ *be an arbitrary subclass of* $\mathfrak{E}$; $\mathfrak{a}(\mathfrak{H}')$ *the ideal consisting of all elements* a *such that* $\mathfrak{E}(a) \subset \mathfrak{H}'$; $I(A, \mathfrak{H})$ *the algebraic system of all classes* $\mathfrak{H}\mathfrak{E}(\mathfrak{a})$ *under the operations of forming unrestricted unions and finite intersections; and* $B(A, \mathfrak{H})$ *the algebraic system of all classes* $\mathfrak{H}\mathfrak{E}(a)$ *under the operations of forming finite unions, symmetric differences, and finite intersections. Then the correspondence* $\mathfrak{E}(\mathfrak{a}) \rightarrow \mathfrak{H}\mathfrak{E}(\mathfrak{a})$ *determines homomorphisms* $I(A) \rightarrow I(A, \mathfrak{H})$, $I(A, \mathfrak{a}(\mathfrak{H}')) \rightarrow I(A, \mathfrak{H})$, *the latter of which is an isomorphism if and only if* $\mathfrak{E}(\mathfrak{a}(\mathfrak{H}')) = \mathfrak{H}'$ *or, equivalently,* $\mathfrak{H} = \mathfrak{E}'(\mathfrak{a}(\mathfrak{H}'))$. *Similarly the correspondence* $\mathfrak{E}(a) \rightarrow \mathfrak{H}\mathfrak{E}(a)$ *determines a homomorphism* $B(A) \rightarrow B(A, \mathfrak{H})$ *and an isomorphism* $B(A, \mathfrak{H}) \longleftrightarrow B(A/\mathfrak{a}(\mathfrak{H}'))$. *The algebra of classes* $B(A, \mathfrak{H})$ *is perfect if and only if* $\mathfrak{E}(\mathfrak{a}(\mathfrak{H}')) = \mathfrak{H}'$; *and, when this condition is satisfied,* $B(A, \mathfrak{H})$ *is equivalent to* $B(A/\mathfrak{a}(\mathfrak{H}'))$. *If* $\mathfrak{b}$ *is an arbitrary ideal, then we have in particular the result that* $B(A/\mathfrak{b})$ *is equivalent to* $B(A, \mathfrak{E}'(\mathfrak{b}))$. *The ideal* $\mathfrak{a}(\mathfrak{H}')$ *is equal to* $\mathfrak{e}$ *when* $\mathfrak{H}$ *is void and to the product of the prime ideals in* $\mathfrak{H}$ *otherwise.*

Theorem 56 establishes the homomorphism $B(A) \rightarrow B(A, \mathfrak{H})$ at once; and an argument similar to that given in the proof of Theorem 56 shows that $I(A) \rightarrow I(A, \mathfrak{H})$. Since the correspondence $a \rightarrow \mathfrak{E}(a) \rightarrow \mathfrak{H}\mathfrak{E}(a)$ defines a homomorphism $A \rightarrow B(A, \mathfrak{H})$ by virtue of Theorem 67 and the result just proved, we see that there exists an ideal $\mathfrak{b}$ in A such that $A/\mathfrak{b} \longleftrightarrow B(A, \mathfrak{H})$ in accordance with Theorem 43. Since $a \rightarrow \mathfrak{E}(a) \rightarrow \mathfrak{O}$ if and only if $\mathfrak{H}\mathfrak{E}(a) = \mathfrak{O}$ or, equivalently, $\mathfrak{E}(a) \subset \mathfrak{H}'$, we see that this ideal coincides with the class $\mathfrak{a}(\mathfrak{H}')$ described above. Now Theorems 46 and 48 give detailed information concerning the prime ideals in the Boolean rings A, $A/\mathfrak{b}$, and $B(A, \mathfrak{H})$ under the indicated correspondence. If $\mathfrak{p}$ is a prime ideal divisor of $\mathfrak{b}$, then its image $\mathfrak{p}^*$ in $A/\mathfrak{b}$ is a prime ideal, and the image of $\mathfrak{p}^*$ in $B(A, \mathfrak{H})$ is also a prime ideal; conversely, a prime ideal in $B(A, \mathfrak{H})$ is the image of a prime ideal $\mathfrak{p}^*$ in $A/\mathfrak{b}$, and $\mathfrak{p}^*$ is in turn the image of a unique prime ideal divisor of $\mathfrak{b}$. Thus we see that the class of prime ideals in $B(A, \mathfrak{H})$ is in biunivocal correspondence with the class $\mathfrak{E}^*$ of prime ideals in $A/\mathfrak{b}$ and also with the class $\mathfrak{E}'(\mathfrak{b})$ of those prime ideals in A which divide $\mathfrak{b}$. If an ideal $\mathfrak{a}$ in A has the image $\mathfrak{a}^*$ in $A/\mathfrak{b}$, then the prime ideal divisors of $\mathfrak{a}^*$ are in biunivocal correspondence with those prime ideal divisors of $\mathfrak{a}$ which contain $\mathfrak{b}$. Hence the biunivocal correspondence between $\mathfrak{E}'(\mathfrak{b})$ and $\mathfrak{E}^*$ takes $\mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a})$ into $\mathfrak{E}^*(\mathfrak{a}^*)$; and $\mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a}_1) = \mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a}_2)$ whenever $\mathfrak{a}_1$ and $\mathfrak{a}_2$ have the same image in $A/\mathfrak{b}$. It follows that the correspondence $a \rightarrow \mathfrak{E}(a) \rightarrow \mathfrak{H}\mathfrak{E}(a)$ determines a correspondence $\mathfrak{E}^*(\mathfrak{a}^*) \rightarrow \mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a}) \rightarrow \mathfrak{H}\mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a}) = \mathfrak{H}\mathfrak{E}(\mathfrak{a})$ which is a homomorphism $I(A/\mathfrak{b}) \rightarrow I(A, \mathfrak{H})$. We have here used the obvious fact that $\mathfrak{E}(\mathfrak{b}) \subset \mathfrak{H}'$ to write $\mathfrak{H}\mathfrak{E}'(\mathfrak{b}) = \mathfrak{H}$. Since the principal ideal $\mathfrak{a}^*$ in $A/\mathfrak{b}$ is the image of at least one principal ideal $\mathfrak{a}(a)$ in A, we may specialize

this homomorphism to the systems $B(A/\mathfrak{b})$ and $B(A, \mathfrak{H})$. We shall now show that it becomes an isomorphism $B(A/\mathfrak{b}) \longleftrightarrow B(A, \mathfrak{H})$ when so specialized. In order that the principal ideals $\mathfrak{a}(a)$ and $\mathfrak{a}(b)$ in A have the same image in $A/\mathfrak{b}$ we must have $\mathfrak{a}(a) \vee \mathfrak{b} = \mathfrak{a}(b) \vee \mathfrak{b}$, hence $a \vee c_1 = b \vee c_2$ where c_1 and c_2 are in $\mathfrak{b}$, and hence $a \equiv b \pmod{\mathfrak{b}}$, by Theorems 46, 16, and 44 respectively; and the converse is also true. On the other hand, $\mathfrak{H}\mathfrak{E}(a) = \mathfrak{H}\mathfrak{E}(b)$ is equivalent to $\mathfrak{H}\mathfrak{E}(a+b) = \mathfrak{H}\mathfrak{E}(a)\Delta\mathfrak{H}\mathfrak{E}(b) = \mathfrak{O}$ and hence to $\mathfrak{E}(a+b) \subset \mathfrak{H}'$, $a+b \in \mathfrak{b}$, and $a \equiv b \pmod{\mathfrak{b}}$. It follows immediately that the asserted relation of isomorphism holds. In the case where $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$ or, equivalently, $\mathfrak{E}(\mathfrak{b}) = \mathfrak{E}(\mathfrak{a}(\mathfrak{H}')) = \mathfrak{H}'$, it is evident that the correspondence $\mathfrak{E}^*(\mathfrak{a}^*) \rightarrow \mathfrak{H}\mathfrak{E}(\mathfrak{a}) = \mathfrak{E}'(\mathfrak{b})\mathfrak{E}(\mathfrak{a})$ yields an isomorphism $I(A/\mathfrak{b}) \longleftrightarrow I(A, \mathfrak{H})$. Furthermore, it is evident that the correspondence between $\mathfrak{E}^*$ and $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$ renders the two algebras of classes $B(A/\mathfrak{b})$ and $B(A, \mathfrak{H})$ equivalent. Thus $B(A, \mathfrak{H})$ is a perfect reduced algebra of classes in this case, in accordance with Theorems 67 and 55. On the other hand, if $\mathfrak{E}(\mathfrak{b}) \neq \mathfrak{H}'$, there exists a prime ideal $\mathfrak{p}$ in A which belongs to $\mathfrak{H}'$ but not to $\mathfrak{E}(\mathfrak{b})$. It follows that $\mathfrak{p} \supset \mathfrak{b}$ and $\mathfrak{E}(\mathfrak{p}) \supset \mathfrak{H}$. Since $\mathfrak{p}$ is a divisor of $\mathfrak{b}$, its correspondent $\mathfrak{p}^*$ in $A/\mathfrak{b}$ is a prime ideal; and the classes $\mathfrak{H}\mathfrak{E}(a)$ where a is in $\mathfrak{p}$ constitute a prime ideal in $B(A, \mathfrak{H})$. Now the homomorphism $I(A/\mathfrak{B}) \rightarrow I(A, \mathfrak{H})$ takes $\mathfrak{E}^*(\mathfrak{p}^*)$ into $\mathfrak{H}\mathfrak{E}(\mathfrak{p}) = \mathfrak{H}$ and therefore cannot be an isomorphism since it also takes $\mathfrak{E}^* = \mathfrak{E}^*(\mathfrak{e}^*)$ into $\mathfrak{H}$. Furthermore the union of the classes $\mathfrak{H}\mathfrak{E}(a)$, where a is in $\mathfrak{p}$, is given by

$$\sum_{a \in \mathfrak{p}} \mathfrak{H}\mathfrak{E}(a) = \mathfrak{H} \sum_{a \in \mathfrak{p}} \mathfrak{E}(\mathfrak{a}(a)) = \mathfrak{H}\mathfrak{E}\left(\mathrm{S}_{a \in \mathfrak{p}} \mathfrak{a}(a)\right) = \mathfrak{H}\mathfrak{E}(\mathfrak{p}) = \mathfrak{H}.$$

The algebra of classes $B(A, \mathfrak{H})$ therefore fails to have property (2) of Theorem 59, and cannot be perfect. Finally we prove that $\mathfrak{b} = \mathfrak{a}(\mathfrak{H}')$ is characterized in the manner indicated in the statement of the theorem. If $\mathfrak{H}$ is void, then $\mathfrak{E}(a) \subset \mathfrak{H}'$ for every a and $\mathfrak{a}(\mathfrak{H}')$ is obviously equal to $\mathfrak{e}$. If $\mathfrak{H}$ is not void, then the product of all the prime ideals in $\mathfrak{H}$ is an ideal $\mathfrak{c}$. Since $\mathfrak{E}(\mathfrak{p}) \supset \mathfrak{a}(\mathfrak{H}')$ when $\mathfrak{p}$ is in $\mathfrak{H}$, it is evident that $\mathfrak{p} \supset \mathfrak{a}(\mathfrak{H}')$ when $\mathfrak{p}$ is in $\mathfrak{H}$, and hence that $\mathfrak{c} \supset \mathfrak{a}(\mathfrak{H}')$. On the other hand, if a is an element of $\mathfrak{c}$, we have $\mathfrak{a}(a) \subset \mathfrak{c} \subset \mathfrak{p}$ for every $\mathfrak{p}$ in $\mathfrak{H}$ or, equivalently, $\mathfrak{E}(a) \subset \mathfrak{E}(\mathfrak{p})$ for every $\mathfrak{p}$ in $\mathfrak{H}$. Since $\mathfrak{E}(\mathfrak{p})$ does not contain $\mathfrak{p}$, it follows that $\mathfrak{E}(a) \subset \mathfrak{H}'$ and that a is in $\mathfrak{a}(\mathfrak{H}')$. Thus we have $\mathfrak{c} \subset \mathfrak{a}(\mathfrak{H}')$ as well as $\mathfrak{a}(\mathfrak{H}') \subset \mathfrak{c}$, and conclude that $\mathfrak{c} = \mathfrak{a}(\mathfrak{H}')$ as desired. This result shows in particular that, if $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$ where $\mathfrak{b}$ is an arbitrary ideal in A, then $\mathfrak{a}(\mathfrak{H}') = \mathfrak{b}$.

We now complete the theory of representations by means of the following result:

THEOREM 69. *If B is an algebra of classes homomorphic to a Boolean ring A and if $\mathfrak{b}$ is the ideal in A determined by the homomorphism $A \rightarrow B$, then there*

exists a class $\mathfrak{H}$ *of prime ideals in* A *related to* $\mathfrak{b}$ *through the equation* $\mathfrak{a}(\mathfrak{H}') = \mathfrak{b}$ *such that* B *is equivalent to* $B(A, \mathfrak{H})$. *In order that* B *be perfect it is necessary and sufficient that* $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$. *The only perfect algebras of classes isomorphic to* A *are those equivalent to* $B(A)$.

The prime ideals in B are in biunivocal correspondence with the prime ideal divisors of $\mathfrak{b}$ in A, by Theorem 48. Those prime ideals in B which determine one-element subclasses of the basic class E of B in accordance with Theorem 57 (9) thus define a subclass $\mathfrak{H}$ of $\mathfrak{E}'(\mathfrak{b})$. This correspondence between E and $\mathfrak{H}$ is biunivocal and defines the equivalence between B and $B(A, \mathfrak{H})$: for if a is any element of A, the prime ideals which contain it and also contain $\mathfrak{b}$ constitute the class $\mathfrak{E}'(\mathfrak{b})\mathfrak{E}'(a)$; these prime ideals are carried by the homomorphism $A \rightarrow B$ into the prime ideals in B which contain the image of a; of the latter ideals those and only those which determine one-element classes disjoint from the image of a can correspond to ideals in $\mathfrak{H}$; and the indicated correspondence between $\mathfrak{H}$ and E thus takes $\mathfrak{H}\mathfrak{E}'(a)$ into the complement of the image of a, $\mathfrak{H}\mathfrak{E}(a)$ into the image of a. Now those elements a which are taken by the homomorphism $A \rightarrow B$ into the void class in B are precisely those for which $\mathfrak{H}\mathfrak{E}(a)$ is void, as we see from the foregoing remarks. Thus it follows that the ideal $\mathfrak{b}$ determined by the homomorphism in question coincides with the ideal $\mathfrak{a}(\mathfrak{H}')$. If B is perfect, then every prime ideal in B determines a one-element class by Theorem 59; and it follows that $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$. On the other hand, if $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b})$, then $B(A, \mathfrak{H})$ is perfect by Theorem 68; and B, being equivalent to $B(A, \mathfrak{H})$, is obviously perfect also. If B is isomorphic to A, then $\mathfrak{b} = \mathfrak{o}$. Since $\mathfrak{H} = \mathfrak{E}'(\mathfrak{b}) = \mathfrak{E}'(\mathfrak{o}) = \mathfrak{E}$ in this case, B is thus equivalent to $B(A, \mathfrak{E})$, and hence to $B(A)$, if it is perfect. Since $B(A)$ is isomorphic to A and is perfect, any algebra of classes equivalent to $B(A)$ also has these properties.

We may bring the discussion to a close by formulating in precise terms our remarks in §1 concerning the relation between the representation theory and the Fundamental Proposition of Ideal Arithmetic. We have

THEOREM 70. *The following propositions are equivalent without the use of transfinite methods or the well-ordering hypothesis*:

(1) *every Boolean ring possesses an isomorphic algebra of classes*;

(2) *the Fundamental Proposition of Ideal Arithmetic is valid in every Boolean ring.*

In Theorem 67, we have shown that (2) implies (1), without the use of transfinite arguments. In Theorem 58 (4) we showed without the use of such arguments that (1) implies the existence of a prime ideal in any Boolean ring

which is a reduced algebra of classes with a basic class E which is non-void; and hence that (1) implies the Fundamental Existence Proposition, proved as Theorem 63 by other methods. The work of §2 shows that Theorem 63 implies (2), without the use of transfinite arguments, as indicated in Theorem 66.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.