ON THE RING-LOGIC CHARACTER OF CERTAIN RINGS

Adil Mohamed Yaqub
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 \(x^n = x(n \text{ fixed, } \geq 2)\) 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, \(\xi\);

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

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

**Theorem 1.** Let \(F_{p^k}\) be a Galois field, and let \(\xi\) be a generator of \(F_{p^k}\). Then the mapping \(x \to x^\wedge\) defined by

\[
\]
(1.1) \[ x^- = \xi x + (1 + \xi x + \xi^2 x^2 + \cdots + \xi^{p^k-2} x^{p^k-3}) \]
is a permutation of \( F_{p^k} \), with inverse given by

(1.2) \[ x^\sim = \xi^{p^k-2}(1 + x + x^2 + \cdots + x^{p^k-3}) + \xi^{p^k-2} x . \]

Furthermore, the permutation \( \sim \) is of period \( p^k \),

(1.3) \[ x^{\sim p^k} = (\cdots (x^-)^{\sim - 1} \cdots)^{\sim - 1} = x . \]

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

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

Moreover, if \( x \neq 0 \) and \( x \neq 1/\xi \), then \( x^- = \xi x \), and hence \( x^- = (1/\xi)x \). 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 \( \sim \), \( F_{p^k} \) suffers the cyclic permutation

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

Following [1], we call \( x^- \) the normal negation of \( x \), and call the cyclic group \( D \) whose generator is \( x^- \) the normal group. By Theorem 1, it is now clear that

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

As in [1], we define

(1.5) \[ a \times \sim b = (a^- \times b^-)^- . \]

It is readily verified that

(1.6) \[ a \times \sim 0 = a = 0 \times \sim a . \]

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
and the corollary follows.

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

\[
\delta_\mu(x) = \begin{cases} 
1 & \text{if } x = \mu \\
0 & \text{if } x \neq \mu .
\end{cases}
\]

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

\[
\delta_\mu(x) = \delta_0(x^{-r}) \quad \text{where } \mu^{-r} = 0 .
\]

Now, let \( \sum_{\alpha_i \in F} \alpha_i \) denote \( \alpha_1 \times \alpha_2 \times \alpha_3 \times \cdots \), 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]

\[
f(x, y, \cdots) = \sum_{\alpha, \beta, \cdots \in F_{p^k}} f(\alpha, \beta, \cdots)(\delta_\alpha(x)\delta_\beta(y)\cdots) .
\]

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, \( \delta_0(x) = ((x^{p^k-1})^{-1})^{p^k-1} \). 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,

\[
x + y = \sum_{\alpha, \beta \in F_{p^k}} (\alpha + \beta)(\delta_\alpha(x)\delta_\beta(y)) .
\]

Now, by Corollary 3, \( \alpha + \beta \) is equationally definable in terms of the
D-logic. Moreover, by Lemma 4, each of the characteristic functions $\delta_a(x)$ and $\delta_p(y)$ is equationally definable in terms of the D-logic. Hence the "+" of $F_{p^k}$ is 

**equationally** definable in terms of the D-logic ($F_{p^k}, \times, \leftarrow, \rightarrow$). Next, we show that $(F_k, \times, +)$ is fixed by its D-logic. Suppose then that there exists another ring $(F_{p^k}, x, +')$, with the same class of elements $F_{p^k}$ and the same "x" as $(F_{p^k}, x, +)$ and which has the same logic as $(F_{p^k}, \times, +)$. To prove that $+' = +$. Since both $(F_{p^k}, x, +)$ and $(F_{p^k}, x, +')$ have the same class of elements and the same "x", it readily follows that $(F_{p^k}, x +')$ 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, therefore, $+' = +$, 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 $\tilde{A} = \{A_1, A_2, \ldots, A_n\}$ be a finite set of algebras of the same species $S_p$. We say that the algebras $A_1, A_2, \ldots, A_n$ are independent if, corresponding to each set $\{\varphi_i\}$ of expressions of species $S_p$ ($i = 1, \ldots, n$) there exists at least one expression $\psi$ such that $\psi = \varphi_i (\text{mod } A_i)$ ($i = 1, \ldots, n$). By an expression we mean some composition of one or more indeterminate-symbols $\xi, \ldots$ in terms of the primitive operations of $A_1, A_2, \ldots, A_n$; $\psi = \varphi \pmod{A}$ means that this is an identity of the algebra $A$.

We now examine the independence of the D-logics $(F_{p^k}, x, \leftarrow, \rightarrow)$. Indeed, we have the following (compare with [2]).

**THEOREM 6.** Let $p_1, \ldots, p_t$ be distinct primes. Then the D-logics $(F_{p_i}, \times, \leftarrow, \rightarrow)$ are independent.

**Proof.** Let $n_i = p_i^{\epsilon_i}$, $F_i = F_{p_i^{\epsilon_i}} = \{0, 1, \lambda, \lambda^2, \ldots, \lambda^{n_i-2}\}$, $n = \max_{1 \leq i \leq t} \{n_i\}$, $N = \prod_{j=1}^t n_j$, $n_iN_i = N$, $E = \xi_1^{\xi_2^{\xi_3^{\ldots^{\xi_{n-1}}}}}$.

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

$$|\delta(\xi) = (E^\leftarrow)^{n_i-1} = \begin{cases} 1 \pmod{F_i} & (j \neq i) \\ 0 \pmod{F_j} & \end{cases}.$$  

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

$$K(\varphi_1, \ldots, \varphi_t) = (\varphi_1 \cdot |\delta(\xi)) \times (\varphi_2 \cdot |\delta(\xi)) \times \cdots \times (\varphi_t \cdot |\delta(\xi)).$$
Then it is easily seen that \( K(\varphi_i, \cdots, \varphi_t) = \varphi_i \pmod{F_i^t} \) \((i = 1, \cdots, t)\), since \( a \times 0 = 0 \times a = a \), 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 \((\text{not necessarily finite})\) subdirect powers of the Galois fields \( F_{p_i}^{h_i} \) \((i = 1, \cdots, t)\). Then \( A \) is a ring-logic \((\text{mod } D)\).

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

\[
x_i + y_i = \varphi_i(x_i, y_i; \times, \circ, \lnot).
\]

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

\[
K = \begin{cases} 
\varphi_1 (\text{mod } F_{p_1}^{h_1}) \\
\cdots \\
\varphi_r (\text{mod } F_{p_r}^{h_r}) 
\end{cases}.
\]

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

\[
x_i + y_i = \varphi_i = K(x_i, y_i; \times, \circ, \lnot).
\]

Hence, the \( D \)-logical expression \( K \) represents the “+” of each \( F_{p_i}^{h_i} \). Since the operations are component-wise in the direct sum \( F_{p_1}^{m_1} + \cdots + F_{p_r}^{m_r} \), therefore, for all \( x, y \) in this direct sum, we have,

\[
x + y = K(x, y; \times, \circ, \lnot).
\]

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 \((A, \times, \lnot, \lnot)\) as the ring \((A, \times, +)\). To prove that \( +' = + \). Now, since \( A \) is a subdirect sum of subdirect powers of \( F_{p_i}^{h_i} \), therefore, a new “+” in \( A \) defines and is defined by a new
"+" in $F_{p^i}$, "+" in $F_{p^2}$, \ldots, "+" in $F_{p^t}$, such that $(F_{p^i}, +, \cdot)$ is a ring ($i = 1, \cdot \cdot \cdot, t$). Furthermore, the assumption that $(A, \times, +')$ has the same logic as $(A, \times, +)$ is equivalent to the assumption that each $(F_{p^i}, \times, +')$ has the same logic as $(F_{p^i}, \times, +)$ ($i = 1, \cdot \cdot \cdot, t$).

Since, by Theorem 5, $(F_{p^i}, \times, +)$ is a ring-logic, and hence with its "+" fixed, it follows that $+_i = +$ ($i = 1, \cdot \cdot \cdot, t$). Hence $+_i = +$, 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 (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 (mod D).

Now, let $n$ be a fixed integer, $n \geq 2$. 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, $n \geq 2$. Then $R$ is a ring-logic (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 (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 (mod D), and hence the "+" of $F_{p^k}$ is equationally definable in terms of the $D$-logic $(F_{p^k}, \times, \wedge)$. Of the two rival logics, $(F_{p^k}, \times, \wedge)$ requires only a knowledge of the multiplication table in $F_{p^k}$ since, by Corollary 2, the effect of $\wedge$ on $F_{p^k}$ is the cyclic permutation $(0, 1, \xi, \xi^2, \cdot \cdot \cdot, \xi^{p^k-1})$. 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 \( \xi \) 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 \( x^+ = x + 1 \) of the natural group \( N \) already involves a limited use of the addition table.

**References**


University of California, Santa Barbara
PACIFIC JOURNAL OF MATHEMATICS

EDITORS

ROBERT OSSERMAN
Stanford University
Stanford, California

M. G. ARSOVE
University of Washington
Seattle 5, Washington

J. DUGUNDJI
University of Southern California
Los Angeles 7, California

LOWELL J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
B. H. NEUMANN
F. WOLF
K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
STANFORD UNIVERSITY
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF TOKYO
UNIVERSITY OF CALIFORNIA
UNIVERSITY OF UTAH
MONTANA STATE UNIVERSITY
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF NEVADA
UNIVERSITY OF WASHINGTON
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
* * *
UNIVERSITY OF OREGON
AMERICAN MATHEMATICAL SOCIETY
OSAKA UNIVERSITY
CALIFORNIA RESEARCH CORPORATION
UNIVERSITY OF SOUTHERN CALIFORNIA
SPACE TECHNOLOGY LABORATORIES
UNIVERSITY OF UTAH
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the Pacific Journal of Mathematics should by typewritten (double spaced), and on submission, must be accompanied by a separate author’s résumé. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The Pacific Journal of Mathematics is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is $18.00; single issues, $5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $8.00 per volume; single issues $2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.
Tom M. (Mike) Apostol and Herbert S. Zuckerman, *On the functional equation* $F(mn)F((m, n)) = F(m)F(n)f((m, n))$ .................................................. 377

Reinhold Baer, *Irreducible groups of automorphisms of abelian groups* .................. 385

Herbert Stanley Bear, Jr., *An abstract potential theory with continuous kernel* .... 407

E. F. Beckenbach, *Superadditivity inequalities* ................................................ 421

R. H. Bing, *The simple connectivity of the sum of two disks* .......................... 439

Herbert Busemann, *Length-preserving maps* .................................................. 457

Heron S. Collins, *Characterizations of convolution semigroups of measures* .... 479

Paul F. Conrad, *The relationship between the radical of a lattice-ordered group and complete distributivity* ................................................... 493

P. H. Doyle, III, *A sufficient condition that an arc in $S^n$ be cellular* ........ 501

Carl Clifton Faith and Yuzo Utumi, *Intrinsic extensions of rings* ................. 505

Watson Bryan Fulks, *An approximate Gauss mean value theorem* ............... 513

Arshag Berge Hajian, *Strongly recurrent transformations* ............................ 517

Morisuke Hasumi and T. P. Srinivasan, *Doubly invariant subspaces. II* ...... 525

Lowell A. Hinrichs, Ivan Niven and Charles L. Vanden Eynden, *Fields defined by polynomials* .................................................. 537

Walter Ball Laffer, I and Henry B. Mann, *Decomposition of sets of group elements* .................................................. 547

John Albert Lindberg, Jr., *Algebraic extensions of commutative Banach algebras* .................................................................................. 559

W. Ljunggren, *On the Diophantine equation $Cx^2 + D = y^n$* .......................... 585

M. Donald MacLaren, *Atomic orthocomplemented lattices* ........................... 597

Moshe Marcus, *Transformations of domains in the plane and applications in the theory of functions* .................................................. 613

Philip Miles, *B* algebra unit ball extremal points .......................................... 627

W. F. Newns, *On the difference and sum of a basic set of polynomials* .......... 639

Barbara Ososky, *Rings all of whose finitely generated modules are injective* .... 645

Calvin R. Putnam, *Toeplitz matrices and invertibility of Hankel matrices* .... 651

Shoichiro Sakai, *Weakly compact operators on operator algebras* .............. 659

James E. Simpson, *Nilpotency and spectral operators* .................................. 665

Walter Laws Smith, *On the elementary renewal theorem for non-identically distributed variables* .................................................. 673

T. P. Srinivasan, *Doubly invariant subspaces* .............................................. 701

J. Roger Teller, *On the extensions of lattice-ordered groups* ...................... 709

Robert Charles Thompson, *Unimodular group matrices with rational integers as elements* .................................................. 719

J. L. Walsh and Ambikeshwar Sharma, *Least squares and interpolation in roots of unity* .................................................. 727

Charles Edward Watts, *A Jordan-Hölder theorem* ........................................ 731

Kung-Wei Yang, *On some finite groups and their cohomology* .................... 735

Adil Mohamed Yaqub, *On the ring-logic character of certain rings* ........... 741

Paul Ruel Young, *A note on pseudo-creative sets and cylinders* ............... 749