Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

ALFRED L. FOSTER

p-rings and ring-logics

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3e série, tome 5, nº 3-4 (1951), p. 279-300
<http://www.numdam.org/item?id=ASNSP_1951_3_5_3-4_279_0>

p-RINGS AND RING-LOGICS

by ALFRED L. FOSTER (Berkeley)

1. **Introduction.** Through the medium of the *K-ality theory* it was shown, in a series of recent communications, that the classical Boolean realm (e. g., Boolean-algebras, - rings, - logic, - duality principle, etc.) is an instance of a much broader ond more general theory, that of *ring-logics* (*mod.* K) - see [1], [3] (1). We recall that this concept of ring logic (mod. K) — in which K is a preassigned (« admissible ») group of « coordinate transformations » in the domain — characterizes, on the K-level, those rings and those logics ($=K$-algebras, $=K$-logical-algebras) in which the ring and the associated « K-logic » uniquely determine or « fix » each other in an equationally interdefinable way, [1]. Such a bond is familiar between Boolean rings and their corresponding Boolean algebras (logics) on the « lowest » or mod C level (where $K=C=$ (*simple*) *complementation group,* of order 2, generated by $x^{*}=1-x$); in particular it was shown in [1] that Boolean rings are ring-logics (mod. C).

The existence of higher level ring-logics was first established in [1], where it was shown that 3-rings are ring-logics mod. N, but not mod. C. Here N is the natural group, generated by the « natural negation » (or « - complement »), $x^{\frown}=1+x$. In [3] this result for 3-rings, — after utilizing various fundamental structure-theorems for p-rings proved in [2] — was extended to the whole latter class; that is, it was established in [3] that all p-rings are ring-logics mod. N. The classical Boolean case ($=2$ rings) is imbedded in this result since, for 2-rings, $N=C$.

The present communication elevates this theory to a still more general level, that of p^{k}-rings ([4], [5]). We shall establish that all such rings are ring-logics (mod. D). Here D is a certain group (« normal » group)

(1) Numbers in square brackets refer to the appended bibliography.

which, like the earlier groups C and N, is cyclic, that is, possesses a single generator $x^{\frown}$ (« normal complementation »). Unlike C and N, however, it develops that the group D does not (in general) possess a *linear* generator, -that is, one linear in x. We here depend on results established in [4], where the methods and structure theorems of [2] are extended to p^k-rings.

One may regard the class of 2 rings (= 2-ring-logics = Boolean realm) as a generalization of the simplest member of this class, the field of residues mod 2. More generally, the class of p-ring-logics constitutes a natural generalization of its simplest member, the field of residues mod p. In this domain of p-ring-logics the *p-ality theory* replaces the duality theory of the special $p = 2 =$ Boolean case; that is, all theorems and concepts fall into p-al sets, -see [1]. The results of the present communication, establishing the class of p^k-rings — whose simplest member is the Galois field of p^k-elements — as ring-logics, in which, via the concept of normal negation, one has the same type of choice between « purely » D-logical or else « mixed » ring-theoretical representations as in the simplest Boolean case, and over which a p^k-ality theory parallel to the p-ality theory on the N-level reigns (see [1]), brings this cycle of developments to a natural stage of completion.

When the present theory is specialized to the simplest case of $F_{p^k} =$ Galois field of p^k elements, we obtain a rather unexpected strictly multiplicative equational definition for the $+$ of F_{p^k}. This is considered in § 12.

We shall freely borrow concepts, results and notation (the latter with some slight simplifications) from various papers listed in the appended bibliography. Readers unfamiliar wit this background may refer to [1], where an introduction to the K-ality theory will be found.

2. *p^k-rings* (2). Let p be a fixed prime and k a fixed positive integer, $k \geq 1$. In agreement with [4] we define a p^k-ring as a

(i) commutative ring, $(P, \times, +)$, with unit element 1, in which

$$(ii) \qquad a^{p^k} = a \qquad (a \in P)$$

(iii) P possesses a sub-ring (= field), $(F, \times, +)$, which is isomorphic with $F_{p^k} =$ Galois field of p^k elements, and such that

$$(iv) \qquad 1 \in F$$

Since such a sub-field F is of characteristic p,

$$(2.1) \qquad p \cdot 1 = 1 + 1 + \ldots + 1 = 0$$

(2) Under a somewhat broader definition, p^k-rings were first introduced by McCoy, [5].

it follows on multiplication by a that a p^k-ring, P, is of characteristic p,

$$(v) \qquad p\, a = 0 \qquad (a \in P) .$$

Furthermore the integers p and k are unique, that is,

Theorem 1. If $(P, \times, +)$ *is a* p^k*-ring and also a* $p_1^{k_1}$*-ring, then* $p = p_1$ *and* $k = k_1$.

Proof: That $p = p_1$ follows from (2.1). However, independently of (2.1), suppose P both a p^k and a $p_1^{k_1}$ ring, and let $(F, \times, +)$ and $(F_1, \times, +)$ be sub fields of P respectively isomorphic with the Galois fields F_{p^k} and $F_{p_1^{k_1}}$, and each satisfying (iv) Let ξ and ξ_1 be (multiplicative) generatos of F and of F_1 respectively. Then

$$(2.2) \qquad \xi^{p^k-1} = 1 , \qquad \xi_1^{p_1^{k_1}-1} = 1$$

For the element $\xi\, \xi_1$ of P we have, using (ii)

$$(2.3) \qquad \begin{aligned} (\xi\, \xi_1)^{p^k} &= \xi\, \xi_1^{p^k} = \xi\, \xi_1 \\ (\xi\, \xi_1)^{p_1^{k_1}} &= \xi^{p_1^{k_1}}\, \xi_1 = \xi\, \xi_1 \end{aligned}$$

Hence, from (2.2), we have

$$(2.4) \qquad \xi_1^{p^k} = \xi_1 , \qquad \xi^{p_1^{k_1}} = \xi \ .$$

from which one has

$$(2.5) \qquad p^k \geq p_1^{k_1} , \qquad p_1^{k_1} \geq p^k .$$

Since we are dealing with prime powers, (2.5) implies the desired conclusion of Theorem 1.

The class of p^k-rings embraces (a) all finite (= Galois) fields and (b) all p rings ($k = 1$; see [3], [1]), and in particular, (c) all Boolean rings ($k = 1$, $p = 2$). Further (d) a (finite or transfinite) direct power of p^k rings is again a p^k ring, and in connection with more general results it was shown in [5] and again in [4] that (e) all p^k rings are (isomorphic with) sub-direct powers of F_{p^k} (= Galois field of p^k elements) and, in particular, that (f) each finite p^k ring is isomorphic with a direct power $F_{p^k} \times F_{p^k} \times \ldots \times F_{p^k}$, whence, for a given finite positive integer t there is (up to isomorphisms) one and only one p^k ring af p^{kt} elements.

For the special case of p-rings the conditions (i), (ii), (v) (with $k=1$) are definitive, -see [3]; then (iii) and (iv) are automatically satisfied with F as the prime field π of P,

$$\pi = \{0, 1, 2, \ldots, p-1\} \cong F_p. \tag{2.6}$$

Furthermore for the still more special Boolean case, (i) and (ii) (with $p=2$, $k=1$) are definitive, as is well known; here even the commutative restriction of (i) is redundant, (see [7]).

In a p^k ring a sub-field F satisfying both (iii) and (iv) we shall call *normal*. A p^k ring will generally possess more than one normal subfield as is shown by the direct product $F_{2^2} \times F_{2^2}$, which is readily shown to be a 2^2-ring with two distinct normal sub-fields F, F'.

The independence and significance of the condition (iv) is shown by the ring

$$R = F_3 \times F_3 \qquad \text{(direct product)}, \tag{2.6}$$

which is not a 3^2-ring (and of course also not a 3-ring). Here the conditions (i), (ii), (iii) (and even (v)) are satisfied (with $p=3$, $k=2$); in particular R contains a sub-field isomorphic with F_{3^2}, - but it contains no normal such subfield, e. g., none which also satisfies (iv).

3. **Notation.** Let $P = (P, \times, +)$ be a p^k-ring, F a normal subfield of P, and J the class of all idempotent elements of P

$$a \in J \qquad \text{if} \qquad a^2 (= a \times a) = a. \tag{3.1}$$

Here J, unlike F, is not in general a sub-*ring* of P; however, by [8], J is a sub-(mod C)-*logic* of the C-logic $(P, \times, \otimes, {}^*)$ of the ring $(P, \times, +)$, where $\times, \otimes$ are the C-dual ring products, * the (self dual) C-complement and $+, \oplus$ the C-dual ring sums, -with inverses $-, \ominus$

$$\begin{aligned} a \otimes b &= a + b - a b \\ a \times b &= (a \oplus b) \ominus (a \otimes b) \\ a^* &= 1 - a = 0 \ominus a. \end{aligned} \tag{3.2}$$

From [8] it further follows that the sub (mod C)-logic $(J, \times, \otimes, {}^*)$ is a Boolean algebra with $\times, \otimes, {}^*$ as Boolean-intersection, -union, and -complement respectively.

Throughout we shall adhere to the following notations: except for the letters k, m, n, p, r, which are reserved for integers, small Roman letters

a, b, x, ect *witheut subscripts* (but possibly with superscripts, e. g., a', $a^{(1)}$, etc.) denote elements of P; small Greek letters $\mu, \nu, \alpha, \beta, \xi$, etc denote elements of a fixed normal sub-field F of P; small Roman letters *with subscripts,* a_0, b_1, x_μ, etc., denote idempotent elements of P, i. e.,

$$
\begin{aligned}
&P = \{\ldots, x\ , \ldots\} \\
&J = \{\ldots, x_\mu, \ldots\} \\
&F = \{\ldots, \mu\ , \ldots\} \\
&J \subseteq P, \qquad F \subseteq P
\end{aligned}
\tag{3.3}
$$

4. **Normal (vector) representation.** In the nototion of § 3 it was shown in [4] that a p^k-ring P is characterized by a *normal subsystem* (F, J) thereof, in the sense of the

Theorem A, Normal Representation Theorem. In a p^k ring, P, each element a may be expressed in one and only one way in the form

$$
a = \overset{+}{\sum_{\mu \in F}} \mu\, a_\mu \tag{4.1}
$$

where the multipliers μ run through the elements of a fixed normal subfield F of P, and where the a_μ are pairwise disjoint idempotent elements which cover J, i. e., where

$$
\begin{aligned}
&a_\mu^2 = a_\mu \\
&a_\mu\, a_\nu = 0 \qquad (\mu, \nu \in F., \mu \neq \nu). \\
&\overset{+}{\sum_{\mu \in F}} a_\mu = 1
\end{aligned}
\tag{4.2}
$$

The a_μ given by (4.1) and (4.2) uniquely determine the element a, and are called the *normal* (*idempotent*) components of a, -relative, of course, to a fixed normal sub field, F. We use square brackets, [ ], to refer to these normal components, e. g.,

$$
a = [\ldots, a_\mu, \ldots]
$$

$$
[a]_\mu = a_\mu .
$$

Not only is each « vector » a uniquely determined by its normal components, but conversely, as shown in [4], we have

Theorem B. If

$$
a = [\ldots, a_\mu, \ldots]
$$

is an element of a p^k-ring, its normal idempotent components, a_μ, are determined from a by the formulas:

$$(4.3)\qquad \begin{aligned} a_\mu &= -\sum_{r=1}^{r=p^k-1} \left(\frac{a}{\mu}\right)^r \qquad (\text{for } \mu \neq 0) \\ a_0 &= 1 - a^{p^k-1} = (a^{p^k-1})^* . \end{aligned}$$

The representation of the elements of a p^k-ring in terms of their normal components is not (in general) hypercomplex, -in particular, the components of a sum are not (generally) given by the sum of the corresponding components. From [4] we have

Theorem C (Addition, etc., Theorem). In the notation of Theorems A and B, in a p^k ring P if

$$(4.4)\qquad a = [\ldots, a_\mu, \ldots], \qquad b = [\ldots, b_\mu, \ldots]$$

are elements with normal components a_μ and b_μ respectively, then the normal components of $a + b$ and of $a\,b$ are given by the formulas

$$(4.5)\qquad [a + b]_\mu = \overset{+}{\sum_{\sigma+\tau=\mu}} a_\sigma b_\tau$$

$$(4.6)\qquad [a\,b]_\mu = \overset{+}{\sum_{\sigma\tau=\mu}} a_\sigma b_\tau .$$

with similar formulas obtaining for other operations in P.

Here Σ stretches over all σ, τ of F such that $\sigma + \tau = \mu$, respectively such that $\sigma\tau = \mu$.

5. From the theory of Ring-logics. For orientational purposes, we briefly present salient fragments of the general theory, see [1].

If $(R, \times, +)$ is a ring and $K = \{\ldots, \mathfrak{W}, \ldots\} = \{\mathfrak{W}_1, \mathfrak{W}_2, \ldots\}$ is a group of cordinate transformations in (= permutations, or $1-1$ selftransformations of) R,

$$(5.1)\qquad x \to \mathfrak{W}(x) \qquad (x, \mathfrak{W}(x) \in R;\ \mathfrak{W} \in K),$$

with inverses written $\mathfrak{W}^-$,

$$(5.2)\qquad x \to \mathfrak{W}^-(x),$$

then the *K-logic* (or *K-logical-algebra*) of the ring $(R, \times, +)$ is the (operationally closed) system

$$(5.3)\qquad (R, \times, K) = (R, \times, \mathfrak{W}_1, \mathfrak{W}_2, \ldots),$$

whose class R is identical with the class of ring elements, and whose operations are the ring product, $\times$, of the ring together with the (unary operations) $\mathfrak{W} \in K$. These operations, as well as any obtainable therefrom by composition, are the *K-logical operations* of the ring. Whereas any K-logical operation may thus eventually be exspressed as some composition of $\times$ and the operations $\mathfrak{W} \in K$, such « ultimate » expressions are frequently less illuminating than expressions making use of other K-logical operations, such as $\times_{\mathfrak{W}_1}, \times_{\mathfrak{W}_2}, \ldots$ which are the *K als* of $\times$, i. e., the ring products expressed in the $\mathfrak{W}_1$, respectively in the $\mathfrak{W}_2$ etc., coordinate systems. Here

$$(5.4)\qquad x \times_{\mathfrak{W}} y = \mathfrak{W}^{-}(\mathfrak{W}(x)\,\mathfrak{W}(y)).$$

In this sense we have, for the K-logic,

$$(5.5)\quad (R, \times, K) = (R, \mathfrak{W}_1, K) = (R, \mathfrak{W}_2, K) = \ldots = (R, \times, \times_{\mathfrak{W}_1}, \times_{\mathfrak{W}_2}, \ldots, K),$$

where the $='s$ refer to the compositional equivalence (= compositional interdefinability) of the systems. If $\mathcal{Y}, \ldots$ are a set of generators of the group K, we may further simplify (5.5) by writing

$$(5.6)\qquad (R, \times, K) = \ldots = (R, \times, \mathcal{Y}, \ldots).$$

For a ring R with unit, 1, the simple group, C, has $*$ (= C — complementation) as generator,

$$(5.7)\qquad x^* = 1 - x$$

and the C-logic of the ring $(R, \times, +)$ is then

$$(5.8)\qquad (R, \times, {}^*) = (R, \otimes, {}^*) = (R, \times, \otimes, {}^*),$$

where $\otimes$ is $\times$ expressed in the $*$ coordinate system:

$$(5.9)\qquad x \otimes y = (x^* \times y^*)^* = x + y - 1.$$

(As in earlier papers, the circle notation, $\bigcirc$, is used to denote operations in the $*$ coordiaute system, e. g. for $+$,

$$(5.10)\qquad x \oplus y = (x^* + y^*)^* = x + y - 1.$$

If further R is taken as a Boolean ring, the C-duals $\times , \circledtimes$ reduce to logical product and logical union, respectively, - in fact the C-logic then reduces to the ordinary Boolean logical algebra corresponding to the (Boolean) ring R.

The *natural group*, N, — in a ring with unit — has $\frown$ as a generator,

$$(5.11) \qquad x^{\frown} = 1 + x$$

with inverse, $\smile$

$$(5.12) \qquad x^{\smile} = x - 1 .$$

Following the notation of previous papers, operations expressed in the $\frown$ respectively in the $\frown^2 (= \frown\frown)$, etc. coordinate systems are primed, respectively double primed, etc., e. g.

$$(5.13) \qquad \begin{aligned} x \times' y &= (x^{\frown} \times y^{\frown})^{\smile} = x + y + xy \\ x \times'' y &= (x^{\frown^2} \times y^{\frown^2})^{\smile^2} \\ &\vdots \\ x +' y &= (x^{\frown} + y^{\frown})^{\smile} = x + y + 1 \\ &\vdots \end{aligned}$$

For a given ring $(R, \times, +)$ and a given group K the ring sum, $+$, is generally not K logically-*equationally* definable, i. e., the ring $+$ is not epressible as some composition of $\times$ and the operations $\mathfrak{V} \in K$. On the other hand it may happen that $+$, while K-logically equationally definable, is not uniquely *fixed* by the K-logic; that is, it may happen that two different (even non-isomorphic !) rings $(R, \times, +)$ and $(R, \times, +_1)$ exist, — on the same class R and with the same ring product, $\times$, but with $+_1 \neq +)$ — each of which has identically the same K logic. A *ring-logic (mod K)* is a ring whose $+$ (and with it, of course, the complete ring) is K-logically equationally definable and moreover fixed by its K-logic. As already recalled, it has been shown that p-rings are ring logics mod N. (See [3]).

6. Normal complementation in p^k-rings, (explicit form). Let P be a p^k-ring and F a normal snb-field of P. Then, as is well known for all Galois fields, F contains a (multiplicative) generator, ξ, an element whose $p^k - 1$ powers yield all elements $\neq 0$ of F,

$$(6.1) \qquad F = \{0, \xi, \xi^2, \xi^3, \ldots, \xi^{p^k-1} (= 1)\} .$$

Of course F will generally have more than one such generator, ξ, in which case any one is selected and kept fixed.

We shall establish the basic

Theorem 2. Let P be a p^k-ring, let F be a normal sub-field of P and let ξ be a generator of F. Then the mapping $x \to x^\frown$ defined by

$$(6.2)\qquad x^\frown = \xi x + (1 + \xi x + \xi^2 x^2 + \xi^3 x^3 + \ldots + \xi^{p^k-2} x^{p^k-2})$$

is a permutation ($= 1 - 1$ self-mapping) of P, with inverse given by

$$(6.3)\qquad x^\smile = \frac{x}{\xi} + \frac{1}{\xi}(1 + x + x^2 + \ldots + x^{p^k-2}).$$

The permutation $^\frown$ is furthermore of period p^k,

$$(6.4)\qquad x^{\frown p^k} = (\ldots(x^\frown)^\frown \ldots)^\frown \qquad (p^k\text{-iterations}) = x .$$

The proof of Theorem 2 will require some preparation, and will be given presently. We shall refer to $x^\frown$ as the *normal complement,* (also normal *negation*) of x. Strictly, since the operation $^\frown$ depends on the choice of generator ξ in F, we have

$$(6.5)\qquad {}^\frown = {}^{\frown(\xi)} = \text{normal negation (with « base » } \xi)$$

However, since this base ξ is kept fixed, we shall only rarely need to use the amplified notation $^{\frown(\xi)}$.

Our eventual purpose is to show that the (cyclic) group, D, generated by the permutation $^\frown$, is *fully adapted* to P, i. e., that $(P, \times, +)$ is a ring logic, mod D, - see [1].

Before turning to the proof of Theorem 2 we first note the special cases given by the

Corollary. In 2-rings ($=$ Boolean rings) and also in 3 rings, normal and natural (i. e., mod N) complementation are identical,

$$(6.6)\qquad x^\frown = 1 + x = x^\wedge.$$

Proof. In a Boolean ring, F and ξ are unique

$$F = \pi = \{0, 1\}; \quad \xi = 1,$$

and (6.2) reduces to $1 + x$. Similarly in 3-rings: F and ξ are unique,

$$F = \pi = \{0, 1, 2\}; \quad \xi = 2,$$

and (6.2) reduces to

$$x^{\frown} = 2\,x + (1 + 2\,x) = 1 + x\,,$$

which proves the Corollary. In is moreover seen that 2 and 3-rings are the only classes of p^k-rings in which the normal complement, (6.2) is a linear function of x; for 2^2 rings $x^{\frown}$ is quadratic, namely

$$\text{(6.7)}\qquad \begin{aligned} x^{\frown} &= 1 + \xi^2\,x^2 \\ x^{\smile} &= \xi^2\,(1 + x^2) \end{aligned} \qquad \text{(for } 2^2 - \text{rings);}$$

for 5 rings

$$\text{(6.8)}\qquad \begin{aligned} x^{\frown} &= 1 + 2\,\xi\,x + \xi^2\,x^2 + \xi^3\,x^3 \\ x^{\smile} &= \xi^3\,(1 + 2\,x + x^2 + x^3) \end{aligned} \qquad \text{(for 5-ring);}$$

etc.

7. **Normal complementation (component form).** The proof of Theorem 2 will be given indirectly. We shall first study a more tractable transformation, $\hat{\cdot}$, which ir given in terms of the (normal idempotent) components of an element x, and shall then identify $\hat{\cdot}$ with $^{\frown}$.

Apart from Theorem 2 it will develop that $\hat{\cdot}$, in the component rather than the explicit-form of normal negation; will be important for later considerations.

Let P, F, ξ be as in § 6, and let x be an element of P. Recalling (6.1) and Theorem A, let

$$\text{(7.1)}\qquad x = [\ldots, x_\mu \ldots] = [x_0\,, x_1\,, x_\xi\,, x_{\xi_2}\,, \ldots, x_{\xi^{p^k-2}}]$$

be the normal idemponent components of $\hat{\cdot}$. (Since

$$\text{(7.2)}\qquad \xi^{p^k-1} = 1$$

we shall, as above, continue to write x_1 instead of $x_{\xi^{p^k-1}}$).

Each x is uniquely determined by and uniquely determines its normal components. In P we now define a mapping

$$\text{(7.2)}'\qquad x \to x^{\hat{\cdot}}$$

where the normal components of $x^{\hat{\cdot}}$ are obtained from those of x by subjecting the latter to the cyclic permutation

$$\text{(7.3)}\qquad (x_0 \quad x_1 \quad x_\xi \quad x_{\xi^2} \quad \ldots \quad x_{\xi^{p^k-2}})\,.$$

That is, with x given by (7.1), we have

$$x^{\frown\cdot} = [x_{\xi^{p^k-2}}, x_0, x_1, x_\xi, x_{\xi^2}, \ldots] \tag{7.4}$$

or, otherwise expressed,

$$[x^{\frown\cdot}]_0 = x_{\xi^{p^k-2}}, [x^{\frown\cdot}]_1 = x_0, [x^{\frown\cdot}]_\xi = x_1, \ldots \tag{7.5}$$

These may also be written:

$$\begin{aligned} &[x^{\frown\cdot}]_0 = x_{\xi^{p^k-2}}, [x^{\frown\cdot}]_1 = x_0, \\ &[x^{\frown\cdot}]_\mu = x_{\frac{\mu}{\xi}} \qquad (\mu \in F;\ \mu \neq 0, \neq 1). \end{aligned} \tag{7.6}$$

From this definition we immediately have

Theorem 3. In a p^k-ring P the mapping $x^{\frown\cdot}$, defined by (7.4) *or* (7.6) *is a permutation of P, and moreover of period p^k,*

$$x^{\frown\cdot\, p^k} = (\ldots (x^{\frown\cdot})^{\frown\cdot} \ldots)^{\frown\cdot} = x \qquad (x \in P).$$

The elements of the normal sub-field F are seen to be vectorially given by

$$\begin{aligned} 0 &= [1, 0, 0, 0, \quad \ldots, 0] \\ 1 &= [0, 1, 0, 0, \quad \ldots, 0] \\ \xi &= [0, 0, 1, 0, \quad \ldots, 0] \\ \xi^2 &= [0, 0, 0, 1, 0, \ldots, 0] \\ &\vdots \end{aligned} \tag{7.7}$$

From this and the definition of $^{\frown\cdot}$ we have

Theorem 4. Under the permutation $^{\frown\cdot}$ of P, the subfield F suffers the cyclic permutation

$$(0 \quad 1 \quad \xi \quad \xi^2 \quad \xi^3 \quad \ldots \quad \xi^{p_k-2}). \tag{7.8}$$

8. **Identification of $^{\frown\cdot}$ wit $^{\frown}$.** We shall next establish

Theorem 5. In a p^k-ring, P, the permutation $^{\frown\cdot}$, of § 7, *and the normal negation $^{\frown}$ of* § 6 *are identical mappings.*

$$x^{\frown} = x^{\frown\cdot} \qquad (x \in P). \tag{8.1}$$

Proof: Let F be a normal sub field of P, and ξ a generator of F. Let $x \in P$, and let its normal idempotent representation (Theorem A) be

$$x = [x_0, x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi^{p^k-2}}],$$

(8.2)

$$x = \sum_{\mu \in F} \mu\, x_\mu = 0\, x_0 + 1\, x_1 + \xi\, x_\xi + \xi^2\, x_{\xi^2} + \ldots + \xi^{p^k-2}\, x_{\xi^{p^k-2}}.$$

From (7.4) we then have

$$x^{\frown} = 0\, x_{\xi^{p^k-2}} + 1\, x_0 + \xi\, x_1 + \xi^2\, x_\xi + \ldots + \xi^{p^k-2}\, x_{\xi^{p^k-3}}. \tag{8.3}$$

Now by Theorem B, each of the normal components x_μ of x may be expressed as a polynomial in x, by (4.3). Therefore by substitution in (8.3), we may obtain an expression for $x^{\frown}$ as a polynomial in x. We shall obtain such an expression by a more elegant and shorter procedure.

By comparison of (8.2) and (8.3) we have the identity,

$$\xi\,(x - \xi^{p^k-2}\, x_{\xi^{p^k-2}}) = x^{\frown} - x_0, \tag{8.4}$$

which, on use of (7.2) may be written

$$x^{\frown} = \xi\, x + x_0 - x_{\xi^{p^k-2}}. \tag{8.5}$$

On substituting for x_0 and for $x_{\xi^{p^k-2}}$ from (4.3), we have

$$x^{\frown} = \xi\, x + 1 - x^{p^k-1} + \left(\frac{x}{\xi^{p^k-2}} + \frac{x^2}{(\xi^{p^k-2})^2} + \frac{x^3}{(\xi^{p^k-2})^3} + \ldots + \frac{x^{p^k-1}}{(\xi^{p^k-2})^{p^k-1}}\right). \tag{8.6}$$

Since $\frac{1}{\xi^{p^k-2}} = \xi$, etc., we finally have

$$x^{\frown} = \xi\, x + 1 + \xi\, x + \xi^2\, x^2 + \xi^3\, x^3 + \ldots + \xi^{p^k-2}\, x^{p^k-2}, \tag{8.7}$$

which is precisely the expression (6.2) for $x^{\frown}$. This proves Theorem 16.

The proof of Theorem 2 is now at hand. That the normal negation, $^{\frown}$ is a permutation of P, ond moreover of period p^k,

$$x^{\frown p^k} = x \tag{8.8}$$

follows from Theorems 5 and 3. The expression (6.3) for $x^{\smile}$, the inverse of $x^{\frown}$, is obtained by considering $x^{\dot\smile}$, the inverse of $x^{\dot\frown}$ (see (7.4)),

$$(8.9) \qquad x^{\dot\smile} = [x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi^{p^k-2}}, x_0],$$

writing $x^{\dot\smile}$ in normal form

$$(8.10) \qquad x^{\dot\smile} = 0\,x_1 + 1\,x_\xi + \xi\,x_{\xi^2} + \ldots + \xi^{p^k-2}\,x_0,$$

and theh espressing $x^{\dot\smile}$ in terms of x in a manner parallel to that used in obtaining (8.7). We shall omit the details. This completes Theorem 2.

9. **Normal ($=$ mod D) logic.** Let now D $(= D(\xi))$ be the group of permutations (or coordinate transformations) in a p^k ring, P, which is generated by the normal negation $^\frown$ $(= {}^{\frown(\xi)})$,

$$D = \{\text{identity}, {}^\frown, {}^{\frown 2}, {}^{\frown 3}, \ldots, {}^{\frown p^k-1}\}.$$

We call D the *normal* group in P, and the operational algebra

$$(9.1) \qquad (P, \times, {}^\frown) = (P, \times_1, {}^\frown) = (P, \times_2, {}^\frown) = \ldots$$
$$= (P, \times, \times_1, \times_2, \ldots, {}^\frown, {}^{\frown 2}, \ldots)$$

the *D-logic,* or *normal logic* of the ring $(P, \times, +)$. Here as elsewhere the notation $\times_1, \times_2, \ldots, \times_{p^k-1}$ denotes the ring product, $\times$, expressed in the $^\frown$, respectively in the $^{\frown 2}$, respectively in the $^{\frown 3}$, etc. coordinate systems, i.e., by (5.4)

$$(9.2) \qquad \begin{aligned} x \times_1 y &= (x^\frown \times y^\frown)^\smile \\ x \times_2 y &= (x^{\frown 2} \times y^{\frown 2})^{\smile 2} \\ &\vdots \end{aligned}$$

We again emphasize that *all D-logical operations may, via equations* (9.2) *or others like them, ultimately be expressed entirely in terms of the two operations* $\times$ *and* $^\frown$ *(or, if one pleases, entirely in terms of* $\times_1$ *and* $^\frown$*, or in terms of* $\times$ *and* $^{\frown 2}$*, etc.).* We shall, however, find it convenient to deal largely with D-logical expressions, which are given in terms of $^\frown$ together with $\times$ and $\times_1$, — without presenting such expressions in « ultimate » $^\frown, \times$ form by the elimination of $\times_1$.

Theorem 6. Let P be a p^k-ring, F a normal sub-field and ξ a generator of F. Then each element of F is D-logically equationally definable as follows:

for any $x \in P$,

$$
(9.3)\quad
\begin{aligned}
0 &= x \times x^{\frown} \times x^{\frown 2} \times x^{\frown 3} \times \ldots \times x^{\frown p^k - 1} \\
1 &= 0^{\frown} = (x \times x^{\frown} \times x^{\frown 2} \times \ldots \times x^{\frown p^k - 1})^{\frown} \\
1^{\frown} &= \xi \\
\xi^{\frown} &= \xi^2 \\
(\xi^2)^{\frown} &= \xi^3 \\
&\vdots \\
(\xi^{p^k-3})^{\frown} &= \xi^{p^k-2} \\
(\xi^{p^k-2}) &= 0
\end{aligned}
$$

Proof: We need merely prove the first of the identiies (9.3), since the rest follow from the first by Theorems 4 and 5. To prove the first of the set (9.3) directly from the explicit form (6.2) for $x^{\frown}$ seems extremely involved. However, if we use the normal component form $x^{\frown}$, given by (7.4 we have

$$
(9.4)\quad
\begin{aligned}
x &= [x_0, x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi p^k-2}] \\
x^{\frown} &= [x_{\xi p^k-2}, x_0, x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi p^k-3}] \\
x^{\frown 2} &= [x_{\xi p^k-3}, x_{\xi p^k-2}, x_0, x_1, x_\xi, \ldots, x_{\xi p^k-4}] \\
&\vdots \\
x^{\frown p^k-1} &= [x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi p^k-2}, x_0]\,.
\end{aligned}
$$

Corresponding to these we have the normal representation, (4.1)

$$
(9.5)\quad
\begin{aligned}
x &= x_1 + \xi\, x_\xi + \xi^2\, x_{\xi^2} + \ldots + \xi^{p^k-2}\, x_{\xi p^k-2} \\
x^{\frown} &= x_0 + \xi\, x_1 + \xi^2\, x_\xi + \ldots + \xi^{p^k-2}\, x_{\xi p^k-3} \\
x^{\frown 2} &= x_{\xi p^k-2} + \xi\, x_0 + \xi^2\, x_1 + \ldots + \xi^{p^k-2}\, x_{\xi p^k-4} \\
&\vdots \\
x^{\frown p^k-1} &= x_\xi + \xi\, x_{\xi^2} + \xi^2\, x_{\xi^3} + \ldots + \xi^{p^k-2}\, x_0\,.
\end{aligned}
$$

Since each of the expressions (9.5) omits exactly one of the normal components of x, and since these normal components are pairwise disjoint, the first of the identities (9.3) follows, and with it the complete Theorem 6.

Theorem 7. Let x be an element of a p^k ring, P, and let x_μ be the normal components of x,

$$(9.6) \qquad x = [\ldots, x_\mu, \ldots] = [x_0, x_1, x_\xi, x_{\xi^2}, \ldots, x_{\xi^{p^k-2}}].$$

Then each component x_μ may be D-logically expressed in terms of x. With η defined by

$$(9.7) \qquad \eta = \frac{1}{\xi^{\frac{p^k(p^k-1)}{2}}} = \xi^{\frac{p^k(p^k-1)}{2}},$$

the components x_μ are given by:

$$(9.8) \qquad \begin{aligned} x_0 &= \eta\, x^{\frown}\, x^{\frown 2}\, x^{\frown 3} \ldots x^{\frown p^k-1} \\ x_1 &= \eta\, x\, x^{\ \ 2}\, x^{\frown 3} \ldots x^{\frown p^k-1} \\ x_\xi &= \eta\, x\, x^{\frown}\ \ x^{\frown 3} \ldots x^{\frown p^k-1} \\ x_{\xi^2} &= \eta\, x\, x^{\frown}\, x^{\frown 2}\, x^{\frown 4} \ldots x^{\frown p^k-1} \\ &\vdots \\ x_{\xi^{p^k-2}} &= \eta\, x\, x^{\frown}\, x^{\frown 2} \ldots x^{\frown p^k-2} \end{aligned}$$

The coefficient $\eta\,(= \epsilon\, F)$ may be replaced by Theorem 5,

$$(9.9) \qquad \eta = (x\, x^{\frown}\, x^{\frown 2}\, x^{\frown 3} \ldots x^{\frown p^k-1})^{\frown \frac{p^k(p^k-1)}{2}}$$

whereupon (9.8) *yields a strict D-logical expression for the x_μ.*

Proof: Since the x_μ are pairwise disjoint, on computing the product of all except the first of the expressions (9.5), -respectively of all except the second, etc., we get

$$(9.10) \qquad \begin{aligned} \xi^{1+2+3+\cdots+p^k-2}\, x_0 &= x^{\frown}\, x^{\frown 2}\, x^{\frown 3} \ldots x^{\frown p^k-1} \\ \xi^{1+2+3+\cdots+p^k-2}\, x_1 &= x\, x^{\frown 2}\, x^{\frown 3} \ldots x^{\frown p^k-1} \\ &\vdots \end{aligned}$$

On summing the arithmetic progression in the exponent of ξ, and on simplification by use of

$$\xi^{p^k-1} = 1$$

together with the verification that

$$\frac{1}{\xi^{\frac{p^k(p^k-1)}{2}}} = \xi^{\frac{p^k(p^k-1)}{2}}$$

we readily got the desired expressions (9.8).

From (9.7) one has the

Corollary. For the coefficient η, given by (9.7), we have

$$\eta = \xi^{\frac{p^k-1}{2}} \qquad (\textit{if } p = \textit{odd prime})$$

$$\eta = 1 \qquad (\textit{if } p = 2).$$

10. **D-logical definition of $+$.** We shall first prove the essential

Theorem 8. Let $(P, \times, +)$ be a p^k-ring and $D = D(\xi)$ its normal group. If x, y are disjoint elements of P,

$$x\,y = 0 \tag{10.1}$$

then

$$x + y = x \times_1 y. \tag{10.2}$$

In particular, if $a\,b = 0$, $a + b$ is thus D-logically equationally definable. Here $\times_1$, as before, is the ring product, $\times$, expressed in the $\frown$ coordinate system, i. e.,

$$x \times_1 y = (x^\frown\, y^\frown)^\smile. \tag{10.3}$$

Proof. We have

$$x^\frown\, y^\frown = (\xi\,x + 1 + \xi\,x + \xi^2 x^2 + \xi^3 x^3 + \ldots + \xi^{p^k-2}\, x^{p^k-2}) \tag{10.4}$$

$$\times (\xi\,y + 1 + \xi\,y + \xi^2 y^2 + \ldots\ldots\ldots + \xi^{p^k-2}\, y^{p^k-2}).$$

If $x\,y = 0$ (10.4) reduces to

$$x^\frown\, y^\frown = \xi\,(x + y) + 1 + \xi\,(x + y) + \xi^2\,(x^2 + y^2) + \xi^3\,(x^3 + y^3) + \ldots \tag{10.6}$$

$$+ \xi^{p^k-2}\,(x^{p^k-2} + y^{p^k-2}).$$

But if $x\,y = 0$ we also have

$$x^n + y^n = (x + y)^n \tag{10.5}$$

Hence, from (10.5), (10.6) and (6.2):

if
$$x\,y = 0\,,$$

$$x^{\frown}\,y^{\frown} = \xi\,(x+y) + 1 + \xi\,(x+y) + \xi^2\,(x+y)^2 + \dots + \xi^{p^k-2}\,(x+y)^{p^k-2}\,.$$

$$= (x+y)^{\frown} \tag{10.7}$$

The desired result (10.2) then follows at once from (10.3) and (10.7). This completes Theorem 8.

We are now able to remove the restriction $x\,y = 0$, and to consider the case of any sum $x + y$.

Theorem 9. Let. $(P, \times, +)$ *be a* p^k*-ring,* $D = D(\xi)$ *its normal group, and* $(P, \times, {}^{\frown})$ *ist D-logic. Then the ring sum,* $+$*, is D-logically equationally definable.*

Proof. Let x, y be $\in P$. Then, by Theorems C and A,

$$x + y = \overset{+}{\underset{\mu \in F}{\Sigma}}\, \mu\,[x+y]_\mu = \overset{+}{\underset{\mu \in F}{\Sigma}}\, \mu \overset{+}{\underset{\alpha+\beta=\mu}{\Sigma}} x_\alpha\, y_\beta\,. \tag{10.8}$$

Now since the normal components of an element of P are pairwise disjoint, for $\mu' \neq \mu''$ the elements

$$\mu' \overset{+}{\underset{\alpha+\beta=\mu'}{\Sigma}} x_\alpha\, y_\beta \quad , \quad \mu'' \underset{\alpha+\beta=\mu''}{\Sigma} x_\alpha\, y_\beta \tag{10.9}$$

are disjoint (i. e., their product $= 0$). Moreover the separate terms in $\overset{+}{\underset{\alpha+\beta=\mu}{\Sigma}} x_\alpha\, y_\beta$ are also pairwise disjoint. Hence, by applying Theorem 8 twice, in (10.8) we may replace $\overset{+}{\Sigma}$ by the D-logical « $\times_1$ product », $\overset{\times_1}{\Sigma}$. By then further replacing the $\mu \in F$ by the powers of the generator ξ, we get the formula

$$x + y = \Big(\overset{\times_1}{\underset{\alpha+\beta=1}{\Sigma}} x_\alpha\, y_\beta\Big) \times_1 \Big(\overset{\times_1}{\underset{\alpha+\beta=\xi}{\Sigma}} \xi\, x_\alpha\, y_\beta\Big) \times_1 \Big(\overset{\times_1}{\underset{\alpha+\beta=\xi^2}{\Sigma}} \xi^2\, x_\alpha\, y_\beta\Big) \tag{10.10}$$
$$\times_1 \dots \times_1 \overset{\times_1}{\underset{\alpha+\beta=\xi^{p^k-2}}{\Sigma}} \xi^{p^k-2}\, x_\alpha\, y_\beta\,.$$

Each of the components $x_0, x_1, x_\xi, x_{\xi^2}, \dots, y_0, y_1, y_\xi, \dots$, and also each of the coefficients $\xi, \xi^2, \dots$ may be D-logically expressed by Theorems 6 and 7. If these D logical expressions are substituted into (10.10) we have a strictly D logical formula for $x + y$, which completes Theorem 9.

Illustration: Applied to a 2^2-ring, we have:

$$x + y = x_0\, y_1 \times_1 x_1\, y_0 \times_1 x_\xi\, y_{\xi^2} \times_1 x_{\xi^2}\, y_\xi$$

$$\times_1 \xi\; x_0\, y_\xi \times_1 \xi\; x_1\, y_{\xi^2} \times_1 \xi\; x_\xi\, y_0 \times_1 \xi\; x_{\xi^2}\, y_1$$

$$\times_1 \xi^2\, x_0\, y_{\xi^2} \times_1 \xi^2\, x_1\, y_\xi \times_1 \xi^2\, x_\xi\, y_1 \times_1 \xi^2\, x_{\xi^2}\, y_0$$

where

$$x_0 = x^{\frown}\;\; x^{\frown 2}\, x^{\frown 3} \qquad\qquad y_0 = y^{\frown}\;\; y^{\frown 2}\, y^{\frown 3}$$

$$x_1 = x\, x^{\frown}\, x^{\frown 2} \qquad ; \qquad \vdots$$

$$x_\xi = x\, x^{\frown}\, x^{\frown 3}$$

$$x_{\xi^2} = x \;\; x^{\frown 2}\, x^{\frown 3}$$

$$\xi = (x\, x^{\frown}\, x^{\frown 2}\, x^{\frown 3})^{\frown 2} = (y\, y^{\frown}\, y^{\frown 2}\, y^{\frown 3})^{\frown 2}$$

$$\xi^2 = (x\, x^{\frown}\, x^{\frown 2}\, x^{\frown 3})^{\frown 3} = (y\, y^{\frown}\, y^{\frown 2}\, y^{\frown 3})^{\frown 3}.$$

11. **Ring-logic.** We now prove

Theorem 10. A p^k ring is a ring-logic, mod. D. Since we have already established that the ring sum, $+$, of a p^k-ring $(P, \times, +)$ is D logically equationally definable there remains only to prove that $(P, \times, +)$ is D-logically fixed. That is, if $(P, \times, +_1)$ is a ring, on the same class P and having the same $\times$, and furthermore having the same D logic, i. e.,

$$(11.1) \qquad x^{\smile} = x^{\frown 1} : \xi x + 1 + \xi x + \xi^2 x^2 + \ldots + \xi^{p^k-2}\, x^{p^k-2} =$$

$$= \xi x +_1 1 +_1 \xi x +_1 \ldots +_1 \xi^{p^k-2}\, x^{p^k-2},$$

then we must show that $+_1 = +$, i. e., the rings are identical.

Since the unit and zero elements are multiplicationally definable, $(P, \times, +_1)$ has the same unit element, 1, and the same zero, 0, as $(P, \times, +)$. We prove the

Lemma 1. *$(P, \times, +_1)$ is of characteristic p,*

$$(11.2) \qquad a +_1 a +_1 a +_1 \ldots +_1 a \;(p \text{ terms}) = 0, \qquad (a \in P).$$

Proof: Let $(F, \times, +)$ be a normal sub-field of $(P, \times, +)$, and let ξ be a generator of F. Putting $x = \xi^{p^k-2}$ in the hypothesis (11.1) we get

$$(11.3) \qquad 0 = 1 +_1 1 +_1 1 +_1 \ldots +_1 1 \;(p^k \text{ terms}),$$

or, otherwise written,

(11.4) $$0 = (1 +_1 1 +_1 1 +_1 \dots +_1 1\ (p \text{ terms}))^k$$

Because of (*ii*) of § 2, $(P, \times, +)$ and hence also $(P, \times, +_1)$ has no non-zero nilpotent elements, Hence (11.4) implies

$$1 +_1 1 +_1 1 +_1 \dots +_1 1\ (p \text{ terms}) = 0\,,$$

which, on multiplication by a, proves (11.2) and Lemma 1.

Lemma 2. *$(P, \times, +_1)$ is a p^k-ring. If $(F, \times, +)$ is a normal subfield of $(P, \times, +)$, then $(F, \times, +_1)$ is a normal subfield of $(P, \times, +_1)$,*

(11.5) $$(F, \times, +) \cong (F, \times, +_1) \cong F_{p^k}\,.$$

Proof. Let

(11.6) $$1 +_1 1 = 2_1\,, \quad 1 +_1 2_1 = 3_1\,, \quad \text{etc.}.$$

By virtue of Lemma 1, if

(11.7) $$\pi_1 = \{0, 1, 2_1, 3_1, \dots, (p-1)_1\}\,,$$

then $(\pi_1, \times, +_1)$ is a subfield of $(P, \times, +_1)$, isomorphic with F_p = field of residues, mod p. Let ξ be generator of a normal sub-field $(F, \times, +)$,

(11.8) $$F = \{0, 1, \xi, \xi^2, \dots, \xi^{p^k-2}\}.$$

If $\xi \in \pi$, so are the powers of ξ, and hence, since ξ is a generator of F, evidently: $k = 1$, the classes π_1 and F are identical and

(11.9) $$(F, \times, +) \cong (F, \times, +_1) \cong F_p\,.$$

If $\xi \in \pi_1$, then, since $\xi^{p^k-1} = 1$, or

(11.10) $$\xi^{p^k-1} - 1 = \xi^{p^k-1} -_1 1 = 0\,,$$

ξ is algebraic over the field $(\pi_1, \times, +_1)$. Let $\pi_1(\xi)$ be the over field resulting from the adjunction ξ to π_1. Now $\pi_1(\xi)$, being a field of characteristic p, is isomorphic with a Galois field F_{p^h} for some h. Since $x^{p^k} = x$ for all $x \in P$, it follows that

(11.11) $$h \leqq k\,.$$

However $\xi \in \pi_1(\xi)$ and ξ has period p^k, whence

(11.12) $$k \leqq h .$$

From (11.11) and (11.12) we have

(11.13) $$h = k$$

Then, since $0, 1, \xi, \xi^2, \ldots, \xi^{p^k-2}$ are distinct $\in \pi_1(\xi)$, it follows that the sets F and $\pi_1(\xi)$ are identical subsets of P, and

(11.14) $$(F, \times, +) \cong (F, \times, +_1) \cong F_{p^k} .$$

Referring now to (i) — (iv) of § 2, we see that $(P, \times, +_1)$ is a p^k-ring, and Lemma 2 is proved.

The proof of Theoreh 10 is now immediate. Let $(P, \times, +)$ be a p^k-ring and let $(P, \times, +_1)$ be a ring (on the same set P, and with the same $\times$) having the same D-logic as $(P, \times, +)$, — see (11.1). Then by Lemma 2 $(P, \times, +_1)$ is a p^k-ring. Hence, by Theorem 9 its ring sum, $+_1$, is D-logically equationally definable, i. e., satisfies an identity of the form

$$x +_1 y = \mathcal{C}(x, y \ ; \ \times, \frown_1),$$

where $\mathcal{C}$ is a strictly D-logical expression, — composed from x and y solely by use of the D-logical operations $\times$, $\frown_1$. Furthermore since $(P, \times, +)$ is a p^k-ring, $x + y$ satisfies precisely the same D-logical identity, with $\frown$ instead of $\frown_1$,

$$x + y = \mathcal{C}(x . y \ ; \ \times . \frown) .$$

Since $x^\frown \underset{x}{\equiv} x^{\frown_1}$, by hypothesis, it follows that $+ = +_1$. This completes Theorem 10.

12. Complete set of operations in a finite field. Consider the foregoing theory specialized to F_{p^k} = Galois field of p^k elements.

Theorem 11. In F_{p^k}, $\times$ and $\frown$ form a complete set of operations. That is, any operation $\theta(x, y, \ldots, z)$ in the class F_{p^k} may be expressed in terms of $x, y, \ldots, z$ by means of the operations $\times$ and $\frown$.

Proof. In a finite field, F, any operation $\theta(x, y, \ldots, z)$ may be « analytically » expressed, i. e., as some polynomial in $x, y, \ldots, z$ with coefficients in F. Each of the coefficients may be expressed in terms of x by means of $\times$ and $\frown$ (see § 9), and since, via Theorem 9, $+$ is also D-logically expressible, Theorem 11 is proved.

While all p^k rings — and hence in particulare p-rings — are ring-logics mod D, it was shown in [3] that p-rings are also ring logics mod N. Moreover, as previously remarked, D and N only coincide for 2-rings and for 3-rings. In particular for $F_p =$ field of residues mod p, corresponding to Theorem 11 we have

Theorem 12. In F_p, $\times$ and $\frown$ form a complete set of operations; also $\times$, $\wedge$ form a complete set of operations.

Of the twe rival complete systems in F_p it is noteworthy that the first, namely $(F_p, \times, \frown)$, requires only a knowledge of the multiplication table in F_p; for, in F_p, $\frown$ $(= \frown^{(\xi)})$ is the cyclic permutation

$$(0\ 1\ \xi\ \xi^2\ \xi^3 \ldots \xi^{p-2}).$$

In this sense the $\frown$, $\times$ equational formula for the ring sum, $+$, (and similarly the formula for any other opertion in F_p) is a strictly multiplicative formula! *Addition is thus equationally definable in terms of multiplication.* The situation is different in the complete system $(F_p, \times, \wedge)$, since $x^\wedge = x + 1$ involves a (limited) use of the addition table. It is intuitively suggestive to think of $x^\wedge$ as the «additive-successor» of x, and $x^\frown$ as the multiplicative successor (relative to the base ξ) of x.

Remark. We have shown that a p^k ring, P, is a ring-logic mod $D(\xi)$ for any choice of generator, ξ. The $D(\xi)$ logical equation for $x + y$ given by Theorem 9 is a certain formula

$$x + y = \Phi(x, y; \times, \frown^{(\xi)}).$$

A careful examination of the proof of Theorem 9 shows that, for a generator $\eta \neq \xi$ the $D(\eta)$-logical expression for $x + y$ is given (in general) by a different formula,

$$x + y = \Psi(x, y; \times, \frown^{(\eta)})$$

That is Ψ and Φ are in general different functions. A similar remark is of course also true for any fixed operation in P.

University of California, Berkeley

BIBLIOGRAPHY

1. A. L. FOSTER, « *On n-ality theories in rings and their logical algebras, including tri-ality principle in three valued logics* », Amer. Jour. of Math., V. LXXII, pp. 101-123.

2. A. L. FOSTER, « *p-Rings and their Boolean vector representation* » Acta Mathematica, Vol. 84 (1950), pp. 231-261.

3. A. L FOSTER, « *p Rings and ring-logics* », University of Calif. publications in mathematics, Vol. 1 : 10 (1951), pp. 385-396.

4. A. L. FOSTER, « *Boolean extensions and sub-direct ring powers* », In process of publication·

5. N. H. MC COY, « *Subrings of direct sums* », Amer. Jour. of Math., Vol. LX (1938), pp 374-382.

6. N. H. MC COY and DEANE MONTGOMERY, « *A representation of generalized Boolean rings* », Duke Math. Jour., Vol. 3, (1937) pp. 455-459.

7. M. H. STONE, « *The theory of representations of Boolean algebra* », Trans. of the Amer Math. Soc., V. 40 (1936), pp. 37-111.

8. A. L. FOSTER, « *The idempotent elements of a commutative ring form a Boolean algebra ; ring duality and transformation theory* », Duke Math. Jour., Vol. 12 (1945), pp. 143-152.

[*Pervenuta in redazione il 10-8-1951*]