PACIFIC JOURNAL OF MATHEMATICS
Vol. 19, No. 1, 1966

SOME CLASSES OF RING-LOGICS

ADIL YAQUB

Let $(R, \times, +)$ be a commutative ring with identity, and let $K = \{\rho_1, \rho_2, \cdots\}$ be a transformation group in R. The K-logic of the ring $(R, \times, +)$ is the (operationally closed) system $(R, \times, \rho_1, \rho_2, \cdots)$ whose operations are the ring product "$\times$" together with the unary operations $\rho_1, \rho_2, \cdots$ of K. The ring $(R, \times, +)$ is essentially a ring-logic, mod K, if the "$+$" of the ring is equationally definable in terms of its K-logic $(R, \times, \rho_1, \rho_2, \cdots)$. Our present object, is to show that any finite direct product of (not necessarilly finite) direct powers of finite commutative local rings of distinct orders is a ring-logic modulo certain suitably chosen (but nevertheless still rather general) groups. This theorem subsumes and generalizes Foster's results for Boolean rings, p-rings, and p^k-rings, as well as the author's results for residue class rings and finite commutative rings with zero radical. Several new classes of ring-logics (modulo certain groups of quite general nature) are also explicitly exhibited. Throughout the entire paper, all rings under consideration are assumed to be commutative and with identity.

The one component case. In this section, we direct special attention to arbitrary direct powers of a finite local ring in regard to the concept of ring-logics. First, we recall the following [9; 228]

DEFINITION 1. A ring R is called a *local ring* if and only if R is Noetherian and the nonunits of R form an ideal.

REMARK. It can be easily shown that for a finite commutative ring R with identity $1(1 \neq 0)$, the concepts "local ring", "primary ring", and "completely primary ring" are equivalent. This readily follows by recalling that a primary ring is a ring R with identity such that R/J is a simple ring satisfying the minimum condition for right ideals, while a completely primary ring is a ring R with identity such that R/J is a division ring. Here, J is the radical of R. Hence the results below still hold if we replace the local rings involved by primary rings or by completely primary rings.

A very useful result for our purposes is the following

LEMMA 2. *Let R be a finite ring with identity $1(1 \neq 0)$. The ring R is a local ring if and only if every element of R is either a unit or is nilpotent.*

Proof. Let R be a finite local ring with radical J, and let N denote the set of nonunits of R. We claim that $J = N$. Clearly, $J \subset N$. Now suppose $z \in N$. Since N is an ideal and $1 \notin N$, therefore, $1 - z \notin N$. Hence, for any x in R, $z \in N$ implies that $1 - zx$ is a unit and thus zx is quasi-regular. Therefore, $N \subset J$. This proves the "only if" part. The "if" part is immediate.

Now, let $(R, \times, +)$ be a finite local ring and let $G = \{1, \xi_2, \cdots, \xi_r\}$ be the group of units in R. Let $\hat{}$ be a *cyclic* $0 \to 1$ permutation of R, i.e., $0\hat{} = 1$, and $x \in R \Rightarrow x = 0^{\hat{}s}$ for some s, where $\alpha^{\hat{}s} = (\cdots((\alpha)\hat{})\hat{}\cdots)\hat{}$ (s-iterations). From [4], we recall the characteristic function $\delta_\mu(x)$, defined as follows: for any given $\mu \in R$, $\delta_\mu(x) = 1$ if $x = \mu$ and $\delta_\mu(x) = 0$ if $x \neq \mu$. Following [4], we also define: $a \times_{\hat{}} b = (a\hat{} \times b\hat{})\check{}$, where $\check{}$ is the inverse of the $0 \to 1$ permutation $\hat{}$.

In the remainder of this paper, juxtaposition will be used in place of "$\times$". Now, it is readily verified that [4]

$$a \times_{\hat{}} 0 = 0 \times_{\hat{}} a = a; \text{ and for any function } f \text{ on } R, \tag{1.1}$$

$$f(x, y, \cdots) = \sum_{\alpha,\beta,\cdots \in R}^{\times\hat{}} f(\alpha, \beta, \cdots)(\delta_\alpha(x)\delta_\beta(y)\cdots). \tag{1.2}$$

In (1.2), $\alpha, \beta, \cdots$ range independently over all the elements of R while $x, y, \cdots$ are indeterminates over R. Also, $\sum_{\alpha_i \in R}^{\times\hat{}} \alpha_i$ denotes $\alpha_1 \times_{\hat{}} \alpha_2 \times_{\hat{}} \cdots$, where $\alpha_1, \alpha_2, \cdots$ are all the elements of R.

The following lemma holds for any finite abstract algebra $(R, \times)$ with zero. For convenience, however, we state the result for rings.

LEMMA 3. *Let $\hat{}$ be any cyclic permutation of a finite ring R, and let K be the transformation group in R generated by $\hat{}$. Then all the elements of R are equationally definable in terms of the K-logic $(R, \times, \hat{})$.*

Proof. Since $\hat{}$ is a *cyclic* permutation of R, therefore,

$$R = \{0, 0\hat{}, 0^{\hat{}2}, \cdots, 0^{\hat{}n-1}\},$$

where n is the number of elements in R. Similarly,

$$xx\hat{}x^{\hat{}2} \cdots x^{\hat{}n-1} = 0 \text{ for all } x \text{ in } R.$$

This shows that 0 (and with it $0\hat{}, 0^{\hat{}2}, \cdots, 0^{\hat{}n-1}$) is expressible in terms of the K-logic. This proves the lemma.

LEMMA 4. *Let R be a finite local ring, and let $G = \{1, \xi_2, \cdots, \xi_r\}$ be the group of units in R. Let $\hat{}$ be a cyclic $0 \to 1$ permutation of*

R satisfying $1\hat{} = \xi_2$, $\xi_2\hat{} = \xi_3$, $\cdots$, $\xi_{r-1}\hat{} = \xi_r$, but otherwise $\hat{}$ is entirely arbitrary. Let K be the transformation group in R generated by $\hat{}$. Then each characteristic function $\delta_\mu(x)$, $\mu \in R$, is equationally definable in terms of the K-logic $(R, \times, \hat{})$.

Proof. Let $\mu \in R$. Since $\hat{}$ is cyclic, there therefore exists an integer k such that $\mu^{\hat{}k} = 0$. Now, choose m so large that $\eta^m = 0$ for *all* nilpotent elements η of R. Using Lemma 2, together with Lagrange's Theorem, it is easily seen that

$$\delta_\mu(x) = \{x^{\hat{}k+1}x^{\hat{}k+2}x^{\hat{}k+3} \cdots x^{\hat{}k+r}\}^{mr},$$

and the lemma is proved.

THEOREM 5. *Let R, K, $\hat{}$ be as in Lemma 4. Then the local ring R is a ring-logic, mod K.*

Proof. By (1.2), $x + y = \sum^{\times}_{\alpha,\beta \in R}(\alpha + \beta)(\delta_\alpha(x)\delta_\beta(y))$. By Lemma 3 and Lemma 4, each of $\alpha + \beta$, $\delta_\alpha(x)$, $\delta_\beta(y)$, is equationally definable in terms of the K-logic. Hence, the "$+$" of R is equationally definable in terms of its K-logic, and the theorem is proved.

REMARK. Formerly, a minor side-line condition (namely, that the ring be "fixed" by its logic) was also included in the definition of a ring-logic [1]. We do not require this condition in our present definition.

THEOREM 6. *Let R, $\hat{}$ be as in Lemma 4, and let $R^* = R^{(m)}$ be a (not necessarily finite) direct power of R. Let $\hat{}$ be the induced permutation of R^* defined by $(x_1, x_2, \cdots)\hat{} = (x_1\hat{}, x_2\hat{}, \cdots)$, and let K be the transformation group in R^* generated by $\hat{}$. Then $(R^*, \times, +)$ is a ring-logic, mod K.*

Proof. This follows readily from Theorem 5, since the operations in $R^{(m)}$ are component-wise.

Let us now consider, for example, the case in which $R = GF(p^k)$. Clearly, the Galois field R is a local ring. But much more than this is true. Indeed, the permutation $\hat{}$ of Lemma 4 is now *any* cyclic $0 \to 1$ permutation of R. Hence, Theorem 6 now yields the following.

COROLLARY 7. *Let $R = GF(p^k)$, and let $R^{(m)}$ be a (not necessarily finite) direct power of $GF(p^k)$. Let $\hat{}$ be any cyclic $0 \to 1$ permutation of $GF(p^k)$, and let K be the transformation group in R^* generated by that permutation of R^* induced by $\hat{}$. Then $(R^*, \times, +)$ is a*

ring-logic, mod K.

It is noteworthy to observe that by choosing $\hat{}$ in the above corollary to satisfy $x\hat{} = 1 - x$, $x\hat{} = 1 + x$, and

$$x\hat{} = \xi x + (1 + \xi x + \xi^2 x^2 + \cdots + \xi^{p^k-2} x^{p^k-2}) \quad (\xi = \text{generator for } GF(p^k)),$$

respectively, one essentially recovers Foster's results [1; 2; 3] for Boolean rings, p-rings, and p^k-rings. For, as is easily seen, the above choices for $\hat{}$ do indeed yield certain cyclic $0 \to 1$ permutations of $GF(2)$, $GF(p)$, and $GF(p^k)$, respectively (compare with the introduction).

Another corollary to Theorems 5, 6, is obtained by adjoining any finite number of commuting nilpotent elements to a given Galois field. The resulting hypercomplex rings, in turn, give rise to new classes of ring-logics. We state this formally in the following.

COROLLARY 8. *Let $F = GF(p^k)$, and let $\eta_1, \cdots, \eta_t$ be a finite set of nilpotent elements such that $\eta_i\eta_j = \eta_j\eta_i$ for all i, j, and $a\eta_i = \eta_i a$ for all i and all a in F. Let $R = F[\eta_1, \cdots, \eta_t]$. Then R is a finite local ring. Furthermore, R is a ring-logic, mod K, where K is the transformation group in R generated by the permutation of R prescribed in Theorem* 5. *Moreover, any direct power of R is a ring-logic (modulo the group prescribed in Theorem* 6).

The proof of Corollary 8 is quite straightforward and will here be omitted.

2. **The general case.** We shall now generalize Theorems 5 and 6 to the situation in which the component rings are not necessarily all identical. To this end, we need the following concept of independence, introduced by Foster [5].

DEFINITION 9. 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 $\psi_i = X(U_i)$ $(i = 1, \cdots, t)$. By an *expression* we mean some composition of one or more indeterminate-symbols in terms of the primitive operations of $U_1, \cdots, U_t$; $\psi_i = X(U_i)$ means that this is an identity of the algebra U_i.

As usual, we 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.

LEMMA 10. *Let $R_1, \cdots, R_t$, be finite local rings, and let $G_i = \{1, \xi_{2i}, \cdots, \xi_{r_i,i}\}$ be the group of units in R_i $(i = 1, \cdots, t)$. Let $\hat{}$ be*

a cyclic $0 \rightarrow 1$ *permutation of* R_i *satisfying*

$$1^{\frown} = \xi_{2i},\ \xi_{2i}^{\frown} = \xi_{3i},\ \cdots,\ \xi_{r_i-1,i}^{\frown} = \xi_{r_i,i}\ ,$$

but otherwise $\frown$ *is entirely arbitrary, and let* K_i *be the transformation group in* R_i *generated by* $\frown$ $(i = 1, \cdots, t)$. *Let the order* (= *number of elements*) *of* R_i *and order of* R_j *be distinct* $(i, j = 1, \cdots, t; i \neq j)$. *Then the* K_i*-logics* $(R_i, \times, \frown)$ $(i = 1, \cdots, t)$ *are independent.*

Proof. Let n be the largest of the orders of $R_1, \cdots, R_t$, and let $E = \xi\xi^{\frown}\xi^{\frown 2} \cdots \xi^{\frown n-1}$. Now, consider first the logics $(R_i, \times, \frown)$ and $(R_j, \times, \frown)$ $(i \neq j)$. We distinguish three cases depending on the orders r_i, r_j of the groups of units of R_i, R_j.

Case 1. $r_i < r_j$. Let λ be chosen so large as to satisfy: $\lambda r_i r_j = \text{def} = q$, and $\eta^q = 0$ for *all* nilpotent elements η in R_i or in R_j. It is now readily verified that

$$|_{ji}(\xi) = \text{def} = (E^{\frown}E^{\frown 2} \cdots E^{\frown r_j})^q = \begin{cases} 1 & (R_j) \\ 0 & (R_i) \end{cases}$$

$$|_{ij}(\xi) = \text{def} = (\{|_{ji}(\xi)\}\{|_{ji}(\xi)\}^{\frown 2})^{\frown} = \begin{cases} 0 & (R_j) \\ 1 & (R_i) \end{cases}$$

Case 2. $r_j < r_i$. By symmetry, this is essentially same as *Case* 1.

Case 3. $r_i = r_j$. Assume, without any loss of generality, that $m = \text{def} = \text{order of } R_i < \text{order of } R_j$. Then, with q as above, it is easily seen that

$$|_{ij}(\xi) = (E^{\frown m+1}E^{\frown m+2} \cdots E^{\frown m+r_i})^q = \begin{cases} 1 & (R_i) \\ 0 & (R_j) \end{cases}$$

$$|_{ji}(\xi) = \text{def} = (\{|_{ij}(\xi)\}\{|_{ij}(\xi)\}^{\frown 2})^{\frown} = \begin{cases} 0 & (R_i) \\ 1 & (R_j) \end{cases}.$$

Now, let $|_i(\xi) = |_{i1}(\xi)\,|_{i2}(\xi) \cdots |_{it}(\xi)(\text{no } |_{ii}(\xi) \text{ term})$ $(i = 1, \cdots, t)$.

Let $\psi_1, \cdots, \psi_t$ be a set of t expressions of species (2, 1), i.e., primitive compositions of indeterminate-symbols in terms of the operations $\times, \frown$. Define

$$X = \{\psi_1 |_1(\xi)\} \times_{\frown} \cdots \times_{\frown} \{\psi_t |_t(\xi)\}\ .$$

It is readily verified that $\psi_i = X(R_i)$ $(i = 1, \cdots, t)$, since $a \times_{\frown} 0 = 0 \times_{\frown} a = a$. Hence the logics $(R_i, \times, \frown)$ are independent, and the lemma is proved.

We are now in a position to prove the following Principal Theorem the case $t = 1$ of which yields Theorem 6.

THEOREM 11. (Principal Theorem). *Let* $R_i, K_i, \hat{}$ $(i = 1, \cdots, t)$ *be as in Lemma* 10 *and let* $R_1, \cdots, R_t$ *have distinct orders. Let* R *be a direct product of (not necessarily finite) direct powers of* $R_1, \cdots, R_t$ *(*t *finite). For every element* $(x_{11}, \cdots, x_{21}, \cdots, x_{t1}, \cdots)$ *in* R, *define* $(x_{11}, \cdots, x_{21}, \cdots, x_{t1}, \cdots)\hat{} = (\hat{x_{11}}, \cdots, \hat{x_{21}}, \cdots, \hat{x_{t1}}, \cdots)$, *and let* K *be the transformation group in* R *generated by* $\hat{}$. *Then* R *is a ring-logic, mod* K.

Proof. By Theorem 5, each ring $(R_i, \times, +)$ is a ring-logic, mod K_i. Hence, for each i, there exists an expression ψ_i such that $x_i + y_i = \psi_i(x_i, y_i; \times, \hat{})$, for all x_i, y_i in R_i. Moreover, by Lemma 10 the K_i-logics $(R_i, \times, \hat{})$ are independent $(i = 1, \cdots, t)$. Hence, there exists a single expression X such that $X = \psi_i(R_i)$ $(i = 1, \cdots, t)$. Since, however, the operations are component-wise in the direct product R, therefore,

$$X(x, y; \times, \hat{}) = x + y, \text{ for all } x, y \text{ in } R .$$

Hence, the "+" of R is *equationally* definable in terms of the K-logic $(R, \times, \hat{})$, and the theorem is proved.

We conclude by applying Theorem 11 to certain familiar classes of rings. To this end, we direct special attention to the cases where (a) $R_i = GF(p_i^{k_i})$, p_i prime, $(i = 1, \cdots, t)$, and (b) each R_i is a residue class ring (mod $p_i^{k_i}$), p_i prime. In case (a), each of the transformation groups K_i of $R_i (= GF(p_i^{k_i}))$ is now generated by *any* cyclic $0 \to 1$ permutation of R_i (there are $(p_i^{k_i} - 2)!$ such permutations), and these, in turn, induce a permutation of the direct product R-which permutation generates a transformation group K in R such that $(R, \times, +)$ is a ring-logic, mod K. In case (b), the choices for K_i are now somewhat more restricted than those in case (a), but otherwise the situation is quite similar. Finally, recalling the familiar direct product structure of (a) finite commutative rings with zero radical, and (b) residue class rings, mod n (n arbitrary), we obtain, as a further corollary to Theorem 11, the following (compare with the introduction; also see [7; 8]).

COROLLARY 12. (a) *Let* R_i *be a finite ring with zero radical* $(i = 1, \cdots, t;$ t *finite), and let* R *be any direct product of (not necessarily finite) direct powers of* $R_1, \cdots, R_t$. *Then there exists a transformation group* K *in* R *such that* $(R, \times, +)$ *is a ring-logic, mod* K *(where* K *is as prescribed in Theorems* 5, 6); (b) *same as* (a) *except that each* R_i *is now a residue class ring, mod* n_i *(*n_i *arbitrary).*

In conclusion, I wish to express my indebtedness and gratitude to the referee for his valuable suggestions.

REFERENCES

1. A. L. Foster, *On n-ality theories in rings and their logical algebras, including tri-ality principle in three-valued logics*, Amer. J. Math. **72** (1950), 101-123.
2. ———, *Ring-logics and p-rings*, Univ. Calif. Publ. **1** (1951), 385-396.
3. ———, *p^k-rings and ring-logic*, Ann. Scu. Norm. Pisa **5** (1951), 279-300.
4. ———, *Generalized "Boolean" theory of universal algebras*, Part I, Math. Z. **58** (1953), 306-336.
5. ———, *The identities of—and unique subdirect factorization within—classes of universal algebras*, Math Z. **62** (1955), 171-188.
6. M. H. Stone, *The theory of representations of Boolean algebras*, Trans. Amer. Soc. **40** (1936), 37-111.
7. A. Yaqub, *On the ring-logic character of certain rings*, Pacific J. Math. **14** (1964), 741-747.
8. ———, *Ring-logics and residue class rings*, Pacific J. Math. **15** (1965), 1465-1469.
9. O. Zariski and P. Samuel, *Commutative algebra*, Univ. Series in Higher Math., Van Nostrand Co., Princeton, **1** (1958).

Received June 15, 1965.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA