p-RINGS AND THEIR BOOLEAN-VECTOR REPRESENTATION.

By

ALFRED L. FOSTER
of UNIVERSITY of CALIFORNIA, BERKELEY.

1. **Introduction.** In a series of earlier papers[1] [1], ..., [7] both the (simple) duality theory of rings, and later the general K-ality theory (not only of rings, but of arbitrary operational disciplines), corresponding to a preassigned group K of admissible "coordinate transformations" in the ring (or discipline) were introduced and studied. Among the interesting concepts which were shown to evolve from this general theory is the notion "ring-logic",—or "ring-algebra" (mod K). In this connection the class of "p-rings" was shown to possess an enveloping "p-ality theory" which generalizes the familiar duality of Boolean rings (and algebras),—which latter are simply 2-rings ($p = 2$). Furthermore for the special cases $p = 2$ and $p = 3$, it was explicitly shown in [1] and [4] that such p-rings are ring-logics (mod N), where N is the "natural group" (see § 2),—with the status of general p-rings, i. e., $p > 3$, left undecided.

Here, for given p (= prime), a p-ring,—as first introduced by Mc Coy and Montgomery [8], is a commutative ring with unit[2] in which for all elements a,

$$a^p = a \tag{1.1}$$

$$pa = 0 \, . \tag{1.2}$$

The concept p-ring is an evident generalization of that of Boolean ring ($p = 2$). (In this Boolean case, $p = 2$, the condition (1.2) is a familiar consequence of (1.1); however for $p > 2$ (1.2) is independent).

The following well known result of Stone [9]:

(1°) *Each Boolean ring is isomorphically representable as a ring of classes, or,*

[1] Square brackets refer to the appended bibliography.

[2] For Mc Coy and Montgomery, [8], the notion "p-ring" does not demand the existence of a unit.

what is equivalent, is isomorphic with a subring of some (finite or infinite) direct power of F_2 (= 2-element Boolean ring = field of residues mod 2),

was generalized by Mc Coy and Montgomery in [8] to:

(2°) *Each p-ring is isomorphic with a sub-ring of some direct power of F_p (=field of residues mod p).*

In connection with this result they showed that

(3°) *Each finite p-ring is isomorphic with a direct power of F_p.*

The present communication is concerned with a further study of p-rings, within the framework of the ring-duality and K-ality theories. In I, for each Boolean ring J and each integer n we define (§ 3) a certain vector ring "over" J, the "J-partition-vector ring" or "Boolean-vector ring" of degree n. Here the definition of the vector sum as well as that of vector product, in terms of ground concepts, is given by means of a symmetric kind of operation, as a consequence of which these Boolean vector-rings are "hypercomplex" over J only in an extended sense[3].

Among other things it is shown that the Boolean-vector rings of degree p-prime are p-rings ((1.1), (1.2)). It is then further established, in II, that each (abstract) p-ring is (uniquely) isomorphically representable as a Boolean-vector ring, and hence that these two classes of rings are identical, up to isomorphisms. This isomorphism, in turn, leads to the complete classification of p-rings in terms of their "idempotent Boolean sub-algebras" (Theorem 10). To mention but one consequence of this theory, it is shown that each element of a p-ring may be expressed as a sum of $\frac{p(p-1)}{2}$ idempotent elements. As another consequence the previously mentioned results (2°) and (3°) of Mc Coy and Montgomery,—in fact a related stronger result (Theorem 12) are derived.

A further application of the present theory leads to an affirmative answer to the above mentioned previously unsolved problem; in fact it may be shown that all p-rings are ring-logics (mod N). A demonstration of this result will not however be given here, but will be presented in a subsequent communication in connection with various applications of p-rings and their N-ality theory.

[3] One may reasonably object to the retention of the "vector" terminology in the face of the non-traditional vector addition. It was however thought desirable to adhere to the familiar expressions since, as will be shown (a) each "vector" is uniquely determined by certain components, and (b) under certain simple conditions the "vector sum" degenerates to the orthodox vector sum.

I

BOOLEAN-VECTOR RINGS

2. Some notions and results from the ring-duality and K-ality theories.

In this section we shall lightly touch on a few points of back-ground taken from [1], ..., [7]. Let $R = (R, +, \times)$ be a ring (here always understood to possess a unit), and let

$$K = \{\ldots, \varrho, \ldots\} = \{\xi, \varrho', \varrho'', \ldots\} \tag{2.1}$$

be a group of "coordinate transformations" in (= 1—1 self mappings or permutations of) R,

$$x \to \varrho(x)\ , \quad (x, \varrho(x) \quad \in\text{'s } R\ , \quad \varrho \in K)\ , \tag{2.2}$$

where ξ is the identity of K, $\xi(x) \equiv x$, and where the inverse of ϱ is written ϱ^-. Each concept of the ring $(R, +, \times)$ may then be expressed in, that is, may be cogrediently transformed with the various coordinate systems $\varrho \varepsilon K$. In particular a multitation[4] (= operation of one or more arguments) $\sigma(x, y, \ldots)$ of the class R "becomes", in the "ϱ coordinate system", the multitation σ_ϱ, where

$$\sigma_\varrho(x, y, \ldots) = \varrho^-\big(\sigma(\varrho(x), \varrho(y), \ldots)\big)\ . \tag{2.3}$$

Here the (isomorphic) multitations σ and σ_ϱ are the "same" operations, expressed in different coordinates. In this sense the rings

$$(R, +, \times)\ , \quad (R, +', \times')\ , \quad (R, +'', \times'')\ , \quad \ldots \tag{2.4}$$

represent the "same" ring, expressed in the $\xi, \varrho', \varrho'', \ldots$ coordinate systems respectively, where the set of "K-al" products

$$\times, \times', \times'', \ldots \tag{2.5}$$

are the "transforms" (2.3) of $\times$ by $\xi, \varrho', \varrho'', \ldots$ respectively, and similarly for the K-al sums, differences, etc.,

$$+, +', +'', \ldots; \quad -, -', -'', \ldots; \quad \text{etc.} \tag{2.6}$$

For instance

$$\begin{aligned} a \times' b &= \varrho^-\big(\varrho(a) \times \varrho(b)\big) \\ a +' b &= \varrho^-\big(\varrho(a) + \varrho(b)\big)\ , \text{ etc.}\ . \end{aligned} \tag{2.7}$$

The "K-algebra"—also called the "K-logic" of the ring R is the (operationally-,

[4] Compare with [5].

i. e., compositionally-closed) algebra

$$(R, \times, \times', \times'', \ldots; \quad \xi, \varrho', \varrho'', \ldots), \tag{2.8}$$

also briefly written

$$(R, \times, K) = (R, \times', K) = (R, \times'', K) = \text{etc.}, \tag{2.9}$$

operating in the same class R as the ring, but whose operations are confined to the set of K-al ring products $\times, \times', \times'', \ldots$ together with the operations (permutations) $\xi, \varrho', \varrho'', \ldots$ comprising the group K. Of the various categories of "K-algebraic ($=$ K-logical) definability",—see [4] and [1], we here recall only one.

Each ring uniquely determines its K-algebra (K-logic), (2.8). If, conversely, a ring $(R, +, \times)$ is "fixed" by its K-algebra, i. e., if: (a) no other ring $(R, +_1, \times)$ exists (on the same class R and with the same $\times$, but with $+_1 \not\equiv +$) which has the same K-algebra as $(R, +, \times)$, and if (b) the ring sum, $+$, of R is equationally definable in terms of its K-algebra, that is, if an identity exists

$$a+b \underset{a,\,b}{\equiv} \varphi(a, b), \qquad (a, b \in\text{'s } R), \tag{2.10}$$

in which $\varphi(a, b)$ is some (compositional) combination of the K-logical operations $\times, \times', \times'', \ldots, \xi, \varrho', \varrho'', \ldots$ we speak of R as a "ring-algebra (K)",—or "ring-logic (K)".

We are here concerned with only two groups of coordinate transformations, namely: (1°) the "simple" or "complementation" group, C,—of order 2, consisting of

$$\begin{aligned} x^* &= 1-x \\ x^{**} &= (x^*)^* = \text{identity}, \end{aligned} \tag{2.11}$$

and (2°) the "cyclic negation" or "natural" group, N, consisting of the group generated by $\hat{}$,

$$x\hat{} = 1+x. \tag{2.12}$$

Unlike the group C the order of the group N will of course depend on the characteristic of the ring R. For a ring of characteristic p,—in particular for p-rings, N is of order p.

Corresponding to the group C the concepts of R occur in (simple) dual pairs, or "C-als". In particular: 0 and 1 are dual elements; $\times, \otimes$; $+, \oplus$; $-, \ominus$; $*$ are respective dual pairs of operations[5],—the latter, $*$, being self dual, where, by ap-

[5] For the simple group C we shall always use the circle notation $\otimes$, $\oplus$, etc. instead of the general $\times', \ldots, +', \ldots$ etc. notation of (2.5), (2.6).

plication of (2.7), these are given by

$$
\begin{aligned}
&\begin{cases} a\otimes b = a+b-a\times b \\ a\times b = a\oplus b\ominus a\otimes b \end{cases} \\
&\begin{cases} a\oplus b = a+b-1 \\ a+b = a\oplus b\ominus 0 \end{cases} \\
&\quad a\ominus b = a-b+1 \\
&\quad a-b = a\ominus b\oplus 0 \\
&\quad a^* = \begin{cases} 1-a \\ 0\ominus \mathrm{a}\ . \end{cases}
\end{aligned}
\tag{2.13}
$$

The relations (2.13) illustrate the

(Simple) Duality Theory for Rings.

If

$$P(0, 1;\quad +, \oplus;\quad \times, \otimes;\quad -, \ominus;\quad {}^*)$$

is a true proposition in a ring $R = (R, +, \times)$, *so also is its (simple) dual,*

$$d1P = P(1, 0;\quad \oplus, +;\quad \otimes, \times;\quad \ominus, -;\quad {}^*)$$

obtained by replacing each argument in P *by its dual,—with* * *left invariant (self-dual).*

The C-algebra (= "simple" algebra, = simple logic) of a ring $(R, +, \times)$ is the system $(R, \times, \otimes, {}^*)$. In case $R = J = (J, +, \times)$ is a Boolean ring, that is (Stone, [9]) if each element of J is idempotent,

$$a^2 (= a\times a) = a\ , \qquad (a \in J)\ , \tag{2.14}$$

—which then further implies characteristic 2,

$$a+a = 0 \qquad (a \in J)\ , \tag{2.15}$$

then its C-algebra $(J, \times, \otimes, {}^*)$ reduces to the Boolean algebra, with the dual products $\times, \otimes$ becoming Boolean intersection and union respectively, and * becoming the Boolean complement; here the Boolean ring $(J, +, \times)$ is interdefinably related to its C-algebra by the familiar equations

$$
\begin{aligned}
&a+b = ab^*\otimes a^*b \qquad [= (a\times b)^*\otimes(a^*\times b)] \\
&1-a (= 1+a) = a^* \\
&a+b-ab (= a+b+ab) = a\otimes b\ .
\end{aligned}
\tag{2.16}
$$

A Boolean ring is an example of a ring-algebra, mod C.

It was further shown in [4] and [1] that a 3-ring ($p = 3$) is not a ring-algebra mod C, but is a ring-algebra mod N. As already remarked in the introduction, by use of results of the present paper it may now be shown that all p-rings are ring-logics mod N. (Note that for $p = 2$, $N = C$).

We shall extensively apply another result established in [2]. If $R = (R, +, \times)$ is a commutative ring with unit, $(R, \times, \otimes, *)$ its C-algebra and J the set of all idempotent elements of R, then $(J, \times, \otimes, *)$ is an operationally closed sub-algebra of $(R, \times, \otimes, *)$,

$$(2.17)\qquad (J, \times, \otimes, *) \subseteq (R, \times, \otimes, *)\,.$$

The following generalization of Stone's Theorem (see [9]) was proved in [2]:

Theorem A. *The sub-algebra $(J, \times, \otimes, *)$ of a ring R is a Boolean algebra with $\times$, $\otimes$ and $*$ as logical product, logical sum, and logical complement respectively. The ring sum, $+_J$ of the corresponding Boolean ring $(J, +_J, \times)$ is however not identical with the ring sum, $+$, of R, but is related to the latter by the equation*

$$(2.18)\qquad a+_J b = (a-b)^2 = a-2ab+b \qquad (a, b \in\text{'s } J)\,.$$

Applied to p-rings the natural group N, now of order p, leads to an extensive "p-ality Theory" along the lines of the simple, or C-duality theory, as shown in [4]. Even a broad sketch of this theory would be too lengthy for consideration here, especially since we are more concerned with the simple group C. At such points as touch on the p-ality theory an effort will be made to make such contacts independently readable.

3. Vector n-rings: partition vectors.

In this and the following two sections we exhibit a certain class of vector rings "over" a given Boolean ring.

Let J be a Boolean ring = Boolean algebra = Boolean ring-algebra (mod C), —see § 2,

$$(3.1)\quad J = \{\ldots, a, b, \ldots\} = (J, +, \times) = (J, \oplus, \otimes) = (J, \times, \otimes, *)\,, \quad \text{etc.}\,.$$

The equations which interdefinably connect ring $(J, +, \times)$ and algebra $(J, \times, \otimes, *)$ have already been recalled in (2.16). In addition, within the algebra itself, the logical sum $\otimes$ and logical product $\times$ are connected by the familiar De Morgan formulas

$$(3.2)\qquad \begin{aligned} a\otimes b &= (a^*\times b^*)^* \\ a\times b &= (a^*\otimes b^*)^* \end{aligned}$$

Let n be an integer, $n \geq 2$. By a vector partition of J, of degree n,—also called a *J-vector*, or *Boolean-vector*, we understand an ordered n-uple of pairwise disjoint elements of J,

$$(3.3) \qquad \begin{aligned} &\boldsymbol{b} = \langle\, b', b'', b''', \ldots, b^{(n)} \,\rangle \\ &b^{(i)} \times b^{(i)} = b^{(i)} \qquad\qquad (i, j = 1, 2, \ldots, n)\,. \\ &b^{(i)} \times b^{(j)} = 0 \qquad (i \neq j)\,. \end{aligned}$$

The $b^{(i)}$ are the "components" of $\boldsymbol{b}$, and two vectors are "equal", $=$, only if their corresponding components are identical,

$$(3.4) \qquad \boldsymbol{b} = \boldsymbol{c} \Leftrightarrow b^{(i)} = c^{(i)} \qquad (i = 1, 2, \ldots, n)\,.$$

Notation: As already anticipated, bold face $\boldsymbol{a}, \boldsymbol{b}$ etc. denote J vectors, and lower case (non bold face) a, b, x, etc. refer to elements of the Boolean ring J,—except the letters $i, j, k, l, m, n, p, r, s, t$ which throughout the paper are reserved for integers.

We shall throughout also employ the $\sum$ notation, $\overset{+}{\sum}$, $\overset{\otimes}{\sum}$, $\overset{+}{\sum}$, etc., even $\overset{\times}{\sum}$ rather than the more conventional product notation, $\prod$, to denote a succession of "terms", separated by (the associative operations) $+$, respectively by $\otimes$, etc.

If a vector partition (3.3) satisfies

$$(3.5) \qquad \sum b^{(i)} = b' + b'' + \cdots + b^{(n)} = 1\,,$$

we speak of a *complete* vector. We shall use square brackets, [,] rather than the $\langle\, , \rangle$ notation (3.3),

$$(3.6) \qquad \boldsymbol{b} = [b', b'', \ldots, b^{(n)}]$$

to designate that the vector $\boldsymbol{b}$ is complete.

Since ring sum, $+$, and logical sum, $\otimes$ ($=$ union) are identical for disjoint elements of J,

$$(3.7) \qquad ab = 0 \Rightarrow a + b = a \otimes b\,,$$

the completeness condition (3.5) is equivalent to

$$(3.5)' \qquad \overset{\otimes}{\sum} b^{(i)} = b' \otimes b'' \otimes \cdots \otimes b^{(n)} = 1\,.$$

Each component of a complete J-vector is determined from the remaining components by equations of the form

$$\begin{aligned} b &= 1-(b''+b'''+\cdots+b^{(n)}) = 1+b''+b'''+\cdots+b^{(n)} \\ &= (b''+b'''+\cdots+b^{(n)})^* = (b''\otimes b'''\otimes\cdots\otimes b^{(n)})^* \\ &= b''^*\times b'''^*\times\cdots\times b^{(n)*}\,. \end{aligned} \tag{3.8}$$

Hence we may establich a $1-1$ correspondence

$$[b_0, b_1, \ldots, b_{n-1}] \longleftrightarrow \langle\, b_1, b_2, \ldots, b_{n-1} \,\rangle \tag{3.9}$$

between $J^{\langle n-1\rangle}$, the class of all J vectors of degree $n-1$, and $J^{[n]}$ the class of all complete J-vectors of degree n. It is this $1-1$ correspondence that we have in mind when we write

$$J^{\langle n-1\rangle} \cong J^{[n]}, \quad \text{or} \quad J^{\langle n-1\rangle} = J^{[n]}. \tag{3.10}$$

Here, by (3.8) and (3.9), we have

$$\begin{aligned} b_0 &= b_1+b_2+\cdots+b_{n-1}+1 = (b_1+b_2+\cdots+b_{n-1})^* \\ &= (b_1\otimes b_2\otimes\cdots\otimes b_{n-1})^* = b_1^* b_2^* \cdots b_{n-1}^*. \end{aligned} \tag{3.11}$$

For the case where J is finite we mention the easily proved

Theorem 1. *If $J = J_{2k}$ is the finite Boolean ring possessing exactly k atoms (and hence 2^k elements), then $J^{[n]}$, (and therefore also $J^{\langle n-1\rangle}$) consists of n^k elements (= vectors).*

4. *J*-vectors (continued), vector *p*-rings, etc.

For each given Boolean ring J and each integer $n \geq 2$ we shall now define a unique sum, $\boldsymbol{+}$, and a unique product, $\boldsymbol{\times}$, which will convert $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$, and similarly $(J^{\langle n-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$, into a vector ring. As already remarked, each such vector ring will be "hypercomplex" over J only in an extended sense, inasmuch as the vector sum, $\boldsymbol{+}$, is here not (in general) merely the traditional vector sum, i. e., not merely the sum of the corresponding components. (The relationship between the general vector sum, $\boldsymbol{+}$, and the traditional vector sum, for which we write $\boldsymbol{+}_{\text{vec}}$, is given by Theorem 15 of § 9).

We augment the previous

Notation: All instances of bold face type,—elements $\boldsymbol{a}$, $\boldsymbol{b}$, etc. and operations $\boldsymbol{+}$, $\boldsymbol{\times}$, etc.,—and later $\boldsymbol{\otimes}$, $\boldsymbol{*}$, etc., refer to the vector ring $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$, or $(J^{\langle n-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$, which is to be defined presently, while ordinary type a, b, $\ldots$, $+$, $\times$, $\otimes$, $*$, etc. continues to refer to the "ground" Boolean ring-algebra J. Furthermore when necessary to avoid ambiguity we shall use the dot subscript notation $\underset{\cdot}{+}$, $\underset{\cdot}{\times}$ and later also $\underset{\cdot}{\otimes}$, $\underset{\cdot}{\times}'$, $\underset{\cdot}{*}$, $\underset{\cdot}{\hat{}}$, etc., to refer to operations in the modular ring (4.1) below; however since certain letters r, s, etc. are reserved for integers (see notation following (3.4)), it is usually unambiguously possible to write simply $r+s$, rs instead of $r\underset{\cdot}{+}s$, $r\underset{\cdot}{\times}s$ etc.

Let

$$((n)) = \big(((n)),\ \underset{\cdot}{+},\ \underset{\cdot}{\times}\big) \tag{4.1}$$

be the ring of residues, mod n. Each multitation φ (= self-mapping) of the set $((n))$,

$$\varphi = \varphi(r, s, \ldots, t)\,, \qquad \big(r, s, \ldots, t, \quad \text{and} \quad \varphi(r, s, \ldots, t) \in\text{'s } ((n))\big) \tag{4.2}$$

may be *projected* to yield a *corresponding* multitation of the class (of vectors) $J^{[n]}$; we denote this projected multitation by bold face $\boldsymbol{\varphi}$. The components of the projection are defined by

$$\varphi_i = [\boldsymbol{\varphi}]_i = [\boldsymbol{\varphi}(\boldsymbol{a}, \boldsymbol{b}, \ldots, \boldsymbol{d})]_i = \sum_{\varphi(r,s,\ldots,t)=i}^{+} a_r b_s \ldots d_t\,, \quad (i = 0, 1, \ldots, n-1)\,. \tag{4.3}$$

Here, on the right, the sum (ring+of J) stretches over all integers $r, s, \ldots, t$, (mod n), for which $\varphi(r, s, \ldots, t) \equiv i$ (mod n) (also written $= i$ (mod n)).

For example, for $n = 4$, if φ is taken as $\underset{\cdot}{\times}$ mod 4,

$$\varphi = \varphi(r, s) = rs \ (\text{mod } 4)\,,$$

its projection $\boldsymbol{\varphi} = \boldsymbol{\times}$ on $J^{[4]}$ has the components

$$\begin{aligned} [\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_0 &= a_0b_0+a_0b_1+a_0b_2+a_0b_3+a_1b_0+a_2b_0+a_3b_0+a_2b_2 = a_0\otimes b_0\otimes a_2b_2 \\ [\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_1 &= a_1b_1+a_3b_3 \\ [\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_2 &= a_1b_2+a_2b_1+a_2b_3+a_3b_2 \\ [\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_3 &= a_1b_3+a_3b_1\,. \end{aligned} \tag{4.4}$$

Similarly, for example, with $n = 4$ and φ taken as $\underset{\cdot}{+}$, mod 4, its projection $\boldsymbol{+}$ on $J^{[4]}$ has the components

$$\begin{aligned} [\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_0 &= a_0b_0+a_1b_3+a_2b_2+a_3b_1 \\ [\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_1 &= a_0b_1+a_1b_0+a_2b_3+a_3b_2 \\ [\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_2 &= a_0b_2+a_1b_1+a_2b_0+a_3b_3 \\ [\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_3 &= a_0b_3+a_1b_2+a_2b_1+a_3b_0\,. \end{aligned} \tag{4.5}$$

In the definition of projection our reference to "components" has anticipated the

Theorem 2. *If $\varphi(r, s, \ldots, t)$ is a multitation of the class $\big((n)\big)$, its projection $\boldsymbol{\varphi}(\boldsymbol{a}, \boldsymbol{b}, \ldots, \boldsymbol{d})$ on $J^{[n]}$,*

$$\boldsymbol{\varphi} = [\varphi_0(\boldsymbol{a}, \boldsymbol{b}, \ldots, \boldsymbol{d}), \varphi_1(\boldsymbol{a}, \boldsymbol{b}, \ldots, \boldsymbol{d}), \ldots, \varphi_{n-1}(\boldsymbol{a}, \boldsymbol{b}, \ldots, \boldsymbol{d})]\ , \tag{4.6}$$

where the φ_i are defined by (4.3), *is a complete J-vector.*

Proof:

$$\varphi_i\varphi_j = \Big(\overset{+}{\sum_{\varphi(r,s,\ldots,t)=i}} a_r b_s \ldots d_t\Big)\Big(\overset{+}{\sum_{\varphi(r',s',\ldots t')=j}} a_{r'} b_{s'} \ldots d_{t'}\Big)\ . \tag{4.7}$$

For $i \neq j$ at least one of the following must hold,

$$r \neq r',\ s \neq s',\ \ldots,\ t \neq t'\ , \tag{4.8}$$

and hence

$$\varphi_i\varphi_j = 0 \qquad (i \neq j)\ . \tag{4.9}$$

This follows from (4.8), the distributivity of the $+$ and $\times$ of J, and the fact that

$$\boldsymbol{a} = [a_0, a_1, \ldots, a_{n-1}],\ \boldsymbol{b} = [b_0, b_1, \ldots, b_{n-1}] \tag{4.10}$$

are complete J-vectors by hypothesis. A similar simple argument shows that

$$\overset{+}{\sum_{(i=0,\ldots,n-1)}} \varphi_i = 1\ , \tag{4.11}$$

and completes Theorem 2.

From Theorem 2 together with (3.7), it is seen that the definition (4.3) of the projection of φ may be equivalently stated in terms of $\otimes$ sums rather than $+$,

$$\varphi_i = [\boldsymbol{\varphi}]_i = \overset{\otimes}{\sum_{\varphi(r,s,\ldots,t)=i}} a_r b_s \ldots d_t\ . \tag{4.3$'$}$$

Theorem 3. *For a given Boolean ring J and a given integer $n (n \geq 2)$, (1°) the system $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$, with $\boldsymbol{+}$ and $\boldsymbol{\times}$ defined by projection according to* (4.3), i. e.,

$$[\boldsymbol{a} \boldsymbol{+} \boldsymbol{b}]_i = \overset{+}{\sum_{r+s=i\,(\mathrm{mod}\ n)}} a_r b_s\ \Big(= \overset{\otimes}{\sum_{r+s=i\,(\mathrm{mod}\ n}} a_r b_s\Big) \qquad (i = 0, 1, 2, \ldots, n-1)\ , \tag{4.12}$$

$$[\boldsymbol{a} \boldsymbol{\times} \boldsymbol{b}]_i = \overset{+}{\sum_{rs=i\,(\mathrm{mod}\ n)}} a_r b_s\ \Big(= \overset{\otimes}{\sum_{rs=i\,(\mathrm{mod}\ n)}} a_r b_s\Big) \tag{4.13}$$

is a (commutative) ring (with unit), (2°) of characteristic n,

$$(4.14) \qquad n\boldsymbol{a} = \boldsymbol{a} \boldsymbol{+} \boldsymbol{a} \boldsymbol{+} \cdots \boldsymbol{+} \boldsymbol{a} = \boldsymbol{0} (\boldsymbol{a} \in J^{[n]}) \, .$$

(3°) *For* $n = p =$ *prime,*

$$(4.15) \qquad \boldsymbol{a}^p = \boldsymbol{a} \boldsymbol{\times} \boldsymbol{a} \boldsymbol{\times} \cdots \boldsymbol{\times} \boldsymbol{a} = \boldsymbol{a} \qquad (\boldsymbol{a} \in J^{[n]}) \, ,$$

and hence $(J^{[p]}, \boldsymbol{+}, \boldsymbol{\times})$ *is a p-ring.*

Proof: The commutativity of $\boldsymbol{+}$ and of $\boldsymbol{\times}$ is immediate from (4.12) and (4.13). We first show that (I): each of the operations $\boldsymbol{+}$ and $\boldsymbol{\times}$ is associative. For $\boldsymbol{+}$ we must show that

$$(4.16) \qquad [\boldsymbol{a} \boldsymbol{+} (\boldsymbol{b} \boldsymbol{+} \boldsymbol{c})]_i = [(\boldsymbol{a} \boldsymbol{+} \boldsymbol{b}) \boldsymbol{+} \boldsymbol{c}]_i \, , \qquad (i = 0, 1, \ldots, n-1) \, .$$

By (4.12) this is equivalent to showing that

$$(4.17) \qquad \overset{+}{\sum_{\substack{r+(s+t)=i \\ \mathrm{mod}\, n}}} a_r(b_s c_t) = \overset{+}{\sum_{\substack{(r+s)+t=i \\ \mathrm{mod}\, n}}} (a_r b_s) c_t \, .$$

This however is immediate from the associativity of × in J and the associativity of the $+$ of the ring $((n))$. The associativity of $\boldsymbol{\times}$ given by (4.13) follows in a similar direct manner.

We next show that (II): $\boldsymbol{+}$ and $\boldsymbol{\times}$ are distributive, that is,

$$(4.18) \qquad [\boldsymbol{a}(\boldsymbol{b} \boldsymbol{+} \boldsymbol{c})]_i = [\boldsymbol{ab} \boldsymbol{+} \boldsymbol{ac}]_i \qquad (i = 0, 1, \ldots, n-1) \, .$$

(Notation: Here, as elsewhere where no ambiguity can arise, we write $\boldsymbol{ab}$ (simple juxtaposition) in place of $\boldsymbol{a} \boldsymbol{\times} \boldsymbol{b}$).

Using (4.12) and (4.13) this is equivalent to showing that

$$(4.19) \qquad \overset{+}{\sum_{r \times (s+t) = i \, (\mathrm{mod}\, n)}} a_r(b_s c_t) = \overset{+}{\sum_{(r \times s)+(r' \times t) = i \, (\mathrm{mod}\, n)}} (a_r b_s)(a_{r'} b_t) \, , \qquad (i = 0, 1, \ldots, n-1) \, .$$

On the right of (4.19) all terms of the sum are 0 except where $r' = r$, because of the pairwise disjunction of the components. The truth of (4.19) is then obvious from the idempotence $a_r^2 = a_r$, together with the distributivity of the $+$ and $\times$ of $((n))$.

We next establish (III): In $(J^{[n]}, \boldsymbol{+})$,

$$(4.20) \qquad \boldsymbol{a} \boldsymbol{+} \boldsymbol{x} = \boldsymbol{b}$$

always has a solution $\boldsymbol{x}$, given by (4.23), for given $\boldsymbol{a}$ and $\boldsymbol{b}$. Here (4.20) is equivalent to the following equations

$$
(4.21)\qquad
\begin{array}{l}
a_0x_0+a_{n-1}x_1+a_{n-2}x_2+ \qquad\qquad \cdots+a_1x_{n-1}=b_0\\
a_1x_0+\ \ a_0x_1+a_{n-1}x_2+ \qquad\qquad \cdots+a_2x_{n-1}=b_1\\
a_2x_0+\ \ a_1x_1+a_0x_2\ \ +a_{n-1}x_3+\cdots+a_3x_{n-1}=b_2\\
\qquad\qquad\qquad\qquad\qquad\qquad\vdots\\
a_{n-1}x_0+a_{n-2}x_1+a_{n-3}x_2+ \qquad\qquad \cdots+a_0x_{n-1}=b_{n-1}\,.
\end{array}
$$

Multiply these in turn by $a_0, a_1, \ldots, a_{n-1}$ and add; making use of (3.3) and (3.5) we then get

$$(4.22)\qquad x_0=b_0a_0+b_1a_1+b_2a_2+\cdots+b_{n-1}a_{n-1}\,.$$

Similarly, if the equations (4.21) are multiplied in turn by the coefficients of x_i and added, upon simplification by (3.3) and (3.5) we get

$$(4.23)\qquad x_i=b_ia_0+b_{i+1}a_1+b_{i+2}a_2+\cdots+b_{i-1}a_{n-1}\,.$$

That the x_i given by (4.23) actually satisfy the equations (4.21) is immediately verified. This proves (III).

The properties (I)-(III) prove part (1°)—that is that $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$ is a ring. Directly from (4.12) and (4.13) one finds the zero, $\mathbf{0}$, the unit, $\mathbf{1}$, and the "integers", $\mathbf{1}\boldsymbol{+}\mathbf{1}$, etc. to be given by:

$$
(4.24)\qquad
\begin{array}{l}
\mathbf{0}=[1,0,0,\ldots,0]=\langle\,0,0,\ldots,0\,\rangle\\
\mathbf{1}=[0,1,0,0,\ldots,0]=\langle\,1,0,0,\ldots,0\,\rangle\\
\mathbf{2}(=\mathbf{1}\boldsymbol{+}\mathbf{1})=[0,0,1,0,\ldots,0]=\langle\,0,1,0,0,\ldots,0\,\rangle\\
\vdots\\
\boldsymbol{n}\mathbf{-1}=[0,0,\ldots,0,1]=\langle\,0,0,\ldots,0,1\,\rangle\\
\boldsymbol{n}(=\mathbf{1}\boldsymbol{+}\mathbf{1}\boldsymbol{+}\cdots\boldsymbol{+}\mathbf{1},\ n\text{ terms})=\mathbf{0}\,.
\end{array}
$$

From the distributive property and (4.24)

$$(4.25)\qquad \boldsymbol{a}\boldsymbol{+}\boldsymbol{a}\boldsymbol{+}\cdots\boldsymbol{+}\boldsymbol{a}\ (n\text{ terms})=\boldsymbol{a}\boldsymbol{\times}(\mathbf{1}\boldsymbol{+}\mathbf{1}\boldsymbol{+}\cdots\boldsymbol{+}\mathbf{1})=\mathbf{0}\,,$$

and hence (2°) of Theorem 3 is proved.

There remains to prove (4.15), for p = prime, that is, to show that

$$(4.26)\qquad [\boldsymbol{a}^p]_i=[\boldsymbol{a}]_i=a_i \qquad (i=0,1,\ldots,p-1)\,.$$

By the definition of vector product, (4.13), this is equivalent to showing that

$$(4.27)\qquad \sum_{r\times r_2\times\cdots\times r_p=i\,(\mathrm{mod}\,p)}^{+} a_ra_{r_2}a_{r_3}\ldots a_{r_p}=a_i\,,$$

where the sum stretches over all indices whose product $\equiv i \pmod p$. From the pairwise disjunction, and the idempotency of the components, terms in (4.27) with different subscripts vanish, and we may write (4.27) as

$$\sum_{r^p=i}^{+} a_r = a_i \,. \tag{4.28}$$

However in $((p))$, the field of residues mod $p =$ prime,

$$r^p = r \qquad \big(r \in ((p))\big)\,, \tag{4.29}$$

and hence (4.28) is verified, since the only term on the left of (4.28) which does not vanish is that for which $r = i$. This proves part (3°) and with it the complete Theorem 3.

We list several useful formulas, all ready consequences of (4.23), (4.24) and (4.12), as

Theorem 4. *In*

$$(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})\,,$$

if $\boldsymbol{a} = [a_0, a_1, \ldots, a_{n-1}]$, *then*

$$-\boldsymbol{a} = [a_0, a_{n-1}, a_{n-2}, a_{n-3}, \ldots, a_1] \tag{4.30}$$

$$\boldsymbol{a}^{\wedge} = \boldsymbol{1}\boldsymbol{+}\boldsymbol{a} = [a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2}] \tag{4.31}$$

$$\boldsymbol{a}^{*} = \boldsymbol{1}-\boldsymbol{a} = [a_1, a_0, a_{n-1}, a_{n-2}, \ldots, a_2]\,. \tag{4.32}$$

In the ring $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$ we may, via (3.11), completely eliminate a_0 and b_0 from each of the components $[\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_i$ and from $[\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_i$. In this way, again by means of (3.11), we may write the ring $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$ in the "non-homogeneous" form $(J^{\langle n-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$. It is convenient to speak of these (isomorphic) rings as different representations of the "same" ring,

$$(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times}) = (J^{\langle n-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})\,. \tag{4.33}$$

In this non homogeneous form it is usually convenient to write all vectors, in particular $\boldsymbol{0}, \boldsymbol{1}$, etc. (see (4.24)) in the $\langle , \rangle$ form.

For the special case $n = 2$ we prove the

Theorem 4. *Via the* $1-1$ *correspondence*

$$a \longleftrightarrow [a^*, a] \longleftrightarrow \langle\, a \,\rangle\,, \qquad (a \in J)\,, \tag{4.34}$$

each Boolean ring J is isomorphic with its complete vector J-ring of degree 2,

$$(J,\, +,\, \times) \cong (J^{[2]},\, \boldsymbol{+},\, \boldsymbol{\times}) = (J^{\langle 1\rangle},\, \boldsymbol{+},\, \boldsymbol{\times})\,. \tag{4.35}$$

Proof.: From (4.12), (4.13), (3.11) and familiar properties of a Boolean ring (see (2.14)-(2.16)),

$$\begin{aligned} &\langle a_1\rangle \boldsymbol{+} \langle b_1\rangle = \langle a_0b_1+a_1b_0\rangle = \langle (1-a_1)b_1+a_1(1-b_1)\rangle = \langle a_1+b_1\rangle \\ &\langle a_1\rangle \boldsymbol{\times} \langle b_1\rangle = \langle a_1\times b_1\rangle\,. \end{aligned} \tag{4.36}$$

From (4.36) the asserted isomorphism is immediate via the correspondence

$$a_1 \longleftrightarrow \langle a_1\rangle \longleftrightarrow [a_0,\, a_1]\,, \tag{4.37}$$

which is (4.34) in different notation.

5. **On completeness.** A ring is *complete* if (1°): the sum, and also the product of an arbitrary (not necessarily denumerable) subset of elements of the ring is defined and is an element of the ring, and (2°): both associativity and distributivity holds for these general sums and products. In a complete ring it is readily shown, for an arbitrary group K of coordinate transformations in the ring (see § 2), that (3°): the general property (1°) holds for any K-algebraic (= logical) operation in the ring, and moreover that any formal K-algebraic property of the ring that holds for arbitrary finite subsets of the ring continues to hold in the above general sense.

Applied to the foregoing vector rings we state without proof the

Theorem 5. *If J is a complete Boolean*[6] *ring, then the vector ring* $(J^{[n]},\, \boldsymbol{+},\, \boldsymbol{\times})$ *over J is a complete ring. If*

$$A = \{\dots,\, \boldsymbol{a},\, \dots\} = \{\boldsymbol{a},\, \boldsymbol{b},\, \boldsymbol{c},\, \dots\} \tag{5.1}$$

is any set of (not necessarily distinct) J-vectors,

$$\boldsymbol{a} = [a_0,\, a_1,\, \dots,\, a_{n-1}],\ \boldsymbol{b} = [b_0,\, b_1,\, \dots,\, b_{n-1}],\ \dots$$

then the components of the sum of the vectors comprising A, and similarly of the product, is given by

$$\Big[\overset{\boldsymbol{+}}{\sum_{\boldsymbol{a}\in A}} \boldsymbol{a}\Big]_i = \overset{+}{\sum_{\substack{r,s,t,\dots, = 0,1,2,\dots,n-1 \\ r\underset{\cdot}{+}s\underset{\cdot}{+}t\underset{\cdot}{+}\dots = i \ (\mathrm{mod}\ n)}}} (a_r b_s c_t \dots) \quad = \overset{\otimes}{\sum_{r\underset{\cdot}{+}s\underset{\cdot}{+}\cdots = i \ (\mathrm{mod}\ n)}} (a_r b_s c_t \dots) \tag{5.2}$$

[6] A complete Boolean ring is also definable as one isomorphic with the ring of all subsets of some set.

$$(5.3)\qquad [\overset{\times}{\sum_{\boldsymbol{a}\in A}} \boldsymbol{a}]_i = \overset{+}{\sum_{r\dot{\times}s\dot{\times}t\dot{\times}\cdots = i \ (\mathrm{mod}\ n)}} (a_r b_s c_t \ldots) = \overset{\otimes}{\sum_{r\dot{\times}s\dot{\times}\cdots = i\ (\mathrm{mod}\ n)}} (a_r b_s c_t \ldots);$$
$$(i = 0, 1, 2, \ldots, n-1)\,.$$

Specialized to the simplest case $n = 2$, by use of Theorem 4 and the correspondence (4.37), or (4.36), the formula (5.2), for instance, yields the familiar representation (either of a finite sum in any Boolean ring-algebra J, or of an arbitrary (not necessarily denumerable) sum in any complete Boolean ring-algebra J),

$$(5.4)\qquad \begin{aligned}(a+b+c+d+e+\cdots) = {} & ab^*c^*d^*e^*\cdots + a^*bc^*d^*e^*\cdots+\cdots\\ & +a^*b^*cd^*e^*\cdots+a^*b^*c^*de^*\cdots+\cdots\\ & +abcd^*e^*f^*\cdots+abc^*de^*f^*\cdots+\cdots\end{aligned}$$

where each term has an odd number of non-complemented factors and the rest complemented (= starred). (This insures that the sum of the subscripts is $\equiv 1$, mod 2). The formula (5.4) may also be written with $\otimes$ instead of $+$ on the right. A corresponding familiar Boolean formula for the product $abcde\ldots$ results from (4.37) and (5.3) by taking $n = 2$, namely

$$(5.5)\qquad abcde\cdots = a^*b^*c^*d^*e^*\cdots+abc^*d^*e^*\cdots+\cdots+ab^*cd^*e^*\cdots+\cdots$$

where (to insure that the product of the subscripts is $\equiv 1$, mod 2), each term contains either no or an even number of non complemented factors, and the rest complemented. We may again write $\otimes$ instead of $+$ on the right of (5.5)

Again for $n = 3$, for example, (5.3) yields

$$(5.6)\qquad \begin{aligned}[\boldsymbol{a}\times\boldsymbol{b}\times\boldsymbol{c}\times\boldsymbol{d}\times\boldsymbol{e}\times\cdots]_1 = {} & a_1b_1c_1d_1e_1\cdots+a_2b_2c_1d_1e_1\cdots\\ & +a_2b_1c_2d_1e_1\cdots+\cdots+a_2b_2c_2d_2e_1\cdots+\cdots\end{aligned}$$

(where each term has no or an even number of "2" components appearing),

$$(5.7)\qquad \begin{aligned}[\boldsymbol{a}\times\boldsymbol{b}\times\boldsymbol{c}\times\boldsymbol{d}\times\boldsymbol{e}\times\cdots]_2 = {} & a_2b_1c_1d_1\cdots+a_1b_2c_1d_1\cdots+\cdots\\ & +a_2b_2c_2d_1e_1\cdots+\cdots\end{aligned}$$

(where each term involves an odd number of "2" components). Here again we may also write $\otimes$ in place of $+$ on the right of (5.6) or (5.7).

Formulas (5.2), (5.3) and the Completeness Theorem 5 will take on additional significance in § 8 after it is shown that any (abstract) *p*-ring (see (1.1) and (1.2) of § 1) may be isomorphically represented as a vector *p*-ring.

6. **Direct projection.** In the vector ring $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times}) = (J^{\langle n-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$, the $\boldsymbol{+}$ and $\boldsymbol{\times}$ of the ring are the direct projections (4.3) of $\underset{\cdot}{+}$ and $\underset{\cdot}{\times}$ from the ring of residues $\big(((n)), \underset{\cdot}{+}, \underset{\cdot}{\times}\big)$, as defined in § 4, whereas all further ring concepts, in particular K-algebraic ($= K$-logical) concepts are, as in any ring, "internally" determined, i. e. *defined* in terms of $\boldsymbol{+}$ and $\boldsymbol{\times}$. For instance for the generators of the simple and of the natural groups, C and N, $\boldsymbol{a}^{*} = \mathbf{1} \boldsymbol{-} \boldsymbol{a}$ and $\boldsymbol{a}^{\wedge} = \mathbf{1} \boldsymbol{+} \boldsymbol{a}$ were found to be given by (4.32) and (4.31).

On the other hand it is easily verified that the direct projections onto $J^{[n]}$ of the corresponding C- and N-logical concepts $\underset{\cdot}{*}$, $\underset{\cdot}{\hat{}}$ of the ring $\big(((n)), \underset{\cdot}{+}, \underset{\cdot}{\times}\big)$,— let us denote these projections by $\boldsymbol{*}^{pr}$, $\boldsymbol{\wedge}^{pr}$, leads to precisely the same formulas; thus, by

$$(6.1) \qquad \begin{aligned} [\boldsymbol{a}^{*pr}]_i &= a_i^{\underset{\cdot}{*}} \\ [\boldsymbol{a}^{\wedge pr}]_i &= a_i^{\underset{\cdot}{\check{}}} \end{aligned} \qquad (i = 0, 1, 2, \ldots, n-1)$$

(where $\underset{\cdot}{\check{}}$ is the inverse of $\underset{\cdot}{\hat{}}$, i. e., $i^{\underset{\cdot}{\check{}}} = i \underset{\cdot}{-} 1$), which is seen to agree with (4.32) and (4.31). Hence we have

$$(6.2) \qquad \begin{aligned} \boldsymbol{a}^{*} &= \boldsymbol{a}^{*pr} \\ \boldsymbol{a}^{\wedge} &= \boldsymbol{a}^{\wedge pr} \end{aligned}$$

Since all C- (respectively all N-) algebraic concepts of $J^{[n]}$ are generated by $\boldsymbol{\times}$ and $\boldsymbol{*}$ (respectively by $\boldsymbol{\times}$ and $\boldsymbol{\wedge}$), we have demonstrated the

Theorem 6. *Each C- (respectively each N-) logical concept of $(J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$ is the same whether determined "internally", from $\boldsymbol{+}$ and $\boldsymbol{\times}$, or by directly projecting onto $J^{[n]}$ the corresponding C- (respectively N-) logical concept of the ring $\big(((n))), \underset{\cdot}{+}, \underset{\cdot}{\times}\big)$. Briefly stated: the ($C$-, respectively N-) algebra of the projection is the projection of the (C-respectively N-) algebra.*

Actually only a trivial addition to the foregoing argument yields the stronger

Theorem 7. *If $\boldsymbol{\psi} = \boldsymbol{\psi}(\boldsymbol{a}, \boldsymbol{b}, \ldots)$ is a multitation of $J^{[n]}$ which is some compositional combination $\mathfrak{G}(\boldsymbol{+}, \boldsymbol{\times}, \boldsymbol{*}, \boldsymbol{\wedge})$ of (any or all of) the operations $\boldsymbol{+}, \boldsymbol{\times}, \boldsymbol{*}, \boldsymbol{\wedge}$, then the components $[\boldsymbol{\psi}]_i$ of $\boldsymbol{\psi}$ are the same whether computed "internally" (in the previous sense) or by direct projection of the same composition $\mathfrak{G}(\underset{\cdot}{+}, \underset{\cdot}{\times}, \underset{\cdot}{*}, \underset{\cdot}{\hat{}})$ of the corresponding operations $\underset{\cdot}{+}, \underset{\cdot}{\times}$, etc. of $\big(((n)), \underset{\cdot}{+}, \underset{\cdot}{\times}\big)$.*

Illustrations.

$$(6.3) \qquad \boldsymbol{a} \otimes \boldsymbol{b} = (\boldsymbol{a}^{*} \boldsymbol{\times} \boldsymbol{b}^{*})^{*} \qquad \text{(internally)} .$$

In this form the components $[\boldsymbol{a}\times\boldsymbol{b}]_i$ are tedious to compute. By direct projection, however,

$$(6.4)\qquad [\boldsymbol{a}\otimes\boldsymbol{b}]_i = \overset{+}{\sum_{r\underset{\cdot}{\otimes}s=i}} a_r b_s = \overset{+}{\sum_{r\underset{\cdot}{+}s\underset{\cdot}{-}r\underset{\cdot}{\times}s=i}} a_r b_s \qquad (i=0,1,\ldots,n-1)\,.$$

Again

$$(6.5)\qquad \boldsymbol{a}\oplus\boldsymbol{b} = (\boldsymbol{a}^*+\boldsymbol{b}^*)^* \qquad \text{(by internal definition)}\,.$$

$$[\boldsymbol{a}\oplus\boldsymbol{b}]_i = \overset{+}{\sum_{r\underset{\cdot}{\otimes}s=i\ (\mathrm{mod}\ n)}} a_r b_s = \overset{+}{\sum_{r+s-1=i\ (\mathrm{mod}\ n)}} a_r b_s \qquad \text{(by direct projection)}\,.$$

Similarly

$$(6.6)\qquad \boldsymbol{a}\times'\boldsymbol{b} = (\boldsymbol{a}^\wedge\times\boldsymbol{b}^\wedge)^\vee \qquad \text{(internal definition)}$$

$$[\boldsymbol{a}\times'\boldsymbol{b}]_i = \overset{+}{\sum_{r\underset{\cdot}{\times}'s=i\ (\mathrm{mod}\ n)}} a_r b_s = \overset{+}{\sum_{r+s+rs=i\ (\mathrm{mod}\ n)}} a_r b_s \qquad \text{(by direct projection)}\,.$$

In any of the above we may also take $\overset{\otimes}{\sum}$ instead of $\overset{+}{\sum}$.

Theorem 7 shows that, while the projection process

$$\big(((n)),\underset{\cdot}{+},\underset{\cdot}{\times}\big) \xrightarrow[\text{proj}]{} (J^{[n]},\boldsymbol{+},\boldsymbol{\times})$$

does not define a ring homorphism in the strict traditional sense, it does define a kind of operational homorphism.

II

ABSTRACT p-RINGS AND THEIR BOOLEAN-VECTOR REPRESENTATION

7. Canonical "linear" decomposition in abstract p-rings.

We turn now from the class of vector p-rings, just considered, to arbitrary p-rings (see § 1), which we also refer to as abstract p-rings. Let

$$S = (S,\boldsymbol{+},\boldsymbol{\times}) = (S,\boldsymbol{+},\boldsymbol{\times},\boldsymbol{\otimes},{}^{\boldsymbol{*}}) = \text{etc.}$$

be any abstract p-ring. To facilitate later contact with vector p-rings we shall parallel the previous

Notation: Bold face $\boldsymbol{+}$, $\boldsymbol{\times}$, $\boldsymbol{\otimes}$, ${}^{\boldsymbol{*}}$, ${}^{\wedge}$, ${}^{\vee}$ etc. denote the familiar ring operations (see § 2), and bold face $\boldsymbol{a}$, $\boldsymbol{b}$, etc. denote general elements of the abstract p-ring S; in addition small (non bold face) Roman letters a, b, etc. (except those reserved for integers,—see notation following (3.4)), always denote idempotent elements of S,

$$(7.1)\qquad a^2 = a\boldsymbol{\times}a = a\,.$$

The C-logic (or simple logic) of the ring S is the algebra $(S, \boldsymbol{\times}, \boldsymbol{\otimes}, {}^{\boldsymbol{*}})$,—see § 2, where

$$\begin{aligned} &\boldsymbol{a}^{\boldsymbol{*}} = \mathbf{1}\boldsymbol{-}\boldsymbol{a}(= \mathbf{0}\boldsymbol{\ominus}\boldsymbol{a}) \\ (7.2) \qquad &\boldsymbol{a}\boldsymbol{\otimes}\boldsymbol{b} = \boldsymbol{a}\boldsymbol{+}\boldsymbol{b}\boldsymbol{-}\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} \\ &\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} = \boldsymbol{a}\boldsymbol{\oplus}\boldsymbol{b}\boldsymbol{\ominus}(\boldsymbol{a}\boldsymbol{\otimes}\boldsymbol{b})\,. \end{aligned}$$

The set I, consisting of the p "integers" of S,

$$(7.3) \qquad I = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots\}$$

where

$$(7.4) \qquad \mathbf{2} = \mathbf{1}\boldsymbol{+}\mathbf{1}, \mathbf{3} = \mathbf{1}\boldsymbol{+}\mathbf{2}, \ldots$$

forms a subring ($=$ sub field) of S,

$$(7.5) \qquad (I, \boldsymbol{+}, \boldsymbol{\times}) \subseteq (S, \boldsymbol{+}, \boldsymbol{\times})\,,$$

which is obviously isomorphic with $((p))$, the field of residues mod p,

$$(7.6) \qquad (I, \boldsymbol{+}, \boldsymbol{\times}) \cong \big(((p)), \underset{\cdot}{+}, \underset{\cdot}{\times}\big) = (F_p, \underset{\cdot}{+}, \underset{\cdot}{\times})\,.$$

As recalled in § 2, the set J of all idempotent elements of S, while not in general (i. e., for $p \neq 2$) a sub*ring* of S, is a (simple) sub-*algebra*

$$(7.7) \qquad (J, \boldsymbol{\times}, \boldsymbol{\otimes}, {}^{\boldsymbol{*}}) \subseteq (S, \boldsymbol{\times}, \boldsymbol{\otimes}, {}^{\boldsymbol{*}})\,,$$

and this sub-algebra is a Boolean algebra (with $\mathbf{0}$ and $\mathbf{1}$ as null and universe, and with $\boldsymbol{\times}$, $\boldsymbol{\otimes}$, ${}^{\boldsymbol{*}}$ as logical product, logical sum and logical complement respectively); the (simple, i. e. C-) algebraic notions of J are identical with those of S. To further facilitate subsequent contact between abstract and vector p-rings we agree to the convention or

Notation: When applied to the idempotent Boolean algebra J of S the (simple) logical operations $\boldsymbol{\times}$, $\boldsymbol{\otimes}$, ${}^{\boldsymbol{*}}$ etc. are also denoted by ordinary (non bold face) type,

$$\begin{aligned} &a\boldsymbol{\times}b = a\times b = ab \\ (7.8) \qquad &a\boldsymbol{\otimes}b = a\otimes b \quad : \quad (J, \boldsymbol{\times}, \boldsymbol{\otimes}, {}^{\boldsymbol{*}}) = (J, \times, \otimes, {}^{*})\,, \\ &a^{\boldsymbol{*}} \ \ = a^{*} \end{aligned}$$

and similarly for the idempotent elements

$$\mathbf{0} = 0, \mathbf{1} = 1\,,$$

(but not for the (in general) non-idempotent $\mathbf{2}, \mathbf{3}, \ldots$). Furthermore, parallel to the abbreviation for vector product (following (4.18)) it is frequently convenient and non-ambiguous even in the case of $\boldsymbol{\times}$ in S, to write simply

(7. 9) $$\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} = \boldsymbol{ab}$$

and similarly

(7.10) $$\boldsymbol{a}^t = \boldsymbol{a}\boldsymbol{\times}\boldsymbol{a}\boldsymbol{\times}\dots\boldsymbol{\times}\boldsymbol{a} \qquad (t \text{ factors}) ,$$

However the *ring* sum, $+$ (non-bold face!) of the Boolean ring $(J, +, \times)$ which corresponds to the Boolean sub-algebra $(J, \times, \otimes, {}^*)$ is not identical with the ring sum, $\boldsymbol{+}$, of S, but is related thereto by

(7.11) $$a+b = a\boldsymbol{-}\mathbf{2}ab\boldsymbol{+}b(= a\boldsymbol{-}ab\boldsymbol{-}ab\boldsymbol{+}b) , \qquad (a, b \in\text{'s } J) ,$$

as reviewed in § 2. Thus, in particular, for *disjoint* elements of J the two degenerate to the same operation,

(7.12) $$ab = 0 \Rightarrow a+b = a\boldsymbol{+}b \qquad (a, b \in\text{'s } J) .$$

Theorem 8. Normal Representation Theorem.

In an abstract p-ring $S = (S, \boldsymbol{+}, \boldsymbol{\times})$, *each* $\boldsymbol{a} \in S$ *may be decomposed in one and only one way in the "normal idempotent form"*

(7.13) $$\boldsymbol{a} = a_1\boldsymbol{+}\mathbf{2}a_2\boldsymbol{+}\mathbf{3}a_3\boldsymbol{+}\cdots\boldsymbol{+}(\boldsymbol{p}\boldsymbol{-}\mathbf{1})a_{p-1}$$
$$(= a_1\boldsymbol{+}a_2\boldsymbol{+}a_2\boldsymbol{+}a_3\boldsymbol{+}a_3\boldsymbol{+}a_3\boldsymbol{+}a_4\boldsymbol{+}\cdots)$$

in which the "normal components" $a_i = (\boldsymbol{a})_i$ *of the element* $\boldsymbol{a}$ *are idempotent elements of* S *and pairwise disjoint,*

(7.14) $$a_i^2 = a_i .$$

(7.15) $$a_ia_j = 0 \qquad (i \neq j) .$$

The normal components a_k *of* $\boldsymbol{a}$ *may be determined from* $\boldsymbol{a}$ *by the equations,*

(7.16) $$a_k = (\boldsymbol{p}\boldsymbol{-}\mathbf{1})(k^{p-2}\boldsymbol{a}\boldsymbol{+}k^{p-3}\boldsymbol{a}^2\boldsymbol{+}k^{p-4}\boldsymbol{a}^3\boldsymbol{+}\cdots\boldsymbol{+}k^0\boldsymbol{a}^{p-1}) , \quad (k = 1, 2, \dots, p-1) .$$

Here the coefficients in (7.16) *are to be taken* mod p.

Proof: We first show that if an element $\boldsymbol{a}$ of S has a normal idempotent decomposition, i. e., is expressible in the form (7.13) with the a_k satisfying (7.14) and (7.15), then these components a_k are unique and are given by (7.16). We have

$$
(7.17)\qquad
\begin{aligned}
\mathbf{a} &= a_1+2a_2+3a_3+4a_4+\cdots+(p-1)a_{p-1}\\
\mathbf{a}^2 &= a_1+2^2a_2+3^2a_3+4^2a_4+\cdots+(p-1)^2a_{p-1}\\
\mathbf{a}^3 &= a_1+2^3a_2+3^3a_3+4^3a_4+\cdots+(p-1)^3a_{p-1}\\
&\vdots\\
a^{p-1} &= a_1+2^{p-1}a_2+3^{p-1}a_3+\cdots+(p-1)^{p-1}a_{p-1}\,.
\end{aligned}
$$

We borrow the following identity from number theory: Let p be a prime integer, and m, n any integers where $m \not\equiv 0, n \not\equiv 0(p)$. Then

$$
(\mathrm{B})\qquad
\begin{aligned}
&m^{p-2}n+m^{p-3}n^2+m^{p-4}n^3+\cdots+m^0n^{p-1}\\
&\qquad\equiv 0 \pmod{p}\,, \qquad \text{if} \quad n \not\equiv m(p)\\
&\qquad\equiv p-1 \pmod{p}\,, \quad \text{if} \quad n \equiv m(p)\,.
\end{aligned}
$$

If we now add the equations (7.17), apply the identity B with $m = 1$ and simplify by use of the identity

$$(7.18)\qquad (p-1)^2 \equiv 1 \pmod{p}\,,$$

we find

$$(7.19)\qquad a_1 = (p-1)(\mathbf{a}+\mathbf{a}^2+\mathbf{a}^3+\cdots+\mathbf{a}^{p-1})\,.$$

Again, if we multiply the equations (7.17) in turn by $2^{p-3}, 2^{p-4}, \ldots, 2^0$, add and again use (B) and (7.18), we get

$$(7.20)\qquad a_2 = (p-1)(2^{p-2}\mathbf{a}+2^{p-3}\mathbf{a}^2+2^{p-4}\mathbf{a}^3+\cdots+2^0\mathbf{a}^{p-1})\,.$$

Similarly, by multiplying the equations (7.17) in turn by $3^{p-2}, 3^{p-3}, 3^{p-4}, \ldots, 3^0$ and adding, respectively by $4^{p-2}, 4^{p-3}, \ldots, 4^0$ and adding, etc., each time applying (B) and (7.18), we get

$$
(7.21)\qquad
\begin{aligned}
a_3 &= (p-1)(3^{p-2}\mathbf{a}+3^{p-3}\mathbf{a}^2+\cdots+3^0\mathbf{a}^{p-1})\\
a_4 &= (p-1)(4^{p-2}\mathbf{a}+4^{p-3}\mathbf{a}^2+\cdots+4^0\mathbf{a}^{p-1})\\
&\vdots\\
a_{p-1} &= (p-1)\big((p-1)^{p-2}\mathbf{a}+(p-1)^{p-3}\mathbf{a}^2+\cdots+(p-1)^0\mathbf{a}^{p-1}\big)
\end{aligned}
$$

These formulas (7.19)-(7.21) are precisely those condensed by (7.16).

To complete the proof of the theorem we must show that for given $\mathbf{a} \in S$, the a_k *defined* by (7.16) actually satisfy the conditions (7.13), (7.14) and (7.15). Let us first take (7.13). Upon substituting the a_k given by (7.16), the right side of (7.13) may be written

$$\begin{aligned}&(\boldsymbol{p}-1)\{(1+2^{p-1}+3^{p-1}+\cdots+(\boldsymbol{p}-1)^{p-1})\boldsymbol{a}+(1+2^{p-2}+3^{p-2}+\cdots+(\boldsymbol{p}-1)^{p-2})\boldsymbol{a}^2\\ (7.22)\quad &+(1+2^{p-3}+3^{p-3}+\cdots+(\boldsymbol{p}-1)^{p-3})\boldsymbol{a}^3+\cdots+(1+2+3+\cdots+(\boldsymbol{p}-1))\boldsymbol{a}^{p-1}\}\,.\end{aligned}$$

Using B in (7.22), the coefficient of $\boldsymbol{a}$ is $\equiv (p-1)$, while all other coefficients are $\equiv 0$, mod p. Further simplification of (7.22) by (7.18) then shows that (7.13) is satisfied.

We next verify that the a_k defined by (7.16) satisfy (7.14) and (7.15). In place of the arithmetic identity (B) we need the following variant: Let p be a prime and let k, l, t be integers where

$$(7.23)\qquad k \not\equiv 0,\, l \not\equiv 0,\, t \not\equiv p-1 \pmod{p}\,.$$

Then

$$(\mathrm{C})\qquad k^0l^t+kl^{t-1}+k^2l^{t-2}+\cdots+k^tl^0+k^{t+1}l^{p-2}+\cdots+k^{p-2}l^{t-p+2}$$

$$\begin{cases}\equiv 0 & \text{if}\quad k \not\equiv l \pmod{p}\\ \equiv p-1 & \text{if}\quad k \equiv l\ (\mathrm{mod\ p})\,.\end{cases}$$

Here, in view of (7.18),

$$(7.24)\qquad l^p \equiv l \pmod{p}\,,$$

and, since all exponents are of course reduced, we have

$$(7.25)\qquad l^s \equiv l^{s'} \pmod{p} \Rightarrow s \equiv s' \pmod{((p-1))}\,.$$

Thus, for instance, for $p=7, t=3$ (C) reads

$$(7.26)\qquad l^3+kl^2+k^2l+k^3+k^4l^5+k^5l^4 \begin{cases}\equiv 0 & \text{if}\quad k \not\equiv l\ (7)\\ \equiv 6 & \text{if}\quad k \equiv l\ (7)\,.\end{cases}$$

From the definition of p-ring S,

$$(7.27)\qquad \boldsymbol{a}^p = \boldsymbol{a} \qquad (\boldsymbol{a} \in S)$$

and hence, similarly to (7.25), we have

$$(7.28)\qquad \boldsymbol{a}^s = \boldsymbol{a}^{s'} \Rightarrow s \equiv s' \pmod{(p-1)}\,.$$

If we compute a_k, a_l by means of (7.16) and reduce the exponents by means of (7.25) and (7.28), we get

$$(7.29)\qquad a_ka_l = A_{kl1}\boldsymbol{a}+A_{kl2}\boldsymbol{a}^2+\cdots+A_{kl(p-1)}\boldsymbol{a}^{p-1},$$

where

$$\begin{aligned}
&A_{kl1} = (p-1)^2(k^0l^{p-2}+kl^{p-3}+k^2l^{p-4}+\cdots+k^{p-2}l^0)\\
&A_{kl2} = (p-1)^2(k^0l^{p-3}+kl^{p-4}+k^2l^{p-5}+\cdots+k^{p-2}l^{p-2})\\
(7.30)\qquad &A_{kl3} = (p-1)^2(k^0l^{p-4}+kl^{p-5}+k^2l^{p-6}+\cdots+k^{p-2}l^{p-3})\\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
&A_{kl(p-1)} = (p-1)^2(k^0l^0+kl^{p-2}+k^2l^{p-3}+\cdots+k^{p-2}l)\,.
\end{aligned}$$

By (C), if $k \not\equiv l \pmod{p}$, it is seen that each $A_{kli} = 0$, and hence by (7.29), (7.15) of Theorem 8 is verified. Again, if $k \equiv l(p)$, then by (C), (7.29) and (7.30) we readily compute,

$$\begin{aligned}
&A_{kk1} = (p-1)^2(p-1)k^{p-2} = (p-1)k^{p-2}\\
(7.31)\qquad &A_{kk2} = (p-1)^2(p-1)k^{p-3} = (p-1)k^{p-3}\\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
&A_{kk(p-1)} = (p-1)^2(p-1) = (p-1)k^0\,.
\end{aligned}$$

Hence from (7.29), (7.31) and (7.16) we have

$$a_ka_k = a_k \qquad (k = 1, 2, \dots, p-1)\,,$$

which proves (7.14). This completes Theorem 8.

8. $\boldsymbol{p}$-Vector representation.

A vector p-ring, as follows from Theorem 3, may of course be conceived as an abstract p-ring. We shall now prove the converse. For this purpose the non-homogeneous vector form $(J^{\langle p-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$ is more convenient than the homogeneous form $(J^{[p]}, \boldsymbol{+}, \boldsymbol{\times})$.

Theorem 9. *Let $(S, \boldsymbol{+}, \boldsymbol{\times})$ be an abstract p-ring, and let J be its idempotent Boolean sub-algebra,*

$$(8.1)\qquad J = (J, \times, \otimes, {}^*)\,,$$

with corresponding Boolean ring $(J, \times, +)$,—(see (7.7)-(7.11)). If

$$(8.2)\qquad \boldsymbol{a} = a_1\boldsymbol{+}2a_2\boldsymbol{+}3a_3\boldsymbol{+}\cdots\boldsymbol{+}(\boldsymbol{p}-1)a_{p-1}$$

is the (unique) normal idempotent decomposition (Theorem 8) of an element $\boldsymbol{a}$ of S, then the $1-1$ correspondence

$$(8.3)\qquad \boldsymbol{a} \longleftrightarrow \langle a_1, a_2, \dots, a_{p-1}\rangle$$

represents an isomorphism between the abstract p-ring $(S, \boldsymbol{+}, \boldsymbol{\times})$ and the vector p-ring $(J^{\langle p-1\rangle}, \boldsymbol{+}, \boldsymbol{\times})$ "over" the Boolean idempotent ring J of S; that is,

$$\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} \longleftrightarrow \langle a_1, a_2, \ldots, a_{p-1}\rangle \boldsymbol{\times} \langle b_1, b_2, \ldots, b_{p-1}\rangle \tag{8.4}$$

$$\boldsymbol{a}\boldsymbol{+}\boldsymbol{b} \longleftrightarrow \langle a_1, a_2, \ldots, a_{p-1}\rangle \boldsymbol{+} \langle b_1, b_2, \ldots, b_{p-1}\rangle\,. \tag{8.4$'$}$$

Proof.: The correspondence of the products is fairly immediate. From (8.1) and (7.6), by direct multiplication of the elements $\boldsymbol{a}$, $\boldsymbol{b}$ of S,

$$\begin{aligned}\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} &= (a_1b_1+\cdots)\mathbf{1}\boldsymbol{+}(a_1b_2+a_2b_1+\cdots)\mathbf{2}\boldsymbol{+}\cdots \\ &= c_1\mathbf{1}\boldsymbol{+}c_2\mathbf{2}\boldsymbol{+}c_3\mathbf{3}\boldsymbol{+}\cdots\boldsymbol{+}c_{p-1}(\boldsymbol{p}\boldsymbol{-}\mathbf{1})\,,\end{aligned} \tag{8.5}$$

where

$$c_i = a_{r'}b_{s'}\boldsymbol{+}a_{r''}b_{s''}\boldsymbol{+}\cdots = \overset{\boldsymbol{+}}{\sum_{rs=i \ (\mathrm{mod}\ p)}} a_r b_s\,. \tag{8.6}$$

Now since the terms $a_{r'}b_{s'}$, $a_{r''}b_{s''}$, ... in (8.6) are pairwise disjoint elements of J, by (2.18) the ring sum $\boldsymbol{+}$ (belonging to S) which occurs may be replaced by the Boolean ring sum, $+(=+_J)$ of J,[7]—see (7.7)-(7.10),

$$c_i = a_{r'}b_{s'}+a_{r''}b_{s''}+\cdots = \overset{+}{\sum_{rs=i \ (\mathrm{mod}\ p)}} a_r b_s \qquad (+=+_J)\,. \tag{8.7}$$

These c_i are thus idempotent and obviously pairwise disjoint,

$$c_ic_j = 0 \qquad (i \neq j)\,, \tag{8.8}$$

consequently the c_i given by (8.7),—or by (8.6) are the actual normal components of the product $\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}$ (Theorem 8). On the other hand, according to (4.13), the right side of (8.7) is seen to be identical with the i^{th} component of the vector product.

$$\langle a_1, a_2, \ldots, a_{p-1}\rangle \boldsymbol{\times} \langle b_1, b_2, \ldots, b_{p-1}\rangle\,. \tag{8.9}$$

Hence, via the correspondence (8.3), (abstract) products correspond to (vector) products, and (8.4) is established.

We turn to the proof of (8.4)$'$. For $\boldsymbol{a}$, $\boldsymbol{b}$ of S, by direct addition

$$\boldsymbol{a}\boldsymbol{+}\boldsymbol{b} = (a_1\boldsymbol{+}b_1)\boldsymbol{+}\mathbf{2}(a_2\boldsymbol{+}b_2)\boldsymbol{+}\mathbf{3}(a_3\boldsymbol{+}b_3)\boldsymbol{+}\cdots\boldsymbol{+}(\boldsymbol{p}\boldsymbol{-}\mathbf{1})(a_{p-1}\boldsymbol{+}b_{p-1})\,. \tag{8.10}$$

However (8.10) does not in general represent the normal idempotent decomposition of $\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}$, (Theorem 8). Let the normal components of $\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}$ be c_i; then by Theorem 8 the elements c_i of S are uniquely determined by the three conditions

[7] In fact, for disjoint idempotent elements a, b of any commutative ring R,

$$a+_R b = a+_J b = a\otimes_R b = a\otimes_J b\,.$$

$$c_i^2 = c_i \tag{8.11}$$

$$c_i c_j = 0 \qquad (i \neq j) \tag{8.12}$$

$$\begin{aligned}(a_1 \boldsymbol{+} b_1) \boldsymbol{+} \mathbf{2}(a_2 \boldsymbol{+} b_2) \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1})(a_{p-1} \boldsymbol{+} b_{p-1}) = \\ c_1 \boldsymbol{+} \mathbf{2}c_2 \boldsymbol{+} \mathbf{3}c_3 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1})c_{p-1} \,.\end{aligned} \tag{8.13}$$

We shall show that the solution of these equations (8.11)-(8.13) is given by

$$\begin{array}{l} c_1 = a_0 b_1 \boldsymbol{+} a_1 b_0 \boldsymbol{+} \cdots = \overset{\boldsymbol{+}}{\sum\limits_{r+s=1 \ (\mathrm{mod}\ p)}} a_r b_s \\ \vdots \\ c_i = a_0 b_i \boldsymbol{+} a_1 b_{i-1} \boldsymbol{+} \cdots = \overset{\boldsymbol{+}}{\sum\limits_{r+p=i \ (\mathrm{mod}\ p)}} a_r b_s \qquad (i = 1, 2, \ldots, p-1) \,. \\ \vdots \qquad\qquad\qquad\qquad\qquad \vdots \end{array} \tag{8.14}$$

Here again, since the terms in c_i are pairwise disjoint idempotent elements, these c_i may also be written with the $\boldsymbol{+}$ (of S) replaced by the Boolean ring $+$ ($= +_J$ of J), i. e.,

$$c_i = a_0 b_i + a_1 b_{i-1} + \cdots = \overset{+}{\sum\limits_{r+s=i \ (\mathrm{mod}\ p)}} a_r b_s \tag{8.15}$$

$$(+ = +_J = \text{ring sum of } J;\ i = 1, 2, \ldots, p-1) \,.$$

From (8.15) the c_i are seen to be idempotent and pairwise disjoint elements of S, that is, (8.11) and (8.12) are satisfied. We procede to show that (8.13) is also satisfied.

Substituting the c_i given by (8.14) into the right side of (8.13), the result may be arranged in the form:

$$\begin{array}{l} \phantom{\boldsymbol{+}}a_0 b_1 \ \boldsymbol{+} \mathbf{2}a_0 b_2 \ \boldsymbol{+} \mathbf{3}a_0 b_3 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1}) a_0 b_{p-1} \\ \boldsymbol{+} a_1 b_0 \ \boldsymbol{+} \mathbf{2}a_1 b_1 \ \boldsymbol{+} \mathbf{3}a_1 b_2 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1}) a_1 b_{p-2} \\ \boldsymbol{+} a_2 b_{p-1} \boldsymbol{+} \mathbf{2}a_2 b_0 \ \boldsymbol{+} \mathbf{3}a_2 b_1 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1}) a_2 b_{p-3} \\ \boldsymbol{+} a_3 b_{p-2} \boldsymbol{+} \mathbf{2}a_3 b_{p-1} \boldsymbol{+} \mathbf{3}a_3 b_0 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1}) a_3 b_{p-4} \\ \vdots \\ \boldsymbol{+} a_{p-1} b_2 \boldsymbol{+} \mathbf{2}a_{p-1} b_3 \boldsymbol{+} \mathbf{3}a_{p-1} b_4 \boldsymbol{+} \cdots \boldsymbol{+} (\boldsymbol{p} \boldsymbol{-} \mathbf{1}) a_{p-1} b_0 \,. \end{array} \tag{8.16}$$

Since a_0 and b_0 are defined by

$$a_0 \boldsymbol{+} a_1 \boldsymbol{+} a_2 \boldsymbol{+} \cdots \boldsymbol{+} a_{p-1} = \mathbf{1};\ b_0 \boldsymbol{+} b_1 \boldsymbol{+} \cdots \boldsymbol{+} b_{p-1} = \mathbf{1} \,, \tag{8.17}$$

that is

$$\begin{aligned} a_0 &= \mathbf{1}\boldsymbol{+}(\boldsymbol{p}-\mathbf{1})(a_1\boldsymbol{+}a_2\boldsymbol{+}\cdots\boldsymbol{+}a_{p-1}) \\ b_0 &= \mathbf{1}\boldsymbol{+}(\boldsymbol{p}-\mathbf{1})(b_1\boldsymbol{+}b_2\boldsymbol{+}\cdots\boldsymbol{+}b_{p-1})\ , \end{aligned} \tag{8.18}$$

we may eliminate a_0 and b_0 from the sum (8.16), after which (*i*): the collected terms in a_1b_s (for fixed $s=1, 2, \ldots, p-1$) have the coefficient $\{s(p-1)+(p-1)+(s+1)\}$, which is $\equiv 0(p)$. (Here $s(p-1)a_1b_s$ comes from the first row of (8.16) and $(p-1)a_1b_s\boldsymbol{+}(s+1)a_1b_s$ from the second row); (*ii*): the collected terms in $b_1a_s \equiv 0(p)$, by symmetry from (*i*); (*iii*): the collected terms in $a_rb_s(r, s = 2, 3, \ldots, p-1)$ have the coefficient $s(p-1)+(r+s)+r(p-1)$, $\equiv 0(p)$. (Here $s(p-1)a_rb_s$ comes from the first row of (8.16), $(r+s)a_rb_s\boldsymbol{+}r(p-1)a_rb_s$ from the $(r+1)^{st}$ row, and no terms from other rows).

From (*i*)—(*iii*) and (8.18), the right side of (8.13), that is, (8.16), immediately reduces to

$$(b_1\boldsymbol{+}\mathbf{2}b_2\boldsymbol{+}\mathbf{3}b_3\boldsymbol{+}\cdots\boldsymbol{+}(\boldsymbol{p}-\mathbf{1})b_{p-1})\boldsymbol{+}(a_1\boldsymbol{+}\mathbf{2}a_2\boldsymbol{+}\cdots\boldsymbol{+}(\boldsymbol{p}-\mathbf{1})a_{p-1})\ . \tag{8.19}$$

This is however seen to be identical with the left side of (8.13) and hence we have shown that the c_i given by (8.14), also by (8.15), are the normal idempotent components of $\boldsymbol{a}+\boldsymbol{b}$. But these normal components (in the $+$ (of J) form, (8.15), are precisely those of the vector sum

$$\langle a_1, a_2, \ldots, a_{p-1}\rangle\boldsymbol{+}\langle b_1, b_2, \ldots, b_{p-1}\rangle\ ,$$

as defined in (4.12). We have thus shown that, under the correspondence (8.3), (abstract) sums correspond to (vector) sums, proving (8.4)′ and with it Theorem 9.

Since for given p and J the vector p-ring $(J^{[p]}, \boldsymbol{+}, \boldsymbol{\times})$ is uniquely defined, Theorem 9 has the corollary

Theorem 10. *The prime p together with the structure of the idempotent sub-algebra J constitute a complete set of invariants (up to isomorphisms) of a p-ring S.*

Thus, a p-ring S with idempotent sub-algebra J and a p'-ring S' with idempotent sub-algebra J' are isomorphic if and only if $p = p'$ and J and J' are isomorphic Boolean algebras. We may accordingly speak of *the* p-ring whose idempotent sub-algebra is (or is isomorphic with) J. Furthermore it is only a matter of convenience whether we conceive a p-ring abstractly or vectorially. We may also transfer classifications of Boolean rings to p-rings; thus, for instance, a complete—(respectively an atomistic—, respectively an atomless,—etc.) p-ring, S, is one whose idempotent Boolean sub-algebra J is complete (respectively atomistic, etc.).

In § 5 a different definition of completeness was given. The equivalence of this earlier with the above definition of completeness for p-rings follows at once from Theorems 5 and 9. We have the

Theorem 11. *A necessary and sufficient condition for a p-ring S to be complete in the sense of § 5 (i. e., to permit sums and products of arbitrary subsets of elements of S) is that S be complete in the above sense (i. e., that its idempotent sub-algebra J be a complete Boolean algebra).*

Theorem 12. *A direct power of F_p (field of residues* mod p*) is a complete p-ring. Conversely, a complete p-ring is isomorphic with a direct power of F_p.*

That a direct power of F_p (in fact of any p-ring) is again a p-ring is evident. We first establish a simple

Lemma. *Let p be a prime, Z any (finite or infinite) cardinal number $Z \geq 1$, and $F_p^{(Z)}$ and $F_2^{(Z)}$ the Z^{th} direct power of F_p and F_2 respectively. Then $(J, \times, \otimes, *)$ and $(F_2, \times_{(2)}, \otimes_{(2)}, *^{(2)})$, the idempotent Boolean sub-algebra of $F_p^{(Z)}$ and $F_2^{(Z)}$ are isomorphic,*

(8.20 $$J \cong F_2\,.$$

Proof. The idempotent elements of a direct power are those elements all of whose direct factors are idempotent. Hence only those $a \in F_2^{(Z)}$ are idempotent each of whose Z direct factors is either $\equiv 0$ or $\equiv 1 \pmod p$, $a \in J$ equivalent: $a = (\ldots, a_i, \ldots)$, each $a_i \equiv 0$ or $\equiv 1 \pmod p$. Let

(8.21) $$a \longleftrightarrow a'$$

be the $1-1$ correspondence between J and F_2, in which corresponding direct factors of a and a' are "the same" (i. e., $a_i \equiv 0(p) \Leftrightarrow a_i' \equiv 0(2)$, and $a_i \equiv 1(p) \Leftrightarrow a_i' \equiv 1(2)$, for all factors, a_i). This correspondence is seen to be such that (8.21) and $b \longleftrightarrow b'$ imply:

(8.22) $$a \times b \longleftrightarrow a' \times_{(2)} b'$$
$$a^* \longleftrightarrow a'^{*(2)}\,.$$

Since the idempotent sub-algebra of a ring is generable by $\times$ and $*$, the Lemma is established. From the Lemma it then follows that the corresponding Boolean rings are also isomorphic, via the correspondence (8.21),

(8.23) $$(J, +_J, \times) \cong (F_2, +_{(2)}, \times_{(2)})\,.$$

Theorem 12 may now readily be proved. Since $F_2^{(Z)}$ is a complete Boolean ring it follows from (8.20) and the definition of completeness that $F_p^{(Z)}$ is a complete p-ring. As for the converse part of Theorem 12, if S is a complete p-ring, its idempotent Boolean sub-algebra is isomorphic with a direct power of F_2, say $F_2^{(Z_0)}$. However the idempotent sub-algebra of the p-ring $F_p^{(Z_0)}$ is isomorphic with $F_2^{(Z_0)}$, by the Lemma. Hence S and $F_p^{(Z_0)}$ are two p-rings with isomorphic Boolean sub-algebras, from which it follows that they are themselves isomorphic, by Theorem 10,

$$S \cong F_p^{(Z_0)} \, . \tag{8.24}$$

This completes Theorem 12.

Since the idempotent Boolean sub-algebra of a finite p-ring is necessarily finite, and since a finite Boolean algebra is always complete, Theorem 12 has the

Corollary 1. *A finite p-ring S is always isomorphic with a direct power of F_p,*

$$S \cong F_p X F_p X \cdot - X F_p \, . \tag{8.25}$$

Again, for an arbitrary p-ring, its idempotent Boolean algebra may be imbedded in a complete Boolean algebra, say $F_2^{(Z)}$. Applying Theorem 12 to $F_p^{(Z)}$, an obvious construction yields the further

Corollary 2. *Each p-ring is isomorphic with a sub-ring of a direct power of F_p.*

These two Corollaries are precisely the results of Mc Coy and Montgomery in [8], (see introduction).

By direct use of Theorem 8, formula (7.16), the normal components $(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})_1$, $(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})_2, \ldots$ of the sum $\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}$ in a p-ring are given as a polynomial in $\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}$,

$$(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})_k = (\boldsymbol{p}\boldsymbol{-}\boldsymbol{1})\left(k^{p-2}(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})\boldsymbol{+}k^{(p-3)}(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})^2\boldsymbol{+}\cdots\boldsymbol{+}k^0(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})^{p-1}\right) . \tag{8.26}$$

By combining (8.26) with Theorem 9, and using both (8.14) and (8.15), we have the

Theorem 13. *If $\boldsymbol{a}$ and $\boldsymbol{b}$ are elements of a p-ring S, and if $\{a_k\colon a_0, a_1, \ldots, a_{p-1}\}$ $\{b_k\colon b_0, b_1, \ldots, b_{p-1}\}$ are the normal idempotent components of $\boldsymbol{a}$ and of $\boldsymbol{b}$, then for* $k = 1, 2, \ldots, p-1$,

$$\begin{aligned} &(\boldsymbol{p}\boldsymbol{-}\boldsymbol{1})\left(k^{p-2}(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})\boldsymbol{+}k^{p-3}(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})^2\boldsymbol{+}\cdots\boldsymbol{+}k^0(\boldsymbol{a}\boldsymbol{+}\boldsymbol{b})^{p-1}\right) \\ &= \sum_{r\underset{\cdot}{+}s=k \text{ (mod } p)}^{\boldsymbol{+}} a_r b_s = \sum_{r\underset{\cdot}{+}s=k \text{ (mod } p)}^{+(=+_J)} a_r b_s \, . \end{aligned} \tag{8.27}$$

Note 1. The idempotent elements of a p-ring S are those for which $\boldsymbol{a} = a_1$ (i. e. for which the normal components $a_2 = a_3 = \cdots = a_{p-1} = 0$). From the isomorphism established in Theorem 9 (or else from an easily given independent argument), in a vector p-ring the idempodent vectors are those and only those of the form

$$(8.28)\qquad \langle a, 0, 0, 0, \ldots, 0 \rangle = [a^*, a, 0, 0, 0, \ldots, 0] .$$

Also capable of ready direct proof (independent of Theorem 9) is the unique normal decomposition theorem in $(J^{\langle p-1 \rangle}, \boldsymbol{+}, \boldsymbol{\times})$:

$$(8.29)\qquad \begin{aligned} \langle a_1, a_2, \ldots, a_{p-1} \rangle &= \langle a_1, 0, 0, \ldots, 0 \rangle \boldsymbol{\times} \langle 1, 0, 0, \ldots, 0 \rangle \\ &\boldsymbol{+} \langle a_2, 0, 0, \ldots, 0 \rangle \boldsymbol{\times} \langle 0, 1, 0, \ldots, 0 \rangle \boldsymbol{+} \langle a_3, 0, 0, \ldots, 0 \rangle \\ \boldsymbol{\times} \langle 0, 0, 1, 0, 0, \ldots, 0 \rangle &\boldsymbol{+} \cdots \boldsymbol{+} \langle a_{p-1}, 0, 0, \ldots, 0 \rangle \boldsymbol{\times} \langle 0, 0, \ldots, 0, 1 \rangle , \end{aligned}$$

which is the formula (7.13) applied to vector p-rings. In this way, by use of (8.28)¸ (8.29) and (4.24), as a kind of converse to Theorem 8, the normal decomposition (7.13) in an abstract p-ring S could be made to follow from an (independent) knowledge of the equivalence (= isomorphism) of the concepts of abstract and vector p-rings.

Note 2. It is further observed that the vector formula (8.29) continues to be true in a general vector ring $(J^{\langle n-1 \rangle}, \boldsymbol{+}, \boldsymbol{\times}) = (J^{[n]}, \boldsymbol{+}, \boldsymbol{\times})$, even when n is composite. In this case, however, the idempotent vectors given by (8.28) will not, in general, be the only idempotent vectors of the ring, and, as a consequence, a vector $\langle a_1, a_2, \ldots, a_{n-1} \rangle$ may have more than one normal decomposition, (8.29).

If in the normal decomposition (7.13) we write

$$(8.30)\qquad \boldsymbol{a} = a_1 \boldsymbol{+} (a_2 \boldsymbol{+} a_2) \boldsymbol{+} (a_3 \boldsymbol{+} a_3 \boldsymbol{+} a_3) \boldsymbol{+} \ldots$$

and if we sum the arithmetic progression $1+2+3+\cdots+(p-1)$, we have as an interesting corollary the

Theorem 14. *In a p-ring $(S, \boldsymbol{+}, \boldsymbol{\times})$, each element $\boldsymbol{a}$ of S may be expressed as the sum, $\boldsymbol{+}$, of $\frac{p(p-1)}{2}$ idempotent elements of S.*

For 2-rings ($p = 2$), which are coextensive with ordinary Boolean rings, Theorem 14 degenerates to a simple restatement of the familiar definition of Boolean ring (Stone [9]).

9. Relation to ordinary vector addition.

In a p-ring $(S, \boldsymbol{+}, \boldsymbol{\times})$, it may happen that the sum of special elements $\boldsymbol{a}, \boldsymbol{b}$ reduces to the traditional vector sum $\boldsymbol{+}_{vec}$ or $\boldsymbol{+}_v$

$$\boldsymbol{a}\boldsymbol{+}\boldsymbol{b} = \boldsymbol{a}\boldsymbol{+}_v\boldsymbol{b}\,, \tag{9.1}$$

that is, that the normal components of the sum reduce to the sums of the respective normal components,

$$[\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}]_i = a_i\boldsymbol{+}b_i\,. \tag{9.2}$$

In this connection we prove the

Theorem 15. *In a p-ring* $(S, \boldsymbol{+}, \boldsymbol{\times})$, *a necessary and sufficient condition for the sum of two elements to reduce to the ordinary vector sum,*

$$\boldsymbol{a}\boldsymbol{+}\boldsymbol{b} = \boldsymbol{a}\boldsymbol{+}_v\boldsymbol{b} = \langle\, a_1\boldsymbol{+}b_1, a_2\boldsymbol{+}b_2, \ldots, a_{p-1}\boldsymbol{+}b_{p-1}\,\rangle \tag{9.3}$$

is that the elements $\boldsymbol{a}, \boldsymbol{b}$ *be "disjoint",*

$$\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b} = 0\,. \tag{9.4}$$

This in turn is equivalent to the pairwise disjunction of all normal components

$$a_ib_{i'} = 0 \qquad (i, i' = 1, 2, \ldots, p-1)\,. \tag{9.5}$$

As a consequence of (9.5) we note that the $\boldsymbol{+}$ in $\langle\;,\;\rangle$ in (9.3) could be replaced by $+ = +_J$ of the idempotent sub-algebra J of S, $\langle\, a_1+b_1, a_2+b_2, \ldots\,\rangle$.

Proof of Theorem 15. (9.5) implies (9.4) since each component (other than the 0th) of $\boldsymbol{a}\times\boldsymbol{b}$, namely

$$[\boldsymbol{a}\boldsymbol{\times}\boldsymbol{b}]_i = \overset{+}{\sum_{\substack{rs = i \ (\mathrm{mod}\ p)\\ r,s=1,\ldots,p-1}}} a_rb_s \qquad (i = 1, 2, \ldots, p-1) \tag{9.6}$$

is patently $= 0$ if (9.5) holds.

Conversely (9.4) implies (9.5). For, if (9.4) holds we have

$$\overset{+}{\sum_{rs = i \ (\mathrm{mod}\ p)}} a_rb_s = 0 \qquad (i = 1, 2, \ldots, p-1)\,. \tag{9.7}$$

Each of the $(p-1)^2$ quantities $a_{i'}b_i(i, i' = 1, 2, \ldots, p-1)$ occurs in (exactly) one of the $(p-1)$ equations (9.7), and moreover its coefficient is 1. Hence if the equation containing $a_ib_{i'}$, is multiplied by $a_ib_{i'}$, one has the desired result (9.5), as follows from the pairwise disjunction of the a_i and the same for the b_i. We have therefore shown that (9.4) and (9.5) are equivalent. The Theorem will be complete if we establish that (9.3) and (9.5) are equivalent.

For the $1, 2, \ldots, (p-1)$st normal components of $\boldsymbol{a}\boldsymbol{+}\boldsymbol{b}$ we have respectively,

$$
\begin{array}{lllll}
a_0b_1+a_1b_0+a_2b_{p-1}+a_3b_{p-2}+\cdots \\
a_0b_2+a_1b_1+a_2b_0 & +a_3b_{p-1}+\cdots \\
a_0b_3+a_1b_2+a_2b_1 & +a_3b_0 \quad +\cdots \\
\vdots & \qquad\qquad \vdots
\end{array} \tag{9.8}
$$

If (9.5) holds, the i^{th} component of $\boldsymbol{a}+\boldsymbol{b}$ thus becomes simply

$$a_0b_i+a_ib_0 = (1-a_1-a_2-\cdots-a_{p-1})b_i+a_i(1-b_1-b_2-\cdots-b_{p-1}) = a_i+b_i\,. \tag{9.9}$$

Hence (9.5) implies (9.3).

Conversely, if (9.3) holds, we have equations

$$
\begin{array}{ll}
a_0b_1+a_1b_0+a_2b_{p-1}+a_3b_{p-2}+\cdots & = a_1+b_1 \\
a_0b_2+a_1b_1+a_2b_0 \quad +\cdots & = a_2+b_2 \\
a_0b_3+a_1b_2+a_2b_1 \quad +a_3b_0 \quad +\cdots & = a_3+b_3\,. \\
\vdots & \quad \vdots
\end{array} \tag{9.10}
$$

By multiplying the i^{th} row in (9.10) by $a_ib_{i'}$ (where $i'\neq 0$, $i'\neq i$), we get

$$a_ib_{i'} = 0 \qquad (i'\neq i)\,. \tag{9.11}$$

That one also has

$$a_ib_i = 0 \tag{9.12}$$

is seen upon multiplying the $(2i)^{\text{th}}$ row of (9.10) by a_ib_i. Here (9.11) and (9.12) correspond to (9.5), and therefore (9.3) implies (9.5). This completes Theorem 15. The Theorem may easily be extended to more than two elements.

Note. For the special case $p = 3$ one may directly verify the formula: for any elements $\boldsymbol{a}, \boldsymbol{b}$ of a 3-ring,

$$(\boldsymbol{a}+\boldsymbol{b})_i = (\boldsymbol{a}+_v\boldsymbol{b})_i+\boldsymbol{ab} \qquad (i = 1, 2)\,. \tag{9.13}$$

From (9.13) the equivalence of (9.3) and (9.4), only of course for the case $p = 3$, follows as an evident corollary.

The results of this paper, in combination with earlier work on the K-ality theory, etc., lend themselves to various interesting applications, particularly to logic, (see [4] and [1] for the tri-ality theory in 3-valued logic), probability theory and geometry. It is expected that these extensions will be presented in the near future.

BIBLIOGRAPHY

1. A. L. Foster, *The n-ality theory of rings*, Proc. of the Nat'l. Acad. of Sc., Vol 35 (1949), pp. 31—38.

2. — *The idempotent elements of a commutative ring form a Boolean algebra; ring duality and transformation theory*, Duke Math J., Vol 13 (1946), pp. 247—258.

3. — *The theory of Boolean-like rings*, Trans. of the Amer. Math. Soc., Vol 59 (1946), pp. 166—187.

4. — *On the n-ality theories in rings and their logical algebras, including tri-ality principle in three-valued logics*, Amer. Journal of Math., Vol 72, No 1 (1950), pp. 101—123.

5. — *On the permutational representation of general sets of operations by partition lattices*, Trans. of the Amer. Math. Soc., July, 1949.

6. — and B. A. Bernstein, *A dual-symmetric definition of field*, Amer. Journal of Math., Vol 67 (1945), pp. 329—349.

7. — — *Symmetric approach to commutative rings, with duality theorem: Boolean duality as special case*, Duke Math. Journal, Vol. 11 (1944), pp. 603—616.

8. N. H. Mc Coy and Deane Montgomery, *A representation of generalized Boolean rings*, Duke Math. Journal, Vol. 3 (1937), pp. 455—459.

9. M. H. Stone, *The theory of representations for Boolean algebras*, Trans. of the Amer. Math. Soc., Vol. 40 (1936), pp. 37—111.