Pacific Journal of Mathematics

RING-LOGICS AND RESIDUE CLASS RINGS

ADIL MOHAMED YAQUB

Vol. 15, No. 4 December 1965

PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 4, 1965

RING-LOGICS AND RESIDUE CLASS RINGS

ADIL YAQUB

Let $(R, \times, +)$ be a commutative ring with unit 1, and let $K = \{\rho_1, \rho_2, \cdots\}$ be a transformation group in R. $(R, \times, +)$ is called a ring-logic, mod K essentially if the "$+$" of R is equationally definable in terms of the "K-logic" $(R, \times, \rho_1, \rho_2, \cdots)$. The Boolean theory results by choosing K to be the group generated by $x^* = 1 - x$ (order 2, $x^{**} = x$). The following result is proved: Let $n = p_1 \cdots p_t$ be square-free, and let R_n be the residue class ring, mod n. Let, $\hat{}$, be any transitive $0 \to 1$ permutation of $R_{p_i} (i = 1, \cdots, t)$. Let, $\hat{}$, be the induced permutation of R_n defined by $(x_1, \cdots, x_t)\hat{} = (x_1\hat{}, \cdots, x_t\hat{})$, $x_i \in R_{p_i} (i = 1, \cdots, t)$, and let K be the transformation group in R_n generated by, $\hat{}$. Then $(R_n, \times, +)$ is a ring-logic, mod K. An extension of this theorem to the case where n is arbitrary is also considered. The present proofs use the Fermat-Euler Theorem as well as a generalized form of the Chinese Residue Theorem.

The motivation for the study of ring-logics stems from the familiar equational interdefinability of Boolean rings $(R, \times, +)$ and Boolean logics (=Boolean algebras) $(R, \cap, *)$ [5]. In a series of recent publications ([1]–[4]), Foster raised this equational interdefinability, as well as the entire Boolean theory, to a more general level. In particular, Foster showed [2; 3] that any p-ring with unit (and more generally, any p^k-ring with unit) is a ring-logic, modulo certain suitably chosen groups. Furthermore, the author proved [6] that R_n, the residue class ring, mod n, is a ring-logic, modulo the "natural group" (generated by $x\hat{} = 1 + x$). Our present object is to further extend these results by considering certain transformation groups in R_n of rather general nature, and with respect to which $(R_n, \times, +)$ is a ring-logic (see Theorem 5).

1. The ring of residues mod p^k. Let $(R_{p^k}, \times, +)$ be the residue class ring, mod p^k, where p is prime and $k \geqq 1$. Let G denote the group of units in R_{p^k}. Then, as is well known, the order of G is $\varphi(p^k) = p^k - p^{k-1}$, where $\varphi(n)$ is the familiar Euler φ-function (=number of positive integers which do not exceed n and which are relatively prime to n). Let, $\hat{}$, be a permutation of R_{p^k}. We call, $\hat{}$, a *transitive* $0 \to 1$ permutation if (i) $0\hat{} = 1$, and (ii) for any elements α, β in R_{p^k}, there exists an integer r such that $\alpha^{\hat{}r} = \beta$, where $\alpha^{\hat{}r} = (\cdots((\alpha\hat{})\hat{})\hat{}\cdots)\hat{}$ (r-iterations).

Received July 6, 1964.

We recall from [4] the *characteristic function* $\delta_\mu(x)$, defined as follows: for any given $\mu \in R_{p^k}$, $\delta_\mu(x) = 1$ if $x = \mu$ and $\delta_\mu(x) = 0$ if $x \neq \mu$. Following [4], we also define: $a \times_\frown b = {}_\frown(a^\frown \times b^\frown)^\smile$, where, $^\smile$, is the inverse of the $0 \to 1$ permutation, $^\frown$. One readily verifies that $a \times_\frown 0 = 0 \times_\frown a = a$. Hence, we have the following "normal expansion formula" [4]:

$$f(x, y, \cdots) = \sum_{\alpha,\beta,\cdots \in R_{p^k}}^{\times_\frown} f(\alpha, \beta, \cdots)(\delta_\alpha(x)\delta_\beta(y)\cdots) \,. \tag{1.1}$$

In (1.1), $\alpha, \beta, \cdots$ range independently over all the elements of R_{p^k} while $x, y, \cdots$ are indeterminates over R_{p^k}. Also, $\sum_{\alpha_i \in R}^{\times_\frown} \alpha_i$ denotes $\alpha_1 \times_\frown \alpha_2 \times_\frown \cdots$, where $\alpha_1, \alpha_2, \cdots$ are all the elements of R.

We now have the following

LEMMA 1. *Let, $^\frown$, be any transitive permutation of R_{p^k}, and let K be the transformation group in R_{p^k} generated by, $^\frown$. Then all the elements of R_{p^k} are equationally definable in terms of the K-logic $(R_{p^k}, \times, ^\frown)$.*

Proof. Since, $^\frown$, is a *transitive* permutation of R_{p^k}, therefore, $R_{p^k} = \{0, 0^\frown, 0^{\frown 2}, \cdots, 0^{\frown p^{k-1}}\}$. Similarly, we have, $xx^\frown x^{\frown 2} \cdots x^{\frown p^{k-1}} = 0$, for all x in R_{p^k}. The last equation shows that 0 (and with it $0^\frown, 0^{\frown 2}, \cdots, 0^{\frown p^{k-1}}$) is expressible in terms of the K-logic, and the lemma is proved.

LEMMA 2. *Let $G = \{1, \zeta_2, \zeta_3, \cdots, \zeta_\varphi\}$ be the group of units in the residue class ring $(R_{p^k}, \times, +)$. Let, $^\frown$, be a transitive $0 \to 1$ permutation of R_{p^k} satisfying $1^\frown = \zeta_2, \zeta_2^\frown = \zeta_3, \cdots, \zeta_{\varphi-1}^\frown = \zeta_\varphi$, but otherwise, $^\frown$, is entirely arbitrary. Let K be the transformation group in R_{p^k} generated by, $^\frown$. Then each characteristic function $\delta_\mu(x)$, $\mu \in R_{p^k}$, is equationally definable in terms of the K-logic $(R_{p^k}, \times, ^\frown)$.*

Proof. Since, $^\frown$, is *transitive*, therefore, there exists an integer r such that $\mu^{\frown r} = 0$. Now, one readily verifies that

$$\delta_\mu(x) = (x^{\frown r+1}x^{\frown r+2}x^{\frown r+3} \cdots x^{\frown r+\varphi})^{p^k - p^{k-1}} \,,$$

since, by the Fermat-Euler Theorem, $a^{p^k - p^{k-1}} = 1$ for all a in G. This proves the lemma.

THEOREM 3. *Let $K, ^\frown$, be as in Lemma 2. Then the residue class ring $(R_{p^k}, \times, +)$ is a ring-logic, mod K.*

Proof. By (1.1), $x + y = \sum_{\alpha,\beta \in R_{p^k}}^{\times_\frown} (\alpha + \beta)(\delta_\alpha(x)\delta_\beta(y))$. By Lemma 1 and Lemma 2, each of $\alpha + \beta$, $\delta_\alpha(x)$, and $\delta_\beta(y)$, is expressible in terms

of the K-logic. Hence, the "$+$" of R_{p^k} is equationally definable in terms of the K-logic. Next, we show that $(R_{p^k}, \times, +)$ is *fixed* by its K-logic. Suppose that $(R_{p^k}, \times, +')$ is another ring with the same class of elements R_{p^k} and the same "$\times$" as $(R_{p^k}, \times, +)$ and which has the *same logic* as $(R_{p^k}, \times, +)$. To prove that $+' = +$. But this follows, since, up to isomorphism, there is only one cyclic group of order p^k.

2. The general case. In attempting to generalize Theorem 3 to the residue class ring $(R_n, \times, +)$, n arbitrary, we need the following concept of independence, introduced by Foster [4].

DEFINITION. Let $\{U_1, \cdots, U_t\}$ be a finite set of algebras of the same species S. We say that the algebras $U_1, \cdots, U_t$ are *independent* or satisfy the *Chinese Residue Theorem*, if, corresponding to each set $\{\Psi_i\}$ of expressions of species S, there exists a single expression X such that $\Psi_i = X \pmod{U_i}$ $(i = 1, \cdots, t)$. By an *expression* we mean some composition of one or more indeterminate-symbols $x, \cdots$ is terms of the primitive operations of $U_1, \cdots, U_t$; $\Psi_i = X \pmod{U_i}$ means that this is an identity of the algebra U_i.

As usual, we shall use the *same* symbols to denote the operation symbols of the algebras $U_1, \cdots, U_t$ when these algebras are of the same species. We now have the following

LEMMA 4. *Let $p_1, \cdots, p_t$ be distinct primes. Let, $\hat{}$, be any transitive $0 \to 1$ permutation of $R_{p_i^{k_i}}$, and let K_i be the transformation group in $R_{p_i^{k_i}}$ generated by, $\hat{}$, $(i = 1, \cdots, t)$. Then the K_i-logics $(R_{p_i^{k_i}}, \times, \hat{})(i = 1, \cdots, t)$ are independent.*

Proof. Let $n = p_1^{k_1} \cdots p_t^{k_t}$ and let $E = xx\hat{}x\hat{}^2 \cdots x\hat{}^{n-1}$. Let $p_i^{k_i} n_i = n$. Since $(p_i^{k_i}, n_i) = 1$, therefore, there exist integers r_i, s_i such that $r_i n_i - s_i p_i^{k_i} = 1$. Now, one readily verifies that

$$\omega_i = \text{def} = E\hat{}^{r_i n_i} = \begin{cases} 1 \pmod{R_{p_i^{k_i}}}, \\ 0 \pmod{R_{p_j^{k_j}}} \end{cases} \qquad (j \neq i).$$

To prove the independence of the logics $(R_{p_i^{k_i}}, \times, \hat{})$, let $\{\Psi_i\}$ be a set of t expressions of species $\times, \hat{}$; i.e., primitive composition of indeterminate-symbols in terms of the operations $\times, \hat{}$. Define

$$X = \Psi_1 \omega_1 \times_{\hat{}} \cdots \times_{\hat{}} \Psi_t \omega_t .$$

It is readily verified that $\Psi_i = X \pmod{R_{p_i^{k_i}}} (i = 1, \cdots, t)$, since $a \times_{\hat{}} 0 = 0 \times_{\hat{}} a = a$. This proves the lemma.

We are now in a position to consider $(R_n, \times, +)$ in regard to the concept of ring-logic. Indeed, let $n = p_1^{k_1} \cdots p_t^{k_t}$, where the p_i are distinct primes $(i = 1, \cdots, t)$, and let $G_i = \{1, \zeta_{i2}, \zeta_{i3}, \cdots, \zeta_{i\varphi_i}\}$ be the group of units in the residue class ring $(R_{p_i^{k_i}}, \times, +)$. For each i, define, $\hat{}$, to be a transitive $0 \to 1$ permutation of $R_{p_i^{k_i}}$ satisfying $1\hat{} = \zeta_{i2}, \zeta_{i2}\hat{} = \zeta_{i3}, \cdots, (\zeta_{i,\varphi_i-1})\hat{} = \zeta_{i\varphi_i}$, but otherwise, $\hat{}$, is entirely arbitrary, and let K_i be the transformation group in $R_{p_i^{k_i}}$ generated by, $\hat{}$. Now, it is well known that the residue class ring R_n is isomorphic to the direct product of $R_{p_1^{k_1}}, \cdots, R_{p_t^{k_t}}$:

$$R_n \cong R_{p_1^{k_1}} \times \cdots \times R_{p_t^{k_t}} \text{ (direct product)}, \quad n = p_1^{k_1} \cdots p_t^{k_t} .$$

Furthermore, it is easily seen that by defining $(x_1, \cdots, x_t)\hat{} = (x_1\hat{}, \cdots, x_t\hat{})$, $(x_1, \cdots, x_t) \in R_n$, we obtain a transitive $0 \to 1$ permutation of R_n. Let K be the transformation group in R_n generated by the above permutation, $\hat{}$. We now have the following

THEOREM 5. *The residue class ring $(R_n, \times, +)$, n arbitrary, is a ring-logic, mod K, where K is the transformation group in R_n above.*

Proof. Let $n = p_1^{k_1} \cdots p_t^{k_t}$, where the p_i are distinct primes $(i = 1, \cdots, t)$. By Theorem 3, each $(R_{p_i^{k_i}}, \times, +)$ is a ring-logic, mod K_i, where K_i is as defined above $(i = 1, \cdots, t)$. Hence, for each i, there exists an expression Ψ_i such that

$$x_i + y_i = \Psi_i(x_i, y_i; \times, \hat{}), \text{ for all } x_i, y_i \text{ in } R_{p_i^{k_i}} .$$

But, by Lemma 4, the K_i-logics $(R_{p_i^{k_i}}, \times, \hat{})$ are independent $(i = 1, \cdots, t)$, and hence there exists a single expression X such that $X = \Psi_i \pmod{R_{p_i^{k_i}}}$ $(i = 1, \cdots, t)$. Now, let $x = (x_1, \cdots, x_t)$, $y = (y_1, \cdots, y_t)$ be any elements of $R_n (\cong R_{p_1^{k_1}} \times \cdots \times R_{p_t^{k_t}})$. Since the operations are component-wise in this direct product, therefore,

$$\begin{aligned} X(x, y; \times, \hat{}) &= X((x_1, \cdots, x_t), (y_1, \cdots, y_t); \times, \hat{}) \\ &= (X(x_1, y_1; \times, \hat{}), \cdots, X(x_t, y_t; \times, \hat{})) \\ &= (\Psi_1(x_1, y_1; \times, \hat{}), \cdots, \Psi_t(x_t, y_t; \times, \hat{})) \\ &= (x_1 + y_1, \cdots, x_t + y_t) \\ &= x + y . \end{aligned}$$

Hence, the "+" of R_n is *equationally* definable in terms of the K-logic $(R_n, \times, \hat{})$. The proof that $(R_n, \times, +)$ is fixed by its K-logic follows as in the "fixed" part of the proof of Theorem 3, since again, up to isomorphism, there is only one cyclic group of order n. This completes the proof of the theorem.

We shall now take a closer look at the case where $n = p_1 \cdots p_t$ is *square-free*. In this case the group G_i of units in $R_{p_i}(=\text{field})$ is precisely the set of all nonzero elements of $R_{p_i}(i = 1, \cdots, t)$, and the, $\hat{}$, described above (see paragraph preceding Theorem 5) for R_{p_i} is now simply *any* transitive $0 \to 1$ permutation of R_{p_i}. Hence, we have the following

COROLLARY 6. *Let* $n = p_1 \cdots p_t$ *be square-free, and let,* $\hat{}$, *be any transitive* $0 \to 1$ *permutation of* $R_{p_i}(i = 1, \cdots, t)$. *Let,* $\hat{}$ *be the induced permutation of* R_n *defined by* $(x_1, \cdots, x_t)\hat{} = (x_1\hat{}, \cdots, x_t\hat{})$, $x_i \in R_{p_i}(i = 1, \cdots, t)$, *and let* K *be the transformation group in* R_n *generated by,* $\hat{}$. *Then* $(R_n, \times, +)$ *is a ring-logic, mod* K.

Thus, if, in particular, we choose $x\hat{} = 1 + x$ in the above Corollary, we obtain the following (compare with [6]).

COROLLARY 7. *Let* n *be square-free, and let* N *be the "natural group", generated by* $x\hat{} = 1 + x$. *Then* $(R_n, \times, +)$ *is a ring-logic, mod* N.

Upon choosing, $\hat{}$, in Theorem 5 in all of the various available ways, we obtain the corresponding transformation groups K with respect to which $(R_n, \times, +)$ is a ring-logic.

REFERENCES

1. A. L. Foster, *On n-ality theories in rings and their logical algebras including triality principle in three-valued logics*, Amer. J. Math. **72** (1950), 101-123.
2. ———, *p-rings and ring-logics*, Univ. Calif. Publ. **1** (1951), 385-396.
3. ———, *p^k-rings and ring-logics*, Ann. Scu. Norm. Pisa **5** (1951), 279-300.
4. ———, *Unique subdirect factorization within certain classes of universal algebras*, Math. Z. **62** (1955), 171-188.
5. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37-111.
6. A. Yaqub, *On the theory of ring-logics*, Canad. J. Math. **8** (1956), 323-328.
7. ———, *On certain finite rings and ring-logics*, Pacific J. Math. **12** (1962), 785-790.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. SAMELSON
Stanford University
Stanford, California

J. DUGUNDJI
University of Southern California
Los Angeles, California 90007

R. M. BLUMENTHAL
University of Washington
Seattle, Washington 98105

*RICHARD ARENS
University of California
Los Angeles, California 90024

ASSOCIATE EDITORS

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

SUPPORTING INSTITUTIONS

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

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should by typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. No separate author's resumé is required. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens, at the University of California, Los Angeles, California 90024.

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.

* Basil Gordon, Acting Managing Editor until February 1, 1966.

Pacific Journal of Mathematics

Vol. 15, No. 4 December, 1965

Robert James Blattner, *Group extension representations and the structure space* 1101

Glen Eugene Bredon, *On the continuous image of a singular chain complex* 1115

David Hilding Carlson, *On real eigenvalues of complex matrices* 1119

Hsin Chu, *Fixed points in a transformation group* 1131

Howard Benton Curtis, Jr., *The uniformizing function for certain simply connected Riemann surfaces* 1137

George Wesley Day, *Free complete extensions of Boolean algebras* 1145

Edward George Effros, *The Borel space of von Neumann algebras on a separable Hilbert space* 1153

Michel Mendès France, *A set of nonnormal numbers* 1165

Jack L. Goldberg, *Polynomials orthogonal over a denumerable set* 1171

Frederick Paul Greenleaf, *Norm decreasing homomorphisms of group algebras* 1187

Fletcher Gross, *The 2-length of a finite solvable group* 1221

Kenneth Myron Hoffman and Arlan Bruce Ramsay, *Algebras of bounded sequences* 1239

James Patrick Jans, *Some aspects of torsion* 1249

Laura Ketchum Kodama, *Boundary measures of analytic differentials and uniform approximation on a Riemann surface* 1261

Alan G. Konheim and Benjamin Weiss, *Functions which operate on characteristic functions* 1279

Ronald John Larsen, *Almost invariant measures* 1295

You-Feng Lin, *Generalized character semigroups: The Schwarz decomposition* 1307

Justin Thomas Lloyd, *Representations of lattice-ordered groups having a basis* 1313

Thomas Graham McLaughlin, *On relative coimmunity* 1319

Mitsuru Nakai, *Φ-bounded harmonic functions and classification of Riemann surfaces* 1329

L. G. Novoa, *On n-ordered sets and order completeness* 1337

Fredos Papangelou, *Some considerations on convergence in abelian lattice-groups* 1347

Frank Albert Raymond, *Some remarks on the coefficients used in the theory of homology manifolds* 1365

John R. Ringrose, *On sub-algebras of a C^*-algebra* 1377

Jack Max Robertson, *Some topological properties of certain spaces of differentiable homeomorphisms of disks and spheres* 1383

Zalman Rubinstein, *Some results in the location of zeros of polynomials* 1391

Arthur Argyle Sagle, *On simple algebras obtained from homogeneous general Lie triple systems* 1397

Hans Samelson, *On small maps of manifolds* 1401

Annette Sinclair, *$|\varepsilon(z)|$-closeness of approximation* 1405

Edsel Ford Stiel, *Isometric immersions of manifolds of nonnegative constant sectional curvature* 1415

Earl J. Taft, *Invariant splitting in Jordan and alternative algebras* 1421

L. E. Ward, *On a conjecture of R. J. Koch* 1429

Neil Marchand Wigley, *Development of the mapping function at a corner* 1435

Horace C. Wiser, *Embedding a circle of trees in the plane* 1463

Adil Mohamed Yaqub, *Ring-logics and residue class rings* 1465

John W. Lamperti and Patrick Colonel Suppes, *Correction to: Chains of infinite order and their application to learning theory* 1471

Charles Vernon Coffman, *Correction to: Non-linear differential equations on cones in Banach spaces* 1472

P. H. Doyle, III, *Correction to: A sufficient condition that an arc in S^n be cellular* 1474

P. P. Saworotnow, *Correction to: On continuity of multiplication in a complemented algebra* 1474

Basil Gordon, *Correction to: A generalization of the coset decomposition of a finite group* 1474