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, $\frown$, be any transitive $0 \to 1$ permutation of $R_{p_i} (i = 1, \cdots, t)$. Let, $\frown$, be the induced permutation of R_n defined by $(x_1, \cdots, x_t)^\frown = (x_1^\frown, \cdots, x_t^\frown)$, $x_i \in R_{p_i} (i = 1, \cdots, t)$, and let K be the transformation group in R_n generated by, $\frown$. 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 $x^\frown = 1 + x$). 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, $\frown$, be a permutation of R_{p^k}. We call, $\frown$, a *transitive* $0 \to 1$ permutation if (i) $0^\frown = 1$, and (ii) for any elements α, β in R_{p^k}, there exists an integer r such that $\alpha^{\frown r} = \beta$, where $\alpha^{\frown r} = (\cdots((\alpha^\frown)^\frown)^\frown \cdots)^\frown$ (r-iterations).

Received July 6, 1964.

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

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

In (1.1), $\alpha, \beta, \cdots$ range independently over all the elements of R_{pk} while $x, y, \cdots$ are indeterminates over R_{pk}. Also, $\sum_{\alpha_i \in R}^{\times_\frown} \alpha_i$ denotes $\alpha_1 \times_\smile \alpha_2 \times_\smile \cdots$, 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_{pk}, and let K be the transformation group in R_{pk} generated by, $^\frown$. Then all the elements of R_{pk} are equationally definable in terms of the K-logic $(R_{pk}, \times, ^\frown)$.*

Proof. Since, $^\frown$, is a *transitive* permutation of R_{pk}, therefore, $R_{pk} = \{0, 0^\frown, 0^{\frown 2}, \cdots, 0^{\frown pk-1}\}$. Similarly, we have, $xx^\frown x^{\frown 2} \cdots x^{\frown pk-1} = 0$, for all x in R_{pk}. The last equation shows that 0 (and with it $0^\frown, 0^{\frown 2}, \cdots, 0^{\frown pk-1}$) 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 $(R_{pk}, \times, +)$. Let, $^\frown$, be a transitive $0 \to 1$ permutation of R_{pk} 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_{pk} generated by, $^\frown$. Then each characteristic function $\delta_\mu(x)$, $\mu \in R_{pk}$, is equationally definable in terms of the K-logic $(R_{pk}, \times, ^\frown)$.*

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

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

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

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

Proof. By (1.1), $x + y = \sum_{\alpha,\beta \in R_{pk}}^{\times_\frown} (\alpha + \beta)(\delta_\alpha(x)\delta_\beta(y))$. 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 $U_1, \cdots, U_t$; $\Psi_i = X(\mathrm{mod}\, U_i)$ 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, $\frown$, be any transitive $0 \rightarrow 1$ permutation of $R_{p_i^{k_i}}$, and let K_i be the transformation group in $R_{p_i^{k_i}}$ generated by, $\frown$, $(i = 1, \cdots, t)$. Then the K_i-logics $(R_{p_i^{k_i}}, \times, \frown)(i = 1, \cdots, t)$ are independent.*

Proof. Let $n = p_1^{k_1} \cdots p_t^{k_t}$ and let $E = xx^\frown x^{\frown 2} \cdots x^{\frown n-1}$. 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

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

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

$$X = \Psi_1\omega_1 \times_\smile \cdots \times_\smile \Psi_t\omega_t \;.$$

It is readily verified that $\Psi_i = X(\mathrm{mod}\, R_{p_i^{k_i}})(i = 1, \cdots, t)$, since $a \times_\smile 0 = 0 \times_\smile a = a$. 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, $\frown$, to be a transitive $0 \to 1$ permutation of $R_{p_i^{k_i}}$ satisfying $1^\frown = \zeta_{i2}, \zeta_{i2}^\frown = \zeta_{i3}, \cdots, (\zeta_{i,\varphi_i-1})^\frown = \zeta_{i\varphi_i}$, but otherwise, $\frown$, is entirely arbitrary, and let K_i be the transformation group in $R_{p_i^{k_i}}$ generated by, $\frown$. Now, it is well known that the residue class ring R_n is isomorphic to the direct product of $R_{p_1^{k_1}}, \cdots, R_{p_t^{k_t}}$:

$$R_n \cong R_{p_1{}^1} \times \cdots \times R_{p_t^{k_t}} \text{ (direct product)}, \; n = p_1^{k_1} \cdots p_t^{k_t} .$$

Furthermore, it is easily seen that by defining $(x_1, \cdots, x_t)^\frown = (x_1^\frown, \cdots, x_t^\frown)$, $(x_1, \cdots, x_t) \in R_n$, 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, $\frown$. 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

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

But, by Lemma 4, the K_i-logics $(R_{p_i^{k_i}}, \times, \frown)$ 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,

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

Hence, the "+" of R_n is *equationally* definable in terms of the K-logic $(R_n, \times, \frown)$. 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}(=field) is precisely the set of all nonzero elements of $R_{p_i}(i = 1, \cdots, t)$, and the, $\frown$, described above (see paragraph preceding Theorem 5) for R_{p_i} is now simply *any* transitive $0 \rightarrow 1$ permutation of R_{p_i}. Hence, we have the following

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

Thus, if, in particular, we choose $x^\frown = 1 + x$ 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 $x^\frown = 1 + x$. Then $(R_n, \times, +)$ is a ring-logic, mod N.*

Upon choosing, $\frown$, 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