THE THEORY OF BOOLEAN-LIKE RINGS

BY

ALFRED L. FOSTER

1. **Introduction.** This paper is mainly concerned with the study of a certain generalization, first touched on in another communication [1](1), of the concept Boolean ring, a generalization in which many of the formal properties, both ring and "logical," of the latter are preserved, and one which arises naturally from general ring-duality considerations previously introduced [2](2). In the following section we first sketch certain basic notions of this theory, into which we further inject such concepts and theorems as point the theory toward a general logical algebra of rings. Within the framework of such a general logical algebra the class of Boolean-like rings is found coextensive with a certain section of the class of rings which are interdefinably equivalent to their logical algebra, namely, the section in which the relations connecting the basic ring and logical notions are formally identical with those which obtain in the special case of Boolean rings.

In terms of the general logical ring-complement, *, the usual concept of Boolean ring B is completely characterized by the idempotency condition: $aa^* = 0$ for all a of B. For Boolean-like rings H it is found that this is replaced by the two (independent) conditions (D'' of §3):

$$aa^*bb^* = 0, \qquad a + a = 0 \qquad (a, b \in H).$$

In place of ordinary idempotence each element a of H is found to be weakly idempotent: $a^4 = a^2$; this condition is however not characteristic of Boolean-like rings.

All simple Boolean-like algebraic extensions of a Boolean ring are given in §4.

In §§5–7 the role of the nilpotent ideal (and its ring-dual, the unipotent ideal) in a ring R is explored, especially in conjunction with the previously introduced ([1], also §5) concept: the idempotent Boolean ring of R. It is found that the three notions of idempotency, nilpotency and unipotency are very symmetrically related in the case of Boolean-like rings H (Theorems 14–

Presented to the Society, February 24, 1945; received by the editors January 7, 1945.

(1) The numbers in brackets denote references given at the end of the paper.

(2) Throughout this paper the term ring is used synonymously with commutative ring with unit element, and this applies in particular to Boolean rings. As shown in [1], the ring duality theory of [2] may be extended to general rings (not necessarily containing a unit element, nor even commutative). By means of such an extension it is not difficult to modify the Boolean-like ring theory of this paper so that the latter constitutes not merely a generalization of the concept Boolean ring (with unit element), but also of the concept Boolean ring (in which no unit element is demanded), as used by Stone [3].

17). Moreover it turns out that in H each element h is uniquely expressible

$$h = b + \eta$$

as the sum of idempotent b and nilpotent η of H (Theorem 18). Finally a new characterization of Boolean-like rings in terms of these notions is given by Theorem 19.

§§7 and 8 are concerned with the abstract synthesis of Boolean-like rings. The structure of all finite Boolean-like rings (as a hypercomplex ring over B_2 = 2-element Boolean ring) is given by Theorem 23.

2. **Ring-duality and logical algebra of rings.** In the communication [2], which deals with a duality theory of general (commutative) rings (with unit element), $(R, +, \times)$, it was shown, among other things, that the theorems and concepts of R can be arranged in *dual pairs* according to a certain duality theorem for rings (see below), and that this duality reduces to the familiar Boolean duality in case R is a Boolean ring.

In particular, in this theory 0 and 1 are dual elements of R, which elements we also refer to as the Logical-null and -universe of R respectively([3]). Again

$$\begin{gathered} a \times b (= ab) = \text{ring product}, \\ a \otimes b \text{ (also written } a \Delta b) = a + b - ab = \text{dual ring product} \end{gathered} \tag{1.1}$$

are dual ring operations (the ring product is also called *Logical product* in R, the dual ring product is also called *Logical sum* in R); and the unary operation, *,

$$a^* = 1 - a = \text{ring } \textit{complement} \tag{1.2}$$

(also called *Logical complement* in R) is a self-dual operation. Further, $+$ and $\oplus$,

$$\begin{gathered} a + b = \text{ring sum}, \\ a \oplus b = a + b - 1 = \text{dual ring sum}, \end{gathered} \tag{2.1}$$

are dual operations in R, as are also their inverses, $-$, $\ominus$,

$$\begin{gathered} a - b = \text{ring subtraction}, \\ a \ominus b = a - b + 1 = \text{dual ring subtraction}. \end{gathered} \tag{2.2}$$

It is not necessary here to consider other sets of dual concepts. Restricted to the above, the ring-duality theorem of [2] reduces to:

DUALITY THEOREM FOR RINGS (RESTRICTED). *If* $P(0, 1; \times, \Delta; *; +, \oplus; -, \ominus)$ *is a true proposition of the ring* R, *so also is its dual,*

$$\text{dl } P = P(1, 0; \Delta, \times; *; \oplus, +; \ominus, -),$$

obtained by replacing each argument in P *by its dual.*

([3]) All Logical notions (capital L) reduce to familiar logical ones if R is a Boolean ring.

Thus, for instance, in any R

(3) $$a(b + c) = ab + ac,$$

dl (3) $$a \Delta (b \oplus c) = a \Delta b \oplus a \Delta c$$

are dual ring propositions. Again, by way of example, in any (commutative) field F:

(4) $(F_0, \times)$ is an Abelian group, with unit element 1, where $F_0 = F$ less the element 0.

dl (4) (F_1, Δ) is an Abelian group, with unit element 0, where $F_1 = F$ less the element 1.

Or, again in any R,

(5) $$a \Delta b = a + b - ab,$$

dl (5) $$a \times b = a \oplus b \ominus (a \Delta b)$$

are dual propositions.

As already anticipated by previous terminology, of the various concepts defined in a ring R we designate

(6) $$\times, \Delta; *; 0, 1$$

as the *basic Logical concepts* of R, and the system

(7) $$(R, \times, \Delta; *; 0, 1)$$

we call the *Logical algebra* of the ring $(R, +, \times)$. Among the Logical theorems of R (that is, theorems which may be formulated entirely in terms of Logical concepts), we recall the following:

(L1) *$(R, \times)$ is a closed, commutative, associative system in which the null* (0) *and universe* (1) *of the ring satisfy*

$$1a = a1 = a; \qquad 0a = a0 = 0.$$

dl (L1) *(R, Δ) is a closed, commutative, associative system in which the null* (0) *and universe* (1) *of the ring satisfy*

$$0 \Delta a = a \Delta 0 = a; \qquad 1 \Delta a = a \Delta 1 = 1,$$

(L2) $$a^{**} = (a^*)^* = a; \qquad 0^* = 1; \qquad 1^* = 0; \qquad a^* = b^* \rightarrow a = b.$$

"DeMorgan" formula for rings.

(L3) $$(ab)^* = a^* \Delta b^*,$$

dl (L3) $$(a \Delta b)^* = a^* b^*.$$

Finally we mention one form of the

(L4) Logical distributive law for rings. *$a(b \Delta c) = ab \Delta ac$ if and only if $aa^*bc = 0$.*

The above expression aa^*bc, representing the difference $(ab\Delta ac)-a(b\Delta c)$, may appropriately be called the (*Logical*) *distributive excess* of a, b, c (in this order).

dl (L4) $a\Delta bc=(a\Delta b)(a\Delta c)$ *if and only if* $a\Delta a^*\Delta b\Delta c=1$ (*equivalent to*: *if and only if* $aa^*b^*c^*=0$).

The dual ring additions (2.1) and subtractions (2.2) are not in general Logical concepts of a ring R. In the case of certain classes of rings, however, $+$ (and $\oplus$) of $(R, +, \oplus; \times, \Delta; ^*)$, and therefore the complete ring R, is Logically definable, that is, definable in terms of the Logical algebra $(R, \times, \Delta; ^*; 0, 1)$. For such rings, then, the two notions, ring and Logical algebra, are interdefinably equivalent.

One such Logically definable class of rings, as shown in [2], is the class of Boolean rings with unit element, that is (Stone [3]), the class of (necessarily commutative) rings with unit element in which each element is idempotent

$$a^2 = a. \tag{8}$$

For such we have the well known definition of $+$,

$$a + b = ab^* \Delta a^*b, \tag{9}$$

$$a \oplus b = (a \Delta b^*)(a^* \Delta b). \quad \text{dl (9)}$$

Here the right of (9) is more familiar in the $\cup$, $\cap$, $^-$ (logical sum, product, complement) notation as $a+b=(a\cap b^-)\cup(a^-\cap b)$.

A second important class of logically definable rings, with which however we are not concerned in this paper, is the class of all (commutative) fields, as indicated in [2] and shown in detail in [4]. In this case the definition of $+$ in terms of logical notions is more complex than in the Boolean case, (9), and will not be repeated here.

3. **Definitions and basic properties.** We now define:

(D) *A Boolean-like ring* $(H, +, \times)$ *is a Logically definable commutative ring with unit element, in which* $+$ *is defined by the formula* (9).

In other words, the class of Boolean-like rings is the most general Logically definable class of commutative rings with unit element, in which the ring sum, $+$, has the same formal Logical definition, (9), as in the case of Boolean rings. Hence, in particular, every Boolean ring is also Boolean-like. That the converse is not true is shown by the following ring, H_4,

(H_4)

$\times$	0	1	p	q
0	0	0	0	0
1	0	1	p	q
p	0	p	0	p
q	0	q	p	1

$+$	0	1	p	q
0	0	1	p	q
1	1	0	q	p
p	p	q	0	1
q	q	p	1	0

in which Δ and $*$, according to (1.1) and (1.2), are computed to be

Δ	0	1	p	q
0	0	1	p	q
1	1	1	1	1
p	p	1	0	q
q	q	1	q	1

	$*$
0	1
1	0 ·
p	q
q	p

It is then easily verified that (9) holds, and hence that H_4 is Boolean-like. Moreover H_4 is clearly not a Boolean ring, as is evident from $p^2=0$. This is the simplest example of a Boolean-like ring which is not also Boolean.

Using (9), (1.1) and (1.2), (D) may be restated as:

(D′) *A Boolean-like ring is a commutative ring with unit element in which, for all elements* a, b,

$$ab(a \Delta b) = 3ab. \tag{10}$$

Proof. $a+b=ab*\Delta a*b=a(1-b)+b(1-a)-ab(1-a)(1-b)$, $3ab=ab(a+b-ab)=ab(a\Delta b)$.

THEOREM 1. *Each element of a Boolean-like ring satisfies*

$$a + a = 0. \tag{11}$$

That is, Boolean-like rings are of characteristic 2.

Proof. Put $b=1$ in (10) and use (1.1):

$$a(a \Delta 1) = 3a, \qquad a(a + 1 - a) = 3a, \qquad a = 3a.$$

If one recalls the definition of the Boolean logical sum, $\cup$, in terms of ring $+$ and $\times$, namely,

$$a \cup b = a + b + ab,$$

one has the following "converse" to (D) as an immediate consequence of (1.1) and Theorem 1:

THEOREM 2. *In a Boolean-like ring,* $(H, +, \times)$, *the Logical sum* Δ *is definable in terms of ring sum and product by the same formal equation as in the case of Boolean rings,*

$$a \Delta b = a + b + ab. \tag{12}$$

As in the case of Boolean rings one has:

THEOREM 3. *In a Boolean-like ring,* $a\Delta a=a^2$.

This is an immediate corollary of Theorem 1. One further has:

THEOREM 4. *A finite Boolean-like ring consists of* 2^k *elements.*

Proof. This again follows from Theorem 1; in fact, as a consequence of the fundamental structure theorem of finite Abelian groups applied to the $+$ of a ring, the conclusion of Theorem 4 holds for any ring of characteristic 2.

THEOREM 5. *Each element, a, of a Boolean-like ring satisfies*

$$a^4 = a^2. \tag{13}$$

Proof. Put $a=b$ in (10), and use Theorems 1 and 3:

$$a^2(a \Delta a) = 3a^2 = a^2, \qquad a^2 \cdot a^2 = a^2.$$

From this one immediately has the following:

COROLLARY. *For each element a of a Boolean-like ring, and for all non-negative integers n,*

$$a^{n+4} = a^{n+2}.$$

That is, there are at most 3 powers a, a^2, a^3 of a which are distinct. (See also §7.)

We may call an element a of a ring R *weakly idempotent* if a satisfies (13). While the ordinary idempotency, (8), of each element of (a commutative ring with unit element) R characterizes R as a Boolean ring, the weak idempotency of every element of R does not guarantee that R is Boolean-like, Thus, for instance, each element of ((4)), the ring of residues mod 4, is weakly idempotent, but not each element satisfies (11), whence ((4)) is not Boolean-like.

Moreover R need not be Boolean-like even when (13) and (11) are both satisfied by each of its elements. This is seen from the quaternion ring, Q, over the field of residues mod 2, that is

$$Q = \{q_1 + q_2 i + q_3 j + q_4 k\}$$
$$(q_i = 0 \text{ or } 1;\ i^2 = j^2 = k^2 = 1;\ ij = ji = k;\ ik = ki = j;\ jk = kj = i).$$

Here (11) and (13) are satisfied for all elements of Q, the former immediately and the latter since

$$(q_1 + q_2 i + q_3 j + q_4 k)^4 = (q_1 + q_2 i + q_3 j + q_4 k)^2 = q_1 + q_2 + q_3 + q_4.$$

But Q is not Boolean-like since (10) is not satisfied for $a=i$, $b=j$.

$$ij(i \Delta j) = k(i + j + k) = 1 + i + j \neq 3ij (= k).$$

Condition (10) of (D′) is clearly equivalent to the pair

$$ab(a \Delta b) = ab, \tag{14.1}$$

$$a + a = 0. \tag{14.2}$$

Again, (14.1) is equivalent to

$$aa^*bb^* = 0, \tag{14.11}$$

since

$$ab(a \Delta b) = ab \leftrightarrow ab(a \Delta b)^* = 0 \leftrightarrow aba^*b^* = 0,$$

by (1.2) and the ring DeMorgan formula dl(L3). Hence we have the equivalent definition:

(D'') *A Boolean-like ring is a commutative ring with unit element in which, for all elements a, b,*

$$aa^*bb^* = 0, \tag{15.1}$$

$$a + a = 0. \tag{15.2}$$

It is instructive to compare (15.1) with the stronger condition

$$aa^* = 0 \tag{15.11}$$

which, by (1.2) and (8), defines the class of Boolean rings; as is well known, (15.11)$\rightarrow$(15.2). By contrast it is to be noted that the conditions (15.1) and (15.2) which define the class of Boolean-like rings are independent: that (15.1) does not imply (15.2) is again seen from ((4)), the ring of residues mod 4, in which (15.1) is satisfied for all elements a, b but not (15.2); that (15.2) does not imply (15.11) is seen, for example, from F_4 = field of 4 elements. (The above observations concerning independence or dependence of conditions (15.1), (15.2), (15.11), both for Boolean and for Boolean-like rings, are of course made with reference to the standard ring postulates.)

We shall later (Theorem 19) arrive at quite a different definition of Boolean-like rings.

THEOREM 6. *Each element a of a Boolean-like ring satisfies*

$$aa^* \Delta a^*a = 0, \tag{16.1}$$

$$\{(aa^*)^*\}^2 = 1. \tag{16.2}$$

Proof. (16.1) follows from (15.2), (9) and (D). (16.2) follows from (16.1), (L2) and dl(L3):

$$aa^* \Delta a^*a = 0 \leftrightarrow (aa^* \Delta a^*a)^* = 1 \leftrightarrow (aa^*)^*(a^*a)^* = 1.$$

It is to be noted that in (D''), (15.2) cannot be replaced by (16.1) or by (16.2), since (15.1) and (16.1), as well as (16.2), are all satisfied by the non-Boolean-like ring ((4)).

4. **Hypercomplex Boolean-like rings.** We give several hypercomplex examples, including all Boolean-like algebraic extensions of a Boolean ring; each proof is direct, by (1.1) and (D''). (Compare with Theorem 23.)

THEOREM 7. *If H and H' are both Boolean-like rings, so is their direct product $H \times H'$.*

Here, under hypothesis,

$$(a, a')(b, b')(a, a')^*(b, b')^* = (aa^*bb^*, a'a'^*b'b'^*) = (0, 0).$$

THEOREM 8. *Let B be a Boolean ring. A necessary and sufficient condition for the hypercomplex ring*

$$B[i] = \{b + b'i\}, \qquad i^2 = \gamma i + \gamma';\ b, b', \gamma, \gamma' \text{ in } B,$$

to be Boolean-like over B is that

$$\gamma\gamma' = 0. \tag{17}$$

Proof. The condition (17) is necessary, since by Theorem 5 we must have $i^4 = i^2$, that is

$$\gamma(\gamma i + \gamma') + \gamma' = \gamma i + \gamma' \rightarrow \gamma\gamma' = 0.$$

On the other hand (17) is also sufficient, for, using (1.2) and putting $\bar{b} = b + b'i$,

$$\bar{b}\bar{b}^* = (bb^* + b'\gamma') + b'\gamma^* i,$$

from which one easily computes that $\bar{b}\bar{b}^*\bar{c}\bar{c}^* = 0$. Hence H is Boolean-like, by (D'').

The particular case $\gamma = 1$, $\gamma' = 0$ is isomorphic with the direct product $B \times B$[4]. Again, the case $\gamma = 0$, $\gamma' = 1$ is isomorphic with H_4 (beginning of §3); in this case $i^2 = 1$ $(= -1)$, that is, $i = (1)^{1/2} = (-1)^{1/2}$. The case $\gamma = 0$, $\gamma' = 0$ is readily seen to be merely a linear transform of (and therefore isomorphic with) the preceding $B[(1)^{1/2}]$; here $i^2 = 0$, that is $i = \text{“}(0)^{1/2}\text{”}$ and

$$B[(1)^{1/2}] = B[(-1)^{1/2}] \simeq B[(0)^{1/2}].$$

In the same direct manner as in Theorem 8 one easily proves each of the remaining theorems of this section.

THEOREM 9. *Let B be a Boolean ring. A necessary and sufficient condition for the hypercomplex ring*

$$B[j] = \{b + b'j + b''j^2\}\ (j^3 = \gamma j^2 + \gamma' j + \gamma'';\ b, b', b'', \gamma, \gamma', \gamma'' \text{ in } B)$$

to be Boolean-like over B is that

$$\gamma'' = 0, \qquad \gamma' = \gamma^*. \tag{18}$$

THEOREM 10. *Let B be a Boolean ring. A necessary and sufficient condition for the hypercomplex ring*

---

(4) Let $R \times R = R^{(2)}$ denote the direct product of the ring R with itself. $R^{(2)}$ is immediately representable as the special hypercomplex ring over R: $R^{(2)} = \{r_1 j_1 + r_2 j_2\}$ $(r_1, r_2 \in R;\ j_1^2 = j_1, j_2^2 = j_2, j_1 j_2 = j_2 j_1 = 0)$. If R (and hence also $R^{(2)}$) has a unit element, it is represented by $j_1 + j_2$. In other coordinates, $R^{(2)}$ is also representable as the hypercomplex system $R^{(2)} = \{r + r'i\}$ $(r, r' \in R,\ i^2 = i)$, a representation in which the unit element of $R^{(2)}$ is $1 = 1 + 0i$. The correspondence which establishes the isomorphism of these two hypercomplex representations of $R^{(2)}$ is given by $r_1 j_1 + r_2 j_2 \rightarrow r_1 + (r_2 - r_1)i$.

$$B[k] = \{b + b'k + b''k^2 + b'''k^3\}$$
$$(k^4 = \gamma k^3 + \gamma' k^2 + \gamma'' k + \gamma'''; b, b', \cdots, \gamma, \gamma', \cdots \text{ in } B)$$

to be Boolean-like over B is that

$$\gamma = \gamma'' = \gamma''' = 0, \qquad \gamma' = 1. \tag{19}$$

In view of Theorem 5 and the corollary, Theorems 8, 9, 10 exhaust the simple Boolean-like algebraic extensions of B.

THEOREM 11. *If B is a Boolean ring, the hypercomplex ring*

$$B[i_1, \cdots, i_t] = \{b + b'i_1 + \cdots + b^{(t)}i_t\}$$
$$(i_\alpha, i_\beta = 0; \alpha, \beta = 1, \cdots, t; b, b', b'', \cdots \text{ in } B)$$

is Boolean-like.

5. **Nilpotency, idempotency, ideals, and so on.** In this section we make some general observations about idempotency, and so on, most of which apply to arbitrary commutative rings with unit element, R.

In any R the concept of *idempotency is self-dual,*

$$a^2 = a \leftrightarrow a \,\Delta\, a = a. \tag{20}$$

This self-duality was exhibited in several forms in [1], in particular, beside the two forms (20), in the form

$$a^2 = a \leftrightarrow a \times (a \,\Delta\, a) = a \,\Delta\, (a \times a), \tag{20.1}$$

in which the self-duality is inspectionally obvious. In any R then, $\times$-idempotency $=\Delta$-idempotency $=$ idempotency.

This self-duality is not shared by the usual concept of nilpotency

$$a^t = 0 \text{ for some } t,$$

whose dual,

$$a^{[t]} = a \,\Delta\, a \,\Delta \cdots \Delta\, a \ (t \text{ factors}) = 1 \text{ for some } t, \tag{21}$$

we shall call *unipotency.* Let $N = \{\eta\}$ and $U = \{\mu\}$ denote respectively the class of all nilpotent and the class of all unipotent elements of R. (As indicated, Greek η and μ are hereafter exclusively used to denote nilpotent and unipotent elements, respectively.) From (20), (21) and the Duality Theorem one has

$$N = \{\mu^*\} = U^*; \quad U = \{\eta^*\} = N^* \qquad (\eta \in N, \mu \in U). \tag{22}$$

Far from being self-dual, the concept of nilpotency is in fact anti-self-dual in each R, that is:

THEOREM 12. *The classes N and U of all nilpotent and all unipotent elements of R, respectively, are disjoint.*

Proof. Suppose the theorem false, that is, suppose $\alpha \in N$, $\alpha \in U$. Then $\alpha^{t'} = 0$, $\alpha^{[t''1]} = 1$, or, by (22),

$$\alpha^t = 0, \qquad (1 - \alpha)^t = 0 \tag{23}$$

where $t = \max(t', t'')$. From (23) one proves

$$\alpha^{t-1} = 0, \qquad (1 - \alpha)^{t-1} = 0 \tag{24}$$

as follows:

$$(23) \rightarrow \left\{ \begin{array}{c} \alpha^{t-1}(1 - \alpha)^t = 0 \\ (1 - \alpha)^t = 1 - t\alpha + \cdots \pm \alpha^t \end{array} \right\} \rightarrow \alpha^{t-1} = 0,$$

which is the first half of (24). The second half of (24) follows from the part just proved by observing that the transformation $\beta = 1 - \alpha$ interchanges the first and second parts of (23), and also of (24). From the proof that (23)$\rightarrow$(24) one then has, by induction on t, the contradiction ($t = 1$ in (23)): $\alpha = 0$, $1 - \alpha = 0$, which establishes Theorem 12.

Dual to the ordinary concept of ideal (now also called $\times$-ideal) in R is the Δ-*ideal*: The subclass $\mathfrak{a}$ of R is a Δ-ideal in R if

$$\begin{array}{l} a \ominus a' (= a - a' + 1) \in \mathfrak{a} \quad \text{if} \quad a, a' \text{ are in } \mathfrak{a}, \\ r \,\Delta\, a (= r + a - ra) \in \mathfrak{a} \quad \text{if} \quad a \in \mathfrak{a}, r \in R. \end{array} \tag{25}$$

If by $\mathfrak{a}^*$, the *complement* of the ideal $\mathfrak{a}$ (or more generally, of the subclass $\mathfrak{a}$), we mean the class $\{a^*\}$, $a \in \mathfrak{a}$, the duality theorem shows that the complement $\mathfrak{a}^*$ of an $\times$-ideal is a Δ-ideal, and conversely.

When the ring R is described in the dual $\oplus$, Δ "coordinate system" (see [1]) rather than in the conventional $+$, $\times$ one, one has of course to replace the usual $\times$-factor ring $R/\mathfrak{a}$ ($= R/\mathfrak{a}_\times$) by the dual Δ-factor ring $R/\mathfrak{a}_\Delta$. From the treatment of duality and general transformation theory of [2] it follows that these are isomorphic,

$$R/\mathfrak{a}_\times \simeq R/\mathfrak{a}_\Delta. \tag{26}$$

The set N of all nilpotent elements of R form an $\times$-ideal in R, the *nilpotent-ideal*, since

$$\eta^{t'} = 0 \rightarrow (r\eta)^{t'} = r^{t'}\eta^{t'} = 0 \qquad (r \in R),$$

$$\eta_1^{t'} = 0 \quad \text{and} \quad \eta_2^{t''} = 0 \rightarrow (\eta_1 - \eta_2)^{2t} = 0, \qquad t = \max(t', t'').$$

The factor ring $R/N_\times$ then has only the one nilpotent element, 0. Dual to this, the unipotent elements U form a Δ-ideal, $U = N^*$ (by 22), and

$$R/U_\Delta \simeq R/N_\times, \tag{27}$$

and further, R/U_Δ has only the one unipotent element, 1.

In [1] the following generalization of Stone's theorem was proved.

IDEMPOTENT-BOOLEAN RING THEOREM. *If J denotes the set of all idempotent elements of a commutative ring with unit element, $R=(R, +, \times, \oplus, \Delta, *, 0, 1)$, then $(J, \times, *)$ is a Boolean ring (algebra) in which*

$$\begin{aligned} &\times \text{ is the Boolean product,} \\ &* \text{ is the Boolean complement,} \\ &0 \text{ is the Boolean zero (null),} \\ &1 \text{ is the Boolean unit (universe),} \\ &\Delta \text{ is the Boolean logical sum.} \end{aligned} \tag{28}$$

The Boolean ring sum, $+_r$, of J is given by

$$a +_r b = (a - b)^2 = a - 2ab + b. \tag{29}$$

The Boolean ring (algebra) J is called the *idempotent-Boolean ring (algebra)* of R. It is to be noted that, for any R, $(J, \times, \Delta, *)$ is a sub-*algebra* of the Logical algebra (see §2) $(R, \times, \Delta, *)$ of R, but in general, in view of (29), $(J, +_r, \times)$ is not also a sub *ring* of $(R, +, \times)$. Applicable to Boolean-like rings, however, we have the immediate:

COROLLARY. *For a ring $(R, +, \times)$ of characteristic 2, $+_r = +$ and the idempotent-Boolean ring J of R is a subring of R.*

For use in the next section we further observe:

THEOREM 13. *In a commutative ring of characteristic 2, with unit element, if an element r is expressible*

$$r = b + \eta$$

as the sum of an idempotent and a nilpotent element, it is uniquely so expressible.

Proof. If

$$r = b + \eta = b' + \eta' \qquad (b, b' \in J, \eta, \eta' \in N)$$

then $b+b'=\eta+\eta'$. By the preceding theorem and corollary together with the definition of nilpotency, we have

$$(b + b')^t = b + b' = (\eta + \eta)^t = 0,$$

for suitable t. Whence $b=b'$, and therefore $\eta=\eta'$.

6. **Fundamental structure theorems.** In the case of Boolean-like rings the dual concepts of nilpotency and unipotency may be restated to "symmetrically" match the self-dual notion of idempotency (20)—the latter of course holding in arbitrary R—as given by the following theorems:

THEOREM 14. *In a Boolean-like ring, H, an element a is nilpotent only if $a^2=0$, unipotent only if $a^2=1$, idempotent only if $a^2=a$.*

THEOREM dl 14. *In a Boolean-like ring, H, an element a is nilpotent only if $a\Delta a=0$, unipotent only if $a\Delta a=1$, idempotent only if $a\Delta a=a$.*

Proof of Theorem 14. *Nilpotency*: If a is nilpotent in H, then the least integer n such that $a^n=0$ must either be 1, 2 or 3, by the corollary to Theorem 5. But $n\neq 3$, for $a^3=0\rightarrow a^4(=a^2)=0$, by Theorem 5, and n would not be least. Hence if $a\neq 0$, $n=2$, and in any case $a^2=0$. *Unipotency*: The dual of the part just proved is: a is unipotent in H only if $a\Delta a=1$. But $a\Delta a=a^2$ in H, by (1.1) and Theorem 1; whence $a^2=1$. This completes Theorem 14. (It is easily noted from this proof that Theorem 14 and its dual also hold in the somewhat weaker class of rings (i) of characteristic 2, and (ii) in which each element is weakly idempotent. (Compare with the quaternion ring Q referred to in §3.)

Another expression of the symmetry referred to above is given by the following theorem.

THEOREM 15. *In a Boolean-like ring H $(h\in H)$: 1. The class N of all nilpotent elements is identical with the set of elements $\{hh^*\}$. 2. The class U of all unipotent elements is identical with the set of elements $\{h\Delta h^*\}$. 3. The class J of all idempotent elements is identical with the set of elements $\{h^2\}=\{h\Delta h\}$.*

Proof. 1. $(hh^*)^2=h^2(1-h)^2=0$, by Theorems 1, 5, whence hh^* is nilpotent. Conversely if η is nilpotent, that is (Theorem 14) if $\eta^2=0$, then $\eta=\eta\eta^*$, by (1.2). This proves 1. 2 is the dual of 1. 3. h^2 is idempotent, since $(h^2)^2=h^2$, by Theorem 5. Conversely if b is idempotent, $b=b^2$. Finally $h\Delta h=h^2$, by Theorem 3, which completes Theorem 15.

The special nature of the nilpotent subring (ideal), N, in Boolean-like rings is shown by the following theorem.

THEOREM 16. *In a Boolean-like ring, if η, η' are any nilpotent elements,*

$$\eta\eta' = 0, \tag{30}$$

$$\eta\,\Delta\,\eta' = \eta + \eta'. \tag{31}$$

Proof. (30)$\rightarrow$(31), by (1.1). As for (30),

$$\begin{aligned}\eta + \eta' &= \eta\eta'^*\,\Delta\,\eta^*\eta' = \eta(1-\eta') + \eta'(1-\eta) - \eta\eta'(1-\eta)(1-\eta')\\ &= \eta + \eta' + \eta\eta'\end{aligned} \tag{32}$$

by (D), (1.1), Theorems 1 and 14. (30) is then immediate from (32).

The following theorems show the close relationship between J and N in a Boolean-like ring.

THEOREM 17. *If H is a Boolean-like ring, J its idempotent-Boolean subring, N its nilpotent ideal and U its unipotent Δ-ideal, the factor ring H/N is isomorphic with J,*

$$H/N_\times \simeq J; \qquad \text{dl (33)} \qquad H/U_\Delta \simeq J. \tag{33}$$

Proof. We first show that (A): H/N is a Boolean ring. By definition of the latter concept it is merely necessary to show that each element of H/N is idempotent, that is, for any h of H,

$$h^2 \equiv h(N). \tag{34}$$

But (34) is equivalent to showing that $hh^* \equiv 0\ (N)$, which however follows from Theorem 15, and proves (A). Finally to show that the Boolean ring H/N is isomorphic with J it is sufficient to establish that (B): each residue class $H^{(i)}$ of H (mod N) contains one and only one idempotent element. If h_i is an element of $H^{(i)}$, then so is $b=h_i^2$ (by the previous part (A)). But b is idempotent, by Theorem 15, hence $H^{(i)}$ contains at least one idempotent element. It is moreover the only such in $H^{(i)}$, for if an element of $H^{(i)}$, say $b+\eta$ ($\eta \in N$), is idempotent,

$$(b+\eta)^2 = b+\eta,$$

it follows that $b=b+\eta$, that is, $\eta=0$, by Theorems 1, 14 (or 16). This completes Theorem 17.

In establishing Theorem 17 we have simultaneously proved:

THEOREM 18. *In a Boolean-like ring, H, each element h may be expressed in one and only one way*

$$h = b + \eta \tag{35}$$

as the sum of an idempotent element, b, and a nilpotent element, η.

THEOREM dl 18. *In a Boolean-like ring, H, each element h may be expressed in one and only one way*

$$h = b \oplus \mu$$

as the sum, $\oplus$, of an idempotent element, b, and a unipotent element, μ.

The essential content of Theorem 18 is the possibility, and not the uniqueness of the representation (35) for each h of H; uniqueness follows from possibility, even for more general rings than H (Theorem 13).

On the other hand Theorem 18 is not exclusively satisfied by Boolean-like rings; there even exist commutative rings with unit element, of characteristic 2, which are non Boolean-like, and which satisfy Theorem 18. Such for example is the quaternion ring, Q, of §3, whose idempotent elements are $\{0, 1\} = J$, and whose nilpotent elements are $\{0, 1+i, 1+j, 1+k, i+j, i+k, j+k, 1+i+j+k\} = N$, from which it is easily seen that each element of Q has a unique additive decomposition (35).

Theorems 18 and 16 together, however, are characteristic of and may be used as a new definition of the class of Boolean-like rings, according to the following theorem.

THEOREM 19. *A ring R is Boolean-like if and only if*:

(1°) *It is commutative, with unit element.*

(2°) *It is of characteristic* 2.

(3°) *Each element may be expressed as the sum of an idempotent and a nilpotent element.*

(4°) $\eta\eta' = 0$ *for all nilpotent elements* η, η'.

Proof. The necessity of the conditions (1°)–(4°) has already been established by (D), Theorems 1, 16, 18; their sufficiency is seen as follows. Let

$$r = b + \eta, \qquad r' = b' + \eta' \qquad (b, b' \text{ idempotent}; \eta, \eta' \text{ nilpotent})$$

be any elements of R. By (D'') we need merely establish that

$$rr^*r'r'^* = 0. \tag{36}$$

But from (1°)–(4°) it is seen that $rr^* = \eta$ and therefore (36), and with it Theorem 19, is satisfied, because of (4°). We have the immediate corollary.

COROLLARY. *A Boolean-like ring is Boolean if and only if* 0 *is its sole nilpotent element.*

Theorem 18 enables us, in a Boolean-like ring, to refer uniquely to the idempotent *component* (or *part*), h_J, and to the nilpotent part, h_N, of an element h:

$$h = h_J + h_N.$$

We compile a number of easily verified properties of h_J, h_N as the following theorem.

THEOREM 20. *For any elements* a, b, c *of a Boolean-like ring,*

$$(a+b)_J = a_J + b_J; \qquad (a+b)_N = a_N + b_N,$$

$$(ab)_J = a_J b_J; \qquad (ab)_N = a_J b_N + a_N b_J$$

$$[\rightarrow: (ab)_J = 0,\ (ab)_N = ab, \text{ if } b \text{ is nilpotent}],$$

$$(a^*)_J = a_J^*; \qquad (a^*)_N = a_N,$$

$$(a \,\Delta\, b)_J = a_J \,\Delta\, b_J; \qquad (a \,\Delta\, b)_N = a_N b_J^* + b_N a_J^*.$$

Referring to (L4) of §1 and the accompanying remark, in a Boolean-like ring one readily computes the distributive excess of a, b, c to be $a_N b_J c_J = a_N (bc)_J$, that is:

THEOREM 21. *In a Boolean-like ring*

$$a(b \,\Delta\, c) = ab \,\Delta\, ac$$

if and only if $a_N b_J c_J = 0$.

THEOREM dl 21. *In a Boolean-like ring*

$$a \,\Delta\, bc = (a \,\Delta\, b)(a \,\Delta\, c)$$

if and only if $a_N^* \Delta b_J \Delta c_J = 1$ (*equivalent to* $a_N b_J^* c_J^* = 0$).

Of the many instances in which the distributive excess is 0, we especially call attention to (see Theorem 15) the following corollary.

COROLLARY. *In a Boolean-like ring*

$$a^2(b \Delta c) = a^2 b \Delta a^2 c, \tag{37}$$

$$a(bb^* \Delta c) = abb^* \Delta ac, \tag{38}$$

$$\text{dl (37)} \qquad a^2 \Delta bc = (a^2 \Delta b)(a^2 \Delta c),$$

$$\text{dl (38)} \qquad a \Delta [(b^* \Delta b)c] = \{a \Delta (b^* \Delta b)\}\{a \Delta c\}.$$

7. **Abstract synthesis.** Theorems 16 and 1 assert that, abstractly, the nilpotent ideal N in a Boolean-like ring H is a *zero-ring*, that is, a ring of characteristic 2 in which

$$ab = 0 \tag{39}$$

for all elements a, b. Obviously any Abelian group $(G, +)$ in which $g+g=0$ may supply the $+$ of a zero-ring $(G, +, \times)$ with $\times$ defined by (39). From this it is moreover clear—a formal proof requires the axiom of choice—that: for given cardinal number, τ, there exists at most one (abstractly distinct) τ-element zero-ring; in particular if τ is finite, the corresponding zero-ring only exists if

$$\tau = 2^n \qquad (n \geqq 0). \tag{40}$$

(Compare with Theorem 4 and its proof.) If $H = H_{2^h}$ is finite, consisting of 2^h elements (Theorem 4), one has the simple addition formula

$$2^h = 2^n \cdot 2^i = 2^{n+i} \tag{41}$$

where $J = J_{2^i}$, $N = N_{2^n}$ consists of 2^i and 2^n elements respectively.

With an eye on Theorem 19 we ask: *Can at least one H be synthesized from given abstract N and J?* More exactly, given an arbitrary abstract Boolean ring $(J, +', \times')$ and an arbitrary abstract zero-ring $(N, +'', \times'')$, does there exist at least one *corresponding* Boolean-like ring $(H, +, \times) = H: (J, N)$, that is one whose idempotent and nilpotent subrings are respectively isomorphic with J and N? (In this connection it should be remarked that the stronger conjecture, made tempting by Theorem 19, that $H = J \times N$ (direct product) is false, except in the trivial case where $N = \{0\}$ (that is, $H = J$), since only then is J (like N) an ideal in H, an obviously necessary condition for direct product representation(5).) We shall immediately answer the above question in the affirmative (Theorem 22). The more general problem bearing on the

(5) In a direct product $H = J \times N$, the set $J = \{(b, 0)\}$ forms an ideal in H: $(b', 0) - (b'', 0) = (b' - b'', 0)$, $(b, \eta)(b', 0) = (bb', 0)$. However if H contains a nonzero nilpotent element η_0, J cannot be an ideal in H since $(\eta_0 b)^2 = 0$ (by Theorem 16) and hence $\eta_0 b \notin J$ for $b = 1$.

classification of the possible H's which correspond to given J and N involves the study of many-one "representations" of J within the algebra N. This problem is of considerable independent interest as a companion to (and one lying closer to the classical representation theory of groups and algebras than) the *class* representation [3] of abstract Boolean algebras. We shall not here enter into this problem. (See however §8.)

From the representation theory of Boolean algebra as given by Stone [3], we require the result that: each Boolean ring contains at least one prime ideal. We now prove:

THEOREM 22. *To each given abstract Boolean ring* $(J, +', \times')$ *and each abstract zero-ring* $(N, +'', \times'')$ *there corresponds at least one Boolean-like ring* $H = H:(J, N)$.

Proof. Let $\mathfrak{p}$ be a prime ideal in J. Let $(H, +, \times)$ be defined as follows:

$$H = \{(b, \eta)\}(b \in J, \eta \in N);\ (b, \eta) = (b', \eta') \rightarrow b = b', \eta = \eta'. \tag{42.1}$$

$$(b_1, \eta_1) + (b_2, \eta_2) = \text{def.} = (b_1 +' b_2, \eta_1 +'' \eta_2). \tag{42.2}$$

We first define

$$b\eta = \eta b = \begin{cases} 0 & \text{if } b \equiv 0\ (\mathfrak{p}) \\ \eta & \text{if } b \not\equiv 0\ (\mathfrak{p}) \end{cases} \qquad (b \in J, \eta \in N). \tag{42.3}$$

Then let

$$(b_1, \eta_1) \times (b_2, \eta_2) = \text{def.} = (b_1 \times' b_2, b_1\eta_2 +'' b_2\eta_1). \tag{42.4}$$

One readily sees that $(H, +, \times)$ defined by equations (42.1)–(42.4) is a commutative ring with unit element, of characteristic 2, whose idempotent Boolean ring and nilpotent subring are respectively isomorphic with J and N. In particular, with regard to the associativity of $\times$, we have

$$(b_1, \eta_1) \times \{(b_2, \eta_2) \times (b_3, \eta_3)\} = (b_1 \times' b_2 \times' b_3, b_1(b_2\eta_3 +'' b_3\eta_2) +'' (b_2 \times' b_3)\eta_1); \tag{42.5}$$

$$\{(b_1, \eta_1) \times (b_2, \eta_2)\} \times (b_3, \eta_3)\} = (b_1 \times' b_2 \times' b_3, (b_1 \times' b_2)\eta_3 +'' b_3(b_1\eta_2 +'' b_2\eta_1)). \tag{42.6}$$

Since $\mathfrak{p}$ is a prime ideal (that is, the factor ring $J/\mathfrak{p}$ is isomorphic with $B_2 = 2$-element Boolean ring), it follows that

$$\begin{aligned} &b \equiv 0 \rightarrow b \times' c \equiv c \times' b \equiv 0 \\ &b \not\equiv 0 \quad \text{and} \quad c \not\equiv 0 \rightarrow b \times' c \not\equiv 0 \end{aligned} \qquad (\mathfrak{p}). \tag{42.7}$$

By use of (42.7) and (42.3) the associativity of $\times$ follows by comparing the second components of the right sides of (42.5) and (42.6) for each of the 8 cases: b_1, b_2, b_3 independently $\equiv 0$ or $\not\equiv 0$ (mod $\mathfrak{p}$). For example, for $b_1 \not\equiv 0$,

$b_2 \neq 0$, $b_3 \equiv 0$ the right sides of (42.5) and (42.6) become respectively

$$(b_1 \times' b_2 \times' b_3, (b_2\eta_3 +'' b_3\eta_2) +'' 0) = (b_1 \times' b_2 \times' b_3, \eta_3)$$

and

$$(b_1 \times' b_2 \times' b_3, \eta_3 +'' 0).$$

Again, for $b_1 \neq 0$, $b_2 \neq 0$, $b_3 \neq 0$ each right side becomes

$$(b_1 \times' b_2 \times' b_3, \eta_1 +'' \eta_2 +'' \eta_3).$$

Using (D'') we need only verify (15.1):

$$(b, \eta)^* = (b^*, \eta), \qquad (b, \eta)(b, \eta)^* = (0, \eta),$$
$$(b_1, \eta_1)(b_1, \eta_1)^*(b_2, \eta_2)(b_2, \eta_2)^* = (0, \eta_1 \times'' \eta_2) = (0, 0).$$

This verifies (15.1), and therefore proves Theorem 22.

Two extreme special cases yield unique (up to isomorphisms) corresponding H's. If $J = J_2 =$ 2-element Boolean ring, and N is arbitrary, the $H: (J_2, N)$ constructed according to Theorem 22 is easily shown to be the only Boolean-like H corresponding to J_2 and N. Again, on the other extreme, if $N = N_2 =$ 2-element zero-ring, it is seen that $H: (J, N_2)$ constructed according to Theorem 22 is the only corresponding H provided that J has only one type of prime ideal, that is, if J is such that any two prime ideals $\mathfrak{p}$, $\mathfrak{q}$ of J are carried into each other by a suitable automorphism of J. This is the case, for example, if J is a finite Boolean ring; or, more generally, if J is a symmetric Boolean ring (one which is isomorphic with the ring of *all* subsets of some set). Compare with Stone [3].

From the above observations the simplest case where more than one H corresponds to given J and N is where

$$(43) \qquad \begin{aligned} J &= J_{2^2} = \{0, 1, a_1, a_2\} = \text{4-element Boolean ring}, \\ N &= N_{2^2} = \{0, \eta_1, \eta_2, \eta_1 + \eta_2\} = \text{4-element zero-ring}. \end{aligned}$$

Here one readily shows that exactly two abstractly different Boolean-like rings $(H, +, \times_1)$, $(H, +, \times_2)$ correspond to J_4, N_4. If we represent the elements of either ring by the same set (42.1), the two $+$'s are of course identical and given by (42.2); $\times_1$ is determined by Theorem 22, while $\times_2$ is generated from the following table:

$$a_1\eta_1 = \eta_1, \qquad a_1\eta_2 = 0, \qquad a_1(\eta_1 + \eta_2) = \eta_1,$$
$$a_2\eta_1 = 0, \qquad a_2\eta_2 = \eta_2, \qquad a_2(\eta_1 + \eta_2) = \eta_2.$$

There are then, for example, exactly 5 abstractly distinct Boolean-like rings of 2^4 elements: the above two, corresponding to J_4, N_4; and one each corresponding to J_{16}, N_1; J_8, N_2; J_2, N_8.

The structure of all finite Boolean-like rings is determined by Theorem 23, in which the notation $H = H_{2^k}$, and so on, is that of (40), (41).

THEOREM 23. *A finite Boolean-like ring* H $(=H_{2^h})$, *with idempotent Boolean and nilpotent subrings* J $(=J_{2^j})$ *and* N $(=N_{2^n})$, *may be represented as a hypercomplex ring* (44) *over the 2-element ring* B_2, *with base satisfying* (45). *Conversely, each such hypercomplex system* (44) *satisfying* (45) *is a finite Boolean-like ring*:

$$r_1 + r_2a_2 + \cdots + r_ja_j + r_{j+1}\eta_1 + \cdots + r_{j+n}\eta_n \qquad (r_i = 0 \text{ or } 1), \tag{44}$$

$$a_ia_{i'} = \begin{cases} 0 & \text{if } i \neq i' \\ a_i & \text{if } i = i' \end{cases} \qquad (i, i' = 2, 3, \cdots, j), \tag{45.1}$$

$$\eta_\alpha\eta_\beta = 0 \qquad (\alpha, \beta = 1, 2, \cdots, n), \tag{45.2}$$

$$a_i\eta_\alpha = \eta_\alpha a_i = \sum_{\beta=1}^{n} t_{i\alpha\beta}\eta_\beta \quad (t_{i\alpha\beta} = 0 \text{ or } 1;\ i = 2, \cdots, j;\ \alpha = 1, \cdots, n), \tag{45.3}$$

$$\sum_{\beta=1}^{n} t_{i\alpha\beta}t_{i'\beta\mu} = \begin{cases} 0 & \text{if } i \neq i', \\ t_{i\alpha\mu} & \text{if } i = i'. \end{cases} \tag{45.4}$$

Proof. As is well known, (I) each finite Boolean ring $B = B_{2^j}$ is a direct power

$$B_{2^j} = [B_2]^{(j)} = B_2 \times B_2 \times \cdots \times B_2 \ (j \text{ factors})$$

of the 2-element ring B_2; B is hypercomplex over B_2, and as a base one may for instance take the set $a_1, a_2, \cdots, a_j$ of atoms (= $\times$-irreducible elements) of B, or also the (normalized) base 1 $(=\sum_{i=1}^{j} a_i)$, $a_2, a_3, \cdots, a_j$ (in which the unit element of B is exhibited), and these elements then satisfy (45.1). (See footnote 5; also van der Waerden [5, vol. 2, chap. 15].) Again, from the remark following Theorem 4, one has (II) each finite zero-ring $N = N_{2^n}$ is hypercomplex over B_2, where as base one may select any base $\eta_1, \eta_2, \cdots, \eta_n$ of the additive group—whose type is (2, 2, 2, $\cdots$, 2), n terms—of N; the η_i then satisfy (45.2). From (I), (II) and Theorem 18 it follows that each finite Boolean-like H is representable in the form (44), with a base satisfying (45.1)–(45.3) (the latter since N is an ideal in H), and (45.4), which follows from the associativity of $\times$ (see below). This proves the direct part of Theorem 23.

Proof of converse part. A hypercomplex system (44) over B_2 with basis elements satisfying (45.1)–(45.3) is obviously a commutative system with unit element, and is seen to be associative if and only if

$$a_i(a_{i'}\eta_\alpha) = (a_ia_{i'})\eta_\alpha \qquad (i, i' = 2, \cdots, j;\ \alpha = 1, \cdots, n) \tag{46}$$

If we use (45.1) and (45.3), equations (46) reduce to the conditions (45.4). Hence a hypercomplex system (44) over B_2 satisfying (45) is a commutative ring with unit element, and there remains only to show that it is Boolean-like. Since (15.2) of (D″) is satisfied, it is only necessary to establish (15.1). If

$$r = r_1 + r_2a_2 + \cdots + r_{j+n}\eta_n, \qquad r' = r'_1 + r'_2a_2 + \cdots + r'_{j+n}\eta_n,$$

one easily computes that

$$rr^* = \sum_{\alpha=1}^{n} r_{j+\alpha}\eta_\alpha$$

and hence $rr^*\, r'r'^* = 0$, thus verifying (15.1). This completes Theorem 23.

8. **On factorization.** This section is essentially a preface to a general theory of prime factorization, both elementary and ideal-theoretic, in arbitrary Boolean-like rings, a study not here undertaken and one which leans heavily on the many-one representations of Boolean rings mentioned in §7 (see also below). We here confine ourselves to an illustration of (elementary) prime factorization in a finite Boolean-like ring, and to several observations on primes, and so on, pertinent thereto.

Let $N = \{\eta\}$ and $J = \{b\}$ be the nilpotent ideal and the idempotent Boolean subring of the Boolean-like ring H. Since N is an ideal in H, the set of all transformations $\{T_b\}$ $(b \in J)$ of the "space" N into (all or part of) itself,

$$T_b\colon \quad \eta \to \eta' = b\eta,$$

constitutes a *zero-ring representation* of the Boolean ring J. Unlike the usual representations of algebras, the transformations T_b of N are not in general 1-1; however, as in any representation, one clearly has

$$T_bT_c = T_{bc}; \qquad T_{b+c} = T_b + T_c.$$

Moreover, using (1.2), one has

$$0\eta = 0, \qquad 1\eta = \eta, \qquad b0 = 0,$$

$$b\eta = \eta' \to b\eta' = \eta', \tag{47}$$

$$b\eta = \eta' \to b^*\eta' = 0.$$

A point (=element) η_0 of N is *fixed* under b $(=T_b)$ if $b\eta_0 = \eta_0$. Obviously 0 is fixed under all b, and each point of N is fixed under 1 (the identity transformation). There are in general elements c other than 1 which leave each point of N fixed,

$$c\eta = \eta \text{ for all } \eta.$$

Such elements are called 1-*like*. Similarly c is 0-*like* if

$$c\eta = 0 \text{ for all } \eta.$$

By (47) one has: If b is 1-like then b^* is 0-like, and conversely.

LEMMA 1. *If b is such that, for each η_0, $b\eta = \eta_0$ has a solution, η, then b is 1-like.*

Proof. Suppose the lemma false, that is, suppose that for some η_0, $b\eta_1 = \eta_0$ with $\eta_1 \neq \eta_0$. Then let η_1' satisfy $b\eta_1' = \eta_1$. By (47) we then have the contradiction

$$b\eta_1 = \eta_1, \qquad b\eta_1 = \eta_0, \qquad \eta_1 \neq \eta_0.$$

LEMMA 2. *The* $(\times)$*-units*(6) *of* H *consist of the set of elements* $\{1+\eta\}$ $(\eta \in N)$.

Proof. Since $(1+\eta)^2=1$, $1+\eta$ is obviously a unit. Conversely, using Theorem 18, if $b+\eta$ is a $\times$-unit, that is,

$$(b+\eta)(b'+\eta') = 1$$

for suitable b', η', then $bb'=1$, $b\eta'+b'\eta=0$; that is, $b=b'=1$, $\eta=\eta'$.

As customary, elements differing only by a unit factor are called *associated*, $\sim$.

THEOREM 24. *Two elements* h $(=b+\eta)$, h' $(=b'+\eta')$ *of* H *are associated,* $h\sim h'$, *if and only if* (i) $b=b'$, (ii) $b(\eta+\eta')=\eta+\eta'$, *that is,* $\eta+\eta'$ *is a fixed point of the transformation* b.

Proof. If (i) and (ii) hold, $h\sim h'$, for then

$$(1+\eta+\eta')(b+\eta) = b+\eta+b\eta+b\eta' = b+\eta+\eta+\eta' = b+\eta',$$

by Lemma 2. Hence (i) and (ii) are sufficient. They are also necessary. For, suppose $b+\eta\sim b'+\eta'$. Then there must exist an η_0 such that

$$(1+\eta_0)(b+\eta) = b'+\eta',$$

that is,

$$b+\eta+b\eta_0 = b'+\eta'.$$

By Theorem 18 one then has $b=b'$, $\eta+b\eta_0=\eta'$. The second of these equations implies (ii), by (47), and completes the proof. Two special cases are worth singling out:

COROLLARY 1. $b\sim b+\eta$ *if and only if* $b\eta=\eta$.

COROLLARY 2. $b+\eta\sim b+\eta'(\sim b)$ *for all* η, η' *if and only if* b *is* 1*-like.*

The prime elements(7) of the Boolean ring J of H are related to certain prime elements of H by the following theorem.

THEOREM 25. *If* p *is a prime element of the Boolean ring* J *of* H: (a) *if* p *is* 1*-like, then* $p+\eta$ *is a prime of* H *for any* η *of* N, *and all these primes are associated,*

$$p+\eta \sim p+\eta'(\sim p);$$

(b) *if* p *is not* 1*-like, then a necessary and sufficient condition for* $p+\eta$ *to be a prime of* H *is that* η *be not fixed under* p,

---

(6) The (two word) terminology "unit element," consistently employed to denote the usual multiplicative-identity, is not to be confused with the single word "unit" used synonymously with "a divisor of 1." This terminology, while sometimes awkward, seems more standard than that used in the earlier papers [1, 2, 4], in which "unity" = "unity element" (German *Einheit*) was used in place of the present "unit."

(7) As is well known J (and hence also H) may of course contain no prime element.

$$p\eta \neq \eta. \tag{48}$$

Proof. If p is a prime of J, then by Theorem 18 and Lemma 2, the only possible factoring of $p+\eta$ into two factors, neither of which is a unit, is of the form

$$p + \eta = (p + \eta_1)(p + \eta_2). \tag{49}$$

Part (a) If for given η any factoring (49) of $p+\eta$ is presented, $p+\eta \sim p+\eta_1 \sim p+\eta_2$, by Theorem 24 and hypothesis (a) on p. This proves (a).

Part (b) *Sufficiency.* The condition (48) is sufficient, for if (48) is satisfied, $p+\eta$ can only have unit divisors, since, using Theorem 18, any other factoring, (49), would imply $p(\eta_1+\eta_2)=\eta$. By (47) this implies $p\eta=\eta$, contradicting (48). *Necessity.* Suppose (48) is false. Then, using our hypothesis on p, we have (1°) $p+\eta=$prime of H, (2°) $p\eta=\eta$, and (3°) $p\eta_1 \neq \eta_1$ for some η_1 of N. From these we have

$$(p + \eta) = (p + \eta_1)(p + \eta_1 + \eta). \tag{50}$$

Now neither factor on the right of (50) is a unit, by Lemma 2, and neither is associated with $p+\eta$, by (3°) and Theorem 24. Hence (50) says that $p+\eta$ is composite, contrary to hypothesis. This contradiction completes the proof of Theorem 25. It is to be noted that, in the case (b) of Theorem 25, there may be many non-associated primes $p+\eta$, $p+\eta'$, $\cdots$ "belonging" to the same prime, p, of J. (Compare with the last example below.)

We illustrate elementary prime factorization in Boolean-like rings with the following example.

Example. As H take the Boolean-like ring of $2^3 \cdot 2^2$ elements, with $J=J_{2^3} = \{0, a_1, a_2, a_3, a_1+a_2, a_1+a_3, a_2+a_3, a_1+a_2+a_3=1\}$ (where a_1, a_2, a_3 are the atoms of J; the primes of J are then $p_1=a_2+a_3$, $p_2=a_1+a_3$, $p_3=a_1+a_2$); with $N=N_{2^2}=\{0, \eta_1, \eta_2, \eta_1+\eta_2\}$; and where the $\times$ of H is determined, according to §7, by the generating equations

$$\begin{aligned} a_1\eta_1 &= \eta_2, & a_1\eta_2 &= \eta_2, \\ a_2\eta_1 &= \eta_1 + \eta_2, & a_2\eta_2 &= 0, \\ a_3\eta_1 &= 0, & a_3\eta_2 &= 0. \end{aligned}$$

The separation of H into classes of associated elements yields:

$$\begin{aligned} 0 &= \{0\}, \quad 1 = \{1, 1+\eta_1, 1+\eta_2, 1+\eta_1+\eta_2\}, \\ E_1 &= \{\eta_1\}, \quad E_2 = \{\eta_2\}, \quad E_3 = \{\eta_1+\eta_2\}, \\ P_1 &= \{a_1+a_2, a_1+a_2+\eta_1, a_1+a_2+\eta_2, a_1+a_2+\eta_1+\eta_2\}, \\ P_2 &= \{a_1+a_3+\eta_1, a_1+a_3+\eta_1+\eta_2\}, \quad P_3 = \{a_2+a_3+\eta_1, a_2+a_3+\eta_2\}, \\ A_1 &= \{a_1, a_1+\eta_2\}, \quad A_2 = \{a_1+\eta_1, a_1+\eta_1+\eta_2\}, \end{aligned}$$

$$A_3 = \{a_2,\ a_2 + \eta_1 + \eta_2\}, \qquad A_4 = \{a_2 + \eta_1,\ a_2 + \eta_2\}, \qquad A_5 = \{a_3\},$$
$$A_6 = \{a_3 + \eta_1\}, \qquad A_7 = \{a_3 + \eta_2\}, \qquad A_8 = \{a_3 + \eta_1 + \eta_2\},$$
$$A_9 = \{a_1 + a_3,\ a_1 + a_3 + \eta_2\}, \qquad A_{10} = \{a_2 + a_3,\ a_2 + a_3 + \eta_1 + \eta_2\}.$$

Here P_1, P_2, P_3 are the prime classes, and with the usual definition of class multiplication, one readily verifies the following unique prime decomposition of each class not equal to 1:

$$E_1 = P_1P_2P_3, \quad E_2 = P_1P_2^2P_3, \quad E_3 = P_1P_2P_3^2, \quad A_1 = P_1P_2^2, \quad A_2 = P_1P_2,$$
$$A_3 = P_1P_3^2, \quad A_4 = P_1P_3, \quad A_5 = P_2^2P_3^2, \quad A_6 = P_2P_3, \quad A_7 = P_2^2P_3,$$
$$A_8 = P_2P_3^2, \quad A_9 = P_2^2, \quad A_{10} = P_3^2, \quad 0 = P_1P_2^2P_3^2.$$

Certain complications may arise, even for finite Boolean-like rings H, in case several non-associated primes of H belong to a given prime of J. Such, for example, is the case for the $H_{2^2\cdot 2^4}$ with $J = J_{2^2}$ (and atoms a_1, a_2), with $N = N_{2^4}$ (and η_1, η_2, η_3, η_4 as generators), and with $\times$ determined by

$$a_1\eta_1 = \eta_2, \qquad a_1\eta_2 = \eta_2, \qquad a_1\eta_3 = \eta_4, \qquad a_1\eta_4 = \eta_4,$$
$$a_2\eta_1 = \eta_1 + \eta_2, \qquad a_2\eta_2 = 0, \qquad a_2\eta_3 = \eta_3 + \eta_4, \qquad a_2\eta_4 = 0.$$

We shall not write down the associated classes in detail; it may, however, be verified, exactly as in the previous example, that each such associated class may be expressed as the product of prime classes, but not always uniquely. The uniqueness of the representation is restored if one agrees not to distinguish between the prime classes belonging to the same prime of J, despite the non-associated nature of these classes. It is planned to take up these matters in detail at another time in connection with the study of zero-ring representations of Boolean rings previously referred to.

Bibliography

1. A. L. Foster, *The idempotent elements of a commutative ring form a Boolean algebra; ring duality and transformation theory*, Duke Math. J. vol. 12 (1945) pp. 143–152.

2. A. L. Foster and B. A. Bernstein, *Symmetric approach to commutative rings with duality theorem: Boolean duality as special case*, Duke Math. J. vol. 11 (1944) pp. 603–616.

3. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc. vol. 40 (1936) pp. 37–111. *Postulates for Boolean algebras and generalized Boolean algebras*, Amer. J. Math. vol. 57 (1935) pp. 703–732.

4. A. L. Foster and B. A. Bernstein, *A dual-symmetric definition of field*, Amer. J. Math. vol. 67 (1945) pp. 329–349.

5. B. L. van der Waerden, *Moderne Algebra*, Springer.

University of California,
Berkeley, Calif.