ON THE RING-LOGIC CHARACTER OF CERTAIN RINGS

ADIL YAQUB

Introduction. Boolean rings $(B, \times, +)$ and Boolean logics ($=$ Boolean algebras) $(B, \cap, {}^*)$ though historically and conceptionally different, are equationally interdefinable in a familiar way [6]. With this equational interdefinability as motivation, Foster introduced and studied the theory of ring-logics. In this theory, a ring (or an algebra) R is studied modulo K, where K is an arbitrary transformation group in R. The Boolean theory results from the special choice, for K, of the "Boolean group," generated by $x^* = 1 - x$ (order 2, $x^{**} = x$). More generally, let $(R, \times, +)$ be a commutative ring with identity 1, and let $K = \{\rho_1, \rho_2, \cdots\}$ be a transformation group in R. The *K-logic* (*or K-logical algebra*) of the ring $(R, \times, +)$ is the (operationally closed) system $(R, \times, \rho_1, \rho_2, \cdots)$ 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 $\rho_1, \rho_2, \cdots$ of K. The ring $(R, \times, +)$ is called a *ring-logic*, mod K if (1) the "$+$" of the ring is *equationally* definable in terms of its K-logic $(R, \times; \rho_1, \rho_2, \cdots)$, and (2) the "$+$" of the ring is *fixed* by its K-logic. Of particular interest in the theory of ring-logics is the *normal group* D which was shown in [1] to be particularly adaptable to p^k-rings. Our present object is to extend further the class of ring-logics, modulo the normal group D itself. A by-product of this extension is the following result, namely, any finite commutative ring with zero radical is a ring-logic, mod D (see Corollary 8). Furthermore, in Corollary 10, we prove that, more generally, any (not necessarily finite) ring with unit which satisfies $x^n = x$(n fixed, $\geqq 2$) is a ring-logic (mod D). Finally, we compare the normal group with the so-called *natural* group in regard to the ring-logic character of a certain important class of rings (see section 3).

1. The finite field case. Let $(F_{p^k}, \times, +)$ be a Galois (finite) field with exactly p^k elements (p prime). Then, as is well known, F_{p^k} contains a multiplicative generator, ξ;

$$F_{p^k} = \{0, \xi, \xi^2, \cdots, \xi^{p^k-1} (=1)\} .$$

We now have the following (compare with [1]).

THEOREM 1. *Let F_{p^k} be a Galois field, and let ξ be a generator of F_{p^k}. Then the mapping $x \to x^\frown$ defined by*

Received August 16, 1963.

$$(1.1)\qquad x^{\frown} = \xi x + (1 + \xi x + \xi^2 x^2 + \cdots + \xi^{p^k-2} x^{p^k-2})$$

is a permutation of F_{p^k}, with inverse given by

$$(1.2)\qquad x^{\smile} = \xi^{p^k-2}(1 + x + x^2 + \cdots + x^{p^k-2}) + \xi^{p^k-2} x \, .$$

Furthermore, the permutation $\frown$ is of period p^k,

$$(1.3)\qquad x^{\frown p^k} = (\cdots (x^{\frown})^{\frown} \cdots)^{\frown} \quad (p^k\text{-iterations}) = x \, .$$

Proof. Since $a^{p^k-1} = 1$, $a \in F_{p^k}$, $a \neq 0$, therefore, by (1.1), $x^{\frown} = \xi x + \{[(1 - (\xi x)^{p^k-1}]/(1 - \xi x)\} = \xi x$, if $x \neq 0$ and $\xi x \neq 1$. Furthermore, by (1.1), $0^{\frown} = 1$ and $(1/\xi)^{\frown} = p^k \cdot 1 = 0$. Hence, $0^{\frown} = 1$, $1^{\frown} = \xi$, $\xi^{\frown} = \xi^2$, $(\xi^2)^{\frown} = \xi^3, \cdots, (\xi^{p^k-2})^{\frown} = 0$. This proves (1.3). To prove (1.2), observe that the right-side of (1.2) is equal to

$$\frac{1}{\xi} x + \frac{1}{\xi}\left\{\frac{1 - x^{p^k-1}}{1 - x}\right\} = \frac{1}{\xi} x \, , \qquad \text{if } x \neq 1 \text{ and } x \neq 0 \, .$$

Moreover, if $x \neq 0$ and $x \neq 1/\xi$, then $x^{\frown} = \xi x$ and hence $x^{\smile} = (1/\xi)x$. Since (1.2) clearly holds for $x = 0$, $x = 1/\xi$, and $x = 1$, therefore (1.2) is true for all elements of F_{p^k}, and the theorem is proved.

COROLLARY 2. *Under the permutation $\frown$, F_{p^k} suffers the cyclic permutation*

$$(1.4)\qquad (0, 1, \xi, \xi^2, \xi^3, \cdots, \xi^{p^k-2}) \, .$$

Following [1], we call $x^{\frown}$ the *normal negation* of x, and call the cyclic group D whose generator is $x^{\frown}$ the *normal group*. By Theorem 1, it is now clear that

$$D = D(\xi) = \{\text{identity}, \frown, \frown^2, \frown^3, \cdots, \frown^{p^k-1}\} \, .$$

As in [1], we define

$$(1.5)\qquad a \times_{\frown} b = (a^{\frown} \times b^{\frown})^{\smile} \, .$$

It is readily verified that

$$(1.6)\qquad a \times_{\frown} 0 = a = 0 \times_{\frown} a \, .$$

COROLLARY 3. *The elements of F_{p^k} are equationally definable in terms of the D-logic.*

Proof. By Corollary 2, it is easily seen that

$$
\begin{aligned}
0 &= x x^{\frown} x^{\frown 2} \cdots x^{\frown p^k-1} \\
1 &= 0^{\frown} \\
\xi &= 1^{\frown} \\
\xi^2 &= \xi^{\frown} \\
&\cdots \\
\xi^{p^k-2} &= (\xi^{p^k-3})^{\frown} ,
\end{aligned}
\tag{1.7}
$$

and the corollary follows.

We recall from [3] the *characteristic function* $\delta_\mu(x)$, defined as follows: for a given $\mu \in F_{p^k}$,

$$
\delta_\mu(x) = \begin{cases} 1 & \text{if } x = \mu \\ 0 & \text{if } x \neq \mu . \end{cases}
\tag{1.8}
$$

In view of Corollory 2, it is easily seen that, for any given $\mu \in F_{p^k}$, there exists an integer r such that $\mu^{\frown r} = 0$. Then, clearly,

$$
\delta_\mu(x) = \delta_0(x^{\frown r}) \qquad \text{where} \quad \mu^{\frown r} = 0 .
\tag{1.9}
$$

Now, let $\sum^{\times\frown}_{\alpha_i \in F} \alpha_i$ denote $\alpha_1 \times_{\frown} \alpha_2 \times_{\frown} \alpha_3 \cdots$, where $\alpha_1, \alpha_2, \alpha_3, \cdots$ are the elements of F. Then, by (1.6) and (1.8), we have the identity [3]

$$
f(x, y, \cdots) = \sum^{\times\frown}_{\alpha,\beta,\cdots \in F_{p^k}} f(\alpha, \beta, \cdots)(\delta_\alpha(x)\delta_\beta(y)\cdots) .
\tag{1.10}
$$

In (1.10), $\alpha, \beta, \cdots$ range over all the elements of F_{p^k} while $x, y, \cdots$ are indeterminates over F_{p^k}. We shall use (1.9) and (1.10) presently.

LEMMA 4. *The characteristic functions $\delta_\mu(x)$, $\mu \in F_{p^k}$, are equationally definable in terms of the D-logic.*

Proof. Since $x^{p^k-1} = 1$, $x \neq 0$, $x \in F_{p^k}$, therefore, $\delta_0(x) = ((x^{p^k-1})^{\smile})^{p^k-1}$. Hence $\delta_0(x)$ is *equationally* definable in terms of the D-logic. Therefore, by (1.9), $\delta_\mu(x)$ is also equationally definable in terms of the D-logic, and the lemma is proved.

We are now in a position to prove the following.

THEOREM 5. *The Galois field $(F_{p^k}, \times, +)$ is a ring-logic* (mod D).

Proof. By (1.10), we have,

$$
x + y = \sum^{\times\frown}_{\alpha\ \beta \in F_{p^k}} (\alpha + \beta)(\delta_\alpha(x)\delta_\beta(y)) .
$$

Now, by Corollary 3, $\alpha + \beta$ is equationally definable in terms of the

D-logic. Moreover, by Lemma 4, each of the characteristic functions $\delta_\alpha(x)$ and $\delta_\beta(y)$ is equationally definable in terms of the D-logic. Hence the "+" of F_{p^k} is *equationally* definable in terms of the D-logic $(F_{p^k}, \times, \frown, \smile)$. Next, we show that $(F_k, \times, +)$ is *fixed* by its D-logic. Suppose then that there exists another ring $(F_{p^k}, \times, +')$, with the same class of elements F_{p^k} and the same "$\times$" as $(F_{p^k}, \times, +)$ and which has the *same logic* as $(F_{p^k}, \times, +)$. To prove that $+' = +$. Since both $(F_{p^k}, \times, +)$ and $(F_{p^k}, \times, +')$ have the *same* class of elements and the *same* "$\times$", it readily follows that $(F_{p^k}, \times +')$ is also a Galois field with exactly p^k elements. Since, up to isomorphism, there is *only one* Galois field with exactly p^k elements, therfore, $+' = +$, and the theorem is proved.

2. The General Case. In order to extend Theorem 5 to *any* finite commutative ring with zero radical, the following concept of independence, introduced by Foster [2], is needed.

DEFINITION. Let $\bar{A} = \{A_1, A_2, \cdots, A_n\}$ be a finite set of algebras of the same species S_p. We say that the algebras $A_1, A_2, \cdots, A_n$ are *independent* if, corresponding to each set $\{\varphi_i\}$ of expressions of species S_p $(i = 1, \cdots, n)$ there exists at least one expression ψ such that $\psi = \varphi_i \pmod{A_i}$ $(i = 1, \cdots, n)$. By an *expression* we mean some composition of one or more indeterminate-symbols $\xi, \cdots$ in terms of the primitive operations of $A_1, A_2, \cdots, A_n$; $\psi = \varphi \pmod{A}$ means that this is an identity of the algebra A.

We now examine the independence of the D-logics $(F_{p_i^{k_i}}, \times, \frown, \smile)$. Indeed, we have the following (compare with [2]).

THEOREM 6. *Let $p_1, \cdots, p_t$ be distinct primes. Then the D-logics $(F_{p_i^{k_i}}, \times, \frown, \smile)$ are independent.*

Proof. Let $n_i = p_i^{k_i}$, $F_i = F_{p_i}k_i = \{0, 1, \lambda, \lambda^2, \cdots, \lambda^{n_i-2}\}$, $n = \max_{1\leqq i\leqq t}\{n_i\}$, $N = \prod_{j=1}^t n_j$, $n_iN_i = N$, $E = \xi\xi^{\frown}\xi^{\frown 2}\cdots\xi^{\frown n-1}$.

It is easily seen, since the n_i's are *distinct prime* powers, that

$$|_i(\xi) = (E^{\frown N_i})^{n_i-1} = \begin{cases} 1 \pmod{F_i} \\ 0 \pmod{F_j} \end{cases} \quad (j \neq i)\,.$$

Now, to prove the indepedence of the logics $(F_i, \times, \frown, \smile)$ $(i = 1, \cdots, t)$ let $\varphi_1, \cdots, \varphi_t$ be any set of t expressions of species $\times, \frown, \smile$, i.e., primitive compositions of indeterminate-symbols in terms of the operations $\times, \frown, \smile$. Define an expression $K(\varphi_1, \cdots, \varphi_t)$ as follows (compare with [2]):

$$K(\varphi_1, \cdots, \varphi_t) = (\varphi_1 \cdot |_1(\xi)) \times_{\frown} (\varphi_2 \cdot |_2(\xi)) \times_{\frown} \cdots \times_{\frown} (\varphi_t \cdot |_t(\xi))\,.$$

Then it is easily seen that $K(\varphi_1, \cdots, \varphi_t) = \varphi_i \pmod{F_i}$ $(i = 1, \cdots, t)$, since $a \times_{\frown} 0 = 0 \times_{\frown} a = a$, and the theorem is proved.

We shall now extend the concept of ring-logic to the direct sum of certain ring-logics. We denote the direct sum of A_1 and A_2 by $A_1 \oplus A_2$. The direct power A^m will denote $A \oplus A \oplus \cdots \oplus A$ (m summands).

THEOREM 7. *Let A be any subdirect sum with identity of (not necessarily finite) subdirect powers of the Galois fields $F_{p_i^{k_i}}$ $(i = 1, \cdots, t)$. Then A is a ring-logic (mod D).*

Proof. Let $q_1, \cdots, q_r$ be the *distinct* primes in $\{p_1, \cdots, p_t\}$. Since the Galois Fields $F_{p^{k_i}}$ and $F_{p^{k_j}}$ are both subfields of $F_{p^{k_i k_j}}$, it is easily seen that A is a *subring* of a direct sum of direct powers of $F_{q_i^{h_i}}$, $(i = 1, \cdots, r)$; i.e., A is a subring of $F_{q_1^{h_1}}^{m_1} \oplus \cdots \oplus F_{q_r^{h_r}}^{m_r}$ for some positive integers $h_1, \cdots, h_r$. Now, by Theorem 5, each $F_{q_i^{h_i}}$ is a ring-logic (mod D), and hence there exists a D-logical expression φ_i such that, for every $x_i, y_i \in F_{q_i^{h_i}}$ $(i = 1, \cdots, r)$,

$$x_i + y_i = \varphi_i(x_i, y_i; \times, \frown, \smile) .$$

Since, by Theorem 6, the D-logics $(F_{q_i^{h_i}}, \times, \frown, \smile)$ $(i = 1, \cdots, r)$ are independent, there exists a D-logical expression K such that

$$K = \begin{cases} \varphi_1 \pmod{F_{q_1^{h_1}}} \\ \cdots \\ \varphi_r \pmod{F_{q_r^{h_r}}} . \end{cases}$$

Therefore, for every $x_i, y_i \in F_{q_i^{h_i}}$ $(i = 1, \cdots, r)$,

$$x_i + y_i = \varphi_i = K(x_i, y_i; \times, \frown, \smile) .$$

Hence, the D-logical expression K represents the "+" of each $F_{q_i^{h_i}}$. Since the operations are component-wise in the direct sum $F_{q_1^{h_1}}^{m_1} \oplus \cdots \oplus F_{q_r^{h_r}}^{m_r}$, therefore, for all x, y in this direct sum, we have,

$$x + y = K(x, y; \times, \frown, \smile) .$$

Hence, *a fortiori*, the "+" of the *subring A* is *equationally* definable in terms of the D-logic.

Next, we show that A is *fixed* by its D-logic. Suppose there exists a "+′" such that $(A, \times, +')$ is a ring, with the same class of elements A and the same "×" as the ring $(A, \times, +)$, and which has the *same logic* $(A, \times, \frown, \smile)$ as the ring $(A, \times, +)$. To prove that $+' = +$. Now, since A is a subdirect sum of subdirect powers of $F_{p_i^{k_i}}$, therefore, a new "+′" in A defines and is defined by a new

"$+_1'$" in $F_{p_1^{k_1}}$, "$+_2'$" in $F_{p_2^{k_2}}$, $\cdots$, "$+_t'$" in $F_{p_t^{k_t}}$, such that $(F_{p_i^{k_i}}, \times, +_i')$ is a ring $(i = 1, \cdots, t)$. Furthermore, the assumption that $(A, \times, +')$ has the same logic as $(A, \times, +)$ is equivalent to the assumption that each $(F_{p_i^{k_i}}, \times, +_i')$ has the same logic as $(F_{p_i^{k_i}}, \times, +)$ $(i = 1, \cdots, t)$. Since, by Theorem 5, $(F_{p_i^{k_i}}, \times, +)$ is a ring-logic, and hence with its "$+$" fixed, it follows that $+_i' = +$ $(i = 1, \cdots, t)$. Hence $+' = +$, and the theorem is proved.

Now, it is well known (see [4]) that any finite commutative ring with zero radical and with more than one element is isomorphic to the complete direct sum of a finite number of finite fields. Hence, Theorem 7 has the following

COROLLARY 8. *Any finite commutative ring with zero radical is a ring-logic* $(\mathrm{mod}\, D)$.

It is also well known (see [1; 5]) that every p-ring (p prime) is isomorphic to a subdirect power of F_p, and every p^k-ring (p prime) is isomorphic to a subdirect power of F_{p^k}. Hence, by letting $t = 1$ in Theorem 7, we obtain the following (compare with [1; 7])

COROLLARY 9. *Any p-ring with identity, as well as any p^k-ring with identity, is a ring-logic* $(\mathrm{mod}\, D)$.

Now, let n be a fixed integer, $n \geqq 2$. It is well known that a ring R which satisfies $x^n = x$ for all x in R is isomorphic to a subdirect sum of (not necessarily finite) subdirect powers of a *finite* set of Galois fields. Hence Theorem 7 has the following

COROLLARY 10. *Let R be a ring with unit such that $x^n = x$ for all x in R, where n is a fixed integer, $n \geqq 2$. Then R is a ring-logic* $(\mathrm{mod}\, D)$.

3. The natural group and the normal group. Let $(R, \times, +)$ be a commutative ring with unit 1. We recall (see [1]) that the *natural group* N is the group generated by $x^\wedge = x + 1$ (with inverse $x^\vee = x - 1$). In [7], it was shown that $(F_{p^k}, \times, +)$ is a ring-logic $(\mathrm{mod}\, N)$, and hence the "$+$" of F_{p^k} is equationally definable in terms of the N-logic $(F_{p^k}, \times, {}^\wedge)$. Moreover, by Theorem 5, $(F_{p^k}, \times, +)$ is a ring-logic $(\mathrm{mod}\, D)$, and hence the "$+$" of F_{p^k} is equationally definable in terms of the D-logic $(F_{p^k}, \times, \frown)$. Of the two rival logics, $(F_{p^k}, \times, \frown)$ requires only a knowledge of the multiplication table in F_{p^k} since, by Corollary 2, the effect of $\frown$ on F_{p^k} is the cyclic permutation $(0, 1, \xi, \xi^2, \cdots, \xi^{p^k-2})$. In this sense, the D-logical formula for the "$+$" of F_{p^k} is a *strictly multiplicative formula, and addition is thus* *equationally definable in terms of multiplication* whenever the generator ξ is chosen (compare with [1]). The situation is quite different in the case of the N-logical formula for the "+" of F_{p^k}, since the generator $x^\wedge = x + 1$ of the natural group N already involves a limited use of the addition table.

REFERENCES

1. A. L. Foster, *p^k-rings and ring-logics*, Ann. Scn. Norm Pisa, **5** (1951), 279-300.

2. ———, *The identities of—and unique subdirect factorization within—classes of universal algebas*, Math. Z., **62** (1955), 171-188.

3. ———, *Generalized Boolean theory of universal algebras, Part I*, Math. Z, **58** (1953), 306-336.

4. N. H. McCoy, *Rings and ideals*, Carus Math. Monog., **8** (1947).

5. N. H. McCoy and D. Montgomery, *A representation of generalized Boolean rings*, Duke Math J., **3** (1937), 455-459.

6. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Soc., **40** (1936), 37-111.

7. A. Yaqub, *On certain finite rings and ring-logics*, Pacific J. Math., **12** (1962), 785-790.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA